Značajke mreže za trgovanje kriptovalutama

Gudić, Matija

Undergraduate thesis / Završni rad

2021

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:781286

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

MATIJA GUDIĆ

ZNAČAJKE MREŽE ZA TRGOVANJE KRIPTOVALUTAMA

ZAVRŠNI RAD

ZAGREB, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Arhitektura telekomunikacijske mreže**

ZAVRŠNI ZADATAK br. 6155

Pristupnik: **Matija Gudić (0135239455)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Značajke mreže za trgovanje kriptovalutama**

Opis zadatka:

U radu je potrebno opisati razvoj kriptovaluta te princip rada tehnologije blockchain. Analizirati značajke pametnih ugovora te opisati značajke mreže za trgovanje kriptovalutama. Analizirati stanje na tržištu kriptovaluta.

Mentor:

doc. dr. sc. Ivan Forenbacher

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ZNAČAJKE MREŽE ZA TRGOVANJE KRIPTOVALUTAMA

CRYPTOCURRENCY NETWORK CHARACTERISTICS

Mentor: doc. dr. sc. Ivan Forenbacher
Student: Matija Gudić
JMBAG: 0135239455

Zagreb, 2021.

SAŽETAK

Trend kriptovaluta sve je više na uzlaznoj putanji, i gotovo da nema osobe koja nije čula za njih. To je trend koji je izazvan pojavom Bitcoina, nakon što je predstavljena ideja o digitalnoj valuti koja nije pod nikakvim utjecajem financijskih institucija. Ideja o digitalnoj valuti postojala je i prije same pojave Bitcoina, ali nije bilo prave tehnologije koja bi to omogućila. Tako je pojavom Bitcoina predstavljena nova i revolucionarna tehnologija pod nazivom blockchain, čiji dizajn predstavlja decentralizirani i sigurni zapis, na kojem je temeljena svaka današnja kriptovaluta. Danas je spektar primjene blockchain tehnologije širok, pa tako omogućuje stvaranje pametnih ugovora, pa sve do poboljšanja sigurnosti u poslovanju raznih organizacija. Ovim radom biti će predstavljene značajke mreže za trgovanje kriptovalutama, uključujući njihov razvoj, opis značajki blockchain tehnologije, pametnih ugovora, te tržišne aktivnosti i tržišno stanje kriptovaluta.

KLJUČNE RIJEČI: kriptovalute; blockchain; Bitcoin; pametni ugovor; tržište kriptovaluta

SUMMARY

The trend of cryptocurrencies is increasingly on an upward trajectory, and there is almost no person who has not heard of them. This is a trend caused by the emergence of Bitcoin in 2009, after the idea of a digital currency that is not under no influence of financial institutions was presented. The idea of digital currency existed even before the introduction of Bitcoin, but there was no real technology to make it possible. Thus, with the introduction of Bitcoin, a new and revolutionary technology called blockchain was introduced, whose design represents a decentralized and secure record on which every cryptocurrency today is based. Today, the range of applications of blockchain technology is wide, from enabling the creation of smart contracts, all the way to improving security in the operations of various organizations. This paper will present cryptocurrency network characteristics and their development, a description of the features of blockchain technology, smart contracts, market activities and market conditions of cryptocurrencies.

KEYWORDS: cryptocurrencies; blockchain; Bitcoin; smart contract; cryptocurrency market

SADRŽAJ

1. Uvod ... 1
2. Razvoj kriptovaluta ... 3
   2.1. Razvoj Bitcoina ... 4
      2.1.1. Inicijalna faza Bitcoina ... 4
      2.1.2. Početni uspon Bitcoina ... 5
      2.1.3. Proliferacija Bitcoina ... 6
   2.2. Pojava alternativa Bitcoinu ... 8
      2.2.1. Razvoj Ethereuma ... 9
      2.2.2. Razvoj ostalih kriptovaluta ... 9
3. Princip rada blockchain tehnologije ... 11
   3.1. Distribuirani sustavi ... 11
   3.2. Osnovne značajke i elementi blockchaina ... 12
      3.2.1. Struktura bloka ... 14
      3.2.2. Čvorovi blockchain mreže ... 15
      3.2.3. Proces rudarenja ... 16
      3.2.4. *Hash* funkcija ... 17
   3.3. Vrste blockchaina ... 19
      3.3.1. Javni blockchain ... 19
      3.3.2. Privatni blockchain ... 20
      3.3.3. Hibridni blockchain ... 20
      3.3.4. Konzorcijski blockchain ... 21
   3.4. Mehanizam konsenzusa ... 22
      3.4.1. *Proof of Work* algoritam ... 22
      3.4.2. *Proof of Stake* algoritam ... 23
   3.5. Kriptografske metode ... 23
      3.5.1. Simetrična kriptografija ... 24
      3.5.2. Asimetrična kriptografija ... 25
   3.6. Decentralizacija ... 27
      3.6.1. Metoda disintermedijacije ... 28
      3.6.2. Metoda konkurencije ... 29
4. Pametni ugovori ... 30

4.1. Povijesni razvoj pametnih ugovora ... 30
4.2. Princip rada pametnih ugovora ... 31
4.3. Platforme za kreiranje pametnih ugovora ... 33
4.3.1. Ethereum Virtual Machine (EVM) ... 33
4.3.2. EOS.IO ... 34
4.3.3. Cardano ... 34
4.4. Primjena pametnih ugovora ... 35
4.4.1. Upravljanje lancem opskrbe ... 35
4.4.2. Industrija osiguranja ... 36
4.4.3. Financijske usluge ... 36
4.4.4. Poljoprivreda ... 37
5. Mreža za trgovanje kriptovalutama ... 38
5.1. Servisi za trgovanje kriptovalutama ... 38
5.1.1. Binance ... 39
5.1.2. Coinbase ... 39
5.1.3. Bisq ... 40
5.2. Novčanici za kriptovalute ... 40
5.3. CFD trgovanje kriptovalutama ... 41
5.4. Bikovo tržište u 2021. godini ... 42
6. Stanje na tržištu ... 43
6.1. Tržišna kapitalizacija kriptovaluta ... 43
6.2. Volumen trgovanja kriptovalutama ... 44
6.3. Analiza cijene kriptovaluta ... 46
6.3.1. Bitcoin ... 47
6.3.2. Ethereum ... 48
6.3.3. Cardano ... 48
7. Zaključak ... 50
Literatura ... 51
Popis kratica ... 55
Popis slika ... 56
Popis tablica i dijagrama ... 57
Popis grafikona ... 58

1. Uvod

Evolucija kriptovaluta napredovala je do te mjere da više nije samo tema razgovora i zapravo je spremna za široku komercijalnu uporabu. Ova evolucija je još jedan aspekt velikog trenda udaljavanja od centraliziranih financija. Posljednjih nekoliko desetljeća monopol stvaranja novca bio je koristan za one na vrhu piramide bogatstva i moći, što je počelo stvarati ideje o neovisnoj valuti bez utjecaja vodećih tijela. Iako su raniji pokušaji stvaranja neovisne digitalne valute bili neuspješni, revoluciju je donio programer pod pseudonimom Satoshi Nakamoto, koji je 2009. godine predstavio globalno poznatu kriptovalutu pod nazivom Bitcoin, temeljenu na blockchain tehnologiji. Obična ideja o decentraliziranoj neovisnoj valuti desetak godina kasnije dovela je do ogromnog tržišnog trenda kupovanja kripotvaluta i razvijanja raznih platforma i mreža temeljenih na blockchainu.

Blockchain tehnologija jedna je od najvećih inovacija 21. stoljeća s obzirom na učinak koji ima na različite sektore, od financijskog do proizvodnog. Otkako je njegova popularnost počela rasti prije nekoliko godina pojavom Bitcoina, pojavile su se brojne primjene ove tehnologije, od pametnih ugovora, pa sve do poljoprivrede i kreiranja raznih aplikacija.

Gledajući iz perspektive arhitekture mreže i njezinih značajki, ova tema je višestruko važna. Prvo, blockchain tehnologija može znatno promijeniti razinu sigurnosti podataka, kreirajući zapise koji ne mogu biti izmijenjeni zbog visoke razine enkripcije, te samim time sprječavaju potencijalne prijevare i neovlaštene aktivnosti. Drugo, pošto ova tehnologija koristi distribuirane zapise, svi sudionici u blockchain mreži imaju pristup istim podacima, što omogućuje potpunu transparentnost. Zadnje, blockchain tehnologija pruža automatizaciju u obliku pametnih ugovora i razne druge primjene poput izgradnje stabilne digitalne valute koja ne ovisi o nekom centralnom tijelu.

U tom kontekstu, ovaj rad podijeljen je u 7 cjelina:

1. Uvod
2. Razvoj kriptovaluta
3. Princip rada blockchain tehnologije
4. Pametni ugovori
5. Mreža za trgovanje kriptovalutama
6. Stanje na tržištu
7. Zaključak

Drugo poglavlje dati će povijesni i evolucijski prikaz kriptovaluta, počevši od samog Bitcoina, pa sve do pojave ostalih kriptovaluta i njihov razvoj.

Treće poglavlje predstavlja detaljan prikaz blockchain tehnologije i njezin princip rada. U ovom poglavlju biti će opisani osnovni elementi koji čine ovu tehnologiju, njezine osnovne vrste i mehanizmi rada, te uslugu decentralizacije.

Četvrto poglavlje opisuje povijesni razvoj pametnih ugovora i njihov princip rada. Također, navedene su neke od popularnijih platforma za kreiranje pametnih ugovora i navedeni su primjeri njihove primjene.

Peto poglavlje odnosi se na primjer mreže za trgovanje kriptovalutama, gdje su opisane mogućnosti transakcija i navedeni su servisi koji za to služe te mogućnosti usluge novčanika. Na kraju se nalazi sažetak bikovog tržišta 2021. godine.

U konačnom šestom poglavlju analizirano je trenutno stanje na tržištu kriptovaluta, i analizirane su tri trenutno najznačajnije kriptovalute na tržištu, a to su Bitcoin, Ethereum i Cardano.

2. Razvoj kriptovaluta

Za većinu ljudi, sektor kriptovaluta relativno je nova pojava, s tim da je taj pojam poznat javnosti već nekih 4 godina. Iako su neki pojedinci svjesni ove pojave i duže vrijeme, pa i od samog početka, u javnosti je bio često povezan sa crnim tržištem i mrežom za anonimnost. Sami koncept digitalne valute postojao je mnogo godina prije pojave Bitcoina. [6]

Prva poznata tvrtka za elektronički novac bila je DigiCash, a osnovao ju je David Chaum 1990. godine. Bila je jedinstvena po tome što se temeljila na nekoliko kriptografskih protokola razvijenih od strane osnivača. Međutim, kompanija je proglasila bankrot 1998. godine i prodala su svoju imovinu sličnoj kompaniji pod nazivom eCash Technologies. Kasnije se pojavila američka kompanija pod nazivom PayPal, koja je nudila usluge prijenosa novca putem interneta. Novac je nešto što funkcionira kao sredstvo razmjene, ima svoju vrijednost, te služi kao računovodstvena jedinica. Međutim, nije postojao konkretan decentralizirani sustav koji bi se udaljio od banaka, te njihovog držanja monopola nad valutama. Jedini mogući ishod takvih sustava je koncentracija bogatstva i moći, te rastuća nejednakost, što je povijest pokazala istinitom. [6]

Trenutni globalni sustav fiat valute[1] u svojoj je jezgri centraliziran, i oslanja se na velike financijske institucije koje djeluju kao „pouzdane treće strane“ kako bi regulirale stvaranje i tijek novca (pozajmice, obrada naplaćivanja, itd.). Dok općenito postoji papirnati novac, većinu novca u sustavu čini digitalna valuta koju stvaraju računala banaka. Međutim, monopol na stvaranje digitalnog novca počeo se osporavati tehnologijom koja omogućuje decentralizirano stvaranje digitalne valute u obliku kriptovaluta. Izvor novaca više ne moraju biti banke i ne mora se posuđivati i distribuirati kroz posrednike na vrhu ekonomske piramide. [5][7]

Primjenom blockchain tehnologije se novac može stvoriti digitalno i distribuirati kroz decentralizirane/distribuirane mreže. Povodom toga, kripto-evolucija je još jedan aspekt

[1] Fiat valuta predstavlja danas svima poznati fizički oblik novca, a služi kao valuta koju vlast određuje kao jedino pravno sredstvo plaćanja i njegovu vrijednost jamče institucije koje ga izdaju.

trenda udaljavanja od centraliziranog sustava banaka i kretanja prema distribuiranom ekonomskom sustavu. [6]

2.1. Razvoj Bitcoina

Na temelju dokumentacije iz 2008. godine napisane od strane anonimnog programera koji se predstavljao pod pseudonimom Satoshi Nakamoto, program pod nazivom Bitcoin (BTC) je implementiran kao otvoreni kôd i objavljen je u siječnju 2009. godine. Bitcoin je temeljen na tehnologiji pod nazivom blockchain, koja putem *peer-to-peer* mreže[2] povezuje zapise svih transakcija izvršenih unutar mreže pomoću kriptografije. To znači da svaki korisnik unutar te mreže mora autorizirati svaku novu transakciju kako bi se ona verificirala. Novi blockchain blokovi stvaraju se pomoću procesa koji se naziva rudarenje (engl. *mining*), koji u Bitcoin ekosustavu koristi računalnu snagu za bilježenje transakcija u blokovima na lancu. Osim svoje sigurnosti, navedene prednosti tehnologije su i to što se transakcije evidentiraju učinkovito, transparentno i na provjerljiv i trajan način. [8]

2.1.1. Inicijalna faza Bitcoina

2009. godine izrudaren je prvi blok Bitcoina. U tom periodu, 50 prvih Bitcoina je kreirano i zabilježeno u njegovoj blockchain mreži. Prva transakcija sadržavala je sadržaj naslovnice Britanskih novina „*The Times*“, a tekst je glasio: „*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*“. Ovaj tekst je služio kao dokaz da blok nije mogao biti miniran ranije od tog navedenog datuma, a naslov je očito bio ciljano izabran zbog podbacivanja banaka i pretpostavljene konkurentnosti Bitcoina. Nakon toga, Satoshi Nakamoto pustio je u javnost Bitcoin program, zajedno sa njegovim izvornim kôdom. Povodom toga, Bitcoin je bio dostupan svima koji su imali mogućnost i želju isprobati program, a to je dozvolilo ljudima da preuzmu program, te tako postanu „knjigovođe“ transakcija i rudari kriptovaluta (engl. *miners*). Nedugo nakon puštanja

[2] *Peer-to-peer* mreža predstavlja koncept umrežavanja računala bez poslužitelja, gdje svako računalo predstavlja jedan čvor mreže.

programa u javnost, zabilježena je prva Bitcoin transakcija, i to od strane njegovog osnivača. [8]

Nakon puštanja programa u javnost, 2010. godina je obilježena time što je kreirana stranica za razmjenu Bitcoina, pod nazivom „*The Bitcoin Market*“. Prije toga, ljudi su razmjenjivali Bitcoin putem raznih nestrukturiranih načina poput online soba za razgovore. Poseban sustav i mjesto za razmjenu bio je prvi korak prema jednostavnoj kupnji i prodaji Bitcoina. Jedna od najpoznatijih i najpopularnijih transakcija, a istovremeno i prva dokumentirana transakcija korištena za plaćanje u stvarnom svijetu, bila je kupovina pizze za 10.000 BTC. Programer pod imenom Laszlo Hanyecz ponudio je na Bitcointalk forumu 10.000 BTC onome tko će mu kupiti i dostaviti pizzu. Drugi programer pod imenom Jeremy Sturdivant prihvatio je ponudu, te je naručio i dao dostaviti 2 pizze iz lanca pizzeria „*Domino's Pizza*“ na adresu Laszloa. Tih 10.000 BTC tada je vrijedilo oko 40 američkih dolara (USD), a pošto je danas vrijednost 1 BTC oko 40.000 USD (cijena bitcoina stalno varira), vrijednost Bitcoina koja je tada bila izdvojena za pizzu danas bi iznosila nevjerojatnih 400 milijuna USD. [6][8]

2.1.2. Početni uspon Bitcoina

Sljedećih 4 godina krenuo je lagani rast Bitcoina i kriptovaluta općenito, jer su se počele pojavljivati razne kriptovalute na tržištu. Razne grupe i organizacije počele su prihvaćati bitcoin kao način plaćanja, poput „*Electronic Frontier Foundation*“ i „*WikiLeaks*“. No ljudi su i dalje bili skeptični u Bitcoin, te ga nisu smatrali pravom i valjanom valutom zbog toga što nije imao posrednika kao regulatora i postojao je u digitalnom obliku. To je zato što su u početku otkriveni propusti Bitcoinovog protokola, te je došlo do toga da su ga napadači uspjeli iskoristiti kako bi mogli stvoriti neograničenu količinu Bitcoina. Propust je bio u obliku nepravilnih verifikacija transakcija prije nego su bile zabilježene unutar transakcijskog zapisa, odnosno blockchaina. Ovaj skandal uzrokovao je generiranje preko 184 milijardi BTC, ali pošto su adrese transakcija uspješno detektirane, obrisane su iz zapisa i sigurnosni propust je bio ispravljen. Zbog toga je osnovana neprofitna organizacija pod nazivom „*Bitcoin Foundation*“, kako bi promovirala i ubrzala globalni rast i razvoj bitcoina kroz standardizaciju, zaštitu i promociju njegovog otvorenog kôda. [6][8]

Kasnije su i ostale razne organizacije i firme počele prihvaćati Bitcoin, ali bilo je i raznih ilegalnih radnji vezanih za razmjenu Bitcoina. Najviše je za to vezana internetska stranica pod nazivom „*Silk Road*“, koja je funkcionirala preko mreže za anonimnost pod nazivom Tor (*The Onion Router*), a odnosila se na crno tržište namijenjeno za prodaju droge, oružja, lažnih dokumenta, te ostalih ilegalnih proizvoda. Povodom toga, FBI je zaplijenio oko 26.000 BTC zarađenih na Silk Road stranici, pa je samim time Bitcoin stekao lošu reputaciju, te je bio izravno povezan sa raznim ilegalnim radnjama. No to nije zaustavilo društvo da implementira podršku Bitcoina kao načina plaćanja. Taj trend je počeo sve više rasti, pa su tako Bitcoin počele prihvaćati razne kockarnice, sveučilišta, računalne kompanije i ostali, dok su se banke iznimno protivile njegovom uvođenju zbog ugrožavanja njihovog poslovanja. [6][8]

Počeli su se uvoditi i bankomati svuda po svijetu gdje se je on lako mogao kupiti ili prodati, a jedna od najbitnijih stavki kod posjedovanja Bitcoina i ostalih kriptovaluta koja je uvedena u samim počecima je novčanik za kriptovalute (engl. *cryptocurrency wallet*). On može biti u fizičkom ili programskom obliku, a predstavlja servis pohrane javnih i privatnih kripto ključeva, koji sadrže podatke o korisnikovim transakcijama. Samim time, kripto novčanici su masovno postali meta raznih napadača i hakera, jer predstavljaju jednostavan pristup prema sredstvima nekog korisnika, a pogotovo je to slučaj kod programskih novčanika, koji se oslanjaju na razne web servise koji nude usluge kripto novčanika. Jedan od primjera takvih servisa bio je „*Mt. Gox*“, koji je 2014. godine bio zadužen za rukovođenje preko 70% svih bitcoin transakcija diljem svijeta, a nakon toga su proglasili bankrot i objavili gubitak od oko 750.000 BTC koji su pripadali njihovim korisnicima, te vlastitih 100.000 BTC. Ali ni to nije spriječilo Bitcoin od njegovog daljnjeg rasta, te je nastavio svoj put prema vrhuncu, a to je počelo primjećivati sve više ljudi. [6][8]

2.1.3. Proliferacija Bitcoina

2017. godina će biti zapamćena kao godina Bitcoina. Te godine uočeno je da su ga ozbiljnije shvatili mediji, regulatori, javnost i klasični financijski sustav. Također, pojavile su se teorije da bi valute poput Bitcoina mogle usvojiti zemlje s lošim monetarnim sustavima. Bitcoin je počeo djelovati s više snage i bogatstva za ponovno ulaganje, te

nastavlja snažno napredovati, a pri tome je okupio razne zajednice, te inspirirao pojedince za upotrebu blockchain tehnologije. [8]

Bitcoin je godinu započeo sa vrijednošću od manje od 1.000 USD po Bitcoinu, a do kraja godine je narasla za više od 1.300 %. Taj uspon je obilježila ekstremna nestabilnost, višestruki rascjepi u njegovoj mreži i skeptici koji su ga ismijavali kao prijevaru i alat za kriminalce. Ovaj uspon je pogotovo privukao pozornost Wall Streeta, a to je omogućilo raznim investitorima da se klade na njegovu vrijednost bez posjedovanja samog Bitcoina. [6][8]

Početkom godine Bitcoin je krenuo loše zbog skandala u Kini. Kina je objavila da započinje istragu o razmjeni Bitcoina zbog sumnje u manipulaciju tržištem, pranje novca, neovlašteno financiranje i druge probleme, te je tada upozorila ulagače na oprez pri ulaganju. Poslije 2 mjeseca, Bitcoin je vratio svoju vrijednost nakon što se je smirila situacija sa Kinom, pa je kasnije Japan proglasio ovu valutu legalnom. Sljedećih mjeseci Bitcoin je imao lagan rast, sve dok nije nastala zabrinutost zbog mogućeg rascjepa Bitcoin mreže, nakon čega mu je vrijednost pala. Zbog ovoga je došlo do procesa *forkinga*[3] ili dijeljenja mreže, što je rezultiralo stvaranjem nove digitalne valute pod nazivom Bitcoin Cash. Na kraju su ulagači ipak odustali od ulaganja u taj projekt, te je cijena narasla na 5.000 USD po Bitcoinu. Cijena je, uz povremene manje padove, nastavila strmoglavo rasti, te je svoj vrhunac dosegnula 18. prosinca, kada je vrijednost dosegla gotovo 20.000 USD. Na kraju godine, cijena je pala na 14.000 USD. Od siječnja do veljače 2018. godine dogodio se veliki pad vrijednosti Bitcoina, i to za 65%. Sljedećih mjeseci uslijedio je strmoglavi pad njegove vrijednosti, te je njegova ukupna tržišna vrijednost pala ispod 100 milijardi USD, a vrijednost jednog Bitcoina do kraja godine pala je na oko 3.000 USD. Ta vrijednost je imala minimalne uspone idućih 2 godine, sve do pojave pandemije COVID-19. [6][8]

Pojava pandemije početkom 2020. godine uzrokovala je lagani pad već niske vrijednosti, ali se je ubrzo oporavila, nakon čeka je počela sa drugim valom rasta vrijednosti. Unatoč pandemiji, prema kraju godine vrijednost je i dalje rasla, te su analitičari

[3] *Forking* predstavlja proces dijeljenja jedne blockchain mreže u dvije neovisne mreže.

predviđali ponovni rast vrijednosti na oko 20.000 USD. Iako se trend rasta nastavio tako što je sredinom veljače Bitcoin dosegao 50.000 USD, financijski savjetnici upozoravali su ljude da ne ulažu u Bitcoin zbog njegove vrijednosne nestabilnosti, te da bi mogli lako izgubiti svoj novac. No u travnju 2021. godine, Bitcoin je dosegao svoj maksimum od gotovo 64.000 USD, što nitko nije očekivao. [6][8]

2.2. Pojava alternativa Bitcoinu

S obzirom na početni uspjeh Bitcoina, pokrenuti su mnogi projekti vezani za alternativne kriptovalute. Prva alternativa predstavljena je 2011. godine pod nazivom Namecoin. Tokom 2013. i 2014. godine, tržište alternativnih valuta eksponencijalno je poraslo i pojavile su se mnoge različite vrste projekata vezane za alternativu Bitcoinu. Nekoliko njih se pokazalo kao uspjeh, dok su mnogi drugi bili neuspjeh zbog manjeg interesa, a nekoliko tih projekata su bile prijevare koje su se pojavljivale neko vrijeme, ali su ubrzo nestale. [9]

Danas postoji preko 4.000 kriptovaluta, a mnoge od njih imaju malu ili nikakvu tržišnu vrijednost.. Alternativne valute moraju biti u mogućnosti privući nove korisnike, ulagatelje i rudare, inače valuta neće imati vrijednost. Valuta dobiva na vrijednosti zbog mrežnog učinka i svoje prihvatljivosti od strane zajednice, a to je pogotovo slučaj u svijetu kriptovaluta. Ako valuta ne uspije privući dovoljno korisnika, uskoro će biti zaboravljena. Međutim, postoji rizik da ako projekt nove valute bude neuspješan, može se izgubiti početno ulaganje u nju. [9]

Postoje različiti čimbenici i novi koncepti uvedeni alternativnim valutama, a mnogi su koncepti izmišljeni čak i prije Bitcoina, ali nisu stekli dovoljno popularnosti i pažnje. Pošto Bitcoin predstavlja kriptovalutu prve generacije, uvođenjem alternativnih projekata pojavljuju se različite nove tehnike i koncepti koji predstavljaju nadogradnju ili poboljšanje samog Bitcoina. Na osnovu svih tih faktora, područje kriptovaluta se uvijek proširuje i nadograđuje, te se nikad ne zna kada će niknuti neka nova digitalna valuta od značaja. [9]

2.2.1. Razvoj Ethereuma

Programer pod imenom Vitalik Buterin napravio je koncept za Ethereum u studenom 2013. godine. Ethereum je najavljen na Bitcoin konferenciji u siječnju 2014. godine u SAD-u, te je konačno mreža puštena u pogon u srpnju 2015. godine. Ethereum je bio stvoren s namjerom da omogući razvojnim programerima da kreiraju razne aplikacije bazirane na blockchainu. To je omogućeno kreiranjem drugačijeg temeljnog sloja, za razliku od Bitcoina, na način da se u sami blockchain ugradi Turingov programski jezik koji omogućuje bilo kome da kreira pametne ugovore i decentralizirane aplikacije. Pored same kriptovalute, Ethereum predstavlja jednu revolucionarnu platformu druge generacije, koja daje više slobode i mogućnosti kod korištenja blockchaina, te predstavlja poboljšanu verziju Bitcoina. [9][10]

Ether (ETH) ili često nazvan Ethereum, je kriptovaluta generirana Ethereum protokolom kao nagrada rudarima u sustavu provjere za dodavanje blokova u blockchain. Također predstavlja fundamentalnu jedinicu cijele Ethereum mreže jer služi kao „gorivo“ koje omogućuje svu aktivnost unutar nje. Ethereum je svoj prvi vrhunac kao valuta doživio u siječnju 2018. godine, kada je njegova vrijednost narasla na 1.400 USD po tokenu[4]. U isto vrijeme, Bitcoinova vrijednost je počela strmoglavo padati. Isti slučaj zadesio je i Ethereum, koji je također prema kraju 2018. godine pao ispod 300 USD. Drugi vrhunac dogodio se početkom 2021. godine, u isto vrijeme kada je i Bitcoin počeo probijati sve rekorde. [9][10]

2.2.2. Razvoj ostalih kriptovaluta

Nakon pojave Bitcoina, pojavljivale su se razne ostale kriptovalute. Namecoin je valuta koja je prva nastala iz izvornog kôda Bitcoina, koji je zapravo proizašao kao rezultat *forkinga*, što znači da je uzet izvorni kôd Bitcoina, kako bi se mreža podijelila. Tvorci Namecoina su ga pustili u javnost u travnju 2011. godine, a stvorili su ga kao eksperiment sa namjerom da poboljša decentralizaciju, sigurnost, cenzuru interneta, te nije direktno

[4] Token predstavlja vrijednosnu jedinicu kod kriptovaluta, kao što je kovanica kod fizičkih valuta.

bio zamišljen kao zamjena za Bitcoin. Krajem 2013. godine dostigao je svoju maksimalnu vrijednost od 13 USD, te nakon toga interes za njim je gotovo nestao. [9]

Jedna od značajnijih je Litecoin, također rezultat kopiranja originalnog Bitcoinovog kôda. Litecoin je 2011. pokrenuo bivši Googleov inženjer Charlie Lee, koji je najavio takozvanu „Lite verziju Bitcoina“ putem objave na popularnom Bitcoin forumu. Iz tog razloga, Litecoin usvaja mnoge značajke Bitcoina za koje su Lee i drugi programeri smatrali korisnima, te mijenjaju neke druge bitne aspekte za koje je razvojni tim smatrao da bi se mogli poboljšati. Svoje vrhunce vrijednosti od oko 350 USD dostiže 2018. i 2021. godine, isto kao i većina značajnih kriptovaluta. [9]

Još jedna od značajnijih kriptovaluta je Bitcoin Cash, koji je također proizašao kao rezultat *forkinga*. Zbog nezadovoljstva grupe programera i rudara sa Bitcoinovim kapacitetom bloka, sredinom 2017. godine odlučili su podijeliti mrežu, te povećati izvorno ograničenje veličine bloka. Bitcoin Cash povećava memorijsko ograničenje jednog bloka sa izvornih 1 MB na 8 MB. To odmah povećava broj transakcija koje mogu biti obrađene u jednom bloku na mnogo veći broj u usporedbi s ograničenjem od 1 MB u izvornom Bitcoin protokolu. 1. kolovoza 2017. godine, kada je i Bitcoin Cash pušten na tržište, počeo se prodavati za oko 240 dolara, Krajem iste godine dosegnuo je svoj maksimum od gotovo 4.000 dolara. [9]

Od ostalih značajnih kriptovaluta tako su se još pojavile Ripple, Dogecoin, Dash, NEO, Zcash, Cardano i ostale. Cardano (ADA) je jedna od novijih valuta, a osnovana je 2015. i javno objavljena 2017. godine. Trenutno je vrlo popularna zbog svojih vrlo malih zahtjeva po pitanju potrošnje električne energije. Jedan od načina na koji Cardano to čini je korištenjem protokola koji ne potiče visoku potrošnju energije i sve je popularniji način za verifikaciju blokova radi sigurnosnih razloga. Cardano uskoro prelazi na omogućavanje pametnih ugovora koji bi trebali biti potpuno operativni do jeseni 2021. godine. [7][9]

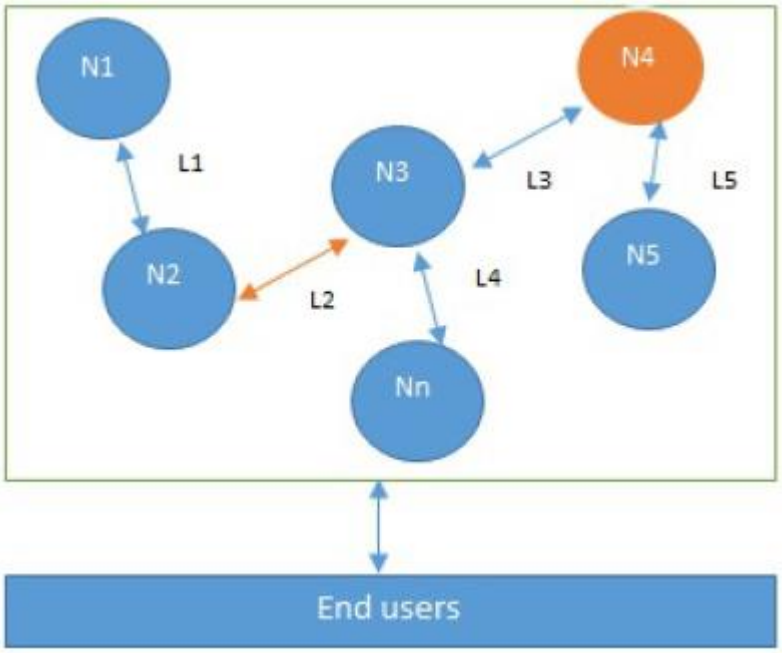
3. Princip rada blockchain tehnologije

Samim predstavljanjem Bitcoina 2009. godine predstavljen je novi koncept koji bi trebao revolucionirati cijelo društvo. Taj koncept je predstavljen s obećanjem da će imati utjecaj na svu industriju, ali pritom ne ograničavajući se na financijski sektor, vladu, medije, pravo i umjetnost. Neki vide blockchain tehnologiju kao revoluciju, dok drugi ju smatraju kao evolutivnu i smatraju da će proći mnogo godina dok se ona ne usavrši i postane korisna u praktičnoj primjeni. Međutim, mnoge svjetske organizacije već masovno koriste blockchain tehnologiju, nakon što je njezin potencijal prepoznat. Blockchain pokazuje kako može imati utjecaj na već postojeće tehnologije i u širem pogledu od samih kriptovaluta. S obzirnom na to, zanimanje za blockchain tehnologiju značajno je poraslo, a pogotovo u posljednjih 4 godine. [1][39]

3.1. Distribuirani sustavi

Kako bi se lakše razumjela blockchain tehnologija, vrlo je bitno razumjeti kako rade distribuirani sustavi. Kada je riječ o distribuiranim sustavima, mogu se pojaviti u centraliziranom ili decentraliziranom obliku. Namjera blockchaina od početka je kreiranje decentralizirane platforme, a može se definirati kao sustav sa decentraliziranim i distribuiranim značajkama. [1]

Distribuirani sustavi su računalna paradigma prema kojoj dva ili više čvora međusobno koordinirano surađuju kako bi postigli zajednički ishod. Modeliran je na način da ga krajnji korisnici vide kao jedinstvenu platformu, ali na logičkoj razini, gdje više fizičkih elemenata čine jedan logički. Čvor se može definirati kao jedan od sudionika unutar distribuiranog sustava, a svi čvorovi mogu komunicirati jedan sa drugim, te razmjenjivati informacije. Čvorovi predstavljaju jedinicu unutar sustava koja ima svoj procesor i memoriju. Postoji vrsta čvora koji pokazuje nedosljedno ili neočekivano ponašanje, a naziva se bizantski čvor. Takav čvor može biti zlonamjeran, a to direktno utječe na pravilan rad mreže. [1]



Slika 1. Dizajn distribuiranog sustava, [1]

Slika 1. prikazuje jednostavan dizajn distribuiranog sustava sa šest čvorova, od kojih je čvor (N4) bizantski čvor, koji može biti uzrok nepravilne distribucije informacija i slično. Također, link (L2) koji je spor ili nefunkcionalan može dovesti do razdvajanja mreže. [1]

Glavni izazov u projektiranju distribuiranog sustava je usklađenost rada između čvorova i tolerancija na greške. Čak i ako neki čvorovi ili linkovi postanu potpuno nefunkcionalni, sustav bi trebao biti u mogućnosti podnijeti kvarove i nastaviti sa normalnim radom. Ovaj izazov predstavlja veliki problem kod projektiranja, pa zbog toga je vrlo teško ostvariti 3 željena svojstva sustava: konzistencija, dostupnost i tolerancija na razdvajanje mreže. [1]

3.2. Osnovne značajke i elementi blockchaina

Za blockchain se može reći da je vrsta baze podataka. Baza podataka je kolekcija informacija koje su pohranjene elektronički na računalnom sustavu. Informacije su u bazama podataka obično unesene u obliku tablica, kako bi lakše pronašli određeni podatak. Takve baze se obično nalaze na poslužiteljima koji sadrže ogromnu količinu

podataka, te imaju ogromnu procesorsku snagu, kako bi bili u mogućnosti pružati pristup informacijama velikoj količini korisnika. Često je takva infrastruktura u vlasništvu neke organizacije koja upravlja njome, te ima potpunu kontrolu nad načinom rada i podacima u njoj. Takva struktura pohrane može se nazvati centraliziranom. [5][39]

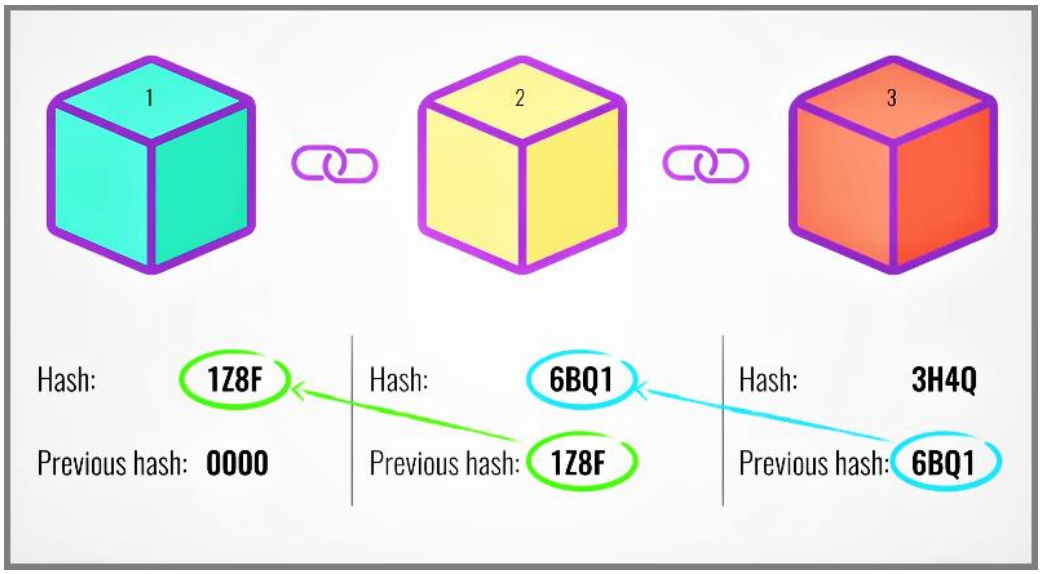
Primjer ovakvog sustava je način rada knjižnice, kako je to opisano u [2]. Osoba može otići u knjižnicu te posuditi željenu knjigu, uz određena pravila i rok vraćanja. Druga osoba živi blizu prve i želi istu knjigu, ali prva ju ne smije direktno uručiti drugoj, nego ju mora vratiti u knjižnicu. Tu knjižnica ostaje centralna baza podataka svih informacija posuđenih knjiga. U drugom slučaju, postoji sustav gdje osoba može posuditi knjigu direktno od osobe koja ju posjeduje, bez posredovanja knjižnice. Takav sustav predstavlja dijeljeni zapis u koji se svatko može pridružiti i posuđivati knjige, te su sve informacije o posuđivanju i vlasniku knjige poznate svim sudionicima. Drugim riječima, iz cijelog se postupka eliminira potreba za posrednikom. Ovo je slučaj kod kojeg se primjećuju prednosti blockchain tehnologije. Blockchain može pružiti decentraliziranu distribuiranu bazu podataka svih zapisa o knjigama u knjižnici. [2]

Jedna ključna razlika između tipične baze podataka i blockchaina je način na koji su podaci strukturirani. Blockchain prikuplja informacije u grupe koje se nazivaju blokovima. Blokovi drže skupove informacija, te imaju određene skladišne kapacitete, a kad su popunjeni, lancem se vežu na prethodno ispunjeni blok, tvoreći lanac podataka poznat kao "blockchain". Sve nove informacije koje se dodaju nakon toga svježe dodanog bloka sastavljaju se u novonastali blok koji će se također dodati u lanac nakon što se ispuni. Dakle, klasične baze podataka pohranjuju svoje informacije u tablice, dok blockchain strukturira svoje informacije u blokove koji su lančano povezani. Unatoč snažnoj povezanosti, blockchain nije Bitcoin. Umjesto toga, blockchain je digitalni zapis koji omogućuje postojanje Bitcoina i drugih kriptovaluta bilježeći u lanac postojanje svakog digitalnog tokena, tko ga posjeduje, kada se prodaje i kome. To je od velike važnosti jer nije moguće povezati vlasništvo nad Bitcoinom bez kriptiranja u digitalnom obliku i zapisom u distribuiranu bazu podataka. Bez blockchaina, kriptovalute ne bi imale vrijednost. [4][5]

3.2.1. Struktura bloka

Osnovna funkcija svakog blockchaina je grupiranje digitalnih informacija u zbirke, nazvane "blokovi", koje se ne mogu mijenjati . Blok se sastoji od tri osnovna elementa, a to su informacije, kôd (*hash*) trenutnog bloka i kôd prethodnog bloka. Te informacije mogu uključivati podatke kao što su izvršene transakcije, odnosno sve što netko želi trajno zabilježiti. Kad je blok pun podataka, jedan od nekoliko složenih procesa koristi se za vremensko označavanje u trajni zapis. Svaki blok je povezan sa sljedećim blokom putem jedinstvenog kôda koji upućuje na sadržaj oba bloka, te ga zato nazivamo lancem. [2]

Na primjeru Bitcoina može se prikazati način ulančavanja blokova. Korisne informacije koje su pohranjene unutar bloka odnose se na transakciju, odnosno pošiljatelja, primatelja i količinu novca. Također, blok kreira jedinstveni kôd koji ga identificira, te identificira i sav ostali sadržaj bloka, i uvijek je jedinstven poput otiska prsta. Ako se pokuša promijeniti bilo kakav sadržaj unutar bloka, to će uzrokovati promjenu kompletnog kôda. To izvršava jedan sigurnosni mehanizam koji na taj način detektira bilo kakve promjene, te osigurava da se jedinstveni kôd uvijek veže samo za jedan blok. Zadnji bitni element bloka je kôd prethodnog bloka u lancu. Na taj se način kreira sami lanac blokova, te je ta tehnika vrlo učinkovita kod postizanja visoke razine sigurnosti blockchaina. [11]



Slika 2. Povezanost blokova u lancu, [10]

Na slici 2. je prikazan odnos između blokova u lancu, koji sadrže vlastiti *hash* i *hash* prethodnog bloka, te je vidljivo kako su povezani jedni s drugima na osnovu jedinstvenih kôdova. Također, prvi blok ne može pokazivati na nijedan drugi blok jer je on taj koji počinje niz, a naziva se „*Genesis block*“ ili izvorni blok. Bilo kakva promjena na jednom od bloka biti će vidljiva na sljedećem koji sadržava originalni kôd prethodnog, te će zbog toga svi novi blokovi u nizu postati nevažeći. Zbog toga postoji mehanizam koji je zaslužen za ponovnu kalkulaciju svih kôdova u nizu, kako bi cijeli blockchain ponovno bio valjan. Kako bi se ublažila potreba za time, Bitcoinov blockchain ima dodatan mehanizam pod nazivom „*Proof of work*“. On usporava kreiranje novih blokova, te samim time otežava mogućnost interferencije i nevaljanosti blokova. Svi ovi mehanizmi zajedno stvaraju snažnu sigurnosnu sposobnost blockchain tehnologije. [11]

3.2.2. Čvorovi blockchain mreže

Čvorovi mogu biti rudari koji stvaraju nove blokove i generiraju kriptovalutu ili potpisnici blokova koji potvrđuju i digitalno potpisuju transakcije. Svatko tko se pridruži blockchain mreži koristeći svoj uređaj smatra se čvorom blockchain mreže. U lancu mogu biti ogromne količine čvorova – što ih ima više, to je pogodnije. Razlog tome je što je blockchain mreža tada otpornija na stvari poput nestanka struje, hakiranje, sistemske greške i ostale nepogodnosti. Velika prednost dizajna blockchain mreže je ta da se sami blockchain replicira i konstantno ažurira na svakom od čvorova. S obzirom na to, ako se promijene informacije u jednom bloku i slijedu blokova nakon njega, tako bi se morale promijeniti i na svakom čvoru u mreži. Na taj se način lako detektira bilo kakva sumnjiva promjena u mreži i blokovima. [1][4] Ukratko, ovo su operacije koje čvorovi obavljaju:

1. Čvorovi provjeravaju je li transakcijski blok važeći, te ga na osnovu toga prihvaćaju ili odbijaju.
2. Čvorovi spremaju i pohranjuju transakcijske blokove (pohranjuju povijest transakcija blockchaina).
3. Čvorovi emitiraju i šire povijest transakcija na druge čvorove koji će se možda trebati sinkronizirati s blockchainom (potrebno ih je ažurirati u povijesti transakcija).

Čvorovi koji se bave procesom rudarenja uvijek trebaju sadržavati potpunu kopiju transakcijske povijesti blockchaina. Takvi čvorovi se nazivaju „*full node*“ ili potpuni čvor. Bez potpune kopije takvi čvorovi ne mogu potvrđivati sve transakcije na osnovu transakcijske povijesti, jer nemaju pristup potpunoj povijesti. S druge strane, klasični čvorovi mogu primati, pohranjivati i emitirati sve transakcijske podatke, bez kreiranja novih blokova. U tom slučaju čvor funkcionira kao prolazna točka mreže sa direktorijem. Postoji još jedna vrsta čvora, od nazivom „*masternode*“. Oni su obično opremljeniji od klasičnih čvorova, te osim validacije transakcija, obavljaju i radnje poput osiguranja izvršavanja raznih protokola i događaja glasovanja, te provođenja definiranog zakona određene blockchain mreže. Za njih se može reći da su kao veliki poslužitelji na mreži, te su uvijek *online*. [13]

3.2.3. Proces rudarenja

Rudarenje (engl. *mining*) je proces kojim se novi dijelovi kriptovalute unose u opticaj, ali je i kritična komponenta održavanja i razvoja blockchaina. Izvodi se pomoću sofisticiranih računala koja rješavaju iznimno složene računske matematičke probleme. Rudarenje kriptovaluta je mukotrpno, skupo i njegova isplativost je upitna. Bez obzira na to, rudarstvo privlači mnoge investitore zainteresirane za kriptovalute zbog činjenice da su rudari nagrađeni za svoj rad u obliku digitalnih kripto tokena. [12]

Rudarenje se svodi na provjeru legitimnosti transakcija određene kriptovalute. Provjerom transakcija rudari pomažu spriječiti bilo kakav pokušaj kopiranja digitalnih tokena. Primjerice, nakon što rudar verificira 1 MB transakcije Bitcoina, odnosno jedan blok , on ispunjava uvjet da bude nagrađen sa određenom količinom Bitcoina. Bitcoin ima ograničenje od 1 MB po bloku, a to može predstavljati problem zbog malog kapaciteta, te samim time usporavati cijeli proces verifikacije transakcija. [12]



Dijagram 1. Proces rudarenja blokova, [1] [12]

Kao što je prikazano na dijagramu 1., cijeli proces rudarenja, odnosno generiranja blokova, prema [1] i [12] može se opisati u 5 koraka:

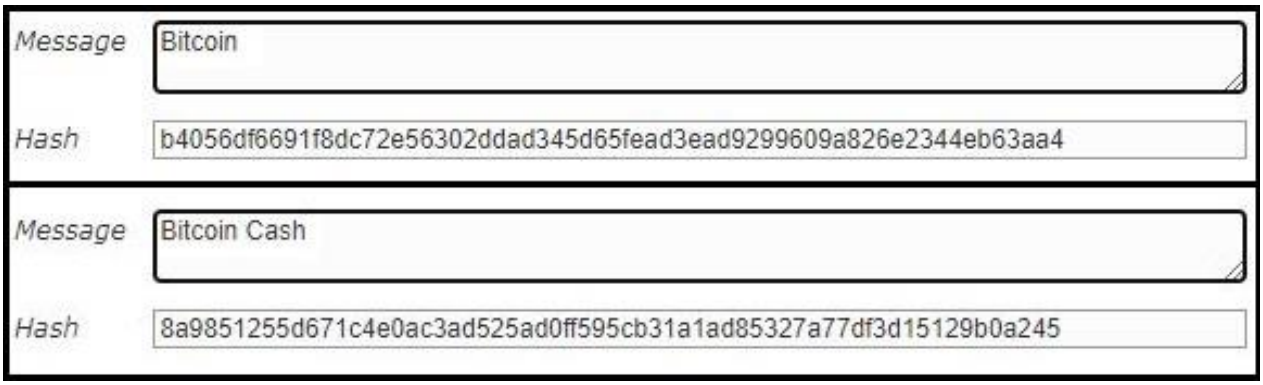
1. Čvor pokreće transakciju tako da ju najprije kreira, pa zatim digitalno potpiše sa svojim privatnim ključem. Transakcija može predstavljati različite radnje u blockchainu. Najčešće je to struktura podataka koja predstavlja prijenos vrijednosti između korisnika na blockchain mreži. Struktura podataka transakcija obično se sastoji od prijenosa vrijednosti, pravila, adrese izvora i odredišta, te drugih validacijskih informacija.
2. Transakcija se propagira (preplavljuje) čvorovima pomoću protokola preplavljivanja (*flooding*), nazvanog „*Gossip protocol*“, a ti čvorovi validiraju transakciju na temelju unaprijed postavljenih kriterija. Obično je za provjeru transakcije potrebno više od jednog čvora.
3. Nakon što je transakcija potvrđena, unosi se u blok, koji se zatim prenosi na mrežu, te se nakon toga transakcija smatra potvrđenom.
4. Novonastali blok sada postaje dio blockchain mreže, a sljedeći se blok kriptografskim ključem povezuje sa ovim blokom.
5. Transakcije se ponovno potvrđuju svaki put kada se stvori novi blok. U Bitcoin mreži obično je potrebno šest potvrda kako bi se transakcija smatrala konačnom.

Kako bi rudar dobio proviziju za provjeru transakcija bitcoina, potrebno je ispuniti dva uvjeta. Prvi je da verificira vrijednost transakcija od 1 MB, a drugi uvjet je da kalkulacijom prvi dođe do kôda koji je jednak ciljnom kôdu. To radi na način da pogađa moguće kôdove/odgovore, a to može zahtijevati ogromne količine računalne snage. Ta snaga se mjeri u jedinicama pod nazivom „*hashes per second*“, odnosno H/s. [1][12]

3.2.4. *Hash* funkcija

Hash predstavlja matematičku funkciju koja pretvara uneseni podatak u šifrirani oblik. Bez obzira na veličinu originalnog podatka, *hash* kôd uvijek ima fiksnu veličinu i duljinu. Primjerice, Bitcoin koristi SHA-256 *hash* algoritam za generiranje slučajnih kôdova, koji generira jedinstveni 256-bitni kriptirani zapis određenog podatka, koji se pohranjuje unutar bloka. Također, u blok se dodaje i broj koji se naziva *Nonce* (*number*

only used once, broj korišten samo jednom), a predstavlja prvi broj koji rudari pokušavaju pronaći, kako bi zauzvrat dobili određeni iznos kriptovalute (provizije). Taj proces zahtjeva dovoljno računalne snage, kako bi se matematički algoritmi lakše savladali. Na slici 3. je prikazan generirani *hash* kôd za dvije poruke uz pomoć SHA-256 algoritma, gdje je vidljiva razlika u generiranom nizu znakova. [1][42]



Slika 3. Primjer šifriranja poruka korištenjem SHA-256 *hash* algoritma, [43]

Bitna značajka ovog kôda je da je nemoguće rekonstruirati izvornu informaciju iz njega, zato jer on funkcionira samo u „jednom smjeru“ i služi samo za kriptiranje originalnog podatka. Ipak, ako se ta funkcija koristi na identičnom podatku, *hash* će biti isti, pa se uz pomoć *hasha* može provjeriti da li je kriptirani podatak isti. *Hash* funkcije su strukture podataka u računalnim sustavima često korištene za bitne zadatke, kao što su provjera integriteta poruka i provjera autentičnosti informacija. Kriptografske *hash* funkcije dodaju sigurnosne značajke tipičnim *hash* funkcijama, otežavajući otkrivanje sadržaja poruke ili podataka. Zaključno, *hash* funkcije predstavljaju vrlo bitan proces kod blockchain tehnologije i provjeravanja transakcija, a za njihovu kalkulaciju zaduženi su rudari. [1][42]

3.3. Vrste blockchaina

Najosnovnija potreba ili primjena blockchaina je obavljanje transakcija ili razmjena informacija putem sigurne mreže. No, način na koji ljudi koriste blockchain ili mrežu razlikuje se od slučaja do slučaja. Pretpostavimo da banka koristi privatnu blockchain mrežu. To će biti ograničena mreža u kojoj samo ovlašteni članovi banke mogu pristupiti povjerljivim podacima. Dakle, nitko iz ove zatvorene mreže ne može dobiti pristup bankovnim podacima. Privatna mreža imat će ograničene i ovlaštene čvorove koje će nadzirati mrežni administrator. Informacije prenesene putem takve privatne blockchain mreže ostaju unutar mreže. Baš kao i ovaj primjer, postoje različiti načini uspostavljanja blockchain mreže ovisno o upotrebi i zahtjevima. Postoje prvenstveno dvije vrste blockchaina, a to su privatni i javni blockchain. Međutim, postoji i nekoliko varijacija, poput konzorcijskih i hibridnih blockchaina. [14][40]

3.3.1. Javni blockchain

Kao što naziv govori, javne blockchain mreže nisu u vlasništvu nikoga. Javni blockchain je distribuirani sustav bez potreba za dozvolama. Svatko tko ima pristup internetu može se prijaviti na blockchain platformu kako bi postao ovlašteni čvor i postao dio blockchain mreže. Čvor ili korisnik koji je dio javnog blockchaina ovlašten je pristupiti tekućim i prošlim zapisima, provjeriti transakcije ili izvršiti *Proof of work* za blokove, te rudariti. Korisnici mogu, ali i ne moraju biti nagrađeni za svoje sudjelovanje. Najosnovnija upotreba javnih blockchaina je za rudarenje i razmjenu kriptovaluta. Javni blockchain je uglavnom siguran ako se korisnici strogo pridržavaju sigurnosnih pravila i metoda. Međutim, riskantno je samo ako sudionici ne slijede sigurnosne protokole. [14]

Jedna od prednosti javnih blockchaina je ta što su potpuno neovisni o organizacijama, pa ako organizacija koja ih je pokrenula prestane postojati, javni će blockchain i dalje moći raditi, sve dok postoje povezana računala na taj blockchain. Nedostatak javnih blockchaina je taj što mreža može biti spora, a tvrtke ne mogu ograničiti pristup ili upotrebu. Također, ako hakeri dobiju većinsku kontrolu nad javnom blockchain mrežom, mogu je promijeniti. Najčešći slučaj korištenja javnih blockchaina je rudarenje i razmjena kriptovaluta poput Bitcoina. Međutim, može se koristiti i za stvaranje fiksne

evidencije poput javne evidencije vlasništva nad nekretninom. Ova vrsta blockchaina idealna je za organizacije izgrađene na transparentnosti i povjerenju, poput grupa za društvenu podršku ili nevladinih organizacija. Zbog javne prirode mreže, privatna poduzeća vjerojatno će izbjeći javni blockchain. [15]

3.3.2. Privatni blockchain

Privatni blockchain je restriktivni blockchain operativan samo u zatvorenoj mreži. Privatni blockchaini obično se koriste unutar organizacije ili poduzeća, gdje su samo odabrani članovi sudionici blockchain mreže. Razina sigurnosti, ovlaštenja, dopuštenja i pristupačnosti u rukama je organizacije koja ga kontrolira. Stoga je privatni blockchain sličan po upotrebi kao javni blockchain, ali ima malu i restriktivnu mrežu. Privatne blockchain mreže koriste se za glasovanje, upravljanje lancem opskrbe, digitalni identitet, vlasništvo nad imovinom i slično. [14]

Prednost korištenja ovog tipa je u tome što organizacija postavlja razine dopuštenja, sigurnost, ovlaštenja i pristupačnost. Na primjer, organizacija koja postavlja privatnu blockchain mrežu može odrediti koji čvorovi mogu pregledavati, dodavati ili mijenjati podatke. Također može spriječiti trećim stranama pristup određenim podacima. Budući da su ograničene veličine, privatni blockchaini mogu biti vrlo brzi i mogu obrađivati transakcije mnogo brže od javnih blockchaina. Nedostaci privatnih blockchaina uključuju tvrdnju da nisu pravi oblik blockchaina, budući da je temeljna filozofija blockchaina decentralizacija. Također je teže u potpunosti postići povjerenje u informacije, budući da centralizirani čvorovi određuju što je valjano. Mali broj čvorova unutar mreže može značiti manju sigurnost, a ako se nekoliko čvorova pokvari, mreža može biti ugrožena. [15]

3.3.3. Hibridni blockchain

Hibridni blockchain je kombinacija privatnog i javnog blockchaina. Koristi značajke obje vrste blockchaina, odnosno može imati privatni sustav temeljen na restrikcijama, kao i javni sustav bez dopuštenja. S takvom hibridnom mrežom korisnici mogu kontrolirati tko će pristupiti kojim podacima pohranjenim u blockchainu. Samo odabrani dio podataka ili zapisa iz blockchaina može biti dopušten da postane javan, a ostatak ostaje povjerljiv u

privatnoj mreži. Transakcija u privatnoj mreži hibridnog blockchaina obično se provjerava unutar te mreže. No korisnici ga mogu objaviti i u javnom blockchainu radi provjere. Javni blockchaini povećavaju *hash* stopu i uključuju više čvorova za provjeru. Time se povećava sigurnost i transparentnost blockchain mreže. [14]

Budući da radi u zatvorenom ekosustavu, jedna od velikih prednosti hibridnog blockchaina je ta što hakeri ne mogu dobiti kontrolu nad mrežom. Također štiti privatnost, ali omogućuje i komunikaciju s trećim stranama. Transakcije su jeftine i brze te nude bolju skalabilnost od javne blockchain mreže. Tvrtke mogu koristiti hibridni blockchain za privatno upravljanje sustavima, ali javnosti pokazuju određene podatke. Maloprodaja isto tako može pojednostaviti svoje procese pomoću hibridnog blockchaina, a visoko regulirana tržišta poput financijskih usluga mogu vidjeti koristi od njegove upotrebe. Također, vlade bi ga mogle koristiti i za privatno pohranjivanje podataka o građanima, ali sigurno dijeliti podatke između institucija. [15]

3.3.4. Konzorcijski blockchain

Konzorcijski blockchain je polu-decentralizirani tip u kojem više od jedne organizacije upravlja blockchain mrežom. To je suprotno onome što je slučaj kod privatnog blockchaina, kojim upravlja samo jedna organizacija. U ovoj vrsti blockchaina više organizacija može djelovati kao čvor i razmjenjivati informacije ili rudariti. Konzorcijski blockchain teži biti sigurniji, skalabilniji i učinkovitiji od javne blockchain mreže. Poput privatnog i hibridnog blockchaina, nudi i kontrolu pristupa. No konzorcijski blockchain manje je transparentan od javnog blockchaina. Bankarstvo i plaćanja dva su načina korištenja ove vrste blockchaina. Različite se banke mogu udružiti i formirati konzorcij, odlučujući koji će čvorovi potvrđivati transakcije. Također, istraživačke organizacije mogu stvoriti sličan model, kao i organizacije koje žele pratiti proizvode, a idealan je za lance opskrbe, osobito za hranu i lijekove. [14][15]

3.4. Mehanizam konsenzusa

Konsenzus je okosnica blockchaina i kao rezultat toga omogućuje decentralizaciju putem procesa rudarenja. On predstavlja proces dogovora između čvorova kako bi stekli povjerenje jedan u drugoga. Mehanizam konsenzusa je skup koraka koje poduzima većina ili svi čvorovi u blockchainu kako bi se dogovorili o predloženom stanju ili vrijednosti. Izborom algoritma konsenzusa definira vrsta blockchaina koja se koristi, odnosno nisu svi algoritmi konsenzusa prikladni za sve vrste blockchaina. Stoga je važno odabrati odgovarajući mehanizam konsenzusa za određeni blockchain. Da bi se postigao konsenzus, koriste se različiti algoritmi. Postići dogovor između dva čvora je lako (npr. u sustavima klijent-poslužitelj), ali kada u distribuiranom sustavu sudjeluje više čvorova i moraju se dogovoriti, postaje veliki izazov postići konsenzus. Svi mehanizmi konsenzusa razvijeni su za rješavanje grešaka u distribuiranom sustavu i za omogućavanje postizanja konačnog dogovora. Postoje različite vrste algoritama mehanizma konsenzusa, od kojih svaki radi po različitim načelima, a dva najosnovnija su „*Proof of Work*“ i „*Proof of Stake*“. [1][40]

3.4.1. *Proof of Work* algoritam

Proof of Work (PoW) ili dokaz o radu je algoritam koji omogućava postojanje mnogih kriptovaluta, uključujući Bitcoin i Ethereum. PoW je potreban kako bi digitalna valuta funkcionirala bez da tvrtka ili vlada imaju kontrolu nad njima. PoW rješava „problem dvostruke potrošnje“, što je teže riješiti bez kontrole. Ako korisnici mogu dvostruko potrošiti svoju imovinu, to čini valutu nepredvidivom i bezvrijednom. Dvostruka potrošnja je problem kod internet transakcija jer se digitalne radnje vrlo lako repliciraju, što čini kriptovalutu nepredvidivom i bezvrijednom. [16]

Uzevši Bitcoinov blockchain za primjer, on je zajednički zapis koji sadrži povijest svake Bitcoin transakcije koja se ikada dogodila. PoW je dio dodavanja novih blokova u Bitcoin blockchain, koje stvaraju rudari. Mreža prihvaća novi blok svaki put kada rudar dođe do novog PoW podatka, što se događa otprilike svakih 10 minuta. PoW je podatak koji je teško generirati, ali ga je drugima lako provjeriti, te zadovoljava određene zahtjeve. Izrada PoW može biti slučajan proces s malom vjerojatnošću, tako da je u prosjeku

potrebno mnogo pokušaja i pogrešaka prije nego što se generira valjani PoW. Bitcoin koristi sustav dokaza rada pod nazivom „*Hashcash*“. [16][17]

3.4.2. *Proof of Stake* algoritam

Proof of Stake (PoS) ili dokaz o udjelu je predložena alternativa *Proof of Work* algoritmu. Poput PoW, PoS pokušava postići konsenzus i sprječavanje dvostruke potrošnje. Ovaj algoritam radi na ideji da čvor ili korisnik ima odgovarajući udio u sustavu, odnosno korisnik je dovoljno uložio u sustav kako bi svaki zlonamjerni pokušaj tog korisnika nadmašio prednosti izvođenja takvog napada na mreži. To znači da korisnici zalaganjem svojih tokena dobivaju veće ovlasti u sustavu, i dokazuju svoju legitimnost. Još jedan važan koncept u PoS -u je dob valute, što je kriterij izveden iz količine vremena i broja tokena koji nisu potrošeni. U ovom modelu šanse za predlaganje i potpisivanje sljedećeg bloka povećavaju se sa starosti tokena. [1]

3.5. Kriptografske metode

Riječ „kripto“ doslovno znači skriveno ili tajno, a „kriptografija“ znači tajno pisanje, odnosno mogućnost razmjene poruka u takvom obliku u kojem ih može pročitati samo primatelj. Ovisno o konfiguraciji, kriptografska tehnologija može osigurati potpunu anonimnost. Kod kriptovaluta, kriptografija jamči sigurnost transakcija i sudionika, neovisnost poslovanja od središnjeg tijela i zaštitu od dvostruke potrošnje. Tehnologija kriptografije koristi se u više svrha poput osiguranja različitih transakcija koje se događaju na mreži, za kontrolu stvaranja novih valutnih jedinica i za provjeru prijenosa digitalne imovine i tokena. [18]

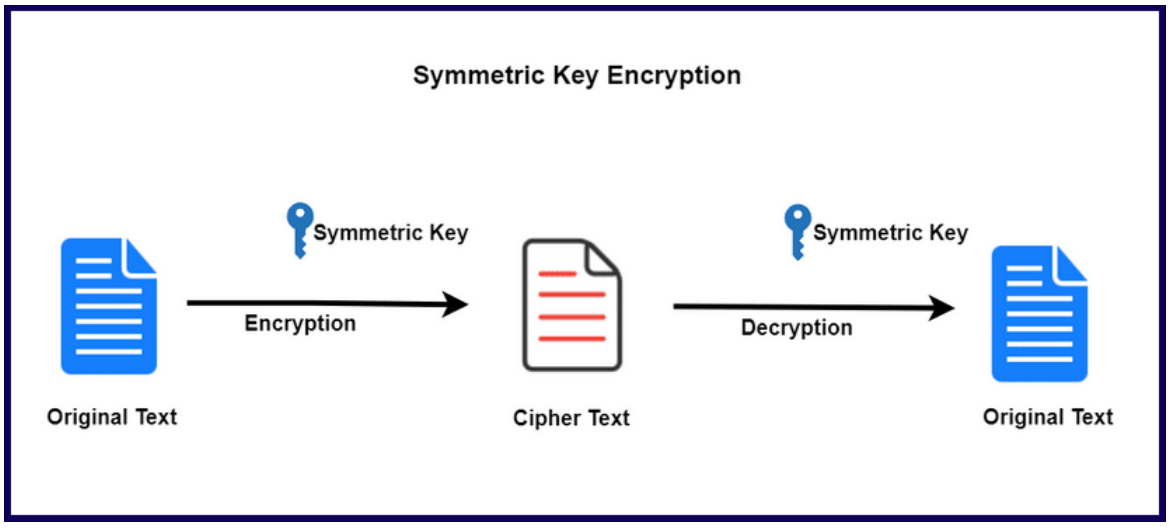
Kriptovalute oponašaju koncept potpisa u stvarnom svijetu pomoću tehnika kriptografije i ključeva za šifriranje. Metode kriptografije koriste napredne matematičke kôdove za pohranu i prijenos vrijednih podataka u sigurnom formatu koji osigurava da samo oni kojima su podaci ili transakcije namijenjeni mogu primati, čitati i obrađivati podatke te osigurati autentičnost transakcije i sudionika, poput potpisa u stvarnom svijetu. Na temelju toga može se zaključiti da je kriptografija tehnika slanja sigurnih poruka između dva ili više sudionika na način da pošiljatelj šifrira poruku pomoću algoritma za šifriranje,

šalje šifrirani oblik poruke primatelju, a primatelj ju dešifrira kako bi generirao izvornu poruku. Ključevi za šifriranje ili enkripcijski ključevi su najvažniji aspekt kriptografije. Oni čine poruku, transakciju ili vrijedne podatke nečitljivima za neovlaštenog čitatelja ili primatelja, a može ih pročitati i obraditi samo namjeravani primatelj. [18]

Mnoge kriptovalute poput Bitcoina ne koriste takve šifrirane poruke, jer je većina informacija koje uključuju Bitcoin transakcije u dobroj mjeri javna. Međutim, postoje i kriptovalute usmjerene na privatnost, poput ZCash-a i Monera, koje mogu koristiti enkripciju kako bi sakrile vrijednost i primatelja transakcije. Neki od alata koji su razvijeni kao dio kriptografije našli su važnu primjenu kod kriptovaluta. Oni uključuju *hash* funkcije i digitalne potpise, koji su sastavni dio obrade kod Bitcoina, makar Bitcoin izravno ne koristi skrivene poruke. [18]

3.5.1. Simetrična kriptografija

U sustavu koji koristi simetričnu kriptografiju pošiljatelj i primatelj koriste dvije instance istog ključa za šifriranje i dešifriranje podataka. Dakle, ključ ima dvostruku funkcionalnost, jer može izvesti i procese šifriranja i dešifriranja. [19]



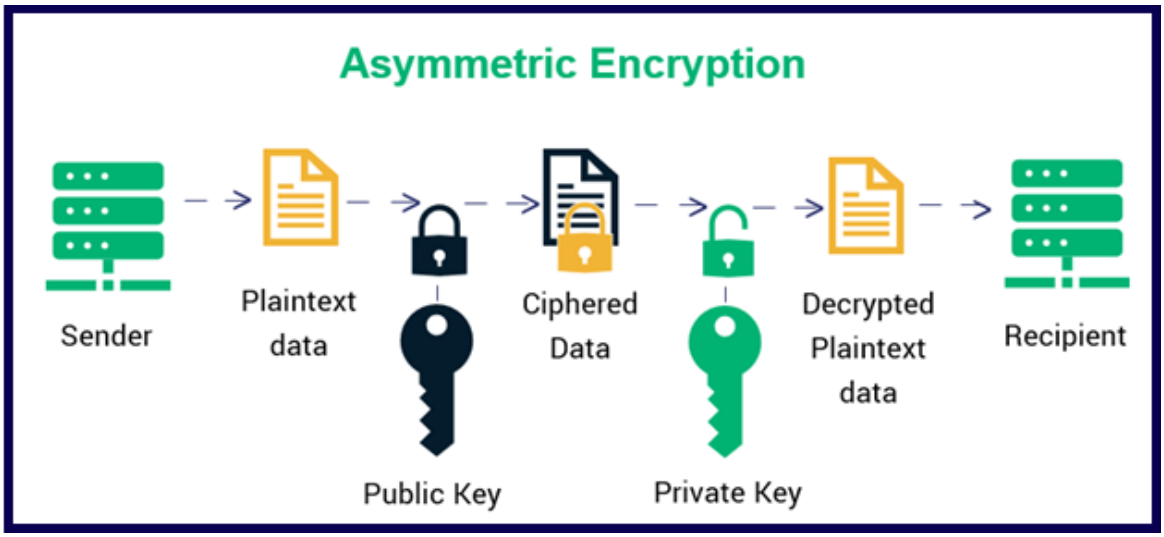
Slika 4. Enkripcija pomoću simetrične kriptografije, [19]

Na slici 4. je prikazan proces šifriranja i dešifriranja pomoću simetričnog ključa. Simetrični ključevi nazivaju se i tajnim ključevima jer se ova vrsta šifriranja oslanja na čuvanje ključa u tajnosti i na odgovarajuću razinu zaštite. Ako bi netko neautoriziran dobio ovaj ključ, mogao bi presresti i dešifrirati svaku poruku šifriranu sa njime. Svaki par korisnika koji žele razmjenjivati podatke pomoću šifriranja simetričnim ključem moraju imati dvije instance istog ključa, a to znači da ako žele komunicirati, obojica moraju nabaviti kopiju istog ključa. Stoga implementacija simetrične kriptografije može biti vrlo učinkovita jer ne postoji značajno vremensko kašnjenje kao rezultat šifriranja i dešifriranja. [19]

Simetrična kriptografija također pruža stupanj provjere autentičnosti jer se podaci šifrirani jednim simetričnim ključem ne mogu dešifrirati bilo kojim drugim simetričnim ključem. Stoga, sve dok dvije strane koriste simetrični ključ u tajnosti, koristeći ga za šifriranje komunikacije, svaka strana može biti sigurna da komunicira s drugom sve dok dešifrirane poruke imaju smisla. Glavni nedostatak šifri nastalih tajnim ključem je razmjena tajnog ključa, jer svaka razmjena mora zadržati privatnost ključa. To obično znači da tajni ključ mora biti šifriran drugim ključem, a primatelj mora već imati ključ koji će biti potreban za dešifriranje šifriranog tajnog ključa, a to može dovesti do neprestane ovisnosti o drugom ključu. [19]

3.5.2. Asimetrična kriptografija

Asimetrična kriptografija odnosi se na vrstu kriptografije u kojoj se ključ koji se koristi za šifriranje podataka razlikuje od ključa koji se koristi za dešifriranje podataka. To je također poznato kao kriptografija s javnim ključem. Koristi i javne i privatne ključeve za šifriranje i dešifriranje podataka. [1]



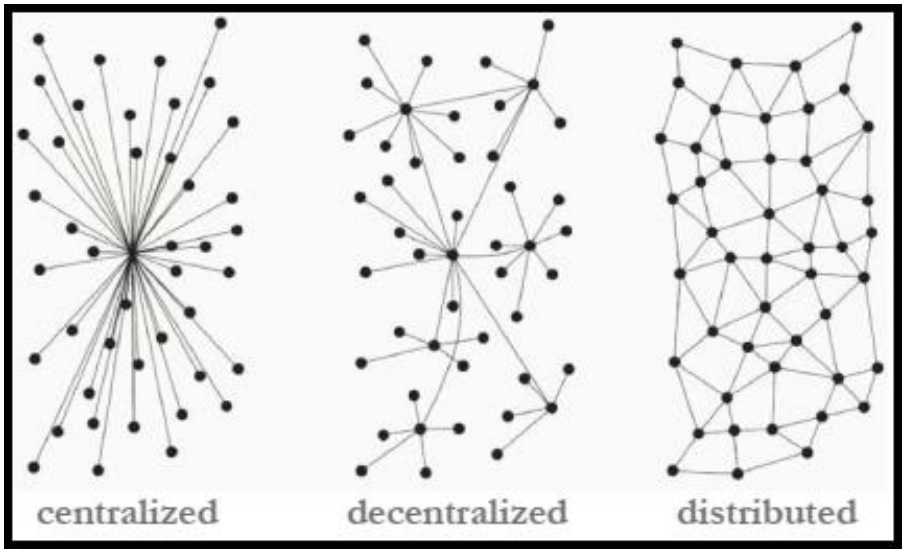
Slika 5. Enkripcija pomoću asimetrične kriptografije, [18]

Na slici 5. je prikazan proces šifriranja pomoću javnog ključa, i dešifriranja pomoću privatnog ključa. Javni ključ može se prikazati otvoreno, poput adrese primatelja sredstava, dok je privatni ključ poznat samo vlasniku. U ovoj metodi osoba može šifrirati poruku pomoću javnog ključa primatelja, ali je može dešifrirati samo primateljevim privatnim ključem. Ova metoda pomaže u postizanju dviju važnih funkcija autentifikacije i šifriranja kod transakcija kriptovaluta. Prva se postiže tako što javni ključ provjerava integritet uparenog privatnog ključa za pošiljatelja poruke, dok je drugi postignut tako što samo vlasnik uparenog privatnog ključa može uspješno dešifrirati šifriranu poruku. [18]

Asimetrična kriptografija predstavlja sporiji proces za razliku od simetrične kriptografije. Zato se obično ne koristi u šifriranju velikih datoteka ili stvarnih podataka koji zahtijevaju šifriranje. Obično se koristi za razmjenu ključeva za simetrično kriptiranje. Nakon što su javni i privatni ključevi sigurnosno uspostavljeni, mogu se koristiti simetrični ključevi za šifriranje samih podataka. [18]

3.6. Decentralizacija

Decentralizacija je ključna usluga koju pruža blockchain tehnologija. Po dizajnu, blockchain je idealna tehnologija za pružanje platforme za koju nisu potrebni posrednici i koja može funkcionirati pomoću mehanizama konsenzusa. Ovaj model omogućuje svakome da se natječe da postane ovlašten za donošenje odluka. Ovim natjecanjem upravlja se mehanizmom konsenzusa, a najčešće korišteni algoritam koji se koristi je PoW. Decentralizacija se primjenjuje u različitim izvedbama, od polu-decentraliziranog modela, pa do potpuno decentraliziranog, ovisno o zahtjevima i okolnostima. Osnovna ideja decentralizacije putem blockchaina se može promatrati kao savršen mehanizam koji pruža način za oblikovanje postojećih ili za izgradnju novih aplikacija i sustava, kako bi korisnicima dali potpunu kontrolu. [1]



Slika 6. Vrste mrežnih sustava, [1]

Slika 6. prikazuje različite vrste sustava koji trenutno postoje: središnji, decentralizirani i distribuirani. Centralizirani sustavi su konvencionalni (klijent-poslužitelj) sustavi u kojima postoji jedno centralno tijelo koje ga kontrolira i odgovara za sve operacije u sustavu. Svi korisnici centraliziranog sustava ovise o jednom izvoru usluge. Većina davatelja internetskih usluga, uključujući Google, Amazon, eBay i drugi koriste ovaj konvencionalni model za pružanje usluga. [1]

Kao što je već navedeno, distribuirani sustav predstavlja sustav kod kojeg su podaci i proračunavanje prošireni na više čvorova u mreži, ali i dalje pod kontrolom centralnog tijela. [1]

S druge strane, decentralizirani sustav je vrsta mreže u kojoj čvorovi ne ovise o nekom glavnom čvoru, nego je kontrola raspoređena među svim čvorovima. Glavna razlika između decentraliziranog i distribuiranog sustava je ta što u distribuiranom sustavu obično još uvijek postoji središnje tijelo koje upravlja cijelim sustavom, dok u decentraliziranom sustavu nema takvog središnjeg tijela. [1]

Samim time, decentralizacija je predstavila bitnu inovaciju u obliku decentraliziranog konsenzusa, koji omogućuje korisnicima da postignu dogovor bez središnjeg tijela, posrednika, ili bilo kakve treće strane, a što se tiče kriptovaluta, one obično koriste kombinaciju decentraliziranog i distribuiranog sustava. Kod postizanja decentralizacije mogu se koristiti dvije metode: metoda disintermedijacije (engl. *disintermediation*) i metoda konkurencije. [1]

3.6.1. Metoda disintermedijacije

Disintermedijacija je proces izbacivanja posrednika. To može omogućiti potrošaču da kupuje izravno od prodavatelja, a ne preko posrednika. Strategija disintermedijacije ključna je za razvoj decentraliziranih kriptovaluta poput Bitcoina. Jedna je značajka ovih sustava da korisnici međusobno obavljaju transakcije izravnim putem, bez potrebe za bankom ili novčanim tijelom za potvrđivanje transakcija. [20]

Koncept disintermedijacije može se objasniti na primjeru slanja novca osobi u drugoj državi. U klasičnom slučaju, banka može obaviti taj proces uz određenu proviziju. U ovom slučaju ovisimo o banci, koja predstavlja centralnu bazu podataka sa potvrdom da smo obavili prijenos novca. Kod blockchain tehnologije, novac se šalje putem adrese koju nam daje primatelj sredstava, na način da se šalju direktno primatelju bez ikakve provizije. Tim putem se izbacuje potreba banke, te je tako postignuta decentralizacija putem metode disintermedijacije. [1]

3.6.2. Metoda konkurencije

U metodi koja uključuje konkurenciju, različiti pružatelji usluga međusobno se natječu kako bi bili odabrani za pružanje usluga od strane sustava. Na ovaj način se ne postiže potpuna decentralizacija, ali osigurava da posrednik nema monopol nad određenom uslugom. Iako nema potpune decentralizacije, moguće je izabrati posrednika po želji, odnosno na temelju njegove reputacije, recenzija, kvalitete usluge i ostalog. Na taj način se postiže okolina u kojoj se pružatelji usluge međusobno natječu da budu izabrani, što rezultira kvalitetnom ponudom usluga. Kod blockchain tehnologije, ovim slobodnim izborom na temelju raznih kriterija može upravljati pametni ugovor. [1]

Iako potpuna decentralizacija ima mnogo prednosti nad centraliziranim sustavom, pojavljuju se izazovi poput sigurnosti, programskih i ljudskih grešaka. Decentralizirani sustav poput Bitcoina osiguran je korištenjem ključeva, ali ne postoji osiguranje od činjenice da se može pojaviti programska greška u sustavu, što može dovesti do gubitka ključa ili otkrivanja ranjivosti od strane napadača. Zbog toga, izbor provjerenog posrednika koji će brinuti o sigurnosti sustava može biti jedna od korisnih opcija. [1]

4. Pametni ugovori

Pametni ugovor je decentralizirani program. Pametni ugovori ne moraju nužno koristiti blockchain za pokretanje, ali zbog sigurnosnih prednosti koje blockchain tehnologija pruža, blockchain je postao standardna decentralizirana platforma za izvršavanje pametnih ugovora. Pametni ugovor obično sadrži poslovnu logiku i ograničenu količinu podataka, a poslovna logika se izvršava ako su ispunjeni određeni kriteriji poput, primjerice, jednostavne *if-then* petlje. Sudionici blockchain mreže koriste pametne ugovore ili se oni samostalno izvršavaju u ime sudionika mreže. [1]

Pametni ugovori je program napisan u blockchainu, i predstavlja digitalni dokument koji se sam izvršava, a uvjeti ugovora između kupca i prodavatelja izravno su zapisani u retke kôda. Kôd i sporazumi sadržani u ugovoru nalaze se u decentraliziranoj blockchain mreži. Kôd kontrolira izvršavanje, a transakcije se mogu pratiti i nepovratne su. Pametni ugovori dopuštaju izvršavanje pouzdanih transakcija i sporazuma između različitih anonimnih strana bez potrebe za središnjim tijelom, pravnim sustavom ili nekim vanjskim mehanizmom provedbe. [21]

Koncept pametnih ugovora nije nov, ali s pojavom blockchain tehnologije, interes za ovu ideju je oživio, te su pametni ugovori postali aktivno područje istraživanja u sklopu blockchaina. Zbog prednosti uštede koju pametni ugovori mogu donijeti u području financijskih usluga smanjenjem troškova transakcija i pojednostavljivanja složenih ugovora, provode se različita istraživanja od strane trgovačkih i akademskih institucija kako bi se formalizirala i olakšala provedba pametnih ugovora. [1]

4.1. Povijesni razvoj pametnih ugovora

Koncept pametnih ugovora opisao je američki kriptograf i programer Nick Szabo 1996. godine, mnogo prije pojave blockchain tehnologije. Prema Szabovoj koncepciji, pametni ugovori su digitalni protokoli za prijenos informacija koji koriste matematičke algoritme za automatsko izvršavanje transakcije nakon što su ispunjeni utvrđeni uvjeti. Ova definicija, koja je bila prikaz tehnologije ispred svog vremena za više od deset godina, ostaje točna do danas. Međutim, 1996. godine ova koncepcija nije se mogla ostvariti zato

jer u to vrijeme nisu postojale potrebne tehnologije poput blockchaina. 2009. godine pojavio Bitcoin kao prva kriptovaluta, nastala na temelju revolucionarne tehnologije blockchaina, koja je poslužila kao poticaj za razvoj pametnih ugovora. Pet godina kasnije, blockchain platforma Ethereum omogućila je korištenje pametnih ugovora u praksi. Danas tržište nudi mnoge platforme koje omogućuju upotrebu pametnih ugovora, ali Ethereum ostaje kao jedna od najraširenijih. [23]

4.2. Princip rada pametnih ugovora

Pametni ugovor je izraz koji se koristi za opisivanje računalnog kôda koji automatski izvršava cijeli ili dio ugovora i pohranjen je na platformi zasnovanoj na blockchainu. Taj kôd može predstavljati dogovor između stranaka ili može nadopuniti tradicionalni ugovor i izvršiti određene odredbe, poput prijenosa sredstava od stranke A do stranke B. Sam kôd je repliciran kroz veliku količinu čvorova blockchain mreže, te time iskorištava sigurnosne prednosti koje nudi blockchain tehnologija. Ako su prilikom izvršavanja transakcije parametri ugovora ispunjeni, kôd će izvršiti potrebne korake koje su pokrenuli ti parametri. U drugom slučaju, kôd neće poduzeti nikakve korake. [22]

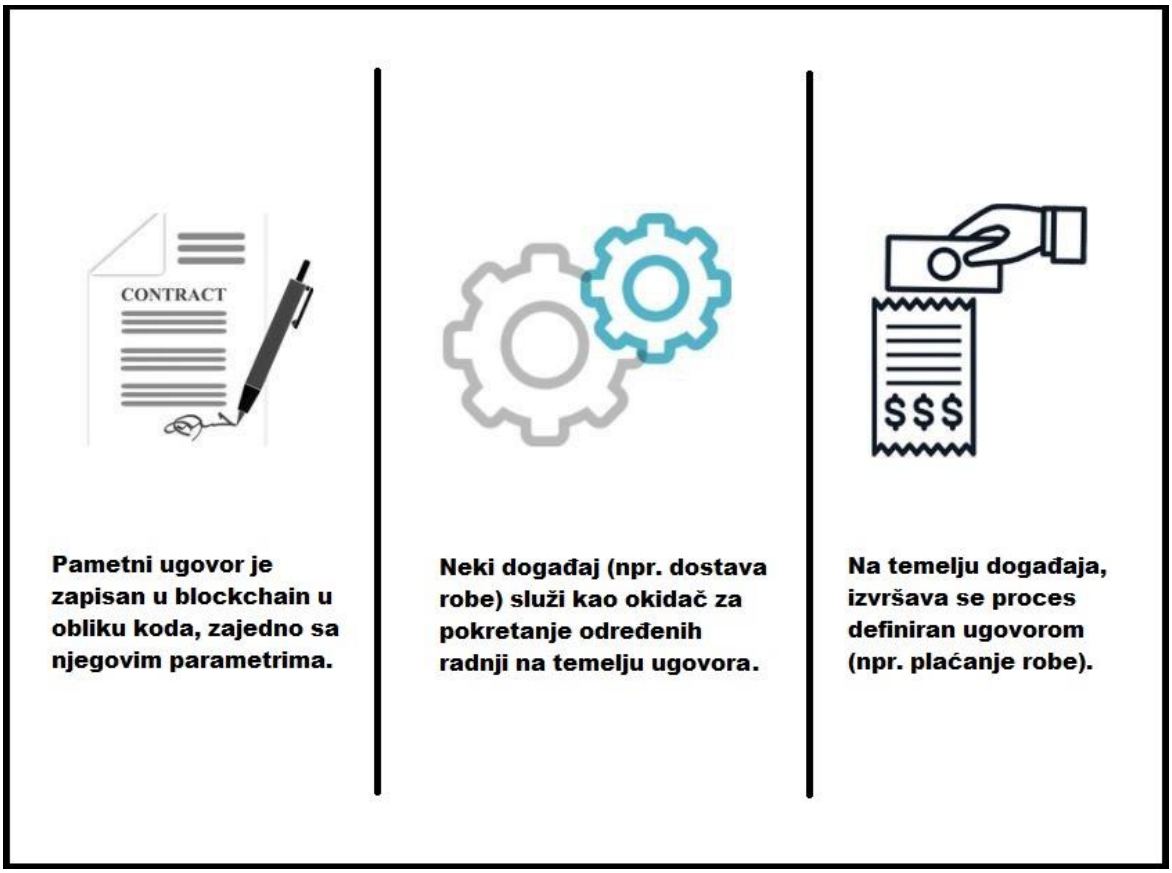
Ulazni parametri i koraci izvršavanja pametnog ugovora moraju biti specifični i objektivni. Drugim riječima, ako na temelju parametara dođe do događaja „x“, izvrši korak „y“. Stoga su stvarni zadaci koje obavljaju pametni ugovori prilično osnovni, poput automatskog premještanja određene količine kriptovalute iz novčanika jedne stranke u novčanik druge kada su zadovoljeni određeni kriteriji. Kako se blockchain tehnologija širi, pametni ugovori postaju sve složeniji i sposobniji za rukovanje sofisticiranim transakcijama, no put prema gotovo savršenom mehanizmu je još dugačak. [22]

Prije nego što se sastavljeni pametni ugovor doista može izvršiti na određenoj blockchain mreži, potreban je dodatni korak u obliku plaćanja naknade za transakciju, kako bi se ugovor dodao u lanac i izvršio. Što je pametni ugovor složeniji (na temelju koraka transakcije koje treba izvesti), to se više naknade mora platiti za izvršenje pametnog ugovora. Dakle, naknada trenutno djeluje kao važan alat za sprječavanje pretjerano složenih ili brojnih pametnih ugovora, kako ne bi preopteretili blockchain

platformu. Pametni ugovori trenutno su najprikladniji za automatsko izvršavanje dviju vrsti transakcija koje se nalaze u mnogim ugovorima:

1. osiguravanje plaćanja sredstava nakon određenih pokretačkih događaja
2. izricanje novčanih kazni ako neki objektivni uvjeti nisu ispunjeni

U svakom slučaju, nakon što je pametni ugovor implementiran i operativan ljudska intervencija nije potrebna, čime se smanjuju troškovi izvršenja i provedbe procesa ugovaranja. [22]



Slika 7. Princip izvršavanja pametnog ugovora, [41]

Slika 7. prikazuje proces izvršavanja pametnog ugovora na primjeru dostave robe. Kao što je vidljivo na slici, prvi korak je implementacija koda u blockchain mrežu i definiranje samog ugovora po dogovoru stranki. Drugi korak predstavlja pokretanje nekog događaja koji je detektiran od strane pametnog ugovora, primjerice, dostava robe do

primatelja. Treći korak predstavlja poduzimanje određenih postupaka nakon detekcije događaja, odnosno izvršenje procesa definiranih ugovorom, poput plaćanja robe. [41]

4.3. Platforme za kreiranje pametnih ugovora

Od pojave blockchain tehnologije, organizacije kontinuirano istražuju aplikacije za pametne ugovore i njihov potencijal za izgradnju decentraliziranih aplikacija (dApps). S obzirom na to, pametni ugovori mogu pojednostaviti poslovanje u mnogim industrijama koje se oslanjaju na ugovorne odnose. Danas postoje razne metode i platforme koje se koriste za izradu pametnih ugovora, a trenutno tri aktualne su: Ethereum, EOS.IO i Cardano, koji je u procesu objave. [1]

4.3.1. Ethereum Virtual Machine (EVM)

Vitalik Buterin je u studenom 2013. godine predstavio koncept pod nazivom Ethereum. Glavna ideja Ethereuma bila je razvoj Turingovog jezika koji dopušta razvoj pametnih ugovora za blockchain i decentralizirane aplikacije. Ovaj koncept je u suprotnosti s Bitcoinom, gdje je programski jezik ograničen i dopušta samo potrebne operacije. Ethereum Virtual Machine (EVM) je jednostavan virtualni stroj koji se bazira na programskom jeziku Solidity. EVM je potpuno izolirano i zaštićeno okruženje za izvođenje. Kôd koji radi na EVM-u nema pristup nikakvim vanjskim resursima, poput mreže ili datotečnih sustava. To rezultira povećanom sigurnošću i ne dopušta da se nepouzdani kôd pokreće na Ethereum blockchainu. [1]

Pametni ugovori u Ethereum mreži imaju ulogu računa. To znači da imaju ravnotežu i da mogu slati transakcije putem mreže. No korisnik ih ne kontrolira, umjesto toga raspoređeni su na mrežu i izvode se programski. Korisnički računi tada mogu komunicirati s pametnim ugovorom podnošenjem transakcija koje izvršavaju funkciju definiranu u pametnom ugovoru. Pametni ugovori mogu definirati pravila poput klasičnog ugovora, i automatski ih primijeniti putem kôda. Pametni ugovori ne mogu se izbrisati prema zadanim postavkama, a interakcije s njima su nepovratne. [24]

Kako bi se pametni ugovor mogao izvršiti, potrebno je platiti određenu naknadu za uslugu izvršavanja. Naknada koja se koristi za izvršavanje procesa pametnog ugovora naziva se „*gas*“, a isplaćuje se u Ethereumovoj kriptovaluti (ETH). Točna vrijednost naknade određena je ponudom i potražnjom između rudara mreže, koji mogu odbiti obradu transakcije ako cijena naknade ne dosegne njihov prag, i korisnika mreže koji traže procesnu snagu. Pametni ugovori su javni na Ethereumu i mogu se smatrati otvorenim API-jima. To znači da je moguće pozvati druge pametne ugovore u vlastiti pametni ugovor kako bi proširili njegove mogućnosti. [24]

4.3.2. EOS.IO

EOS.IO ili EOS pruža decentraliziranu platformu sa karakteristikama operativnog sustava (OS), koja koristi blockchain za održavanje zapisa o događajima i transakcijama na ovoj platformi. EOS koristi PoS algoritam kao mehanizam konsenzusa, što omogućuje veće brzine transakcija zbog manje količine verifikacija. EOS omogućuje stvaranje pametnih ugovora čije se izvršavanje i potrošnja resursa obrađuju baš kao i tipična aplikacija koja radi na OS-u. Pametni ugovori napisani su u programskom jeziku C++ i pretvoreni u WebAssembly. [25]

Za razliku od Ethereum platforme, cilj EOS-a je omogućavanje kreiranja pametnih ugovora koji ne uzimaju naknadu za transakcije, čime potiče korištenje pametnih ugovora. Također, zbog svoje platforme koja funkcionira kao OS, pruža podršku za decentralizirane aplikacije (dApps). Bitno je napomenuti da trajne informacije pametnih ugovora nisu pohranjene u samom blockchainu. Blockchain se koristi samo za zapisivanje transakcija i drugih događaja koji su potaknuti promjenama informacija pametnih ugovora. [25]

4.3.3. Cardano

Cardano je blockchain platforma treće generacije s PoS mehanizmom, te predstavlja prvu platformu zasnovanu na recenziranim istraživanjima i razvijenu metodama utemeljenim na dokazima. Cardano platforma za pametne ugovore trenutno je u procesu objavljivanja, te bi trebala biti puštena u rad do kraja kolovoza 2021. godine.

Cardano kombinira pionirske tehnologije za pružanje visoke razine sigurnosti i održivosti decentraliziranim aplikacijama, sustavima i društvima. [26]

Cardano je osnovan od strane suosnivača Ethereuma Charlesa Hoskinsona, koji se protivio načinu rada Ethereumove platforme zbog velikih provizija na pametne ugovore. Tako je Hoskinson predstavio Cardano kao bolju alternativu koja razvija svoju platformu kroz recenzirana detaljna istraživanja. Njegov tim inženjera i akademika objavilo je više od 100 znanstvenih radova o temeljnoj tehnologiji koja nastoji riješiti skalabilnost i druga probleme njezinih prethodnika. Cardano obećava bolju verziju Ethereum pametnih ugovora, te predstavlja perspektivan projekt za sljedećih 4 godine, kako i sa vlastitom kriptovalutom (ADA), tako i sa cijelom platformom za razvoj raznih aplikacija (dApps). [26]

4.4. Primjena pametnih ugovora

Jedan od najvećih izazova s kojima se organizacije suočavaju je nedostatak povjerenja u suradnji s drugom strankom. Zbog nedostatka povjerenja i transparentnosti, organizacije djeluju oprezno i troše značajno vrijeme i novac na posrednike dok finaliziraju ugovore. Pametni ugovori to mogu poboljšati uklanjanjem posrednika u slučajevima kada se uvjeti ugovora mogu javno promatrati. Ovi ugovori grade povjerenje i transparentnost između dvije strane korištenjem blockchain tehnologije. Pametni ugovori su nova tehnologija koja može povećati učinkovitost u različitim industrijama. Kako tehnologija sazrijeva, očekuje se da će je sve više organizacija iskoristiti kako bi smanjile troškove i omogućile brze i sigurne transakcije. [27]

4.4.1. Upravljanje lancem opskrbe

Upravljanje lancem opskrbe predstavlja zahtjevan proces praćenja i protoka robe, te uključuje razne dodatne aktivnosti vezane za opskrbu. U mreži lanca opskrbe, nakon što proizvod stigne do konačnog odredišta, mijenja se njegov status vlasništva. Pametni ugovori omogućuju da svi koji sudjeluju u lancu opskrbe mogu pratiti sami proizvod kroz cijeli njegov eksploatacijski proces. To omogućuje lokacijsko praćenje proizvoda uz pomoć pametnih ugovora i IoT uređaja. Naprimjer, ako se neki od proizvoda izgubi tokom procesa, pametnim ugovorima se može doći do njegove lokacije. Također, za razne

prehrambene i neprehrambene proizvode postoji opcija provjere starosti, podrijetla, kakvoće i ostalih bitnih parametara koji mogu biti ključni za kupce. Još jedna od mogućnosti pametnih ugovora je automatizacija svih rutinskih zadataka i plaćanja organizacije, tako da ona ne mora voditi računa o velikoj količini klasične dokumentacije. [27]

4.4.2. Industrija osiguranja

Tradicionalno, industrija osiguranja oslanja se na pouzdanog posrednika za izvršavanje transakcije. Uključivanje treće strane čini proces sporijim i skupljim, a pametnim ugovorima moguće je riješiti taj problem ublažavanjem rizika manipulacije posrednika. S obzirom na to da su pametni ugovori pohranjeni na blockchainu, obje strane mogu vidjeti zabilježene transakcije. Pametni ugovori dramatično ubrzavaju obradu zahtjeva i tako snižavaju administrativne troškove za osiguravatelja. Posljedično tome, tvrtke mogu smanjiti premije i povećati tržišni udio. Bitna značajka primjene ugovora je ta da ni osiguratelj ni kupac ne mogu izgubiti podatke o ugovoru, jer su police sigurno pohranjene na blockchainu. [28]

4.4.3. Financijske usluge

Bankarske i financijske usluge koje primjenjuju pametne ugovore mogu povećati svoju učinkovitost i djelotvornost. Zajmovi koji se izdaju mogu se brže obraditi pomoću pametnih ugovora. S nekoliko subjekata uključenih u zajmove, uspostavljanje odnosa, identiteta i održavanje sigurnosti postaje daleko pojednostavljeno s informacijama pohranjenima u blockchainu. Također, organizacije mogu koristiti pametne ugovore za točno, transparentno bilježenje podataka uz poboljšanje brzine i sigurnosti. Pametni ugovor omogućuje jedinstveno čuvanje financijskih podataka u svim organizacijama čime se uklanja potreba za razmjenom drugih dokumenata. Samim time, pametni ugovori poboljšavaju financijsko izvještavanje i integritet podataka što podržava povećanu stabilnost tržišta. [27][29]

4.4.4. Poljoprivreda

Digitalna plaćanja, bilo integrirana u platforme e-trgovine ili u mobilno bankarstvo, smanjuju transakcijske troškove na poljoprivrednim tržištima. Potreba za sigurnim i brzim novčanim transakcijama osobito je očita u ruralnim područjima. Osim toga, digitalna plaćanja mogu omogućiti pristup bankovnim računima, osiguranju i kreditima. Korištenje tehnologije pametnih ugovora jedan je od načina za smanjenje transakcijskih troškova povezanih sa povjerenjem na komercijalnim tržištima. [30]

Mnoge maloprodajne i prehrambene tvrtke udružile su se s IBM-om u razvoju blockchaina i pametnih ugovora koji se odnose na sigurnost i praćenje hrane. Primjerice, kineska grupacija Alibaba testira blockchain kako bi smanjila prijevare u e-trgovini hranom između Kine i Australije. [30]

5. Mreža za trgovanje kriptovalutama

Rastuće tržište kriptovaluta privuklo je različite vrste sudionika. Najdominantniji su kripto trgovci i ulagači. Iako i trgovanje i ulaganje imaju isti krajnji cilj - zaraditi novac, postoji nekoliko temeljnih razlika među njima. Trgovanje uključuje kupnju ili prodaju kriptovaluta na kratak rok. Trgovanje se usredotočuje na maksimiziranje kratkoročnih dobitaka iskorištavanjem nestabilnosti i medijske buke. Trgovci često provode većinu vremena promatrajući obrasce grafikona i analizirajući trendove prije nego što odluče hoće li ići kratko ili dugo. Također, koriste razne vrste naloga kako bi im pomogli pri otvaranju i zatvaranju pozicija pod posebnim tržišnim uvjetima. [31]

Dok neki trgovci nastoje profitirati na tržištu iskorištavanjem kratkotrajne nestabilnosti, drugi kupuju kako bi držali imovinu duže. S time, samo ulaganje uključuje kupnju i držanje imovine na duži ili kraći rok. Ulaganje je usmjereno na širu sliku, a klasični ulagači nastoje zanemariti kratkoročne oscilacije cijena i koncentrirati se na temeljnu kvalitetu imovine. Primarni cilj tih ulagača je postići maksimalni mogući povrat ulaganja držanjem kriptovalute kao imovinu u najvećem mogućem trajanju. Kod takvog ulaganja se vjeruje da će se dugoročno gledano isplatiti. [31]

5.1. Servisi za trgovanje kriptovalutama

Prvi korak prema ogromnoj mreži trgovanja kriptovalutama je pronalaženje pouzdanog servisa za trgovanje kriptovalutama. Ti servisi su imali značajnu ulogu u popularizaciji kriptovaluta. To su postigli tako što su učinili proces otkrivanja cijena učinkovitijim i povećali transparentnost u kripto trgovanju. Zahvaljujući tim servisima, kriptovalute su nadmašile sva očekivanja na tržištu. Najjednostavnija definicija za te servise je da predstavljaju internet platformu na kojoj korisnici mogu kupiti kriptovalute koristeći fiat valute ili zamijeniti jednu kriptovalutu za drugu. Većina servisa također omogućuje trgovanje kriptovalutama s polugom, što znači da se korisnici mogu kladiti na kretanje cijena. Većina pouzdanih servisa omogućuju kupnju i prodaju kriptovaluta po želji uz niske naknade i jake sigurnosne značajke. [31]

Prilikom odabira najboljeg servisa, važno je pogledati podržane valute, cijene, mogućnosti povlačenja sredstava i sigurnost. Trenutno postoji mnogo različitih servisa za razmjenu, a jedni od najpopularnijih su Binance, Coinbase i Bisq. [31]

5.1.1. Binance

Binance je centralizirani servis za trgovanje kriptovalutama koji pruža platformu za kupnju, prodaju i razmjenu velike količine postojećih kriptovaluta. Osnovan je 2017. godine, a sjedište mu je na Kajmanskim otocima. Binance je trenutno najveći svjetski servis za trgovanje u smislu dnevnog obujma trgovanja. Osnovao ga je programer pod imenom Changpeng Zhao. Binance je u početku imao sjedište u Kini, ali je kasnije preselio svoje sjedište iz Kine zbog strogih kineskih regulacija u vezi kriptovaluta. Kasnije je osnovan Binance U.S., zbog obustave usluga američkim trgovcima. Binance U.S. prvenstveno služi američkim ulagačima, a podržava više od 50 kriptovaluta, te nudi mogućnosti ulaganja za pojedince i institucije. Binance nudi dvije opcije za korisnike, a to su Binance Pro i Binance Lite. Binance Pro je opcija koja je namijenjena za naprednije trgovce i nudi razne mogućnosti poput trgovanja na osnovu margina, spot-trgovanje, automatski kupi-prodaj i drugo. Binance Lite je osnovna verzija za početnike koja omogućuje kupnju i prodaju kriptovaluta, i usluge novčanika. [33]

Binance Coin (BNB) je kriptovaluta koju je izdao Binance, a temeljena je na Ethereum blockchainu. Pomoću ove kriptovalute moguće je platiti komisiju za transakcije na servisu. To za korisnike omogućuje dodatne popuste, kako bi promovirali svoj token. Za poticanje rasta cijene BNB tokena postoji politika tvrtke koja će tokene kupovati i uništiti. Programeri planiraju ostaviti samo 100 000 tokena, a ostatak će biti uništen u roku od nekoliko godina. Na temelju toga, vrijednost BNB valute će nastaviti rasti. [33]

5.1.2. Coinbase

Coinbase je Američka tvrtka osnovana 2012. godine od strane Briana Armstronga i Freda Ehrsama. Coinbase predstavlja centralizirani servis za trgovanje kriptovalutama koji nudi više od 50 kriptovaluta, uključujući Bitcoin, Ethereum, Litecoin, Dogecoin i Cardano. Servis također nudi više mogućnosti ulaganja za individualne i institucionalne

klijente. Neke od njegovih značajki uključuju nagrade za ulaganje, mobilnu aplikaciju, te opciju računa Coinbase Earn, koja korisnicima plaća za gledanje obrazovnih videozapisa u obliku kripto tokena. Coinbase pored normalnog načina trgovanja nudi i dvije dodatne mogućnosti za korisnike: Coinbase Pro za napredne trgovce i Coinbase Prime za institucije i klijente sa visokim prihodom (pojedinci s najmanje 1 milijun USD). Korisnici Coinbase Pro imaju pristup naprednijim značajkama poput sigurnih trgovačkih botova, alata za izradu grafikona i zapisa narudžbi u stvarnom vremenu. [32]

5.1.3. Bisq

Bisq je decentralizirana mreža koja omogućuje sigurni i privatni servis za razmjenu kriptovaluta putem interneta. Za razliku od navedenih centraliziranih servisa, Bisq predstavlja *peer-to-peer* mrežu za međusobnu interakciju i implementaciju Bisq protokola za trgovanje. Bisq je potpuno decentraliziran, pa ne zahtjeva poslužitelje s centralnim upravljanjem i nema niti jednu točku kvara. Ovaj servis je izgrađen na čistoj *peer-to-peer* infrastrukturi koju čine softver za računala, Tor, lokalni novčanici i izbacivanje središnjih korisničkih računa, a njezin model upravljanja potiče zaštitu privatnosti i slobodu korisnika. Dok prijenos fiat valuta zahtijeva tradicionalne načine plaćanja poput banaka, Bisq ne ovisi o nijednom davatelju usluga. Bisq je kreiran za one pojedince koji ne vjeruju bilo kakvim drugim posrednicima, i žele osobno čuvati svoju imovinu [34]

5.2. Novčanici za kriptovalute

Novčanik za kriptovalute predstavlja aplikaciju koja vlasnicima kriptovaluta omogućuje pohranu i preuzimanje digitalne imovine. Kao i kod fiat valuta, novčanik nije potreban za trošenje sredstava, ali je bitan alat za držanje svih sredstava na jednom mjestu. Jednostavno rečeno, kada korisnik kupi određenu količinu kriptovalute, može ju pohraniti u digitalni novčanik i odatle je koristiti za obavljanje transakcija. Novčanici za kriptovalute postoje u obliku aplikacija koje se mogu pokrenuti na pametnom telefonu ili računalu, a većina servisa za trgovanje kriptovalutama nude korisnicima usluge novčanika. No takav način može predstavljati sigurnosni propust, te su laka meta za

napadače. Zbog toga postoje razni novčanici u fizičkom obliku, koji posjeduju svojstva čuvanja digitalne imovine na zasebnom memorijskom uređaju. [35]

Prilikom kupovanja kriptovalute, bilo kupovinom na servisu ili primanjem kao prihod, pošiljatelj dobiva jedinstvenu kriptografsku adresu koju izdaje primateljev novčanik. Pošiljatelj unosi tu javnu adresu na vlasititi servis za slanje sredstava, te nakon toga transakcija ulazi u proces verifikacije na blockchain mreži. Nakon što je transakcija potvrđena na blockchainu, primatelj postaje vlasnik određene poslane kriptovalute. Nakon toga, primatelj može raspolagati sa pristiglim sredstvima po vlastitoj želji i slati ih dalje ili razmjenjivati za neku drugu valutu. [35]

5.3. CFD trgovanje kriptovalutama

Klasični način trgovanja je vrlo jednostavan. Jednostavno je moguće odabrati valutu po želji, i plati određenom fiat valutom preko nekog od servisa. No u suvremenom smislu, kratkoročno kripto trgovanje često podrazumijeva trgovanje kripto CFD-ovima. CFD (*Contract for Differences*) trgovanje kriptovalutama je vrsta kratkoročnog trgovanja koja ulagatelju omogućuje da nagađa smjer kretanja cijene kriptovaluta, a da zapravo ne posjeduje digitalnu imovinu. [31]

CFD-ovi također omogućuju trgovcima korištenje poluge. Poluga (margina) predstavlja kredit koji nudi posrednik, a pomaže povećati količinu dobiti tako što je moguće uložiti više sredstava. Na primjer, uzevši polugu koja množi uložena sredstva sa 100, kod uloga od 1000 kuna otvara se šansa za zaradu od 100.000 kuna. Bitno je imati na umu da se poluga može koristiti samo pri trgovanju, a to značajno povećava potencijalni profit. No prilikom odabiranja velikog množitelja, primjerice 100x, postoje veće šanse za gubljenje ukupnog uloženog iznosa, zato što je margina postavljena vrlo blizu trenutnoj vrijednosti kriptovalute. Padne li vrijednost u jednom trenutku ispod margine, gube se sva sredstva. [31]

Nakon odluke o ulogu i načinu ulaganja, bitno je odrediti kojom valutom je pametno trgovati. U naprednom trgovanju kriptovalutama trguje se u obliku valutnih parova, na primjer, BTC/ETH. Cijena valutnog para pokazuje koliko je kotacijske valute potrebno za

kupnju jedne jedinice osnovne valute. Primjerice, kod para BTC/ETH cijena je 1000 USD. To znači da je za kupnju jednog BTC-a potrebno 1000 USD. U ovom slučaju BTC predstavlja osnovnu, a ETH kotacijsku valutu. Trgovci često trguju na taj način s ciljem da cijena osnovne valute raste s duljim periodom vremena, odnosno da je osnovna valuta jača na vrijednosti. Obrnuto, kupovanje kotacijske valute radi se kod pretpostavke da će vrijednost osnovne padati. [31]

5.4. Bikovo tržište u 2021. godini

2021. godine je bilo najduže i najagresivnije tržište bikova za kriptovalute u povijesti. Bikovo tržište (engl. *Bull run*) je pojava kod koje cijene vrijednosnica značajno rastu. U razdoblju od siječnja 2021. do ožujka 2021. godine ukupna je tržišna kapitalizacija cijelog kripto tržišta porasla sa 771 milijardi na 1,5 bilijuna USD. No od siječnja 2020. godine ukupna tržišna kapitalizacija kriptovaluta porasla je sa 188 milijardi na povijesni vrhunac od 1,688 bilijuna USD u veljači 2021. Jedni od najvažnijih razloga tome su bili povećana potražnja za kriptovalutama, prepolovljavanje Bitcoina, rast kripto derivata i velika opća popularnost decentraliziranih financija. [31]

Tržišna kapitalizacija Bitcoina oduvijek je dominirala kripto tržištem, a zbog svoje dominacije, on ima značajan utjecaj na druge kriptovalute. Prepolovljavanje Bitcoina najlakše se može opisati kao ugrađeni antiinflacijski mehanizam unutar Bitcoin kôda. To znači da nakon miniranja određene količine Bitcoin blokova, nagrada (provizija) za rudarenje se prepolovljuje. To se događa nakon rudarenja 210.000 blokova, a to je otprilike svake četiri godine. Kada se nagrada prepolovi, to znači da se stopa po kojoj se na tržište dodaje više Bitcoina smanjuje, jer Bitcoin ima ograničenu ponudu. Kombiniranjem tih činjenica, cijena Bitcoina na tržištu raste. Bitcoin je doživio prepolovljavanje 2012. i 2016. godine, što je rezultiralo naglim porastom vrijednosti. Najnovije prepolovljavanje u 2020. godini rezultiralo je tržištem bikova, te je cijena BTC-a u 2021. godini skočila na gotovo 64.000 USD. Posljedično, Bitcoin je imao utjecaj na ostale kriptovalute, što je rezultiralo naglim porastom vrijednosti ostalih valuta. [31]

6. Stanje na tržištu

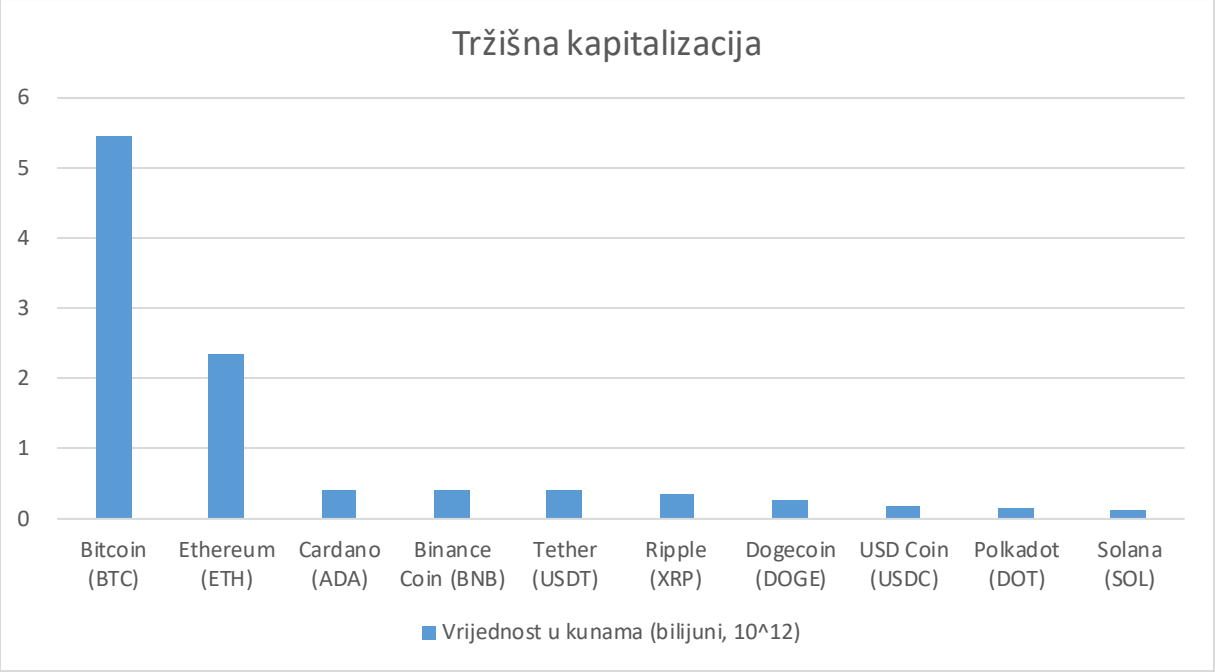
Bitcoin je po mnogima glavna kriptovaluta, ali tržište digitalnih valuta koje se oslanjaju na blockchain tehnologiju mnogo je veće od toga. Uzevši Ethereum za primjer, ETH je postala jedna od nekoliko kriptovaluta s najviše transakcija zapisanih na mreži do 2021. godine. To se odrazilo na cijenu Ethereuma, koja se gotovo udvostručila između prosinca 2020. i siječnja 2021. Bez obzira na to, Bitcoin je i dalje najtraženija kriptovaluta na internetu. No ostale značajne kriptovalute, kao što su Ethereum, Tether, Cardano i Dogecoin, također su zadobile puno pažnje od javnosti. [36]

6.1. Tržišna kapitalizacija kriptovaluta

Tržišna kapitalizacija predstavlja ukupnu tržišnu vrijednost kriptovaluta. Računa se na način da se pomnoži trenutna jedinična vrijednost kripto tokena sa ukupnim brojem tokena u opticaju. Važno je napomenuti da je tržišna kapitalizacija dinamična i mijenja se svake sekunde, a razlog tome je stalno povećanje ponude kriptovaluta na tržištu zbog procesa rudarenja. Tablica i grafikon 1. prikazuju deset kriptovaluti sa najvećom tržišnom kapitalizacijom na dan 17. kolovoza 2021. godine, te njihove jedinične cijene. [31][37]

Tablica 1. Deset kriptovaluti s najvećom tržišnom kapitalizacijom, Izvor: [37]

#	Naziv	Jedinična cijena	Tržišna kapitalizacija
1	Bitcoin (BTC)	290.700 kn	5.467.470.149.050 kn
2	Ethereum (ETH)	20.020 kn	2.356.500.660.580 kn
3	Cardano (ADA)	13 kn	417.471.410.828 kn
4	Binance Coin (BNB)	2.666 kn	410.900.903.554 kn
5	Tether (USDT)	6,36 kn	408.938.559.198 kn
6	Ripple (XRP)	7,39 kn	344.085.376.121 kn
7	Dogecoin (DOGE)	2 kn	263.610.295.280 kn
8	USD Coin (USDC)	6,37 kn	174.710.886.815 kn
9	Polkadot (DOT)	160,77 kn	163.667.178.718 kn
10	Solana (SOL)	418 kn	120.073.184.711 kn



Grafikon 1. Deset kriptovaluti s najvećom tržišnom kapitalizacijom, Izvor: [37]

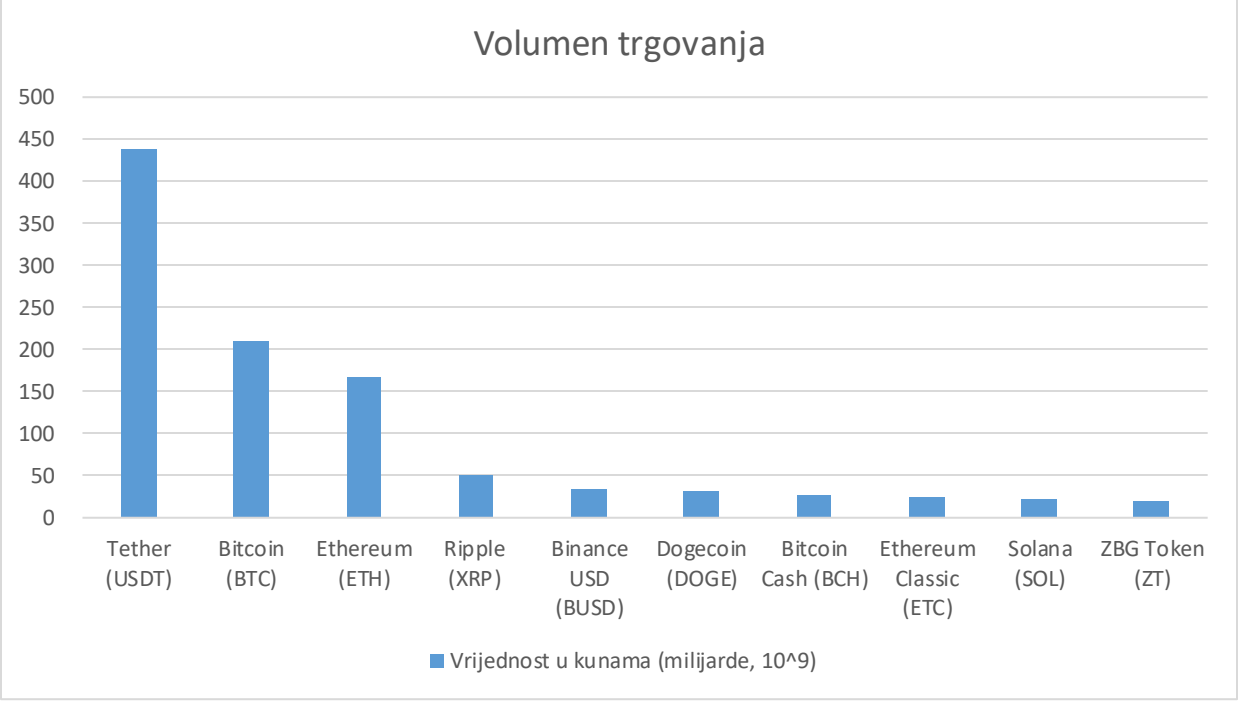
6.2. Volumen trgovanja kriptovalutama

Volumen trgovanja predstavlja ukupnu vrijednost kriptovalute kojom se trgovalo u prethodna 24 sata. Ova metrika je vrlo korisna zato jer pomaže utvrditi trenutnu popularnost među kriptovalutama. Ona predstavlja trgovačku aktivnost koja okružuje određenu valutu, a koja može biti bitna pri planiranju aktivnosti trgovanja i ulaganja. Najvažnija upotreba volumena trgovanja kriptovalutama je identificiranje pouzdanih kriptovaluta. Bitno je uočiti da li kriptovaluta ima određeni volumen trgovanja, kako bi izbjegli neprovjerene valute. [31]

Budući da trgovanje uključuje kupnju i prodaju, ova metrika pomaže učiniti proces otkrivanja cijena kriptovaluta učinkovitijim. Dakle, što je veći obujam trgovanja, to je kriptovaluta pouzdanija i pravednija. Tablica i grafikon 2. prikazuju 24-satni volumen deset kriptovaluta sa najvećim volumenom trgovanja na dan 17. kolovoza 2021. godine. Ovaj poredak se često mijenja, no tu su uvijek aktualne kriptovalute poput Bitcoina, Ethereuma i Tethera. [31][37]

Tablica 2. Deset kriptovaluti s najvećim volumenom trgovanja, Izvor: [37]

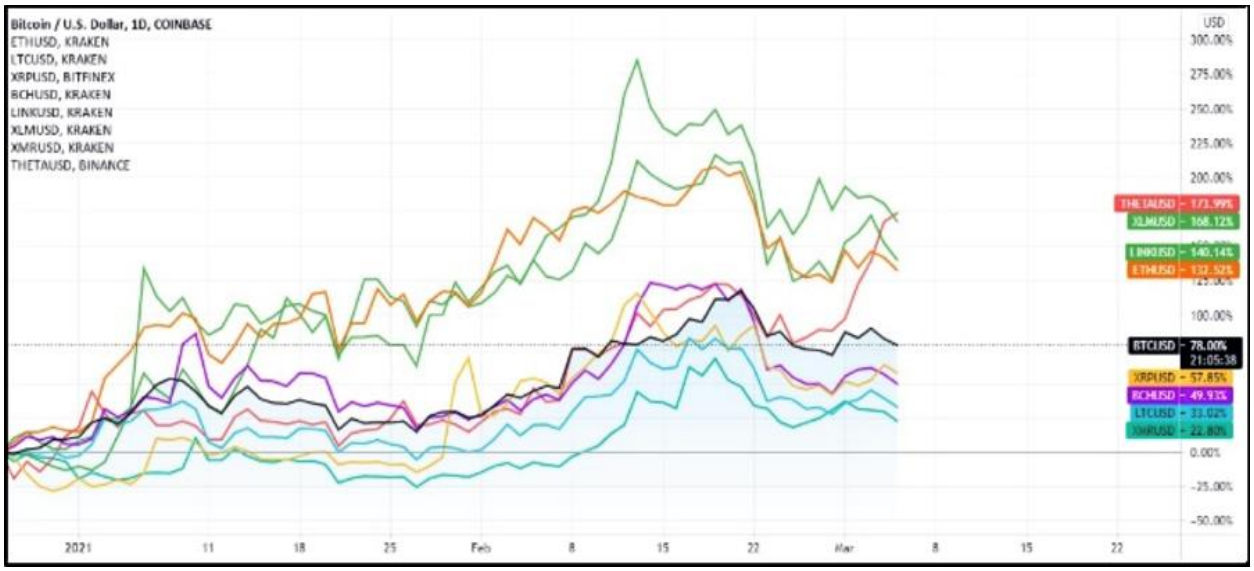
#	Naziv	Volumen (24h)
1	Tether (USDT)	438.457.764.512 kn
2	Bitcoin (BTC)	210.665.970.172 kn
3	Ethereum (ETH)	167.148.103.226 kn
4	Ripple (XRP)	51.699.312.593 kn
5	Binance USD (BUSD)	34.550.599.576 kn
6	Dogecoin (DOGE)	30.849.737.545 kn
7	Bitcoin Cash (BCH)	28.184.989.531 kn
8	Ethereum Classic (ETC)	24.305.774.959 kn
9	Solana (SOL)	22.646.519.362 kn
10	ZBG Token (ZT)	20.542.787.392 kn



Grafikon 2. Deset kriptovaluti s najvećim volumenom trgovanja, Izvor: [37]

6.3. Analiza cijene kriptovaluta

Analiza cijena je bitan proces u kojem trgovci i analitičari kriptovaluta pronalaze obrasce na tržištu kako bi odredili optimalne strategije trgovanja kriptovalutama. Dva glavna pokazatelja koja se traže su rast ili pad tržišne cijene. Tržište kriptovaluta je vrlo povezano, a cijene alternativnih kriptovaluta često su u korelaciji sa kretanjem cijene Bitcoina. To potvrđuje činjenica da tržišna kapitalizacija Bitcoina čini više od pola ukupnog kripto tržišta, a to postavlja sami Bitcoin kao „zlatnu sredinu“ u svijetu trgovanja kriptovalutama. [31]



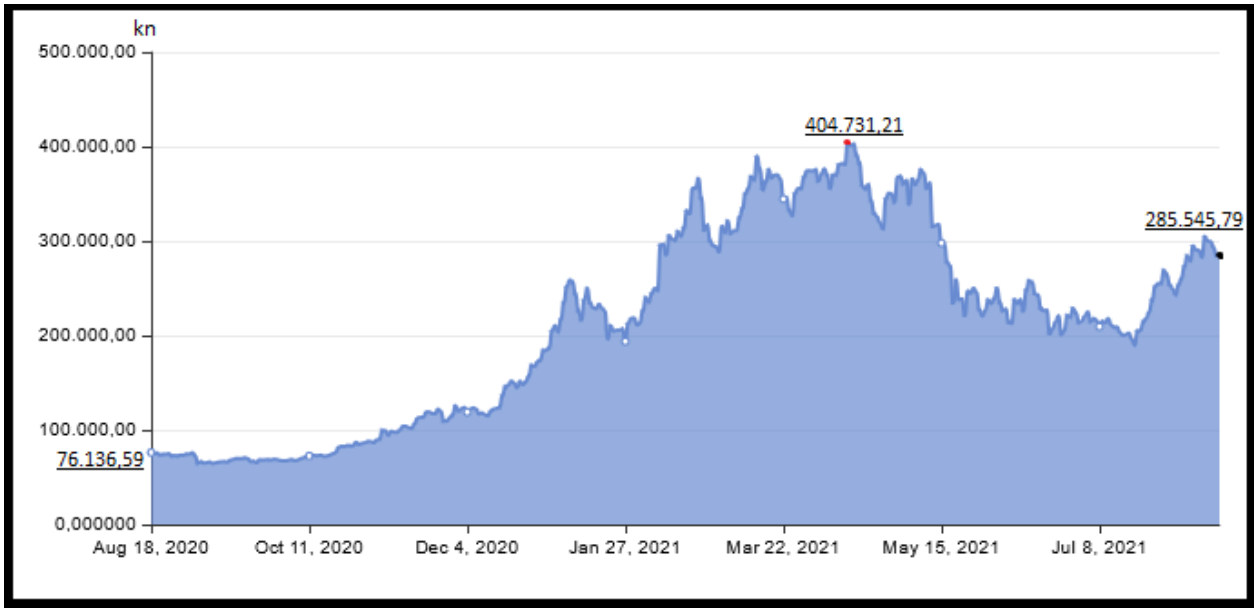
Grafikon 3. Trend rasta i pada cijene Bitcoina i alternativa, [31]

Grafikon 3. prikazuje odnos rasta cijene alternativnih kriptovaluta, poput Ethereuma (narančasta linija), Stellara (zelena linija) i Bitcoina (crna linija), na kojem je lako vidljiva korelacija između oscilacija vrijednosti, odnosno vidljivo je da u periodima rasta vrijednosti Bitcoina, rastu i vrijednosti drugih kriptovaluta . Budući da je Bitcoin glavna kriptovaluta, vrijednost ostalih valuta obično se temelji na njemu. Zbog ovisnosti vrijednosti kriptovaluta i potražnje, vrijednost na cijelom kripto tržištu isključivo je subjektivna. [31]

6.3.1. Bitcoin

Početkom 2021. godine, globalno tržište svjedočilo je još jednoj eksploziji rasta vrijednosti Bitcoina. Cijena jednog Bitcoina narasla je preko 700% u malo manje od godinu dana, i dosegla je nevjerojatnu vrijednost od 40.000 USD. Sredinom travnja Bitcoin je dostigao svoj maksimum od gotovo 64.000 USD (404.730 kuna). Eventualno, vrijednost je počela ponovno padati zbog zabrinutosti o globalnom utjecaju Bitcoina na okoliš, a koju je izazvalo masovno miniranje Bitcoina i ogromna potrošnja električne energije. Trenutna vrijednost jednog Bitcoina je oko 44.500 USD (285.500 kuna) i drži prvo mjesto kao najvrjednija kriptovaluta sa najvećom tržišnom kapitalizacijom. U opticaju ima preko 18,7 milijuna BTC tokena, a maksimalna količina postavljena je na 21 milijun BTC. [8][38]

Grafikon 4. prikazuje kretanje cijene Bitcoina u posljednjih godinu dana, gdje je vidljiva pojava bikovog tržišta 2021. godine, odnosno naglog porasta vrijednosti Bitcoina i naglog rasta kapitalizacije cijelog tržišta kriptovalutama. [38]



Grafikon 4. Kretanje cijene Bitcoina, [37]

6.3.2. Ethereum

Već krajem 2020. godine vrijednost Ethereuma je narasla na gotovo 700 USD, te je 12. svibnja 2021. godine dosegla preko 4.000 USD. Trenutna vrijednost kreče se oko 3000 USD (19.200 kuna), te Ethereum trenutno zauzima drugo mjesto po tržišnoj kapitalizaciji, odmah iza Bitcoina. Ethereum u opticaju trenutno ima preko 117 milijuna ETH tokena. Na grafikonu 5. je vidljivo kretanje cijene Ethereuma u posljednjih godinu dana, te je vidljiv sličan uzorak rasta cijene kao i kod Bitcoina. [10][38]



Grafikon 5. Kretanje cijene Ethereuma, [37]

6.3.3. Cardano

Cardano je vrlo aktualna i perspektivna kriptovaluta temeljena na blockchainu treće generacije koja ima za cilj izravno konkurirati Ethereumu i drugim decentraliziranim aplikacijskim platformama na tržištu. Trenutna vrijednost ove kriptovalute kreće se oko 2 USD (13 kuna), ali unatoč tome drži ukupno treće mjesto po tržišnoj kapitalizaciji. Maksimum od 2,30 USD (14,69 kuna) dosegnut je u svibnju 2021. godine. Trenutno je u opticaju preko 32 milijarde ADA tokena, dok je maksimum postavljen na 45 milijardi. Grafikon 6. prikazuje kretanje cijene Cardana u posljednjih godinu dana, i očit je trend rasta i pada po uzorku na Bitcoin i Ethereum. [38]



Grafikon 6. Kretanje cijene Cardana, [37]

7. Zaključak

Blockchain tehnologija stvara novi val digitalne imovine u obliku kriptovaluta, koje su otporne na cenzuru i nezaustavljivu automatizaciju. Po prvi put u povijesti ljudi mogu elektronički prenositi digitalnu vrijednost diljem svijeta bez potrebe za odobrenjem transakcije od trećih strana. Također, uplate se mogu slati transparentnim pametnim ugovorima koji jamče određene ishode, bez samostalnih ručnih koraka ili bez potrebe za trećom stranom i njihovih obećanjima. Blockchain tehnologija istražuje se za širok raspon upotreba, od plaćanja pa do prikupljanja sredstava i vođenja evidencije. Razne tvrtke ulažu u blockchain tehnologiju kako bi provjerile mogu li smanjiti troškove i rizik, povećati prihode ili stvoriti nove poslovne modele. Blockchain tehnologija svakim danom se razvija i poboljšava, te samim time predstavlja svjetlu budućnost kriptovaluta i digitalne sigurnosti.

Blockchain predstavlja revoluciju u arhitekturi suvremenih mreža zbog svojih kompleksnih i sigurnih kriptografskih metoda i načina pohrane važnih podataka. Samim time pruža podlogu za kreiranje sigurne mreže za razne organizacije i projekte, te za kreiranje suvremenih decentraliziranih aplikacija i platforma, neovisnih o nekom posredniku.

Mreža novih kriptovaluta i dalje se širi i sve se više ulaže na tržištu kriptovalutama. Popularnost kriptovaluta i njihov potencijal za poboljšanje tradicionalnih financijskih sustava doveli su do sve šireg popisa medijskih reakcija, istraživačkih radova i izvješća. Dok su neke od valuta opstale, te danas imaju svoju vrijednost, mnoge od njih propadaju i služe kao alat za malverzacije i otimanje novca. Kako će se kriptovalute dalje razvijati i kakvo će biti stanje na tržištu je teško predvidjeti, a samo vrijeme može pokazati.

Literatura

[1] Imran Bashir, Mastering Blockchain – Second Edition, BIRMINGHAM – MUMBAI, 2018.

[2] Anthony Idalion, Blockchain: The complete guide to understanding Blockchain Technology for beginners in record time, 2017.

[3] The Financial Freedom Foundation, Cryptocurrency Evolution, 2017.

[4] Stephen P. Williams, Blockchain: The Next Eveything, 2019.

[5] Luke Conway, Blockchain Explained, 2021., Preuzeto sa: https://www.investopedia.com/terms/b/blockchain.asp [Pristupljeno: srpanj 2021.]

[6] Andrew Norry, History of cryptocurrency, 2018., Preuzeto sa: https://parameter.io/history-of-cryptocurrency/ [Pristupljeno: srpanj 2021.]

[7] Criptocurrency, Preuzeto sa: https://en.wikipedia.org/wiki/Cryptocurrency [Pristupljeno: srpanj 2021.]

[8] History of Bitcoin, Preuzeto sa: https://en.wikipedia.org/wiki/History_of_bitcoin [Pristupljeno: srpanj 2021.]

[9] Luke Conway, Most important cryptocurrencies other than Bitcoin, 2021., Preuzeto sa: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/ [Pristupljeno: srpanj 2021.]

[10] Ethereum, Preuzeto sa: https://en.wikipedia.org/wiki/Ethereum [Pristupljeno: srpanj 2021.]

[11] How does a blockchain work, 2017., Preuzeto sa: https://www.youtube.com/watch?v=SSo_EIwHSd4 [Pristupljeno: kolovoz 2021.]

[12] Euny Hong, How does Bitcoin mining work, 2021., Preuzeto sa: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/ [Pristupljeno: kolovoz 2021.]

[13] Jimi S., Blockchain: What are nodes, 2018., Preuzeto sa: https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f [Pristupljeno: kolovoz 2021.]

[14] Blockchain – Types, 2021., Preuzeto sa: https://data-flair.training/blogs/types-of-blockchain/ [Pristupljeno: kolovoz 2021.]

[15] Christine Parizo, Types of blockchain, 2021., Preuzeto sa: https://searchcio.techtarget.com/feature/What-are-the-4-different-types-of-blockchain-technology [Pristupljeno: kolovoz 2021.]

[16] Alyssa Hertig, What is Proof of Work, 2020., Preuzeto sa: https://www.coindesk.com/what-is-proof-of-work [Pristupljeno: kolovoz 2021.]

[17] Proof of Work, Preuzeto sa: https://en.bitcoin.it/wiki/ [Pristupljeno: kolovoz 2021.]

[18] Shobhit Seth, Cryptography, 2021., Preuzeto sa: https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/ [Pristupljeno: kolovoz 2021.]

[19] Symmetric Cryptography, Preuzeto sa: https://www.ibm.com/docs/en/ztpf/1.1.0.14?topic=concepts-symmetric-cryptography [Pristupljeno: kolovoz 2021.]

[20] Adam Hayes, Disintermediation, 2021., Preuzeto sa: https://www.investopedia.com/terms/d/disintermediation.asp [Pristupljeno: kolovoz 2021.]

[21] Jake Frankenfield, Smart Contracts, 2021., Preuzeto sa: https://www.investopedia.com/terms/s/smart-contracts.asp [Pristupljeno: kolovoz 2021.]

[22] Stuart D. Levi, Alex B. Lipton, Introduction to smart contracts, 2018., Preuzeto sa: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ [Pristupljeno: kolovoz 2021.]

[23] What are smart contracts, Preuzeto sa: https://www.cryptoninjas.net/what-are-smart-contracts/ [Pristupljeno: kolovoz 2021.]

[24] Ethereum Smart Contracts, 2021., Preuzeto sa: https://ethereum.org/en/developers/docs/smart-contracts/ [Pristupljeno: kolovoz 2021.]

[25] QuillHash Team, EOS Smart Contract, 2019., Preuzeto sa: https://medium.com/quillhash/eos-fundamentals-for-developers-essential-concepts-for-starting-eos-development-9d8e1a263724 [Pristupljeno: kolovoz 2021.]

[26] Cardano Testnets, 2021., Preuzeto sa: https://testnets.cardano.org/en/ [Pristupljeno: kolovoz 2021.]

[27] Atakan Kantarci, Smart Contracts in 2021, 2020., Preuzeto sa: https://research.aimultiple.com/smart-contracts/

[28] Ivan Kot, Smart Contracts in Insurance, 2020., Preuzeto sa: https://www.insurancethoughtleadership.com/smart-contracts-in-insurance/ [Pristupljeno: kolovoz 2021.]

[29] Antonio Grasso, Smart Contracts: Real-Life Use Cases, 2019., Preuzeto sa: https://antgrasso.medium.com/smart-contracts-real-life-use-cases-f1dd03a76d5 [Pristupljeno: kolovoz 2021.]

[30] Digital agriculture, Preuzeto sa: https://en.wikipedia.org/wiki/Digital_agriculture [Pristupljeno: kolovoz 2021.]

[31] Brandon Smith, Cryptocurrency Trading Strategies For Beginners, 2021.

[32] Rickie Houston, The best cryptocurrency exchanges for trading bitcoin and other assets, 2021., Preuzeto sa: https://www.businessinsider.com/personal-finance/best-crypto-bitcoin-exchanges [Pristupljeno: kolovoz 2021.]

[33] Binance, Preuzeto sa: https://en.wikipedia.org/wiki/Binance [Pristupljeno: kolovoz 2021.]

[34] Bisq, 2021., Preuzeto sa: https://bisq.wiki/Main_Page [Pristupljeno: kolovoz 2021.]

[35] Cryptocurrency wallet, Preuzeto sa: https://www.bankrate.com/glossary/c/cryptocurrency-wallet/ [Pristupljeno: kolovoz 2021.]

[36] Raynor de Best, Cryptocurrencies - statistics & facts, 2021., Preuzeto sa: https://www.statista.com/topics/4495/cryptocurrencies/ [Pristupljeno: kolovoz 2021.]

[37] Kriptovalute, Kriptotržište, Preuzeto sa: https://www.kriptovalute.hr/ [Pristupljeno: kolovoz 2021.]

[38] CoinMarketCap, Top 100 Crypto Coins, Preuzeto sa: https://coinmarketcap.com/currencies/ [Pristupljeno: kolovoz 2021.]

[39] Tiana Laurence, Introduction to Blockchain Technology, Van Haren, 2019. [Pristupljeno: kolovoz 2021.]

[40] Kuan-Ching Li, Xiaofeng Chen, Hai Jiang, Essentials of Blockchain Technology, 2019. [Pristupljeno: kolovoz 2021.]

[41] Oscar Flynt, Smart Contracts: How to Use Blockchain Smart Contracts for Cryptocurrency Exchange, Createspace Independent Publishing Platform, 2016. [Pristupljeno: kolovoz 2021.]

[42] Thomas Mailund, The Joys of Hashing: Hash Table Programming with C, Apress, 2019. [Pristupljeno: rujan 2021.]

[43] SHA-256 Cryptographic Hash Algorithm, Preuzeto sa: https://www.movable-type.co.uk/scripts/sha256.html [Pristupljeno: rujan 2021.]

Popis kratica

ADA	Cardano
API	(Application programming interface) aplikacijsko programsko sučelje
BNB	Binance Coin
BTC	Bitcoin
CFD	(Contract for Differences) ugovori za razliku
dApps	(Decentralized Apps) decentralizirane aplikacije
EVM	(Ethereum Virtual Machine) Ethereum virtualni stroj
ETH	Ether, Ethereum
H/s	(Hashes per second) kôdova po sekundi
IoT	(Internet of Things) Internet stvari
MB	(Megabyte) megabajt
OS	(Application programming interface) aplikacijsko programsko sučelje
PoS	(Proof of Stake) dokaz o udjelu
PoW	(Proof of Work) dokaz o radu
USD	(United States dollar) Američki dolar

Popis slika

Slika 1. Dizajn distribuiranog sustava, [1] 12

Slika 2. Povezanost blokova u lancu, [10] 14

Slika 3. Primjer šifriranja poruka korištenjem SHA-256 hash algoritma, [43] 18

Slika 4. Enkripcija pomoću simetrične kriptografije, [19] 24

Slika 5. Enkripcija pomoću asimetrične kriptografije, [18] 26

Slika 6. Vrste mrežnih sustava, [1] 27

Slika 7. Princip izvršavanja pametnog ugovora, [41] 32

Popis tablica i dijagrama

Tablica 1. Deset kriptovaluti s najvećom tržišnom kapitalizacijom, [37] 43

Tablica 2. Deset kriptovaluti s najvećim volumenom trgovanja, [37] 45

Dijagram 1. Proces rudarenja blokova, [1] [12] 16

Popis grafikona

Grafikon 1. Deset kriptovaluti s najvećom tržišnom kapitalizacijom, [37]... 44

Grafikon 2. Deset kriptovaluti s najvećim volumenom trgovanja, [37]..... 45

Grafikon 3. Trend rasta i pada cijene Bitcoina i alternativa, [31] 46

Grafikon 4. Kretanje cijene Bitcoina, [37]..... 47

Grafikon 5. Kretanje cijene Ethereuma, [37]..... 48

Grafikon 6. Kretanje cijene Cardana, [37]..... 49

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

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

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

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

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom Značajke mreže za trgovanje kriptovalutama

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

U Zagrebu, 22.8.2021

Student/ica:

(potpis)