Sveučilište Josipa Jurja Strossmayera u Osijeku

Odjel za matematiku

Sveučilišni preddiplomski studij Matematika i računarstvo

Blockchain tehnologija

Završni rad

Mentor:

doc. dr. sc. Domagoj Ševerdija

Kandidat:

Marko Kovačević

Osijek, 2023

Sažetak

Blockchain tehnologija predstavlja distribuirani sustav za čuvanje podataka koji omogućava sigurnu, transparentnu i neizmjenjivu razmjenu informacija i vrijednosti. Ključne karakteristike ove tehnologije uključuju decentralizaciju, kriptografsku zaštitu, transparentnost i nepovratnost transakcija. Prvobitno razvijena kao osnova za kriptovalute, Blockchain se brzo proširio na različite sektore kao što su financije, logistika, zdravstvo, i mnogi drugi. Istražit ćemo arhitekturu i način funkcioniranja Blockchain tehnologije, istaknuti ključne prednosti koje donosi, te analizirati njene raznovrsne primjene u stvarnom svijetu. Također, razmotrit ćemo potencijalne izazove i buduće trendove koji će oblikovati daljnji razvoj ove tehnologije. Blockchain tehnologija obećava da će se promijeniti način na koji se posluje i čuvaju podaci, te će vjerojatno ostaviti dubok i dugotrajan utjecaj na globalnu ekonomiju i društvo.

Ključne riječi

Blockchain, Blockchain tehnologija, kriptovalute, transakcije, Bitcoin, Ethereum, pametni ugovori, distribuirani ledger, konzensus algoritmi, tokenizacija

Blockchain technology

Abstract

Blockchain technology represents a distributed system for storing data that enables secure, transparent, and immutable exchange of information and value. Key characteristics of this technology include decentralization, cryptographic protection, transaction transparency, and irreversibility. Originally developed as the foundation for cryptocurrencies, Blockchain has quickly expanded into various sectors such as finance, logistics, healthcare, and many others. We will explore the architecture and functioning of Blockchain technology, highlight the key advantages it brings, and analyze its diverse real-world applications. Additionally, we will consider potential challenges and future trends that will shape the further development of this technology. Blockchain technology promises to change the way businesses operate and store data and is likely to have a profound and lasting impact on the global economy and society.

Key words

Blockchain, Blockchain technology, cryptocurrencies, transactions, Bitcoin, Ethereum, smart contracts, distributed ledgers, consensus algorithms, tokenization

Sadržaj

1 | Uvod

Blockchain tehnologija predstavlja jedan od najznačajnijih inovacija u svijetu digitalnih tehnologija i informacijske sigurnosti. Ova tehnologija prvi put se pojavila kao ključni element iza kriptovalute Bitcoin, no njenoj primjeni nije kraj. Blockchain je brzo pronašao svoje mjesto u raznim industrijama i sektorima širom svijeta. Ovaj rad bavi se istraživanjem osnovnih koncepata i karakteristika Blockchain tehnologije, kao i njenom ključnom ulogom u promjeni načina na koji komuniciramo, čuvamo podatke i upravljamo digitalnim transakcijama te njenoj primjeni. Naslovi koje ćemo istražiti u ovom radu obuhvaćaju:

1. Osnove Blockchain Tehnologije: Prvo ćemo razmotriti povijest i osnovne principe na kojima se zasniva Blockchain tehnologija. To uključuje decentralizaciju, distribuiranu knjigu transakcija i kriptografsku zaštitu.

2. Arhitektura Blockchain-a: Detaljnije ćemo se upustiti u tehničku strukturu Blockchain-a. Ovdje ćemo razjasniti kako se transakcije grupiraju u blokove, kako se verificiraju i dodaju u lanac.

3. Primjene Blockchain Tehnologije: Analizirat ćemo širok spektar primjena Blockchain tehnologije, od financijskih usluga i lanaca opskrbe do zdravstvene zaštite i pametnih ugovora.

4. Prednosti i Izazovi: Istaknut ćemo prednosti i potencijalne izazove koji prate upotrebu Blockchain tehnologije

5. Budući Trendovi: Na kraju, razmotrit ćemo buduće trendove u razvoju Blockchain tehnologije i kako bi ona mogla oblikovati našu digitalnu budućnost.

Kroz ovaj rad, detaljnije ćemo istražiti tehnologiju za koju se smatra da će značajno promijeniti način na koji poslujemo, komuniciramo i oslanjamo se na digitalne resurse.

2 | Povijest blockchain tehnologije

Iako blockchain kao takav nije postao poznat sve do pojave Bitcoina, rani koncepti distribuirane knjige transakcija i kriptografije postojali su tijekom 90-ih godina. Ključna točka u povijesti blockchaina je objava Bitcoina(2008. godine). Osoba ili grupa pod pseudonimom Satoshi Nakamoto objavila je dokument pod naslovom "Bitcoin: A Peer-to-Peer Electronic Cash System", predstavljajući prvi konkretni primjer blockchaina. Bitcoin je postao prva prava kriptovaluta i koristio je blockchain tehnologiju za stvaranje sigurnog sustava za transakcije i pohranu vrijednosti bez potrebe za centralnim autoritetom. Prva transakcija Bitcoina, poznata kao "Genesis Block", dogodila se 3. siječnja 2009. godine. To je označilo početak stvarne upotrebe blockchain tehnologije za razmjenu vrijednosti. Poslije toga nastaje sve više kriptovaluta i projekata koji su koristili blockchain tehnologiju za različite svrhe. Ethereum, druga važna blockchain platforma, počela je operirati 2015. godine i omogućila pametne ugovore. Ovo razdoblje također obuhvaća brzi rast vrijednosti Bitcoina i povećano zanimanje investitora i različitih sektora za blockchain tehnologiju.

3 | Osnovni principi

U ovom poglavlju ćemo navesti i objasniti osnovne principe na kojima se zasniva blockchain tehnologija koji su ključni za razumijevanje ove inovativne tehnologije

3.1 Decentralizacija

Ključni princip blockchain tehnologije je decentralizacija. To znači da nema centralnog autoriteta ili posrednika koji kontrolira sustav. Umjesto toga, podaci i transakcije distribuiraju se na mreži računala (čvorova) širom svijeta. Svaki čvor ima kopiju cijele blockchain mreže, čime se eliminira potreba za posrednicima i centralnim točkama kontrole.

3.2 Distribuirana Knjiga Transakcija

Centralni element blockchaina je distribuirana knjiga transakcija, poznata i kao blockchain. Ova knjiga sadrži zapise o svim transakcijama koje su ikada izvršene u mreži. Transakcije se grupiraju u blokove, a svaki blok sadrži informacije o prethodnom bloku, čineći neprekinuti lanac transakcija. Ovaj sustav osigurava transparentnost i nepovratnost podataka.

3.3 Kriptografija

Kriptografija se koristi za osiguranje sigurnosti na blockchainu. Svaka transakcija je šifrirana kako bi se zaštitila privatnost i sigurnost podataka. Također, koristi se za potvrdu identiteta korisnika i digitalno potpisivanje transakcija, čime se sprečava lažiranje i prevara.

3.4 Nepovratnost Transakcija

Nakon što se transakcija zabilježi u blockchainu, postaje gotovo nemoguće izmijeniti ili izbrisati. Ova karakteristika osigurava integritet podataka i pomaže u sprečavanju prevara.

3.5 Mehanizam Konsenzusa

Da bi se dodao novi blok u blockchain, čvorovi u mreži moraju postići suglasnost ili konsenzus o valjanosti transakcija. Postoji nekoliko različitih mehanizama konsenzusa, kao što je Proof of Work (PoW) ili Proof of Stake (PoS), koji se koriste kako bi se osiguralo da samo valjane transakcije budu prihvaćene.

3.6 Transparentnost

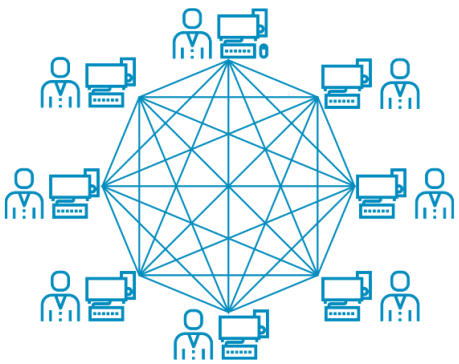
Sve transakcije na blockchainu su javno vidljive i dostupne za pregled svim sudionicima mreže. To povećava transparentnost i omogućava korisnicima da provjere valjanost transakcija.

4 | Blockchain arhitektura

Sada ćemo dublje istražiti tehničku strukturu blockchain-a. Ovdje ćemo pojasniti kako se transakcije grupiraju u blokove, kako se verificiraju i dodaju u lanac.

4.1 Čvorovi

Svaki blockchain sastoji se od distribuirane mreže čvorova, koji su zapravo računala ili uređaji povezani putem interneta. Svaki čvor u blockchain mreži posjeduje svoju kopiju cjelokupnog lanca transakcija, što ga čini neovisnim o ostalima. Ovi čvorovi surađuju kako bi postigli konsenzus i potvrdili valjanost svih transakcija. Postoje različite vrste čvorova u blockchainu, uključujući rudarske čvorove, punopravne čvorove i svjetlosne čvorove. Rudarski čvorovi odgovorni su za dodavanje novih blokova u blockchain putem procesa poznatog kao rudarenje, dok punopravni čvorovi čuvaju cjelokupnu kopiju blockchaina i provjeravaju svaku transakciju. Svjetlosni čvorovi ne čuvaju cjelokupnu kopiju blockchaina, već se oslanjaju na punopravne čvorove za provjeru transakcija. Oni su manje resursno zahtjevni i često se koriste u mobilnim i resursno ograničenim uređajima. Bitno je napomenuti da su čvorovi u blockchainu raspoređeni diljem svijeta, što čini mrežu otpornom napade. U slici 4.1 možemo vidjeti decentralizaciju koja osigurava da nema jedne centralne točke kontrole čime se povećava sigurnost i transparentnost blockchaina. Svi čvorovi u mreži moraju se složiti oko valjanosti transakcija, čime se postiže konsenzus, a nevaljane transakcije automatski se odbacuju.



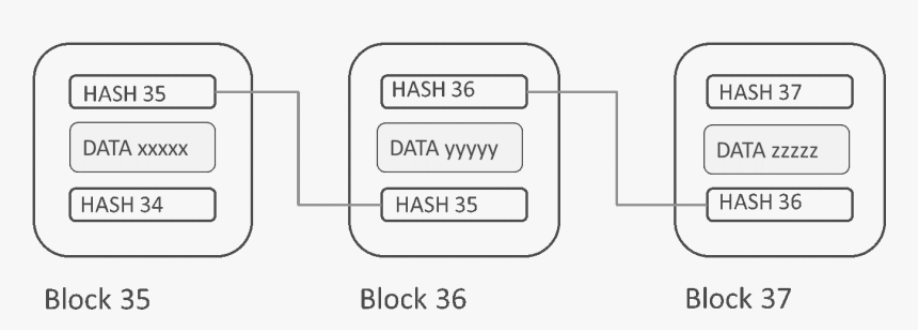
Slika 4.1: Decentralizirani čvorovi

4.2 Transakcije

Svaka transakcija zabilježava se kao digitalni zapis koji sadrži informacije o promjeni vlasništva ili izvršavanju određenih uvjeta unutar mreže. Ove transakcije nisu ograničene samo na prijenos kriptovaluta; mogu sadržavati različite vrste podataka, uključujući i izvršavanje pametnih ugovora. Svaka transakcija u blockchainu prolazi kroz proces validacije kako bi se osigurala njena autentičnost i integritet. Ovaj proces uključuje provjeru potpisa, dostupnost dovoljnih sredstava za transakciju, kao i ispunjenje uvjeta u pametnim ugovorima. Nakon validacije, transakcija se dodaje u mempool(privremena memorija), gdje čeka na uključivanje u sljedeći blok. Rudari, ili članovi mreže odgovorni za stvaranje novih blokova, natječu se za uključivanje transakcija u svoj blok. Kada je transakcija konačno potvrđena i uključena u blockchain, postaje nepovratna i trajno zabilježena u distribuiranom registru, osiguravajući transparentnost i pouzdanost transakcija unutar sustava.

4.3 Blockchain

Svaki blok u distribuiranom sustavu sadrži kolekciju podataka koja može uključivati financijske transakcije, pametne ugovore ili druge informacije relevantne za specifičnu primjenu. Ono što čini svaki blok jedinstvenim i ključnim elementom je njegova jedinstvena hash vrijednost. U blockchainu svaki blok sadrži referencu na prethodni blok u lancu. To znači da svaki blok zna koji je blok prethodio njemu. Ova referenca na prethodni blok stvara neprekinuti niz blokova koji zajedno čine blockchain što možemo vidjeti na slici 4.2.



Slika 4.2: Povezanost blokova u blockchainu

4.4 Hash funkcija

Hash funkcija je matematička funkcija koja pretvara proizvoljan ulaz u fiksan duljinski niz znakova, poznat kao hash vrijednost. Ključne karakteristike hash funkcije uključuju jednostranu prirodu, gdje je lako generirati hash iz ulaznih podataka, ali praktički nemoguće rekonstruirati ulaz iz hash vrijednosti, jedinstvenost, gdje različiti ulazi daju različite hash vrijednosti, konstantnu duljinu hash vrijednosti bez obzira na duljinu ulaza, brzu izračunljivost, te avalanche efekt, gdje i najmanja promjena u ulazu značajno mijenja hash vrijednost. Najčešće korištena hash funkcija u blockchainu je SHA-256 (Secure Hash Algorithm 256-bit).

Primjer 1. *Iako se ova dva ulaza razlikuju samo u jednom znaku SHA-256 generira potpuno različite hash vrijednosti.*

Ulaz: "aaabb"
SHA-256 Hash Vrijednost: 461e752b9934261c96ec0de55c68e68e89e84f7bc

Ulaz: "aaabbb"
SHA-256 Hash Vrijednost: a577f8e4db5e8f58f7d84bb3cfe9e2c4c205b05ab7

4.5 Mehanizam Konsenzusa

Mehanizam konsenzusa je ključna komponenta blockchain tehnologije koja omogućava različitim sudionicima u mreži da se slažu o stanju blockchaina, redoslijedu transakcija i validaciji novih podataka. Konsenzus je neophodan kako bi se osigurala integritet, sigurnost i dosljednost podataka u decentraliziranim sustavima. Najpoznatiji su Proof of Work(Pow) i Proof of Stake(Pos).

4.5.1 Proof of Work

Proof of Work(PoW) je vrsta konsenzusa gdje se rudari (mineri) natječu za rješavanje složenih matematičkih problema. Prvi rudar koji uspješno riješi problem ima pravo dodati novi blok u blockchain i time dobiva nagradu. Napoznatiji blockchain koji ga koristi je Bitcoin. Ovaj mehanizam je efikasan za sprečavanje napada i osigurava sigurnost mreže, ali zahtijeva velike količine računalne snage i energije.

4.5.2 Proof of Stake

Umjesto da se koristi računalna snaga, Proof of Stake koristi ulog (stake) kriptovalute kao mehanizam za određivanje tko će validirati transakcije. Korisnici sa većim ulogom imaju veću šansu biti izabrani kao validatori. Koristi ga Ethereum 2.0 kako bi poboljšao skalabilnost i energetsku učinkovitost, također resursno je manje zahtjevan od PoW.

4.6 Rudari

Rudari su važna karika u svijetu blockchain tehnologije, a njihova prisutnost i uloga su ključni za funkcioniranje blockchain mreža poput Bitcoina i Ethereuma. U početku, rudari se bave prikupljanjem transakcija koje su poslane u mrežu. Ove transakcije uključuju sve moguće oblike digitalnih interakcija, od razmjene kriptovaluta do izvršavanja pametnih ugovora. Nakon što su prikupljene, rudari obavljaju temeljitu provjeru svake transakcije kako bi osigurali da su valjane i da nije riječ o pokušajima prijevare. Nakon verifikacije, rudari grupiraju ove transakcije u nove blokove. Najizazovniji dio za rudare je rješavanje kompleksnih kriptografskih slagalica putem mehanizama konsenzusa. U tom procesu, rudari koriste svoje računalne resurse i troše energiju kako bi prvi pronašli ispravan "hash" za novi blok. Nagrada za uspješno rješavanje slagalice i dodavanje novog bloka u blockchain dolazi u obliku kriptovaluta zajedno s transakcijskim naknadama koje su korisnici platili za obradu svojih transakcija.

5 | Primjena blockchain tehnologije

Primjena blockchain tehnologije seže mnogo dalje od kriptovaluta, iako je Bitcoin bio prva i najpoznatija upotreba ove tehnologije. Blockchain tehnologije primjenjuje se u mnogim sferama, od financija i zdravstva do opskrbnog lanca, energetike, obrazovanja i izbornih sustava. Omogućava nove načine razmjene vrijednosti, automatizacije procesa putem pametnih ugovora, te transparentnost i povjerenje u podacima i transakcijama. U nastavku ćemo navesti neke od bitnijih primjena ove tehnologije te opširnije objasniti ulogu blockchaina u tim sferama.

5.1 Kriptovalute

Blockchain tehnologija predstavlja temeljni stup u kriptovalutama, omogućujući im sigurne i transparentne transakcije. Ovaj distribuirani, decentralizirani sustav čuva podatke o transakcijama u blokovima koji su povezani lančano, čime se sprječava manipulacija podataka. Osim toga, blockchain omogućuje sudionicima u mreži potpunu kontrolu nad svojim financijama, izbjegavajući potrebu za posrednicima poput banaka. Brze i jeftine transakcije, često s nižim troškovima u odnosu na tradicionalne financijske usluge, čine kriptovalute privlačnima za međunarodne transakcije i male transakcije. Najpoznatije kriptovalute su Bitcoin i Ethereum.

5.1.1 Bitcoin

Bitcoin(BTC) je prva i najpoznatija kriptovaluta. Izazvao je revoluciju u financijskom svijetu i bio je preteča za stvaranje mnogih drugih kriptovaluta koje su slijedile te je potaknuo interes za blockchain tehnologijom. Svojim jednostavnim, ali inovativnim konceptom, Bitcoin je promijenio način na koji razmišljamo o novcu i financijama. Često se uspoređuje s digitalnim zlatom zbog svoje sposobnosti za dugoročnu pohranu vrijednosti i zaštitu od inflacije.

5.1.2 Ethereum

Ethereum (ETH) je druga najpoznatija kriptovaluta koja se izdvaja po svojoj sposobnosti za izvođenje pametnih ugovora na blockchainu. Ovo znači da Ethereum nije samo digitalni novac, već i platforma koja omogućuje programabilnost na blockchainu. Ethereum je stvoren 2015. godine od strane Vitalika Buterina i omogućio je razvoj različitih decentraliziranih aplikacija (DApps) koje se izvode na njegovoj blockchain mreži. Pametni ugovori na Ethereumu automatski izvršavaju uvjete ugovora bez potrebe za posrednicima. Ethereum je ključni element u svijetu decentraliziranih financija (DeFi) i tokenizacije imovine te je potaknuo inovaciju u mnogim sektorima izvan kriptovaluta. Svojom fleksibilnošću i mogućnošću prilagodbe, Ethereum je ostavio dubok i trajan utjecaj na razvoj blockchain tehnologije.

5.2 Pametni ugovori

Pametni ugovori su računalni programi koji se izvršavaju automatski na blockchainu kada se ispune određeni uvjeti. Pametni ugovori imaju širok spektar primjena, uključujući financijske usluge, lanac opskrbe, zdravstvo, nekretnine, upravljanje imovinom i mnoge druge industrije. U financijskom sektoru, pametni ugovori omogućavaju automatizaciju transakcija i financijskih usluga. To uključuje izdavanje kriptovaluta, provođenje ICO-a i STO-a (Security Token Offering), te stvaranje decentraliziranih platformi za trgovinu vrijednostima. U lancu opskrbe, pametni ugovori pomažu u praćenju proizvoda od izvora do potrošača. U sektoru nekretnina, pametni ugovori mijenjaju način na koji se kupuju i prodaju nekretnine. Oni olakšavaju digitalizaciju vlasničkih dokumenata i omogućavaju sigurnu razmjenu imovine.

5.3 Financijski sektor

Blockchain osigurava brže i jeftinije međunarodne transakcije i razmjenu vrijednosti. Ripple je primjer takvog projekta koji se bavi upravo ovom svrhom. Umjesto tradicionalnih bankovnih međunarodnih prijenosa, blockchain omogućava da se kriptovalutama ili digitalnim tokenima vrijednosti šalju gotovo trenutačno, s nižim troškovima transakcija. Osim toga, blockchain može poboljšati upravljanje identitetom i KYC(Know Your Customer) procese. Korisnici mogu imati digitalne identitete pohranjene na blockchainu koji su sigurni i kontrolirani samo od strane vlasnika. Ovo olakšava verifikaciju identiteta za usluge kao što su otvaranje bankovnih računa i pristup online uslugama. Nadalje, blockchain omogućava izdavanje sigurnosnih tokena koji predstavljaju vlasništvo ili udjele u nekoj imovini, poput dionica ili nekretnina. Ovo se koristi za kapitalno prikupljanje, a proces je transparentan i može se automatizirati putem pametnih ugovora. STO(Security Token Offering) tokeni omogućuju pristup investicijama širem broju ljudi i pojednostavljuju proces izdavanja i trgovine ovim tokenima.

5.4 Lanci opskrbe

Blockchain omogućuje transparentno praćenje svakog koraka u proizvodnom procesu, od sirovina do gotovih proizvoda. Ovo je posebno važno za hranu, luksuzne proizvode, farmaceutske proizvode i druge proizvode gdje je važno znati točno porijeklo i putovanje proizvoda. Također, blockchain može pratiti podatke o kvaliteti i sigurnosti proizvoda tijekom cijelog lanca opskrbe što je važno za identifikaciju i povlačenje proizvoda ako postoji problem sa sigurnošću ili kvalitetom. Nadalje ova tehnologija omogućuje real-time praćenje zaliha, što pomaže tvrtkama u održavanju optimalnih razina zaliha i sprječava nestašicu ili prekomjerno zalihe.

5.5 Energetika

Blockchain omogućuje praćenje proizvodnje energije iz obnovljivih izvora, kao što su solarna ili energija vjetroelektrane. Ovi podaci se mogu sigurno pohraniti na blockchainu i omogućiti potrošačima praćenje izvora svoje električne energije. Važna ulogu ima u trgovini energijom. Uz blockchain P2P (peer-to-peer) trgovina energijom između proizvođača i potrošača postaje moguća. Ovo smanjuje potrebu za posrednicima i omogućava potrošačima da direktno trguju energijom s drugima.

6 | Prednosti i izazovi

6.1 Prednosti

Blockchain tehnologija donosi niz izvanrednih prednosti. U nastavku ćemo objasniti koje su to prednosti korištenja ove tehnologije.

6.1.1 Sigurnost

Sigurnost je ključna prednost zbog korištenja snažne kriptografije i decentraliziranog sistema. Ovo čini podatke na blockchainu iznimno otpornima na hakiranje i promjene, čime se štite osjetljive informacije i transakcije. Transparentnost također igra ključnu ulogu jer svi sudionici u mreži imaju pristup istim podacima, stvarajući visoku razinu povjerenja i sprječavajući nesporazume ili prijevare.

6.1.2 Decentralizacija

Druga značajna prednost je decentralizacija, koja omogućava izravne transakcije između sudionika bez potrebe za posrednicima kao što su banke ili vlade. Ovo može značiti značajne uštede u vremenu i troškovima transakcija te povećanje kontrole pojedinaca nad vlastitim financijama i podacima.

6.1.3 Brzina i učinkovitost

Brzina i učinkovitost blockchaina su također impresivne. Transakcije se mogu provoditi brže i jeftinije u usporedbi s tradicionalnim financijskim sustavima, posebno kada se radi o međunarodnim transakcijama.

6.1.4 Neizmjenjivost podataka

Neizmjenjivost podataka je ključna za očuvanje povijesti transakcija i podataka. Nakon što se podaci zapišu na blockchain, vrlo je teško, ako ne i nemoguće, promijeniti ih bez suglasnosti svih sudionika u mreži. Ovo je korisno za praćenje i osiguranje integriteta podataka tijekom vremena.

6.1.5 Korištenje pametnih ugovora

Pametni ugovori, kao posebna vrsta blockchain tehnologije, donose dodatnu prednost automatizacije poslovnih procesa i ugovornih obveza. Oni omogućavaju izvršenje uvjeta ugovora automatski, bez potrebe za intervencijom treće strane, što povećava učinkovitost i smanjuje rizik od ljudske greške ili nepoštenosti.

6.2 Izazovi

Zajedno s impresivnim prednostima koje donosi, blockchain se također suočava s nizom složenih izazova koji utječu na njegovu daljnju široku usvajanje i integraciju u različite sektore. U nastavku ćemo objasniti neke od mana blockchain tehnologije.

6.2.1 Skalabilnost

Skalabilnost predstavlja značajan izazov jer se neke blockchain mreže suočavaju s ograničenjima u obradi velikog broja transakcija u kratkom vremenu. To može dovesti do usporavanja i povećanja troškova transakcija, što je posebno izazovno u kriptovalutnim mrežama s visokim prometom.

6.2.2 Pravni problemi

Pravni i regulatorni problemi često nisu u potpunosti definirani ili su neujednačeni u različitim jurisdikcijama. To stvara pravnu nesigurnost i može otežati priznavanje blockchain transakcija i pametnih ugovora kao valjanih i pouzdanih.

6.2.3 Energetska potrošnja

Jedan od glavnih problema je energetska potrošnja, posebno za blockchainove koji koriste dokaz o radu (Proof of Work) za sigurnost mreže. Ova metoda zahtijeva velike količine električne energije i podložna je kritikama zbog ekoloških problema.

6.2.4 Privatnost

Privatnost podataka je još jedan izazov, s obzirom na transparentnost blockchaina. Unatoč tome, postoje situacije u kojima je potrebno čuvati osjetljive informacije izvan dosega javnosti.

6.2.5 Kompleksnost

Integracija blockchain tehnologije s postojećim sustavima može biti kompleksna i skupa, što otežava prihvaćanje tehnologije u većini organizacija.

7 | Trendovi

Blockchain tehnologija, od svojeg prvog izuma putem Bitcoina 2009. godine, prošla je kroz impresivan evolucijski put i neprestano se razvija. Kao temeljni koncept decentralizirane knjige transakcija, blockchain je pružio platformu za revoluciju u načinima na koje upravljamo podacima, provodimo financijske transakcije i obavljamo poslovne operacije. Budući trendovi u razvoju blockchain tehnologije obećavaju još dublje promjene u našem digitalnom krajoliku, stvarajući novo okruženje koje će oblikovati našu budućnost.

7.1 DeFi

DeFi (Decentralized Finance) predstavlja inovativnu transformaciju financijskog sektora putem blockchain tehnologije, omogućavajući sudionicima da izravno sudjeluju u raznim financijskim aktivnostima, poput posuđivanja, štednje i trgovanja, bez potrebe za posrednicima kao što su tradicionalne banke. Otvorenost, decentralizacija i transparentnost karakteriziraju ovu novu paradigmu financijskih usluga, pružajući korisnicima globalni pristup i veću kontrolu nad vlastitim financijama. Iako DeFi donosi brojne prednosti, uključujući veću pristupačnost financijskim uslugama, suočava se s izazovima kao što su sigurnosni rizici i potreba za razvojem održivih modela kako bi se osigurala njegova dugoročna stabilnost i prihvaćenost.

7.2 CBDC

CBDC (Central Bank Digital Currency) predstavlja novi korak u razvoju financijskog sektora, jer centralne banke istražuju izdavanje vlastitih digitalnih valuta koje bi funkcionirale kao digitalna verzija tradicionalnog nacionalnog novca. Ova inicijativa otvara vrata za duboke promjene u načinu na koji ljudi posjeduju, koriste i razmjenjuju novac. Jedna od ključnih prednosti CBDC-a je mogućnost bržih i jeftinijih transakcija, što bi moglo poboljšati financijsku dostupnost i olakšati međunarodne plaćanja. Također, CBDC bi omogućio centralnim bankama bolji uvid u novčane tokove i olakšao provedbu monetarne politike. Međutim, postoji niz izazova koji prate ovu inicijativu, uključujući pitanja sigurnosti, privatnosti podataka i regulacije. Unatoč tim izazovima, CBDC ostaje intrigantan trend koji bi mogao oblikovati budućnost financijskog sustava i načina na koji koristimo novac.

7.3 NFT

NFT-ovi, kratica za Non-Fungible Tokens, predstavljaju inovativan koncept u svijetu digitalnih dobara. Ovi digitalni tokeni omogućavaju jedinstveno vlasništvo i autentičnost digitalnih ili fizičkih predmeta koristeći blockchain tehnologiju. Ključna karakteristika NFT-ova je nezamjenjivost - svaki NFT je jedinstven i ne može se razmjenjivati jedan-na-jedan s drugim NFT-om. Ovaj koncept se oslanja na transparentnost i sigurnost blockchaina kako bi zabilježio vlasništvo i povijest transakcija na nepobitnim i sigurnim platformama kao što su Ethereum, Binance Smart Chain i Flow. NFT-ovi su pronašli primjenu u različitim industrijama, od umjetnosti, glazbe i igara do nekretnina, omogućavajući kreatorima i kolekcionarima da tokeniziraju i trguju digitalnim i fizičkim vrijednostima. Unatoč kontroverzama, NFT-ovi su postali ključni dio digitalne ekonomije, otvarajući nove mogućnosti za umjetnike, kreatore sadržaja i investitore diljem svijeta.

7.3.1 Everydays: The First 5000 Days

Ovo je digitalno umjetničko djelo prodano kao NFT za preko 69 milijuna dolara. To je postalo jedno od najpoznatijih NFT-a i naglasilo je potencijal za prodaju digitalne umjetnosti putem NFT platformi.

7.3.2 CryptoKitties

CryptoKitties je popularna igra na Ethereum blockchainu u kojoj igrači mogu kupovati, prodavati i trgovati digitalnim mačkama kao NFT-ovima. Svaka mačka je jedinstvena i može se razmjenjivati na tržištima NFT-a.

7.3.3 Crossroads

Kanadska glazbenica Grimes prodala je svoj digitalni umjetnički video "Crossroads" kao NFT za više od 6 milijuna dolara. Ovaj primjer naglašava kako glazbenici mogu koristiti NFT-ove za monetizaciju svoje glazbe i umjetničkih projekata.

8 | Programska podrška

Programabilni pristupi igraju ključnu ulogu u razvoju i implementaciji blockchain tehnologija, posebno kada je riječ o postavljanju pametnih ugovora. Ovi pristupi omogućavaju razvijateljima da komuniciraju s blockchain mrežama, koristeći ih kao osnovu za različite aplikacije i usluge. Ethereum, kao jedna od najpoznatijih blockchain platformi, pruža izvrsnu osnovu za razvoj pametnih ugovora, a programabilni pristupi poput Web3 pružaju alate i biblioteke koji omogućavaju programerima da se povežu s Ethereum mrežom i izvršavaju transakcije na njoj.

8.1 Solidity

Da bi razvijatelji komunicirali s pametnim ugovorima na Ethereum mreži, koriste programski jezik Solidity za njihovo pisanje. Solidity je programski jezik posebno stvoren za pisanje pametnih ugovora na Ethereum blockchainu. Ovaj jezik omogućava programerima da definiraju poslovnu logiku pametnih ugovora, uključujući transakcije, funkcije i upravljanje digitalnim sredstvima. Solidity kombinira sintaksu sličnu JavaScriptu i Pythonu s elementima specifičnim za blockchain.

Kada se pametni ugovor napiše, Solidity kod se kompilira u bytecode, točnije niz instrukcija koje izvršava Ethereumov virtualni stroj (EVM). EVM je odgovoran za izvršavanje tih instrukcija i osigurava dosljednost operacija na Ethereumu. Ova kombinacija omogućava razvijateljima da stvaraju i izvršavaju pametne ugovore na blockchainu.

8.2 Application Binary Interface

ABI (Application Binary Interface) u Ethereum sustavu predstavlja ključnu komponentu koja omogućava aplikacijama da komuniciraju s pametnim ugovorima i izvršavaju transakcije na Ethereum mreži. Ona definira kako se podaci strukturiraju i kako se funkcije pozivaju unutar tih pametnih ugovora. ABI je bitan jer osigurava da vanjske aplikacije pravilno formatiraju transakcije i pozive funkcija, omogućujući Ethereum mreži da razumije i obradi te zahtjeve. Zapravo, ABI je ključ za integraciju različitih dijelova Ethereum sustava, omogućujući interoperabilnost između različitih aplikacija i pametnih ugovora na mreži te poboljšavajući ukupnu funkcionalnost Ethereum blockchaina.

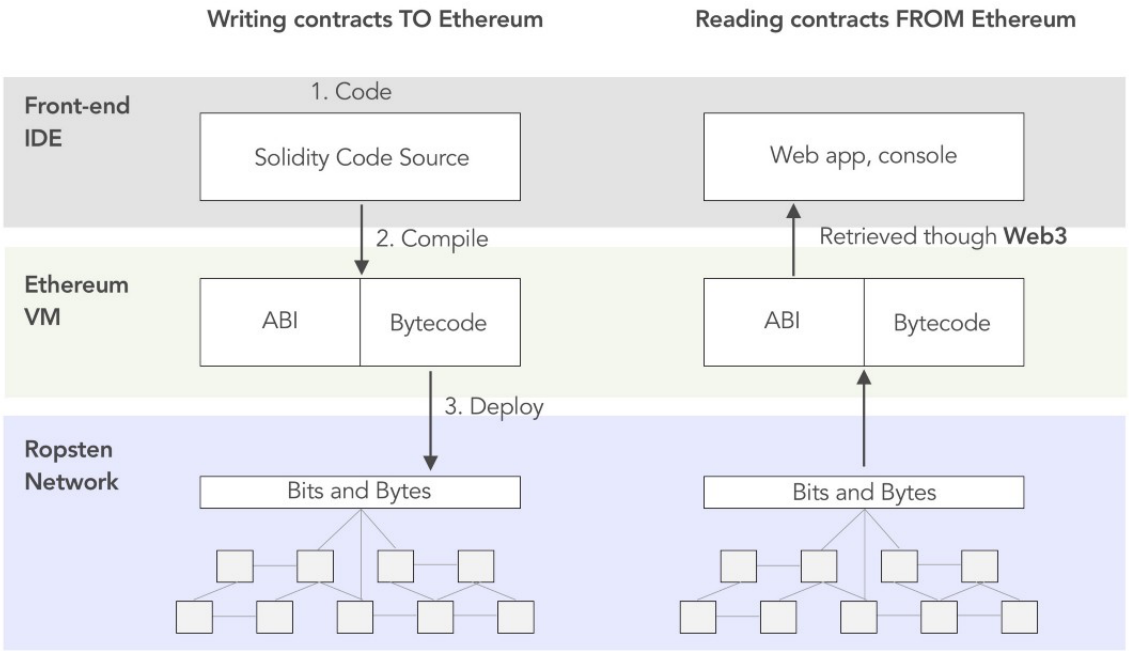
8.3 Web3

Web3 predstavlja kompleksni skup alata i biblioteka koji omogućavaju razvijateljima duboku integraciju s Ethereum mrežom putem programskog koda. Ova platforma omogućava širok spektar operacija, uključujući slanje transakcija, čitanje podataka s blockchaina, izvođenje funkcija pametnih ugovora te mnoge druge napredne radnje. Takva fleksibilnost čini razvoj decentraliziranih aplikacija (dApps) i njihovu integraciju s Ethereum mrežom pristupačnim i visoko prilagodljivim. To znači da programeri mogu stvarati inovativne aplikacije koje rade bez potrebe za centralnim posrednicima i osiguravaju potpunu transparentnost u svakom koraku procesa. Web3 također otvara vrata za napredne integracije s Ethereum mrežom, potičući neprestane inovacije u području blockchain tehnologije i decentralizacije. Ovaj sveobuhvatan pristup Web3 tehnologiji postao je ključan za razvoj novih digitalnih ekosustava i revolucioniranje načina na koji se pružaju i koriste usluge i aplikacije na globalnoj razini.

8.4 Testne mreže

Testne mreže su važan dio blockchain razvojnog procesa, simulirajući glavne blockchain mreže poput Ethereum-a, no pružajući razvijateljima lažni Ether (ETH) i eliminirajući stvarne troškove transakcija. Ova replika omogućava razvijateljima da sigurno testiraju aplikacije i pametne ugovore, identificirajući i ispravljajući probleme prije nego što ih implementiraju na stvarnim mrežama, čime se osigurava pouzdanost i sigurnost konačnih proizvoda. Najpoznatije testne mreže u svijetu blockchaina, posebno za Ethereum, su: Ropsten, Rinkeby i Hardhat Network.

Na slici 8.1 možemo vidjeti kako se Ethereum, Solidity, ABI, Web3.js i testne mreže međusobno povezuju kako bi omogućili razvoj aplikacija na blockchain tehnologiji.



Slika 8.1: Shema koja prikazuje kako su povezani Ethereum, ABI, bytecode, Web3 i testne mreže

Literatura

[1] Web izvor dostupan na https://www.blockchain-council.org/blockchain/blockchain-nodes

[2] Web izvor dostupan na https://medium.com/@eiki1212/explaining-ethereum-contract-abi-evm-bytecode-6afa6e917c3b

[3] Web izvor dostupan na https://www.ibm.com/topics/blockchain

[4] Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*

[5] Andreas M. Antonopoulos, *Mastering Bitcoin*

[6] Ritesh Modi, *Solidity Programming Essentials*

[7] Roger Wattenhofer, *The science of the Blockchain*

[8] Web3x 2023,*Introduction to Blockchain and Web3.* https://www.edx.org/learn/blockchain/web3-foundation-introduction\-to-blockchain-and-web3