Blockchain tehnologije i njezina primjena u financijskom sektoru

Dubić, Gabrijel

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Gabrijel Dubić

BLOCKCHAIN TEHNOLOGIJE I NJEZINA PRIMJENA U FINANCIJSKOM SEKTORU

ZAVRŠNI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Gabrijel Dubić

Matični broj: 0016148704

Studij: Informacijski i poslovni sustavi, modul Analiza i dizajn poslovnih sustava

BLOCKCHAIN TEHNOLOGIJE I NJEZINA PRIMJENA U FINANCIJSKOM SEKTORU

ZAVRŠNI RAD

Mentor:

Izv. prof. dr. sc. Igor Pihir

Varaždin, rujan 2024.

Gabrijel Dubić

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Auto potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

U radu su istražene, analizirane i opisane blockchain tehnologije te njihov utjecaj na financijski sektor, s naglaskom na prednosti, izazove i perspektive koje ova tehnologija donosi. U istraživačkom radu identificirani su izazovi i prepreke povezane s uvođenjem blockchaina u financijski sektor. Razmotren je budući razvoj i trendovi blockchain tehnologije u financijskom sektoru, a također su razmotrena regulativna pitanja proizašla iz upotrebe blockchaina, uključujući pravne aspekte, zaštitu potrošača i druge zakonodavne izazove. U radu su detaljno analizirane, opisane i prikazane konkretne primjene blockchaina u financijskom sektoru kroz nekoliko studija slučaja uz pripadajuće modele i analize. Osim toga, istraženo je kako blockchain može poboljšati efikasnost i sigurnost financijskih transakcija, smanjiti operativne troškove te unaprijediti transparentnost i povjerenje u financijske institucije. Također je razmotrena uloga pametnih ugovora u automatizaciji i pojednostavljenju financijskih procesa. Analizirane su uspješne implementacije blockchain tehnologije u različitim financijskim institucijama te njihovi rezultati.

Ključne riječi: inovacije, poslovna primjena, financijski sektor, primjena tehnologije, digitalna transformacija, blockchain tehnologija, pametni ugovori, kriptovaluta

Sadržaj

1. Uvod 1
2. Metode i tehnike rada 2
3. Blockchain tehnologija 3
3.1. Definiranje osnovnih pojmova 3
3.1.1. Privatni i javni ključevi 4
3.1.2. Digitalni potpis 6
3.2. Vrste blockchaina 7
3.3. Kreiranje blokova i hash-evi 9
3.4. Decentralizirane aplikacije 11
3.5. Algoritmi Proof of Work 12
3.5.1. Algoritam Proof of Work 12
3.5.2. Algoritam Proof of Stake 13
3.5.3. Ostali tipovi mehanizama konsenzusa 14
3.5.4. Usporedba algoritama Proof-of-wok i proof-of-stake 14
4. Ethereum i pametni ugovori 15
4.1. Ether 16
4.2. Pametni ugovori 17
4.2.1. Standardi pametnih ugovora 19
4.3. Platforme za pametne ugovore 20
4.3.1. Binance Smart Chain 20
4.3.2. Cardano 21
4.3.3. Polkadot 23
5. Financijske primjene blockchaina 24
5.1. Token i novčići 24
5.2. Novčanici 25
5.2.1. Digitalni novčanici 25

5.2.2. Hardverski novčanici 26
5.3. Spaljivanje novčića 27
5.4. Decentralizirana autonomna organizacija....28
5.5. Igre riječi i financije 29
6. Primjeri primjene blockchain tehnologija u financijskom sektoru 30
6.1. IBM Blockchain World Wire....30
6.2. JPMorgan's Quorum 32
7. Zaključak 35
8. Popis literature....37
9. Popis slika 41
10.Popis tablica....42

1. Uvod

Kao što je već i naglašeno, tema završnog rada odnosi se na blockchain tehnologiju i njezinu primjenu u financijskom sektoru. Blockchain tehnologija se na hrvatski jezik direktno prevodi kao lanac blokova, odnosno niz blokova koji su međusobno povezani i svaki blok ovisi o svom prethodniku. Ovi blokovi se povezuju pomoću kriptografije, što omogućava siguran i nepromjenjiv zapis podataka. U današnje vrijeme, blockchain tehnologija postaje sve popularnija i njezin razvoj ubrzano raste. Prisjetimo se situacije iz 2009. godine kada se prvi put pojavio pojam bitcoin. Bitcoin je digitalna valuta koja je potaknula razvoj same blockchain tehnologije. Na početku, vrijednost bitcoina bila je nevjerojatno niska u usporedbi s današnjom vrijednošću. Iz godine u godinu, vrijednost bitcoina se mijenjala, bilježeći značajne skokove, ali i padove. Trenutna vrijednost 1 bitcoina iznosi oko 52 tisuća i 400 eura.

Nadalje, rad će se fokusirati na primjenu blockchain tehnologije u financijskom sektoru, uključujući analizu njezinih prednosti, izazova i perspektiva. Posebna pažnja bit će posvećena pametnim ugovorima, koji su također dio blockchain tehnologije. Pametni ugovori su digitalni ugovori koji se sami izvršavaju, pružajući sigurnost poslovanju između stranaka koje nemaju međusobno povjerenje. Ovi ugovori imaju potencijal značajno unaprijediti efikasnost i sigurnost financijskih transakcija. U sljedećim poglavljima rada detaljnije će se razmotriti primjena blockchain tehnologije u različitim segmentima financijskog sektora. Također će se istražiti regulativna pitanja i zakonodavni izazovi vezani uz primjenu blockchaina u financijskom sektoru.

2. Metode i tehnike rada

Proučavanjem blockchain tehnologije u financijskom sektoru, odnosno temeljem istraživanja i pregleda literature, čitatelju je pojašnjen koncept blockchaina, pametnih ugovora i decentraliziranih aplikacija. Pomoću alata Canva izrađeni su različiti dijagrami i vlastite ilustracije temeljene na originalnim slikama (Canva, 2024).

Za izradu teorijskog dijela završnog rada korišteni su sekundarni izvori. To je uključivalo odabrane stručne knjige, znanstvene i stručne članke s interneta, publikacije te web stranice platformi i poduzeća. Korištene su metode dedukcije, analize i opisne metode za definiranje i objašnjavanje tehnologije blockchaina, pametnih ugovora te svih platformi koje funkcioniraju na principu blockchain tehnologije korištene u financijskom sektoru.

Tehnologije su istražene u kontekstu primjene u različitim poduzećima i bankama. Korištenje blockchaina u financijskom sektoru istraženo je na primjerima poduzeća, dok su pametni ugovori i decentralizirane aplikacije analizirani kroz primjere platformi. Rezultati istraživanja pokazali su kako ove tehnologije doprinose učinkovitosti, sigurnosti i transparentnosti u financijskim transakcijama, smanjuju operativne troškove te unapređuju povjerenje u financijske institucije.

3. Blockchain tehnologija

Blockchain je decentralizirana i distribuirana digitalna knjiga koja se koristi za bilježenje transakcija i pohranu podataka na siguran i otporan način. Izvorno je dizajnirana za podršku digitalnoj valuti, Bitcoinu, ali je od tada evoluirala i koristi se u raznim aplikacijama (Laurence, 2019).

U svojoj osnovi, blockchain se sastoji od lanca blokova, pri čemu svaki blok sadrži skup transakcija ili podataka.

Ovi blokovi su međusobno povezani kronološkim redoslijedom, tvoreći digitalnu knjigu koja je distribuirana preko mreže računala (Bitstore.net, 2022). Sve informacije u digitalnoj knjizi su kronološki poredane i zaštićene kriptografijom .

Budući da je tehnologija zaživjela s pokretanjem Bitcoina, mnogi će se referentni izvori u ovom dijelu fokusirati na način rada Bitcoina kako biste razumjeli osnove (Plavljanić, 2024). Međutim, mnogo toga se dogodilo u međuvremenu, pa ćemo još istražiti Ethereum i druge vrste mreža koje trenutno postoje u današnjem svijetu ICT-a.

3.1. Definiranje osnovnih pojmova

Ključne značajke blockchain tehnologije su:

1. Decentralizacija: Umjesto da se pohranjuje na centraliziranom mjestu, blockchain je pohranjen na mreži računala, čime postaje sigurniji i otporniji na neovlaštene izmjene (Nožinić, 2022).
2. Transparentnost: Sve transakcije na blockchainu su vidljive svim sudionicima, čime sustav postaje transparentniji i odgovorniji (ne nužno sve, danas postoje i privatni blockchains, poput Calimero Network (Calimero, 2024)) (Bitstore.net, 2022).
3. Sigurnost: Svaki blok je osiguran kriptografijom, što čini izuzetno teško za hakere da manipuliraju podacima pohranjenim na blockchainu (Bitstore.net, 2022).
4. Neizmjenjivost: Kada se blok doda u lanac, ne može se mijenjati ili brisati, što čini blockchain pouzdanim izvorom informacija (Nožinić, 2022).

Blockchain tehnologija ima brojne primjene, kao što su upravljanje lancem opskrbe, zdravstvo, glasanje i financijske usluge. Ima potencijal revolucionirati način na koji pohranjujemo i razmjenjujemo informacije, čineći naše transakcije sigurnijima i učinkovitijima. Tehnologija se u biti temelji na "lancu digitalnih potpisa.

Svaki vlasnik prenosi coin sljedećem tako što digitalno potpisuje hash prethodne transakcije i javni ključ sljedećeg vlasnika te dodaje to na kraj coina. Primatelj može provjeriti potpise kako bi potvrdio lanac vlasništva" (Arunović, 2018).

3.1.1. Privatni i javni ključevi

Javni i privatni ključevi su u osnovi sredstva za osiguranje enkripcije. Enkripcija je proces uzimanja poruke i izmjene sadržaja poruke tako da je samo određeni pojedinci mogu pročitati. U kontekstu digitalne komunikacije, javni i privatni ključevi se koriste na sličan način kako bi se osigurala sigurnost poruka poslanih putem interneta.

Javni ključ se koristi za enkripciju poruka koje se šalju vama, dok se vaš privatni ključ koristi za dekriptiranje tih poruka i njihovo čitanje. Postoje dvije vrste enkripcije: simetrična i asimetrična. Bitcoin i druge kriptovalute oslanjaju se na asimetričnu kriptografiju (RapidSSLonline, 2022).

Objasnimo enkripciju na vrlo osnovnom primjeru, a potom ćemo se proširiti na asimetričnu enkripciju: zamislite da imate poštanski sandučić na kraju prilaza. Koristite taj sandučić za primanje pošte iz različitih izvora, poput prijatelja, obitelji i računa od komunalnih poduzeća.

Kako biste osigurali sigurnost svoje pošte, imate dva ključa: javni ključ i privatni ključ. Vaš javni ključ je poput adrese na vašem poštanskom sandučiću - svatko ga može koristiti kako bi vam poslao poštu (Kriptomat.cash, 2020). Svoj javni ključ slobodno možete dati bilo kome tko vam želi poslati poštu. U kontekstu poštanskog sandučića, to bi bilo kao davanje vaše adrese i broja poštanskog sandučića nekome tko vam želi poslati pismo. Pismo bi bilo transakcija.

S druge strane, vaš privatni ključ je poput ključa koji otključava vaš poštanski sandučić. Vi ste jedina osoba koja ima pristup vašem privatnom ključu, i trebate ga koristiti kako biste otvorili poštanski sandučić i pristupili svojoj pošti (Kriptomat.cash, 2020).

U kontekstu poštanskog sandučića, to bi bilo kao fizički ključ kojim otvarate svoj poštanski sandučić i preuzimate poštu.

Kada vam netko želi poslati pismo, kao na slici 1, koristi vaš javni ključ (vašu adresu i broj poštanskog sandučića) kako bi adresirao omotnicu i poslao je vama. Kada poštar dostavi poštu u vaš poštanski sandučić, ona je sigurno zaključana unutra. Da biste preuzeli svoju poštu, trebate koristiti svoj privatni ključ (svoj fizički ključ) kako biste otključali poštanski sandučić i pristupili sadržaju unutra.

Slika 1.Primjer privatnog i javnog ključa (Izvor: (RapidSSLonline, 2022)

U nastavku ću navesti još jedan primjer kako bi bolje razumjeli odnos javnog i privatnog ključa.

Recimo da želite šifrirati radne dokumente koje pokušavate poslati svojim kolegama putem interneta. Napravili ste dokument u Google Docs i dodali lozinku koja otključava dokument kako biste omogućili samo određenim osobama u vašoj tvrtki da ga pročitaju. Na taj način te osobe trebaju lozinku kako bi mogle otvoriti dokument.

Da biste poslali lozinku, morali biste je zapisati na papir ili poslati u tekstualnoj poruci ili e-mailu. Što ako netko ukrade vaš telefon, provali u vaš e-mail ili izgubite papir? Nastao bi veliki problem, ali zato postoji asimetrična enkripcija (Kriptomat.cash, 2020).

U asimetričnoj enkripciji, obje strane trebaju generirati par ključeva (nazovimo ih g. Ivan i gđa. Ana). Iako su ključevi povezani, ne mogu se izvesti jedan iz drugog.

Drugim riječima, ako znate nečiji javni ključ, ne možete iz njega izvesti privatni ključ (RapidSSLonline, 2022).

Da bi sigurno komunicirali, g. Ivan i gđa. Ana trebaju razmijeniti svoje javne ključeve. Sada, recimo da g. Ivan želi poslati šifrirani (zaključani) dokument i želi biti siguran da ga samo gđa. Ana i SAMO gđa. Ana može pročitati. G. Ivan šifrira ili zaključava dokument koristeći javni ključ gđe. Ane (jer je gđa. Ana već ranije podijelila svoj javni ključ s g. Ivanom). G. Ivan zatim šalje dokument gđi. Ani koja koristi svoj privatni ključ da otključa dokument i pročita ga. U ovom trenutku znamo da SAMO gđa. Ana ima privatni ključ koji može dešifrirati ili otključati dokument jer je gđa. Ana jedina osoba koja posjeduje par ključeva koji mogu otključati javni ključ koji je gđa. Ana podijelila (i korišten je za zaključavanje poruke u ovom primjeru). Čak ni g. Ivan, koji je prvotno šifrirao dokument, ne može ga otključati jer je g. Ivan samo imao javni ključ gđe. Ane. Jedini način na koji bi g. Ivan i ostatak svijeta mogli otključati ili dešifrirati dokument bio

bi da je gđa. Ana jako loše čuvala svoj privatni ključ u tajnosti. Na primjer, ako je bila prisiljena podijeliti svoj privatni ključ.

Postoji mnogo matematičkih algoritama dostupnih za generiranje javnih i privatnih ključeva. Evo tri popularna i cijenjena algoritma:

1. Digital Signature Standard (DSS): Ovaj algoritam je Federalni standard za obradu informacija koji specificira algoritme koji se mogu koristiti za generiranje digitalnih potpisa koje koristi Nacionalni institut za standarde i tehnologiju (NIST) (GeeksForGeeks, 2024).
2. Kriptografija eliptičke krivulje (ECC): Algoritam ECC koristi eliptičke krivulje za generiranje ključeva i obično se koristi za digitalne potpise i dogovaranje ključeva (EITCA, 2023).
3. Rivest-Shamir-Adleman (RSA): Ovaj algoritam je najstariji od sustava kriptografije s javnim i privatnim ključem. Često se koristi za prijenos zajedničkih ključeva za simetričnu kriptografiju. RSA je cijenjen zbog teškoće pronalaženja prostih faktora kompozitnog broja (Simplilearn, 2024).

3.1.2. Digitalni potpis

Digitalni potpisi su kriptografska tehnika koja se koristi za provjeru autentičnosti i integriteta digitalnih dokumenata i transakcija. Oni osiguravaju siguran i pouzdan način da se potvrdi da informacije koje se prenose nisu izmijenjene ili na bilo koji način manipulirane.

U shemi digitalnog potpisa s jednim potpisom (eng. singlesig), potreban je samo jedan ključ za potpisivanje transakcije ili dokumenta. Vlasnik privatnog ključa potpisuje dokument, a primatelj koristi odgovarajući javni ključ za provjeru potpisa (Microsoft, 2024). Ovo je slično potpisivanju fizičkog dokumenta olovkom, ali potpis je jedinstven za pojedinca i pruža dokaz identiteta i namjere.

Višestruki potpis (eng. multisig) je digitalna shema potpisa koja zahtijeva da više strana potpiše transakciju ili dokument prije nego što se može izvršiti. Ovo pruža dodatni sloj sigurnosti i može biti korisno u situacijama gdje je potrebno da se više strana složi oko određene radnje, kao što je korporativno donošenje odluka ili velike financijske transakcije (Microsoft, 2024). Na primjer, multisig shema 2-od-3 zahtijevala bi odobrenje bilo koje dvije od tri uključene strane za potpisivanje i izvršenje transakcije. To znači da čak i ako je jedan od privatnih ključeva ugrožen, transakcija se ne može izvršiti bez odobrenja druge dvije strane. Sličan primjer u stvarnom svijetu su notarske usluge. Ako potpišete fizički dokument olovkom, ali ga ne ovjerite kod javnog bilježnika, nećete ga moći koristiti kao dokaz na sudu. Multisig

sheme se također mogu koristiti za stvaranje složenijih struktura odobrenja, kao što je shema 2-od-2 gdje dvije osobe moraju odobriti transakciju, ili shema 3-od-5 gdje tri od pet osoba moraju odobriti.

Za kreiranje digitalnog potpisa potreban vam je certifikat za potpisivanje koji potvrđuje vaš identitet. Kada šaljete digitalno potpisanu makronaredbu ili dokument, šaljete i certifikat te javni ključ. Certifikate izdaju certifikacijske ustanove, a poput vozačke dozvole, certifikat može biti opozvan. Certifikat je obično valjan godinu dana, nakon čega potpisnik mora obnoviti certifikat ili dobiti novi kako bi potvrdio svoj identitet (Microsoft, 2024). Certifikacijska ustanova (Certificate Authority, CA) je entitet sličan javnom bilježniku. Ona izdaje digitalne certifikate, potpisuje ih kako bi potvrdila njihovu autentičnost te vodi evidenciju o opozvanim certifikatima i onima čija je valjanost istekla (Svijet-kvalitete, 2012).

3.2. Vrste blockchaina

U prethodnom dijelu ovog poglavlja mogli smo zaključiti da mnogo čimbenika čini blockchain. Kada bi se fokusirali na vrste blockchaina, uočavamo nekoliko njih. Iako posjeduju različite karakteristike, često imaju i sličnosti. Razlikujemo: javni blockchain, privatni blockchain i hibridni blockchain. U nastavku ćemo se ukratko objasniti svaki od njih.

A. Javni blockchain

Jedna od ključnih karakteristika javne blockchain mreže je ta da se svaki sudionik može pridružiti bilo kada. Ova vrsta blockchain mreže nema ograničenja kada je riječ o sudjelovanju. Također, svi mogu vidjeti kreirane blokove i obavljene kriptirane transakcije.

Glavne prednosti javnog blockchaina su: transparentnost, potpuna decentralizacija i nepromjenjivost. Posebno zanimljiv aspekt blockchain tehnologije je taj da nudi visoku razinu transparentnosti dok je identitet korisnika skriven, prepoznatljiv samo po javnoj adresi korisnika (Filipovic, 2020). Blockchain omogućuje mnogim računalima sudjelovanje u mreži dijeljenjem računalne moći. Na primjer, Amazon kupuje i održava privatni skup računala za AWS (Amazon Web Services) (Service, 2024) (GeeksForGeeks.org, 2023). Nasuprot tome, blockchain omogućuje gotovo svakome da "posudi" svoje računalo mreži i tako je održava aktivnom. Decentralizacija smanjuje rizik od neovlaštenih modifikacija, prijevara i kibernetičkog kriminala. Nepromjenjivost se smatra jednom od najvećih prednosti jer, jednom kada je transakcija odobrena i podijeljena na distribuiranoj mreži, nemoguće ju je poništiti ili promijeniti njen sadržaj.

B. Privatni blockchain

Za razliku od javnog blockchaina, privatni blockchain ima ograničenja u pogledu sudionika na mreži i validatora transakcija. Svaki sudionik privatne blockchain mreže mora biti pozvan od strane administratora. Privatni blockchain se može smatrati kao platforma koju koriste ljudi zainteresirani za prednosti koje nudi blockchain tehnologija, ali koji žele zadržati veću razinu kontrole nego što to omogućava javna blockchain mreža (Filipovic, 2020).

On omogućuje implementaciju tehnologije za računovodstvene i evidencijske postupke unutar organizacije bez ugrožavanja autonomije ili izlaganja određenih podataka javnosti. Osnovne prednosti privatnog blockchaina uključuju niske provizije, mogućnost regulacije i sprječavanje ilegalnih aktivnosti. Budući da svaka transakcija na blockchainu zahtijeva određenu vrstu "provizije", privatni blockchain nudi znatno niže provizije za prijenos raznih vrsta transakcija. Ova karakteristika čini ga posebno atraktivnim za mnoge tvrtke.

S obzirom na to da je privatni blockchain pod kontrolom administratora, moguće je postaviti interna pravila koja se moraju poštovati kako bi sustav bio održiv i uređen (Filipovic, 2020). Nepoštivanje tih pravila znači da transakcije i prijenosi vlasništva neće biti mogući. Za razliku od javnog blockchaina, gdje ne postoji regulatorno tijelo, na privatnom blockchainu jasno se može prepoznati pokušaj ilegalnih radnji, a problem se može brzo identificirati i riješiti.

C. Hibridni (konzorcijski) blockchain

Konzorcijski blockchain je oblik blockchain mreže koji kombinira elemente javnog i privatnog blockchaina. U ovom modelu, sudionici na mreži nisu otvoreni za javnost kao kod javnog blockchaina, ali nisu ni potpuno zatvoreni kao kod privatnog blockchaina. Umjesto toga, sudionici su ograničeni na odabrani skup organizacija ili entiteta koji čine konzorcij ili partnerstvo (GeeksForGeeks.org, 2023).

Glavna obilježja konzorcijskog blockchaina uključuju:

- Ograničeni pristup: Sudionici na mreži su ograničeni na odabrane organizacije ili entitete koji su dio konzorcija ili partnerstva. To znači da samo odobrene strane imaju pristup mreži.
- Dijeljena kontrola: Kontrola nad mrežom dijele sudionici konzorcija. Ovo omogućuje veću kontrolu nad mrežom u usporedbi s javnim blockchainom, ali manju centralizaciju u usporedbi s privatnim blockchainom.
- Višestruki validatori: Transakcije se verificiraju putem više čvorova u mreži, što osigurava veću sigurnost i integritet u odnosu na privatni blockchain.
- Veća efikasnost i skalabilnost: Budući da su sudionici unaprijed poznati i surađuju u konzorciju, može se postići veća efikasnost i skalabilnost u usporedbi s javnim blockchainom.

- Pouzdanost i transparentnost: Konzorcijski blockchain osigurava visoku razinu pouzdanosti i transparentnosti jer su transakcije transparentne za sve sudionike u konzorciju, dok se istovremeno osigurava privatnost informacija za vanjske strane.

Primjene konzorcijskog blockchaina uključuju upotrebu u financijskom sektoru, logistici, lancu opskrbe, zdravstvu i drugim sektorima gdje postoji potreba za dijeljenjem podataka i procesa između odabranih organizacija ili entiteta.

3.3. Kreiranje blokova i hash-evi

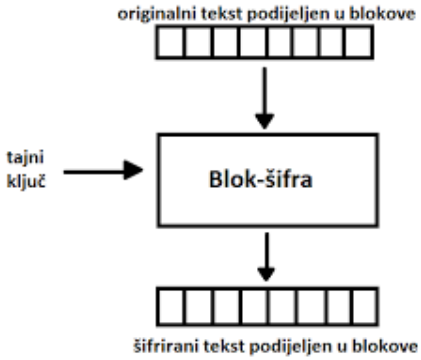
Kriptografska hash funkcija je matematički algoritam koji prima podatke bilo koje veličine i vraća vrijednost fiksne veličine. U osnovi, to je proces pretvaranja ulaza bilo koje duljine u niz teksta fiksne veličine korištenjem matematičkih funkcija. Poruka koja se treba “hash-irati“ naziva se ulaz, algoritam koji to radi naziva se hash funkcija, a izlaz se naziva hash vrijednost. Kriptografske hash funkcije imaju svojstvo da čak i mala promjena u ulaznim podacima rezultira znatno različitom izlaznom hash vrijednošću.

To znači da bi trebalo biti nemoguće proizvesti istu hash vrijednost ulazeći različite ulaze i stoga bi ista poruka uvijek trebala proizvesti istu hash vrijednost. Neke uobičajene kriptografske hash funkcije uključuju SHA-256, SHA-3 i MD5 (Cvijović-Gorša, 2023).

U blockchainu, hashovi se koriste za predstavljanje trenutnog stanja blockchaina i osiguravanje njegove nepromjenjivosti. Svaka transakcija sadrži određene informacije o sebi, poput iznosa, adresa ili vremenskih oznaka. Sve te informacije kombiniraju se u formulu koja proizvodi hash funkciju. Ta hash funkcija naziva se ID transakcije. To je potvrda da se transakcija dogodila na blockchainu. Zamislite to kao račun koji potvrđuje da ste kupili laptop.

Ako pokušavate izaći iz trgovine, a netko vas optužuje da ste ukrali laptop, uvijek možete izvući račun koji potvrđuje vašu transakciju.

U osnovi, koristite privatni ključ kako biste potpisali transakciju koja sadrži javni ključ sljedećeg vlasnika. Možete koristiti javni ključ u prethodnom bloku kako biste provjerili da je transakcija koju promatrate zapravo potpisana određenim privatnim ključem (RapidSSLonline, 2022).



Slika 2.Primjer korištenja hash funkcije (Izvor: Cvijović-Gorša, 2023)

U blockchainu, transakcije se "paketiraju" i slažu zajedno u blokove. Sve transakcije u jednom bloku se kombiniraju i proizvode hash. Kada se stvara sljedeći blok, hash iz prethodnog bloka se dodaje svim novim transakcijama u novom bloku, a novi blok proizvodi novi jedinstveni hash na temelju tih novih transakcija, gdje je "stari" hash uključen. Ovaj proces, na slici 2, se ponavlja iznova i iznova, svaki put kada se novi blok doda u lanac. Blokovi se istovremeno ažuriraju na svim računalima u mreži. Svaka promjena na blockchainu zahtijeva odobrenje većine korisnika mreže. Trenutni potencijalni rizik je tzv. 51% napad - ako jedna strana preuzme većinu hash stope blockchaina - to bi omogućilo "upravljanje" mrežom i manipulaciju podacima. Da bi promijenili stanje svakog bloka i njegove hashe, napadač bi morao imati ogromnu računalnu moć za izmjenu zapisa na blockchainu. To ih čini korisnima za osiguravanje integriteta podataka i otkrivanje bilo kakvih manipulacija podacima. Također je izuzetno teško odrediti ulaz, na temelju hash vrijednosti.

Da bismo lakše shvatili kako se blokovi povezuju u blockchain, možemo upotrijebiti analogiju s numeriranim stranicama u knjizi. Zamislite da su blokovi kao stranice u knjizi, svaki s vlastitim brojem ili indeksom. Svaki blok također sadrži referencu na prethodni blok, poput veze između stranica u knjizi. Ova numeracija omogućuje nam da održimo redoslijed blokova. Ako bi se blokovi izmiješali ili izgubili, mogli bismo ih ponovno složiti koristeći brojeve i veze s prethodnim blokovima (Cvijović-Gorša, 2023). Osim toga, svaki blok ima hash vrijednost koja funkcionira kao pečat koji potvrđuje integritet podataka. Ako bi netko pokušao promijeniti podatke u bloku, to bi rezultiralo promjenom hash vrijednosti tog bloka i svih budućih blokova u lancu. To bi odmah upozorilo ostale sudionike u mreži na pokušaj manipulacije podacima (Arunović, 2018).

Dakle, blockchain nam omogućuje da pratimo redoslijed i integritet podataka koristeći jednostavnu strukturu blokova i referenci između njih. Ova tehnologija omogućuje nam da pouzdano pratimo transakcije i osiguramo njihovu autentičnost, što je ključno za funkcioniranje financijskih sustava i drugih aplikacija koje se oslanjaju na pouzdane evidencije.

Korištenje tehnologije lanca blokova i interakcija s njom zahtijevaju od korisnika određenu razinu poznavanja tehnologije. Ovo može predstavljati izazov za mnoge ljude, jer iako je digitalna pismenost sve raširenija među mlađim i starijim generacijama, još uvijek postoji velik broj ljudi koji nisu dovoljno upoznati s ovim konceptom da bi ga brzo i intuitivno usvojili (Laurence, 2019).

Decentralizirane aplikacije su razvijene s ciljem da budu pristupačne i korisne svima, ne samo stručnjacima. Ovo je ključno za širenje uporabe tehnologije lanca blokova u širem ekonomskom kontekstu. Za uspješno uključivanje blockchain tehnologije u svakodnevni život, ključno je olakšati pristup i upotrebljivost aplikacija zasnovanih na ovoj tehnologiji, čineći ih jednostavnijima za korištenje i razumijevanje za širu populaciju.

3.4. Decentralizirane aplikacije

Decentralizirane aplikacije (eng. dapps) donose novi model digitalne ekonomije koja se temelji na peer-to-peer uslugama. Iako su centralizirane aplikacije poput Facebooka ili Netflixa postale neizostavni dio našeg svakodnevnog života, decentralizirane aplikacije pružaju rješenja koja ciljaju povećanje korisničke autonomije i privatnosti.

Na prvi pogled, decentralizirana aplikacija djeluje slično kao bilo koja druga digitalna aplikacija koju možemo koristiti na pametnom telefonu ili računalu, ali s jednom bitnom razlikom – koristi blockchain tehnologiju za pohranu podataka, čime se izbjegava centralizirana kontrola nad korisničkim informacijama. Kao što su kripto valute poput Bitcoina i Ethereuma decentralizirani oblici novca, tako i decentralizirane aplikacije predstavljaju decentralizirani način interakcije s aplikacijama i uslugama (Milosns.eth, 2022).

Ove vrste aplikacija omogućuju novi način upravljanja osobnim financijama, zaobilazeći posrednike poput banaka ili financijskih institucija. Tradicionalno, financijske aktivnosti poput posuđivanja novca, štednje ili ulaganja ovise o središnjim tijelima koja upravljaju tim procesima. S pojavom decentraliziranih financija (eng. DeFi), ove funkcije sada se mogu obavljati putem blockchaina, pružajući korisnicima veću kontrolu i sigurnost. Kripto valute, kao što su Bitcoin i Ethereum, otvorile su put za ovaj novi način poslovanja, omogućujući financijske transakcije bez posrednika i na globalnoj razini.

Standardna web aplikacija, npr. Instagram, radi na računalnom sustavu u vlasništvu i pod upravom organizacije koja ima potpunu kontrolu nad aplikacijom i njezinim radom. Na web mjestu može biti više korisnika, ali pozadinu kontrolira jedna organizacija. Decentralizirana aplikacija može raditi na P2P mreži ili blockchain mreži (Milosns.eth, 2022).

3.5. Algoritmi Proof of Work

Proof of Work (eng. PoW) i Proof of Stake (eng. PoS) su dva glavna algoritma konsenzusa koja se koriste u blockchain tehnologiji. Proof of Work je stariji i koristi se u Bitcoin mreži, gdje rudari natječu u rješavanju složenih matematičkih problema kako bi potvrdili transakcije i dodali ih u blockchain. Ovaj proces zahtijeva značajnu količinu energije i računalnih resursa. S druge strane, Proof of Stake je energetski učinkovitiji i koristi se u mrežama poput Ethereum 2.0. U PoS sustavu, validatori su odabrani na temelju količine kriptovalute koju "stakeaju" ili zaključavaju kao zalog, čime se smanjuje potreba za intenzivnim rudarenjem.

3.5.1. Algoritam Proof of Work

Proof of Work (eng. PoW) je algoritam konsenzusa koji se koristi u blockchain mrežama za validaciju transakcija i stvaranje novih blokova. Ovaj algoritam temelji se na računalnoj zagonetki koju rudari moraju riješiti kako bi potvrdili transakcije i kreirali nove blokove (Curry, 2024). U PoW sustavu, rudari se natječu u rješavanju složenih matematičkih problema koristeći računalnu snagu. Prvi rudar koji riješi problem nagrađuje se kriptovalutom i dobiva pravo na validaciju transakcija te stvaranje novog bloka. Kako bi riješili problem, rudari koriste računalnu snagu za izvođenje računskih operacija koje su resursno intenzivne i zahtijevaju značajnu količinu električne energije. Težina problema se prilagođava kako bi se održala konstantna stopa stvaranja blokova, obično svakih 10 minuta.

Jedna od glavnih prednosti PoW-a je ta što je provjerena i sigurna metoda za validaciju transakcija i stvaranje novih blokova. Budući da je računalna zagonetka izazovna za rješavanje, napadačima je teško promijeniti povijest blockchaina bez značajne računalne snage. Još jedna prednost PoW-a je njegova decentraliziranost, jer bilo tko s dovoljno računalne snage može sudjelovati u rudarenju. To otežava jednoj osobi ili entitetu da kontrolira mrežu, čineći je manje podložnom centralizaciji u usporedbi s drugim algoritmima konsenzusa (Nevile, 2024).

Međutim, PoW ima i nekoliko nedostataka. Jedna od glavnih briga vezanih uz PoW je njegova potrošnja energije, koja je znatna zbog količine električne energije potrebne za rješavanje računalnih zagonetki. Proces rudarenja troši veliku količinu energije, što doprinosi ugljičnom otisku i utjecaju na okoliš blockchain mreža. Također, PoW je podložan napadu od 51%, gdje napadač kontrolira više od 50% računalne snage mreže (Nevile, 2024). S tom kontrolom, napadač može manipulirati transakcijama i kreirati nove blokove, što može dovesti do dvostruke potrošnje i drugih napada na mrežu. Još jedan nedostatak PoW-a je taj što je teško skalirati sustav jer se potrebna računalna snaga za rudarenje i validaciju transakcija

povećava s vremenom. Kako mreža raste, postaje sve izazovnije i skuplje sudjelovati u procesu rudarenja, što može dovesti do centralizacije i smanjenja ukupne sigurnosti mreže (Curry, 2024).

3.5.2. Algoritam Proof of Stake

Proof of Stake (eng. PoS) je algoritam konsenzusa koji se koristi u blockchain mrežama za validaciju transakcija i stvaranje novih blokova. Za razliku od Proof of Work (eng. PoW) koji zahtijeva od rudara da rješavaju složene matematičke probleme kako bi verificirali transakcije i kreirali nove blokove, PoS funkcionira na način da korisnici zaključavaju svoju kriptovalutu kao kolateral kako bi postali validatori (Curry, 2023). Validatori se biraju za validaciju transakcija i stvaranje novih blokova na temelju njihovog udjela, odnosno količine kriptovalute koju su zaključali. Validatori su potaknuti na pošteno ponašanje jer riskiraju gubitak svog udjela ako budu uhvaćeni u varanju, što se naziva "slashing". Proces odabira validatora poznat je kao "staking". Korisnici mogu sudjelovati u stakingu zaključavanjem svoje kriptovalute u namijenjenom novčaniku. Količina kriptovalute potrebna za postajanje validatorom varira ovisno o blockchain mreži, a validatori mogu dobiti nagrade za validaciju transakcija i stvaranje novih blokova, kao što je prikazano na slici 3.

Jedna od prednosti PoS-a u odnosu na PoW je njegova energetska učinkovitost, budući da ne zahtijeva istu količinu računalne snage kao PoW. To smanjuje utjecaj blockchain mreža na okoliš i čini ih dugoročno održivijima. Druga prednost PoS-a je smanjeni rizik od napada od 51%. U PoS-u bi napadač morao posjedovati značajan dio opskrbe kriptovalute kako bi izveo sličan napad, što je manje vjerojatno (Curry, 2023).

Međutim, PoS ima i neke nedostatke. Na primjer, može se pojaviti fenomen "bogati postaju bogatiji" gdje validatori s velikim udjelima imaju veću šansu da budu odabrani za validaciju transakcija i stvaranje novih blokova. To može dovesti do centralizacije moći i smanjenja decentralizacije mreže. Također postoji rizik od problema "ništa na kocki", koji se javlja kada su validatori potaknuti da validiraju više konkurentskih verzija blockchaina kako bi maksimizirali svoje nagrade (Mckinsey&Company, 2023). U PoW-u, ovo nije problem jer rudari moraju odabrati koju verziju blockchaina će ruditi, dok u PoS-u, validatori mogu validirati sve verzije bez ikakvog troška, što može dovesti do potencijalne konfuzije i nestabilnosti u mreži.

Slika 3.Primjer mehanizma Proof of Stake (Izvor prema: (Ledger, 2023))

3.5.3.Ostali tipovi mehanizama konsenzusa

Postoji nekoliko drugih vrsta mehanizama konsenzusa koji se koriste u blockchain mrežama, osim PoW-a i PoS-a. Neki od tih uključuju:

Delegirani Proof of Stake (eng. DPoS): DPoS je varijanta PoS-a gdje vlasnici tokena biraju delegate koji su odgovorni za validaciju transakcija i stvaranje novih blokova. Broj delegata je obično fiksiran, a oni su potaknuti da djeluju pošteno jer mogu izgubiti svoju poziciju ako budu uhvaćeni u varanju.

Proof of Authority (eng. PoA): PoA je mehanizam konsenzusa koji se koristi u privatnim blockchain mrežama. U PoA, čvorovi su identificirani i pouzdani, a grupa autoriziranih čvorova odgovorna je za validaciju transakcija i stvaranje novih blokova.

3.5.4.Usporedba algoritama Proof-of-wok i proof-of-stake

Proof of Work (eng. PoW) i Proof of Stake (eng. PoS) su dva najpoznatija mehanizma konsenzusa u blockchain tehnologiji, ali se razlikuju po načinu na koji osiguravaju mrežu i validiraju transakcije.

Proof of Work (eng. PoW) je stariji i tradicionalniji mehanizam, koji se koristi u mrežama kao što je Bitcoin. U PoW-u, rudari koriste veliku računalnu snagu kako bi rješavali složene matematičke probleme, a prvi koji riješi problem dobiva pravo da dodaje novi blok u blockchain. Proces je vrlo energetski intenzivan i zahtijeva značajnu količinu električne energije, što povećava troškove i stvara ekološke izazove. Također, PoW mreže su potencijalno ranjive na 51% napade, gdje zlonamjerni entitet preuzima kontrolu nad većinom mrežnog računalnog kapaciteta i može manipulirati podacima (Kerner, 2022).

S druge strane, Proof of Stake (eng. PoS) koristi drugačiji pristup. Umjesto rudarima, transakcije verificiraju validatori koji "ulože" ili zaključaju određeni iznos svoje kriptovalute kao kolateral. Što više kriptovalute validator uloži, to su veće šanse da bude odabran za validaciju novog bloka (Kerner, 2022) (Srivastav, 2024). Ovaj proces zahtijeva znatno manje energije jer se ne oslanja na intenzivne računalne operacije, što PoS čini ekološki prihvatljivijim. Međutim, PoS također ima svoje izazove, poput mogućnosti centralizacije moći kod onih koji posjeduju velike količine kriptovalute, te problema "ništa na kocki", gdje validatori mogu pokušati verificirati više verzija blockchaina bez rizika.

Ukratko, dok je PoW dokazano siguran, energetski je neučinkovit i sklon centralizaciji, dok PoS nudi energetsku učinkovitost i smanjen rizik od 51% napada, ali može dovesti do centralizacije bogatstva i drugih izazova, a u tablici 1 vidimo ključne razlike navedenih algoritama.

Tablica 1: Usporedba između Proof of Work (POW) i Proof of Stake (POS) algoritama

Osnova	POW	POS
Čvorovi za validaciju	Rudari	Validatori
Potrošnja energije	Vrlo visoka	Relativno niska
Nagrada	Nagrada za blok	Nagrada za transakcije
Hakiranja	Haker treba 51% računalne snage	Haker treba 51% udjela
Sigurnost	Lakše za hakirati	Teže nego POW

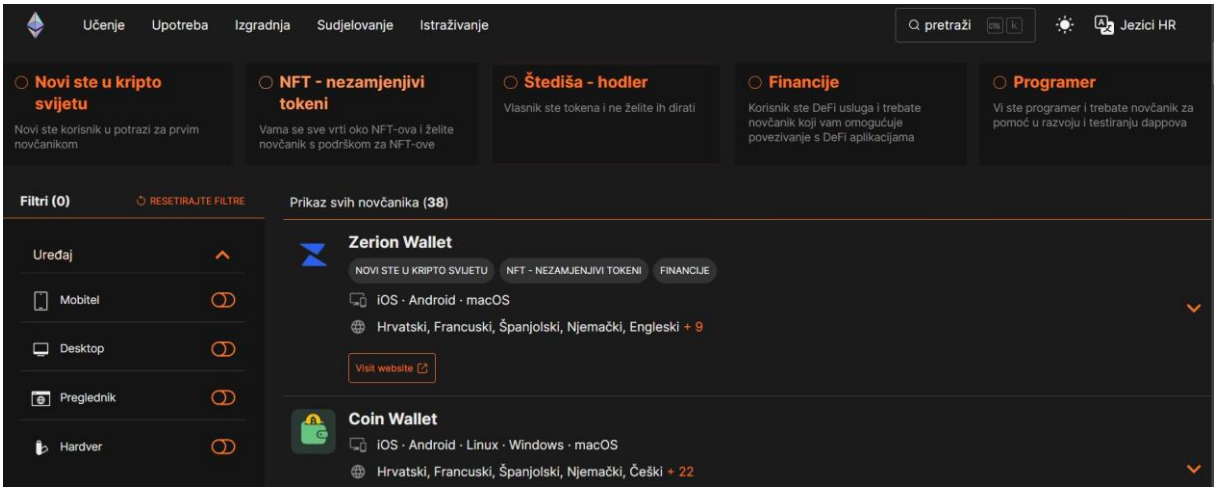
(Izvor prema: (Srivastav, 2024))

4. Ethereum i pametni ugovori

Ethereum je decentralizirana platforma temeljena na blockchainu koja omogućuje stvaranje i izvršavanje pametnih ugovora i decentraliziranih aplikacija (eng. dApps). Prvi ju je predložio 2013. godine Vitalik Buterin, programer i entuzijast blockchaina, a platforma je lansirana 2015. godine (Ethereum, 2024).

Za razliku od Bitcoina, koji se uglavnom koristi kao sustav za elektroničko plaćanje među korisnicima, Ethereum je osmišljen kao decentralizirana platforma za izgradnju širokog spektra aplikacija temeljenih na blockchainu, od financijskih usluga i upravljanja lancem opskrbe do igara i mnogih drugih područja. Ethereum ima svoju vlastitu kriptovalutu nazvanu Ether (eng. ETH), koja se koristi za plaćanje transakcija i računalnih usluga na Ethereum mreži. Također, Ethereum omogućuje razvoj prilagođenih tokena koji se mogu koristiti za predstavljanje imovine ili digitalnih valuta unutar određenih aplikacija (Ethereum, 2024).

Jedna od ključnih značajki Ethereuma je podrška za razvoj pametnih ugovora, koji su samostalno izvršni ugovori s uvjetima dogovora napisanima izravno u kodu. To omogućuje transakcije bez potrebe za povjerenjem banke ili odvjetnike, čineći ih što više pouzdanijima (Adams, 2024). Početnu stranicu platforme Ethereum možemo vidjeti na slici 4.



Slika 4.Prikaz Ethereum platforme (Izvor: (Ethereum, 2024))

4.1. Ether

Kao i svaki složen sustav, Ethereum zahtijeva resurse za svoj rad. Budući da je riječ o distribuiranoj mreži, nema centralnog vlasnika, ali računala, odnosno njeni čvorovi, koji ga održavaju u radu trebaju energiju i druge resurse. Zbog toga je potreban način za nadoknadu tih troškova (Adams, 2024).

Tu stupa na scenu Ether, Ethereumova kriptovaluta. Kada koristite Ethereum za neku aplikaciju ili transakciju, plaća se mala naknada u ETH-u. Ove naknade pokrivaju troškove onih koji održavaju čvorove, poput električne energije i hardvera. Također, te naknade djeluju kao poticaj za ljude da pridonose korištenjem svojih računalnih sustava kao čvorova unutar šire Ethereum mreže (Reiff, 2024).

Kada govorimo o cijeni Ethereuma, zapravo govorimo o vrijednosti ETH-a. Ether je sredstvo plaćanja u Ethereum Virtual Machine (eng. EVM) i koristi se za plaćanje sudionicima mreže za njihove troškove (i nešto dodatno) koje preuzimaju osiguravajući blockchain i validirajući transakcije (Adams, 2024).

Ether ima tržišnu vrijednost koja se može provjeriti na bilo kojoj burzi kriptovaluta ili većini financijskih platformi. Često ćete vidjeti naziv Ethereum, iako se zapravo misli na ether, samu valutu. Ether možete koristiti za plaćanje roba ili usluga kod trgovaca i prodavača koji prihvaćaju tu kriptovalutu. Naravno, investitori trguju etherom i radi spekulacija, nastojeći zaraditi novac putem ulaganja. Koriste strategije slične onima na burzi, poput kupnje i držanja, dnevnog trgovanja (kupnja i prodaja ETH-a tijekom dana kako bi se iskoristile kratkoročne promjene cijena), scalping-a (izvršavanje mnogih malih trgovanja kako bi se profitiralo od malih fluktuacija cijena) i arbitraže (iskorištavanje razlika u cijeni između različitih burzi ethera) (Reiff, 2024).

4.2. Pametni ugovori

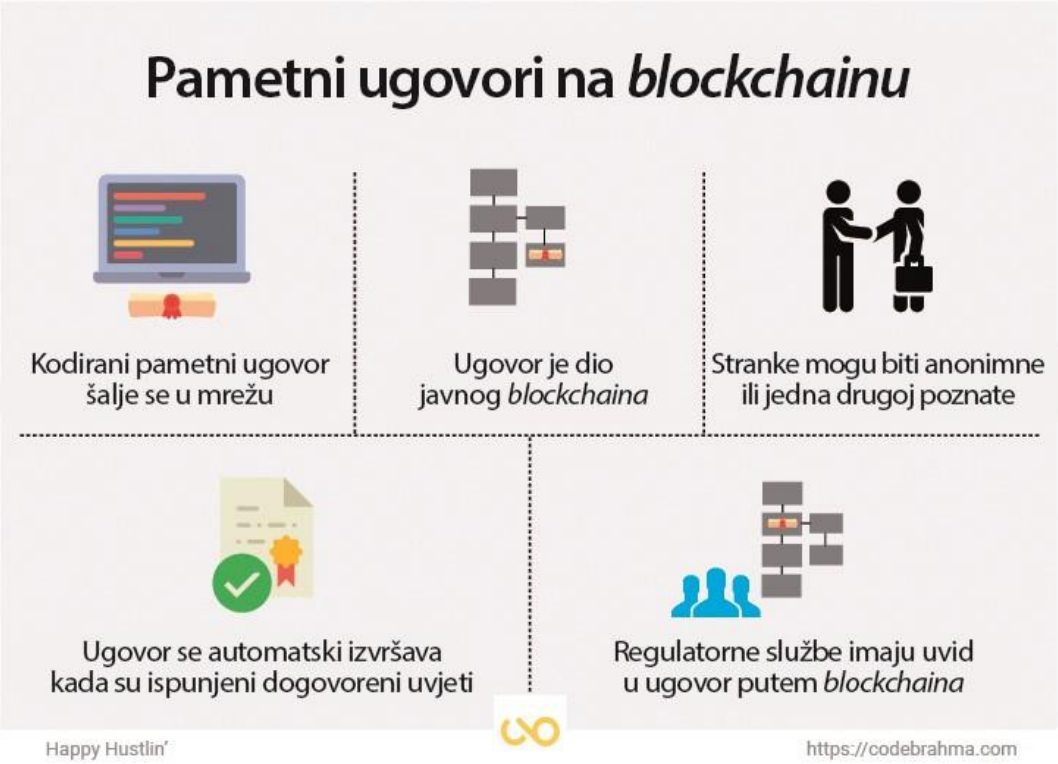
Pametni ugovori su zapravo računalni programi koji kodiraju uvjete ugovora i automatski se izvršavaju kada su određeni uvjeti ispunjeni. Ti uvjeti obično se temelje na unaprijed definiranim pravilima i okidačima, kao što su primanje uplate ili istek vremena. Jednom kada su uvjeti ispunjeni, pametni ugovor automatski izvršava odredbe ugovora, bez potrebe za ljudskom intervencijom (GeeksForGeeks.org, 2024).

Budući da se pametni ugovori izvršavaju na blockchainu, oni su transparentni i otporni na manipulacije, što pomaže u osiguravanju integriteta ugovora. Također su i bez povjerenja, što znači da ne zahtijevaju posrednike poput odvjetnika ili banaka kako bi se potvrdili uvjeti ugovora (Arunović, 2018).

Kako bi se pokrenuo pametni ugovor na Ethereum platformi, potrebno je izvršiti posebnu transakciju koja će uvesti pametni ugovor na blockchain. Tijekom ovog procesa, pametnom ugovoru se dodjeljuje jedinstvena adresa. U ovom slučaju, riječ je o 160-bitnim adresama na koje se ugovor postavlja. Nakon što je pametni ugovor implementiran na blockchain, moguće je slati transakcije koje će se provjeravati putem tog ugovora. Svaki pametni ugovor ima svoju adresu, saldo ugovora, unaprijed definiran kod koji se izvršava prilikom aktivacije ugovora te status ugovora koji pokazuje je li ugovor aktivan ili ne.

Kako bi se pokrenuo pametni ugovor na Ethereum platformi, kao što je prikazano na slici 5, potrebno je izvršiti posebnu transakciju koja će uvesti pametni ugovor na blockchain. Tijekom ovog procesa, pametnom ugovoru se dodjeljuje jedinstvena adresa. U ovom slučaju,

riječ je o 160-bitnim adresama na koje se ugovor postavlja. Nakon što je pametni ugovor implementiran na blockchain, moguće je slati transakcije koje će se provjeravati putem tog ugovora. Svaki pametni ugovor ima svoju adresu, saldo ugovora, unaprijed definiran kod koji se izvršava prilikom aktivacije ugovora te status ugovora koji pokazuje je li ugovor aktivan ili ne (GeeksForGeeks.org, 2024).



Slika 5.Princip rada pametnog ugovora pomoću blockchaina (Izvor: (Arunović, 2018))

Identifikacija sporazuma: Više strana prepoznaje priliku za suradnju i željene ishode, a sporazumi mogu uključivati poslovne procese, razmjene imovine i slično (GeeksForGeeks.org, 2024).

Postavljanje uvjeta: Pametni ugovori mogu biti pokrenuti od strane sudionika ili kada su ispunjeni određeni uvjeti, poput pokazatelja na financijskim tržištima, događaja poput GPS lokacija i slično (GeeksForGeeks.org, 2024).

Programiranje poslovne logike: Računalni program se piše kako bi se automatski izvršio kada su zadani uvjetni parametri ispunjeni (Adams, 2024).

Enkripcija i blockchain tehnologija: Enkripcija omogućuje sigurnu autentifikaciju i prijenos poruka između strana koje su uključene u pametne ugovore (Laurence, 2019).

Izvršenje i obrada: U blockchain sustavu, kada se postigne konsenzus između strana u vezi autentifikacije i verifikacije, tada se kod izvršava, a ishodi se bilježe radi usklađenosti i provjere (Laurence, 2019).

Ažuriranje mreže: Nakon što se pametni ugovori izvrše, svi čvorovi na mreži ažuriraju svoje knjige kako bi odražavali novo stanje. Jednom kada se zapis objavi i verificira na blockchain mreži, više ga nije moguće mijenjati, već se samo dodaju novi zapisi (GeeksForGeeks.org, 2024).

4.2.1. Standardi pametnih ugovora

U Ethereum ekosustavu postoji nekoliko standarda za pametne ugovore, od kojih je svaki dizajniran za određenu svrhu ili primjenu. Slično kao što tradicionalni ugovori pokrivaju različite slučajeve uporabe—na primjer, prodajni ugovor određuje uvjete prodaje različitih dobara ili usluga, a ugovor o zaposlenju definira odnos između zaposlenika i poslodavca—tako i pametni ugovori imaju svoje specifične standarde. Svaki od tih standarda reguliran je različitim skupom pravila i zahtjeva, prilagođenim za specifične funkcionalnosti i svrhe pametnih ugovora.

ERC-20: Standard ERC-20 najšire je korišteni standard pametnih ugovora za kreiranje zamjenjivih tokena na Ethereum mreži. Ovi tokeni su međusobno zamjenjivi i mogu predstavljati sredstva poput kriptovaluta, digitalnih vrijednosnih papira i tokena za korištenje (Crypto.com, 2022).

ERC-721: Standard ERC-721 koristi se za stvaranje nezamjenjivih tokena (NFT-ova) na Ethereum mreži. Ovi tokeni su jedinstveni i ne mogu se međusobno zamijeniti. Obično se koriste za predstavljanje digitalnih sredstava kao što su umjetnička djela, kolekcionarski predmeti i stavke unutar igara.

ERC-1155: Standard ERC-1155 je hibridni standard tokena koji omogućuje kreiranje kako zamjenjivih, tako i nezamjenjivih tokena unutar jednog ugovora. Ovo čini proces učinkovitijim za stvaranje tokena koji se mogu koristiti u igrama i drugim aplikacijama.

ERC-948: Standard ERC-948 koristi se za stvaranje "ERC-20 kompatibilnih" tokena na drugim blockchain mrežama, koji se mogu lako razmjenjivati s Ethereum baziranim ERC-20 tokenima (Crypto.com, 2022).

ERC-4337: Standard ERC-4337 je najnoviji standard lansiran u ožujku 2023. godine. U trenutku pisanja ovog teksta, nije bilo mnogo korisnih resursa za detaljnije informacije o ovom standardu.

Ovo su samo neki od primjera standarda pametnih ugovora koji postoje u Ethereum ekosustavu. Svaki standard ima svoje specifične slučajeve uporabe i prednosti, a programeri mogu odabrati onaj koji najbolje odgovara njihovim potrebama prilikom stvaranja vlastitih pametnih ugovora.

4.3. Platforme za pametne ugovore

Platforme za pametne ugovore su decentralizirane tehnologijske infrastrukture koje omogućuju stvaranje, izvršavanje i upravljanje pametnim ugovorima. Pametni ugovori su programi koji automatski provode uvjete dogovora kada su određeni kriteriji ispunjeni, bez potrebe za posrednicima poput banaka ili pravnika. Ove platforme omogućuju korisnicima i developerima da koriste blockchain tehnologiju za kreiranje aplikacija koje su transparentne, sigurnije i decentralizirane.

Danas postoji mnogo različitih platformi za pametne ugovore, no u ovom radu fokusirat ćemo se na one koje su trenutno najzastupljenije i najčešće spominjane na internetskim izvorima. Uz osnovne informacije o svakoj od tih platformi, prikazat ćemo i njihove specifične karakteristike te dati primjere njihove primjene. Na temelju istraživanja dostupnih online resursa, odlučio sam da ćemo se posebno osvrnuti na platforme Binance Smart Chain (BSC), Cardano i Polkadot, a Ethereum smo već opisali u poglavlju prije.

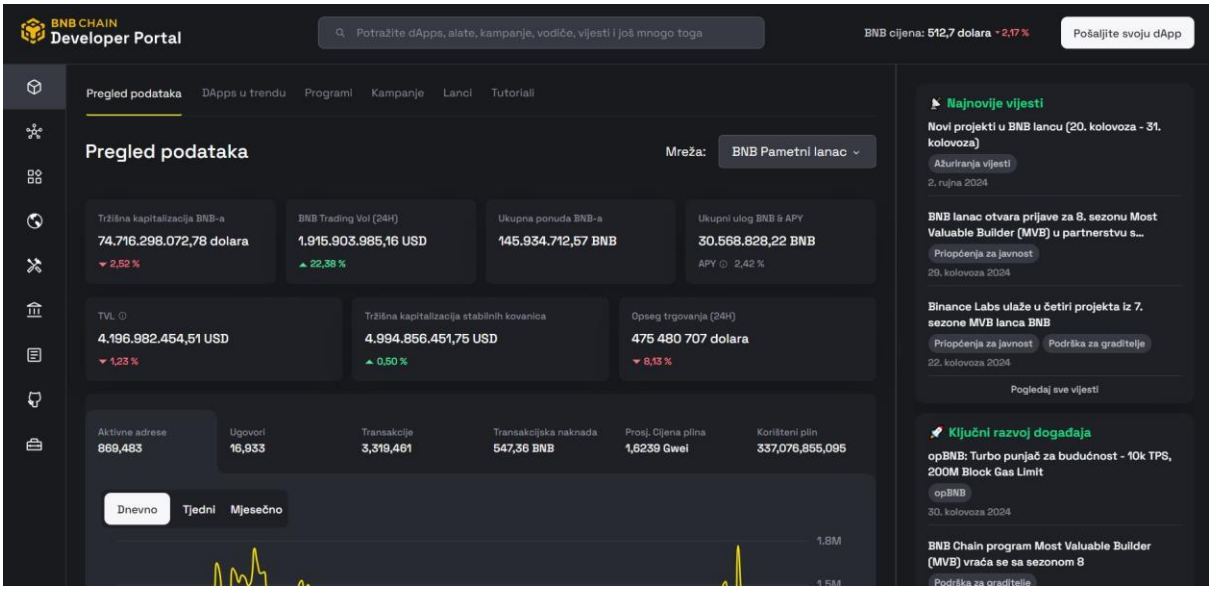
4.3.1. Binance Smart Chain

Binance Smart Chain (eng. BSC) je blockchain mreža koju je pokrenuo Binance u rujnu 2020. godine. Dizajnirana je kao visokoučinkovita blockchain platforma kompatibilna s Ethereum Virtual Machine-om (eng. EVM) te podržava pametne ugovore. Binance Smart Chain temelji se na konsenzusnom mehanizmu Proof of Stake (eng. PoS) i koristi dvo-lančanu arhitekturu koja omogućuje kompatibilnost s Ethereum mrežom uz pružanje bržih transakcijskih brzina i nižih naknada za transakcije (Chain, 2024).

Glavna prednost Binance Smart Chain-a je njegova brza obrada transakcija, s kapacitetom do 100 transakcija po sekundi. Zbog toga je popularan izbor za decentralizirane aplikacije (eng. DApps) koje zahtijevaju visoku brzinu i niske troškove transakcija, poput decentraliziranih burzi (DEX-ova) i gaming platformi. Binance Smart Chain također podržava interoperabilnost između različitih lanaca, što mu omogućuje povezivanje s drugim blockchain mrežama poput Ethereuma i Bitcoina kroz razne protokole za mostove. Ovo korisnicima omogućuje prijenos imovine između različitih mreža i korištenje prednosti obiju blockchain tehnologija.

Za korištenje Binance Smart Chain-a, korisnici mogu stvoriti novčanik kompatibilan s mrežom, kao što su Trust Wallet ili MetaMask, te početi koristiti DApps na platformi. Također mogu koristiti Binance Smart Chain explorer za pregled i praćenje transakcija na mreži (Chain, 2024).

Ukratko, Binance Smart Chain je visokoučinkovita blockchain mreža kompatibilna s Ethereum Virtual Machine-om koja podržava pametne ugovore. Pruža brze transakcijske brzine i niske troškove transakcija, što ga čini popularnim izborom za dApps koji zahtijevaju visoku brzinu i niske troškove transakcija. Binance Smart Chain također podržava interoperabilnost među različitim mrežama, omogućujući korisnicima prijenos imovine između njih (Chain, 2024). Na slici 5 nam je prikazana početna stranica Binance Smart Chain mreže.



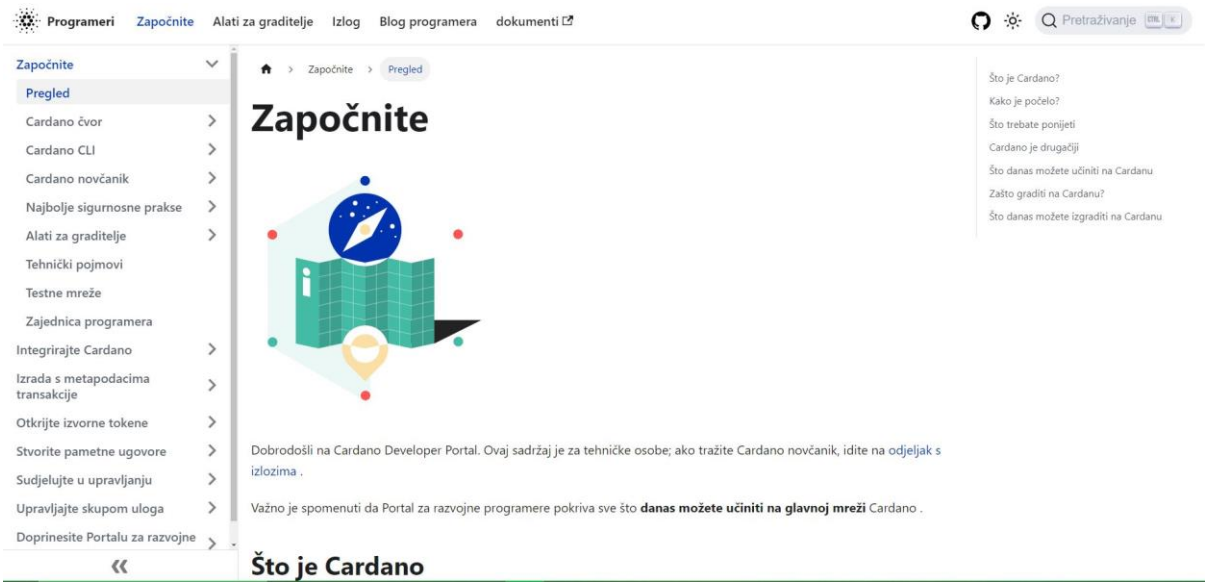
Slika 6.Prikaz Binance Smart Chain mreže (Izvor: (BNB Chain, 2024))

4.3.2.Cardano

Cardano je jedna od najvećih kriptovaluta prema tržišnoj kapitalizaciji. Dizajniran je kao sljedeća generacija razvoja Ethereum ideje, s blockchainom koji je fleksibilan, održiv i skalabilan, omogućujući pokretanje pametnih ugovora. To će omogućiti razvoj širokog spektra decentraliziranih financijskih aplikacija, novih kripto tokena, igara i još mnogo toga.

Slično kao što je ETH osnovna kriptovaluta na Ethereum blockchainu, ADA je osnovna kriptovaluta na Cardano blockchainu — i može se kupovati ili prodavati putem mjenjačnica poput Coinbase-a. Danas se ADA može koristiti za pohranu vrijednosti (možda kao dio vašeg

investicijskog portfelja), za slanje i primanje uplata, te za staking i plaćanje transakcijskih naknada na Cardano mreži (Cardano, 2024), što je i prikazano na slici 7.



Slika 7.Cardano aplikacija (Izvor: (Cardano, 2024))

Na slici 8 vidimo trenutno stanje Cardano kriptovalute, odnosno njezinu vrijednost na datum 20.08.2024.

Slika 8. Sažetak tržišta Cardano – a (Izvor: snimka zaslona 20.08.2024.)

4.3.3.Polkadot

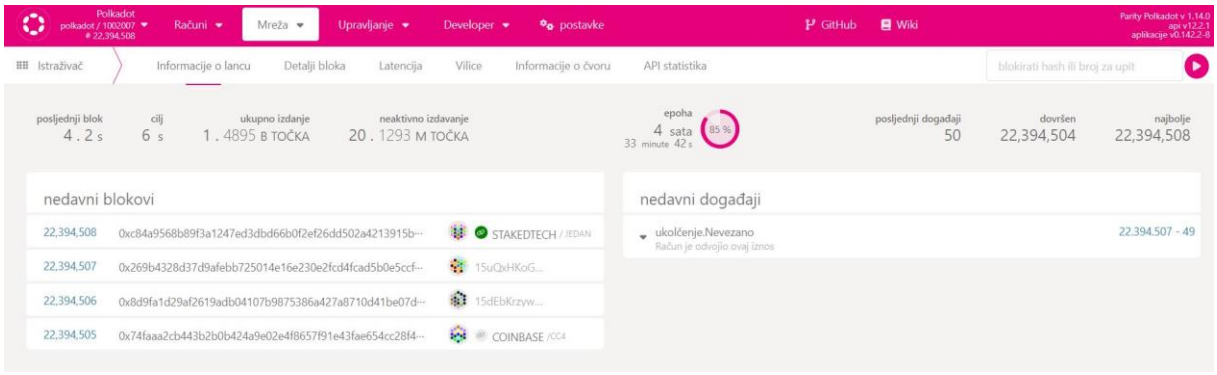
Polkadot je skalabilna, sigurna i decentralizirana mreža s više lanaca, namijenjena razvoju budućeg interneta, izgrađena korištenjem Substrate-a, okvira koji omogućuje stvaranje prilagođenih blockchainova kompatibilnih međusobno, koristeći unaprijed definirane ili prilagođene komponente (Nambiampurath, 2024).

Cilj Polkadot-a je omogućiti potpuno decentraliziran internet gdje korisnici imaju potpunu kontrolu, pružajući protokol koji koristi segmente za skaliranje mreže. Ova mreža može povezivati privatne blockchainove, javne mreže i oracle, olakšavajući novi oblik interneta gdje neovisni blockchainovi mogu sigurno razmjenjivati podatke i transakcije.

DOT je izvorna valuta unutar Polkadot mreže, a njena najmanja jedinica naziva se Planck. DOT omogućuje obavljanje plaćanja, sudjelovanje u upravljanju mrežom, staking, poticanje nagrada, plaćanje transakcijskih naknada, te povezivanje novih blockchainova s Polkadot mrežom ili preuzimanje drugih uloga unutar ekosustava.

Za razliku od mnogih drugih kriptovaluta, DOT nema fiksnu ponudu. Ovaj dizajn osmišljen je kako bi poticao sudjelovanje u mreži i dinamički se prilagođavao stopama sudjelovanja korisnika u stakingu, omogućujući godišnji rast od do 10%. Polkadot omogućuje

prijenos sredstava između digitalnih novčanika koristeći sustav kriptografije javnih i privatnih ključeva, pri čemu javni ključ predstavlja adresu za primanje sredstava, dok privatni ključ služi za autorizaciju i potvrdu transakcija na mreži, što i možemo vidjeti na slici 9. Svakih nekoliko sekundi, transakcije se potvrđuju i dodaju u blok, a niz blokova zajedno čini Polkadot blockchain (Nambiampurath, 2024).



Slika 9. Polkadot (DOT) sustav (Izvor: (Polkadot, 2024))

5. Financijske primjene blockchaina

Blockchain tehnologija donosi značajne promjene u financijskom sektoru kroz niz inovativnih primjena. Jedna od glavnih prednosti je transparentnost i sigurnost transakcija, koje se mogu provoditi bez posrednika poput banaka. Blockchain se koristi za brze međunarodne prijenose novca, smanjujući troškove i vrijeme obrade transakcija. Također omogućuje kreiranje pametnih ugovora, koji automatski izvršavaju uvjete ugovora bez potrebe za trećom stranom. U područjima poput osiguranja, kreditiranja i tržišta kapitala, blockchain donosi veću učinkovitost, smanjenje rizika od prijevara te povećava povjerenje korisnika u financijske institucije.

5.1. Token i novčići

Tokeni i novčići (eng. Coins) su dvije različite vrste digitalnih sredstava koje se često koriste u svijetu kriptovaluta. Iako imaju određene sličnosti, postoje i važne razlike između njih. Novčić je jedinica digitalne valute koja funkcionira samostalno na vlastitom blockchainu. Primjeri novčić uključuju Bitcoin, Litecoin i Ethereum. Coins imaju svoju vlastitu kriptovalutu i prvenstveno se koriste kao sredstvo plaćanja i čuvanja vrijednosti (Coinbase, 2024).

Tokeni, s druge strane, stvaraju se i postoje na vrhu postojećeg blockchaina, poput Ethereuma ili Binance Smart Chain-a. Tokeni se obično kreiraju kako bi predstavljali određenu imovinu ili uslugu, poput dionica tvrtke ili pristupa određenoj usluzi. Mogu se koristiti u različite svrhe, kao što su prikupljanje sredstava, crowdfunding ili kao sredstvo plaćanja unutar određenog ekosustava (Skrill, 2024).

Za digitalne tokene vrijedi isto što i za obične tokene - sve dok ih posjedujemo, možemo ih koristiti. Kada posjedujemo kriptovalute, kao vlasnici imamo jedinstveni ključ koji nam omogućuje pristup tim kriptovalutama. Ovo je samo jedan od načina na koji možemo koristiti digitalne tokene, no važno je istaknuti da posjedovanjem tokena također možemo sudjelovati u transakcijama.

Ključna razlika između coins i tokena je u tome što novčići imaju vlastiti blockchain i koriste se prvenstveno kao oblik valute, dok se tokeni kreiraju na postojećem blockchainu i mogu predstavljati bilo što, od fizičke imovine do usluge ili korisničke pogodnosti. Još jedna razlika je ta što novčići često imaju ograničenu ponudu, dok se tokeni mogu stvarati i uništavati prema potrebi. Osim toga, novčići se često trguju na kripto burzama, dok se tokeni obično kupuju i prodaju putem inicijalnih ponuda tokena (ICO-a) ili decentraliziranih burzi (DEX-ova) (Coinbase, 2024).

U sažetku, iako su novčići i tokeni oba digitalna sredstva koja se mogu trgovati i pohraniti na blockchainu, oni služe različitim svrhama i funkcioniraju na različite načine. Novčići su neovisne valute, dok se tokeni stvaraju na postojećem blockchainu kako bi predstavljali određenu imovinu ili uslugu.

5.2. Novčanici

Kripto novčanici (eng. Wallets) čuvaju vaše privatne ključeve, odnsono lozinke koje vam omogućuju pristup vašim kripto valutama – osiguravajući njihovu sigurnost i dostupnost te vam omogućuju slanje i primanje kripto valuta poput Bitcoina i Ethereuma (Coinbase, 2024).

Postoje dvije glavne vrste kripto novčanika: "vrući" novčanici i "hladni" novčanici. "Vrući" novčanik je povezan s internetom i koristi se za česte transakcije, dok je "hladni" novčanik pohranjen izvan mreže i namijenjen za dugoročno čuvanje sredstava.

5.2.1. Digitalni novčanici

Digitalni novčanik (eng. Digital wallets) je softverska aplikacija koja korisnicima omogućuje sigurno pohranjivanje, upravljanje i prijenos njihovih digitalnih sredstava, poput kriptovaluta, tokena i drugih digitalnih valuta. To je virtualni novčanik koji se koristi za pohranu

privatnih ključeva potrebnih za pristup i upravljanje tim sredstvima na blockchainu (Coinbase, 2024).

Digitalni novčanici mogu se koristiti na raznim uređajima, uključujući računala, pametne telefone i tablete, a mogu se koristiti za slanje i primanje digitalnih sredstava od drugih korisnika ili trgovaca. Obično uključuju funkcije poput povijesti transakcija, tečajeva i stanja računa, što korisnicima olakšava praćenje svojih sredstava i upravljanje financijama.

Glavna prednost korištenja digitalnog novčanika je to što pruža siguran i praktičan način za pohranu i upravljanje digitalnim sredstvima. Budući da su privatni ključevi sigurno pohranjeni unutar novčanika, korisnici mogu biti sigurni da su njihova sredstva zaštićena od krađe ili gubitka (Coinbase, 2024).

Osim pohranjivanja digitalnih sredstava, neki digitalni novčanici također nude dodatne funkcije, poput mogućnosti zamjene jednog digitalnog sredstva za drugo, pristupa decentraliziranim aplikacijama i mogućnosti ostvarivanja nagrada za držanje određenih digitalnih sredstava.

Primjeri nekih od najpoznatijih digitalnih novčanika su Metamask, Exodus i Trust Wallet.

5.2.2. Hardverski novčanici

Hardverski novčanici (eng. Hardware wallets) su fizički uređaji dizajnirani za sigurno pohranjivanje privatnih ključeva kripto valuta izvan mreže. Privatni ključevi su tajni kodovi koji vam omogućuju pristup vašim kripto valutama i potpisivanje transakcija (Coinbase, What is a crypto wallet?, 2024).

Hardverski novčanici su obično mali, prijenosni uređaji koji se povezuju s vašim računalom ili mobilnim uređajem putem USB-a ili Bluetootha. Dizajnirani su tako da generiraju i pohranjuju privatne ključeve sigurno na samom uređaju, bez izlaganja tih ključeva internetu. To značajno smanjuje rizik od hakiranja ili krađe vaših privatnih ključeva od strane zlonamjernih aktera.

Kada želite pristupiti svojim kripto valutama ili potpisati transakciju, spojite svoj hardverski novčanik na računalo ili mobilni uređaj i unesete PIN ili lozinku kako biste otključali uređaj. Ovo vam omogućuje siguran pristup vašim privatnim ključevima i potpisivanje transakcija, bez izlaganja ključeva potencijalnim prijetnjama.

Hardverski novčanici smatraju se jednim od najsigurnijih načina pohrane kripto valuta jer pružaju visoku razinu zaštite od hakiranja i krađe. Međutim, važno je napomenuti da hardverski novčanici nisu potpuno otporni na napade i mogu biti ranjivi na fizičke prijetnje,

poput krađe ili gubitka. Stoga je uvijek važno slijediti najbolje prakse za zaštitu hardverskog novčanika, kao što je držanje uređaja na sigurnom mjestu i korištenje jakih lozinki (Coinbase, 2024).

Primjeri nekih od najpoznatijih digitalnih novčanika su Ledger i Trezor.

5.3. Spaljivanje novčića

Proces spaljivanja novčića (eng. Burning Coins) uključuje uklanjanje kovanica iz ukupne ponude. Da bi se izvršilo spaljivanje kovanica, korisnici šalju svoju kripto valutu na "eater adresu" ili burn novčanik, što je kripto novčanik koji može primati tokene, ali ih ne može slati. Na taj način, te kovanice su efektivno zaključane i uklonjene iz opticaja. Ta transakcija, potvrđena na blockchainu, čini spaljivanje kovanica trajnim i nepovratnim. Ima puno razloga zašto bi netko spaljivao kovanice, a neki od njih su navedeni i opisani u nastavku.

Kao mehanizam konsenzusa: neke kriptovalute koriste proof-of-burn (PoB) kao mehanizam konsenzusa u mreži. To zahtijeva od rudara i korisnika da redovito spaljuju dio svojih kovanica. Zagovornici ove metode smatraju je učinkovitim načinom verifikacije transakcija jer ne koristi stvarne resurse.

Za zaštitu od spama: spaljivanje kovanica može pomoći u zaštiti mreže od napada tipa Distributed Denial-of-Service (eng. DDoS) i spriječiti usporavanje mreže zbog neželjenih transakcija. Slično kao što korisnici Bitcoina plaćaju malu naknadu za slanje transakcija, ili korisnici Ethereuma plaćaju gas naknadu za izračune pametnih ugovora, neke mreže zahtijevaju da rudari/validatori spaljuju naknade koje dobiju za transakcije (CryptoForInnovation, 2023).

Za povećanje vrijednosti kovanica: osnovni ekonomski zakon ponude i potražnje kaže da ako se ponuda nečega smanji, cijena će rasti, pod uvjetom da potražnja ostane ista. Spaljivanje kovanica može služiti sličnoj svrsi. Smanjenjem ponude kroz spaljivanje, može se povećati vrijednost kovanica.

Za stabilnost stablecoina: u slučaju stablecoina, spaljivanje dijela ponude može biti nužno kako bi se održala vrijednost stabilne valute u odnosu na fiat valutu (poput dolara). Na primjer, ako potražnja za stablecoinom raste i cijena mu poraste iznad vezanosti uz dolar, protokolov pametni ugovor automatski će izdati nove tokene kako bi snizio cijenu — ili spaliti kovanice kako bi podigao cijenu i održao stabilnost vezanosti uz dolar (Becher, 2023).

Kao znak dugoročne predanosti: vlasnici kripto projekta ponekad spaljuju kovanice na svojoj mreži kao znak predanosti očuvanju oskudice. Održavanje određene razine oskudice može povećati vrijednost kovanica koje drže korisnici, čineći ih bogatijima (Reiff, 2024).

Za promicanje ravnoteže u rudarenju: u nekim slučajevima, sustav PoB može uspostaviti redovito spaljivanje kripto valuta koje pomaže u održavanju ravnoteže između novih korisnika i onih koji su ušli ranije, navedimo primjer prvih i ponekad najvećih ulagača na toj platformi. Budući da PoB mehanizam konsenzusa zahtijeva spaljivanje kovanica kako bi se potvrdile transakcije, time se potiče rudarenje novih kovanica. To omogućuje ravnotežu između novih korisnika i starih sudionika. Na slici 10 nam je grafički prikazano, odnosno ilustrirano uklanjanje kripto valute iz opticaja.

Slika 10.Spaljivanje kovanica (Izvor: (CryptoForInnovation, 2023))

5.4. Decentralizirana autonomna organizacija

Decentralizirana autonomna organizacija (eng. DAO) predstavlja novi oblik pravne strukture koja nema centralno upravljačko tijelo, a članovi dijele zajednički cilj djelovanja u najboljem interesu organizacije. DAO-ovi su postali popularni među kripto entuzijastima i korisnicima blockchain tehnologije, te se koriste za donošenje odluka kroz pristup upravljanja odozdo prema gore.

Inspirirani decentralizacijom kripto valuta, grupa developera osmislila je koncept decentralizirane autonomne organizacije (eng. DAO) 2016. godine. Ideja DAO-a je da omogućuje nadzor i upravljanje entitetom slično korporaciji, ali s ključnom razlikom u odsutnosti centralne vlasti, to jest kolektivna grupa lidera i sudionika djeluje kao upravljačko tijelo (TheEconomist, 2022).

U nastavku ćemo opisati princip rada decentralizirane autonomne organizacije. DAO-ovi se uvelike oslanjaju na pametne ugovore. Ovi logički kodirani sporazumi određuju donošenje odluka na temelju aktivnosti na blockchainu. Na primjer, ovisno o ishodu odluke, određeni kod može biti implementiran kako bi se povećala cirkulirajuća ponuda, spalio određeni iznos rezervnih tokena ili izdali specifični nagrade postojećim vlasnicima tokena (TheEconomist, 2022). Proces glasanja za DAO-ove odvija se na blockchainu. Korisnici često biraju između uzajamno isključivih opcija. Glasovna moć je često raspodijeljena među korisnicima na temelju broja tokena koje posjeduju. Na primjer, korisnik koji posjeduje 100 tokena u DAO-u imat će dvostruko veću glasovnu moć od korisnika koji posjeduje 50 tokena.

Teorija iza ove prakse je da su korisnici koji su financijski više uključeni u DAO motivirani da djeluju u dobroj vjeri. Zamislite korisnika koji posjeduje 25% ukupne glasovne moći. Taj korisnik može sudjelovati u lošim postupcima, no time bi ugrozio vrijednost svojih 25% udjela. DAO-ovi često imaju riznice koje sadrže tokene koje se mogu zamijeniti za fiat valutu. Članovi DAO-a mogu glasovati o tome kako koristiti ta sredstva; na primjer, neki DAO-ovi koji imaju namjeru nabaviti rijetke NFT-ove mogu glasovati o tome hoće li upotrijebiti sredstva iz riznice za kupnju tih imovina (Reiff, 2024).

5.5. Igre riječi i financije

GameFi je spoj igre riječi i financije. Odnosi se na blockchain igre u kojima igrači mogu zaraditi dok igraju, nudeći im ekonomske poticaje. GameFi ekosustav koristi kripto valute, nezamjenjive tokene (NFT-ove) i blockchain tehnologiju kako bi stvorio virtualno okruženje za igranje (Chainlink, 2024).

Igrači obično mogu zaraditi nagrade unutar igre ispunjavanjem zadataka, borbom s drugim igračima i napredovanjem kroz različite razine igre. Također, svoje stečene digitalne imovine mogu prenijeti izvan igre kako bi ih trgovali na kripto burzama i NFT tržištima. U sljedećem odlomku će biti opisano način na koji GameFi radi.

U GameFi-u nagrade mogu doći u različitim oblicima, poput kripto valuta ili unutar-igračkih resursa kao što su virtualna zemljišta, avatari, oružja i kostimi. Svaki GameFi projekt usvaja drugačiji model i ekonomiju igre. U većini slučajeva, unutar-igrački resursi su NFT-ovi koji se nalaze na blockchainu, što znači da se mogu trgovati na NFT tržištima. Međutim, u nekim slučajevima, igrači moraju prvo pretvoriti te resurse u NFT-ove prije nego što ih mogu trgovati ili prodavati (GameFi.org, 2024).

Unutar-igrački resursi obično pružaju određene prednosti igračima, omogućujući im da ostvare veće nagrade. No, neke igre također uključuju avatare i kozmetičke dodatke koji su isključivo vizualni i nemaju utjecaj na samu igru ili zaradu.

Ovisno o igri, igrači mogu zarađivati nagrade ispunjavanjem zadataka, borbom s drugim igračima ili izgradnjom unovčenih struktura na svojoj zemlji. Neke igre omogućuju igračima generiranje pasivnog prihoda bez aktivnog igranja, bilo kroz staking ili posuđivanje svojih igračkih resursa drugim igračima. Pogledajmo neke od uobičajenih značajki u GameFi-u (Chainlink, 2024).

6. Primjeri primjene blockchain tehnologija u financijskom sektoru

Blockchain tehnologija našla je primjenu u financijskom sektoru kroz različite inovacije. Primjeri uključuju brže i sigurnije međunarodne transakcije putem platformi kao što je Ripple, koja omogućava gotovo trenutni prijenos sredstava s nižim troškovima u usporedbi s tradicionalnim bankama. JPMorgan je razvio Quorum, vlastiti blockchain za poboljšanje privatnosti i skalabilnosti u financijskim transakcijama. Decentralizirane financijske platforme (DeFi) poput Aave i Compound omogućuju korisnicima posuđivanje i zarađivanje kamata na digitalnu imovinu bez potrebe za posrednicima. Također, IBM-ova Blockchain World Wire mreža koristi se za olakšavanje prekograničnih plaćanja između banaka koristeći digitalne valute.

6.1. IBM Blockchain World Wire

IBM Blockchain World Wire bila je blockchain platforma razvijena od strane IBM-a, osmišljena da revolucionira način na koji se provode međunarodne financijske transakcije. Cilj platforme bio je omogućiti bankama i drugim financijskim institucijama brže, jeftinije i sigurnije obavljanje prekograničnih plaćanja korištenjem blockchain tehnologije (IBM, 2024).

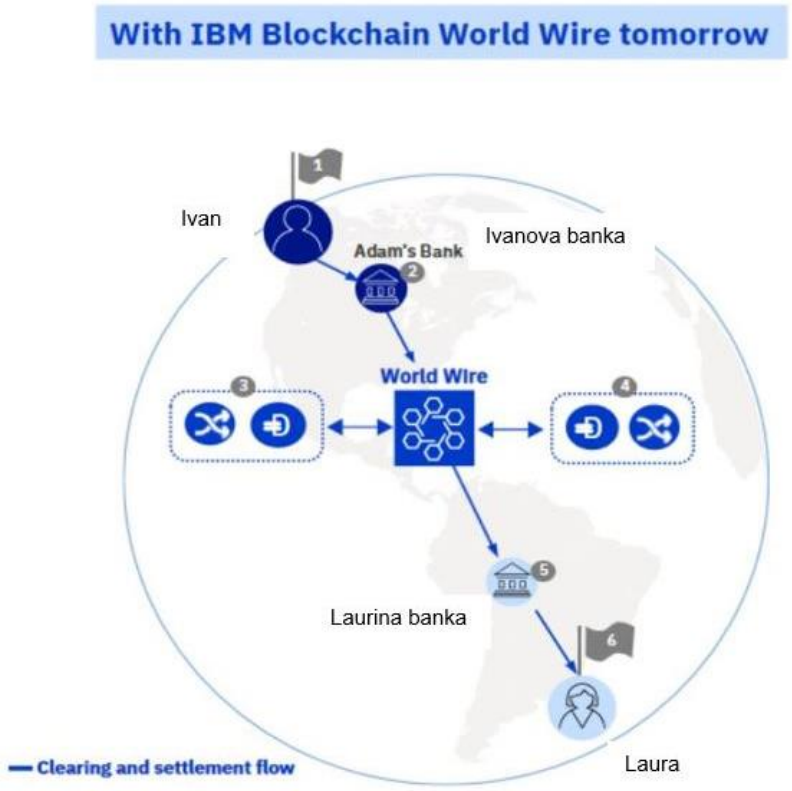
U nastavku će biti navedene glavne značajke IBM Blockchain World Wire-a. IBM Blockchain World Wire koristi blockchain za prekogranična plaćanja. World Wire je bio osmišljen kao globalna mreža za financijske institucije koja omogućava izravna prekogranična plaćanja između različitih valuta. Korištenjem blockchain tehnologije, World Wire omogućio je instantna poravnanja i smanjenje troškova povezanih s tradicionalnim bankarskim kanalima.

Jedna od ključnih inovacija World Wire-a bila je podrška za digitalne valute i stabilne kovanice. Ove digitalne valute mogle su se koristiti kao sredstvo za trenutne transakcije između dviju strana, čime se eliminirao potreban za posrednike i značajno smanjio vrijeme potrebno za poravnanje transakcija (IBM, 2024). Simbolični postupak nam je prikazan na slici 11.

IBM Blockchain World Wire bio je dizajniran tako da se lako integrira s postojećim bankovnim sustavima. To je omogućavalo bankama da koriste prednosti blockchain tehnologije bez potrebe za značajnim promjenama u svojim poslovnim procesima.

Platforma je omogućavala transparentnost svih transakcija putem nepromjenjivog blockchaina, što je pružalo visoku razinu sigurnosti i povjerenja. Svaka transakcija bila je zabilježena na blockchainu, omogućujući korisnicima da prate i verificiraju sve aspekte transakcijskog procesa.

World Wire podržavao je širok raspon fiat valuta, digitalnih valuta i stabilnih kovanica, što je omogućavalo fleksibilnost u plaćanjima između različitih jurisdikcija i tržišta. IBM je surađivao s brojnim bankama i financijskim institucijama diljem svijeta kako bi izgradio globalnu mrežu korisnika World Wire platforme. To je omogućavalo da platforma ima široku primjenu na različitim tržištima i regijama (IBM, 2024).



Slika 11.Prikaz sustava plaćanja pomoću IBM WW (Izvor prema: (IBM Support, 2024))

Unatoč ambicioznim ciljevima i snažnoj podršci od strane IBM-a, Blockchain World Wire nije uspio ostvariti značajniji uspjeh na tržištu. Projekt je imao poteškoća s postizanjem opsežnog usvajanja i suočavao se s konkurencijom drugih blockchain rješenja za prekogranična plaćanja. IBM je u konačnici odlučio ugasiti World Wire kao samostalni proizvod, ali je nastavio istraživati i razvijati druge blockchain projekte i rješenja. World Wire je bio jedan od ranih pokušaja korištenja blockchain tehnologije za poboljšanje prekograničnih plaćanja, iako nije postao dominantno rješenje, doprinio je razvoju ideje o korištenju blockchaina u financijskim uslugama.

6.2. JPMorgan's Quorum

Quorum je blockchain platforma koju je razvila JPMorgan Chase, jedna od najvećih američkih investicijskih banaka. Ova platforma je dizajnirana za potrebe financijske industrije, ali i za širu primjenu u različitim sektorima. Quorum je temeljena na Ethereum blockchainu, ali je prilagođena za poslovne potrebe, s fokusom na privatnost, performanse i sigurnost (Zapotochnyi, 2022), dok je logo same platforme prikazan na slici 12.

Quorum je prvi put predstavljen 2016. godine kao dio JPMorganovih nastojanja da istraži mogućnosti blockchain tehnologije za financijski sektor. Platforma je brzo postala jedan od najpoznatijih primjera privatnog blockchaina prilagođenog za poslovne potrebe. JPMorgan i ConsenSys: u 2020. godini, JPMorgan je odlučio prodati Quorum ConsenSysu, poznatoj blockchain softverskoj kompaniji koja se fokusira na Ethereum. Ovaj potez omogućio je širu primjenu i daljnji razvoj Quoruma, dok je JPMorgan zadržao mogućnost korištenja platforme za svoje interne potrebe (Zapotochnyi, 2022).

Slika 12.Quorum logo (Izvor: (Chainstack, 2024))

U nastavku su navedene ključne značajke Quoruma. Quorum koristi Ethereum kao baznu tehnologiju, što omogućava korištenje svih prednosti koje donosi Ethereum ekosustav, uključujući pametne ugovore (eng. smart contracts) i decentralizirane aplikacije (eng. dApps).

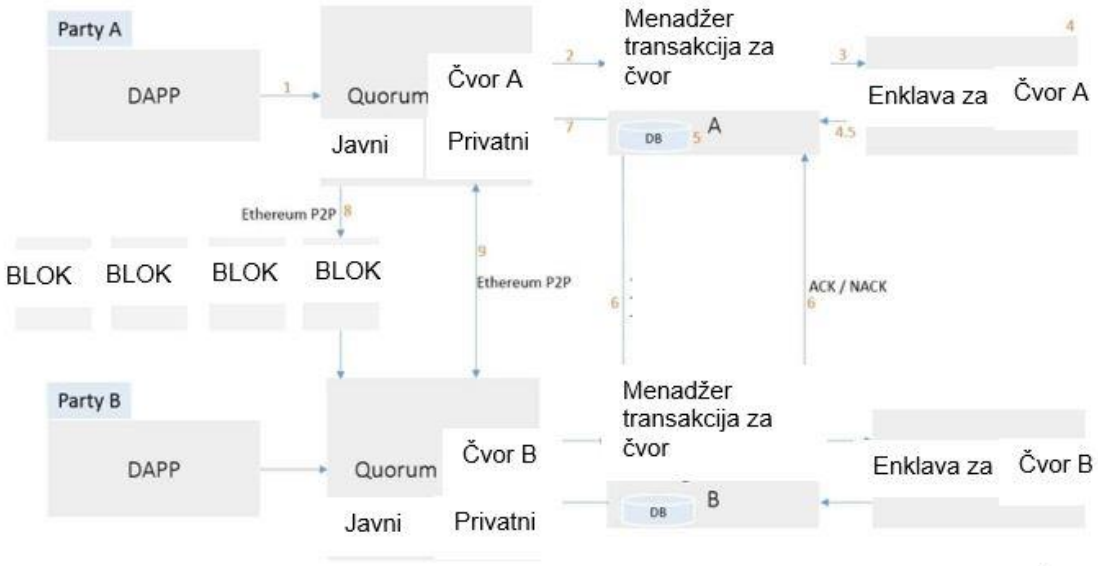
Međutim, Quorum je modificiran kako bi ispunio specifične zahtjeve poduzeća, osobito u financijskom sektoru.

Jedna od najvažnijih značajki Quoruma je njegova sposobnost da osigura privatnost transakcija. U javnim blockchainima poput Ethereuma, sve su transakcije vidljive svim sudionicima mreže. Quorum, s druge strane, omogućuje privatne transakcije koje su vidljive samo sudionicima u toj transakciji, koristeći tzv. "private transaction manager" (privatni upravitelj transakcijama). Cijeli postupak nam je vidljiv na slici 13.

Quorum je dizajniran da podrži veću propusnost transakcija i smanjene latencije u usporedbi s javnim blockchainima. To je omogućeno optimizacijama koje smanjuju vrijeme potrebno za postizanje konsenzusa i omogućuju bržu obradu transakcija, što je ključno za aplikacije u financijskom sektoru.

Quorum koristi dva konsenzusna algoritma – Raft i Istanbul Byzantine Fault Tolerance (eng. IBFT). Ovi algoritmi su osmišljeni kako bi omogućili brže i sigurnije postizanje konsenzusa u privatnim mrežama, za razliku od Proof of Work (PoW) algoritma koji koristi Ethereum i koji je energetski intenzivan (Zapotochnyi, 2022).

Kao i Ethereum, Quorum podržava pametne ugovore koji se mogu koristiti za automatizaciju složenih poslovnih procesa. Međutim, Quorum dodaje slojeve sigurnosti i privatnosti kako bi osigurao da se osjetljive informacije ne otkrivaju cijeloj mreži što je vidljivo i na slici 13.



Slika 13.Princip rada Quorum platforme pomoću blockchaina (Izvor prema: (Zapotochnyi, 2022))

Quorum je izvorno bio projekt otvorenog koda (eng. open source), što znači da je bio dostupan za preuzimanje i prilagodbu od strane drugih organizacija. Ovo je omogućilo široku prilagodbu i primjenu u različitim industrijama.

Quorum je korišten u nekoliko velikih projekata, posebno u financijskom sektoru. Također, Quorum je korišten i u Interbank Information Networku, platformi koja povezuje više od 300 banaka diljem svijeta radi poboljšanja brzine i transparentnosti međunarodnih plaćanja (Kaleido, 2024).

Quorum je značajan korak u primjeni blockchain tehnologije u poslovnom svijetu, posebno u financijskom sektoru. Svojim fokusom na privatnost, sigurnost i performanse, Quorum je postao privlačan izbor za mnoge organizacije koje traže sigurno i učinkovito rješenje za svoje blockchain potrebe. Njegova prodaja ConsenSysu dodatno je osigurala njegovu budućnost i omogućila daljnji razvoj i integraciju s Ethereum ekosustavom (Kaleido, 2024).

7. Zaključak

Zaključak o blockchain tehnologiji u financijskom sektoru može se sagledati kroz njezin potencijal, izazove te razvoj u budućnosti. Ova tehnologija, koja je svoju prvu primjenu našla u kriptovalutama poput Bitcoina, pruža mnoge inovativne mogućnosti koje imaju potencijal da revolucioniraju financijski sektor. Ipak, njezin utjecaj na ovaj sektor nije jednoznačan i suočava se s nizom prepreka koje treba nadvladati kako bi se ostvarilo njeno korištenje u tradicionalnim financijskim sustavima.

Jedna od najznačajnijih karakteristika blockchain tehnologije je njena decentraliziranost. Umjesto centraliziranih autoriteta poput banaka, blockchain omogućuje direktnu interakciju između sudionika transakcija, eliminirajući potrebu za posrednicima. To ne samo da može smanjiti troškove transakcija, već također povećava sigurnost i transparentnost, jer su sve transakcije zabilježene na javnom, nepromjenjivom zapisu. Ova transparentnost može pomoći u borbi protiv financijskih prevara i pranja novca, što su značajni problemi u tradicionalnim financijskim sustavima.

Pametni ugovori (eng. smart contracts), koji su omogućeni kroz blockchain platforme poput Ethereuma, predstavljaju dodatni korak naprijed. Ovi samostalno izvršni ugovori omogućuju automatizaciju složenih financijskih procesa bez potrebe za posrednicima, što dodatno smanjuje troškove i povećava učinkovitost. Međutim, kako su pametni ugovori još uvijek relativno novi, njihov pravni status i primjena nisu u potpunosti regulirani, što predstavlja izazov za njihovu širu primjenu.

Jedan od glavnih izazova za blockchain tehnologiju u financijskom sektoru je regulacija. Tradicionalni financijski sustavi strogo su regulirani kako bi se zaštitili potrošači i osigurala stabilnost tržišta. Blockchain tehnologija, s druge strane, zbog svoje decentralizirane prirode, otežava primjenu postojećih regulatornih okvira. Iako decentralizacija donosi brojne prednosti, ona također stvara rizike, posebno kada je riječ o zaštiti potrošača i sprječavanju ilegalnih aktivnosti. Stoga je suradnja između regulatora i blockchain industrije ključna za osiguranje da ova tehnologija može rasti na siguran i održiv način. Još jedan značajan izazov je skalabilnost. Trenutni blockchain sustavi, posebno oni koji koriste Proof of Work algoritam, suočavaju se s problemima u pogledu brzine transakcija i potrošnje energije. Kako bi blockchain postao održivo rješenje za globalni financijski sustav, potrebno je razviti učinkovitije algoritme konsenzusa koji mogu podržati veći volumen transakcija uz manju potrošnju resursa.

Unatoč ovim izazovima, blockchain tehnologija nastavlja privlačiti sve više pažnje i investicija. Velike financijske institucije, poput JPMorgana, razvijaju vlastite blockchain platforme (npr. Quorum) kako bi istražile načine na koje mogu iskoristiti prednosti ove

tehnologije. Također, sve više novih projekata koristi blockchain za stvaranje inovativnih financijskih rješenja, kao što su decentralizirane financije (eng. DeFi) i tokenizacija imovine.

Zaključno, iako blockchain tehnologija još uvijek nije u potpunosti transformirala financijski sektor, njezin potencijal za promjene je ogroman. Ako se uspješno riješe izazovi vezani uz regulaciju, skalabilnost i sigurnost, blockchain bi mogao postati temelj budućeg financijskog ekosustava. No, da bi se to dogodilo, potrebna je daljnja suradnja između tehnoloških inovatora, financijskih institucija i regulatora kako bi se stvorio okruženje u kojem blockchain može ostvariti svoj puni potencijal.

8. Popis literature

1. Adams, M. (21. 05 2024). *What Is Ethereum? How Does It Work?* Preuzeto 21. 08 2024 iz Forbes: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-ether/
2. Arunović, D. (24. 02 2018). *Što je u stvari blockchain i kako radi?* Preuzeto 13. 08 2024 iz Bug: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011
3. Becher, B. (21. 07 2023). *What Does 'Burning Crypto' Mean?* Preuzeto 29. 08 2024 iz BuiltIn: https://builtin.com/articles/what-does-burning-crypto-mean
4. Bitstore.net. (19. 04 2022). *Što je blockchain i kako funkcionira? Kompletni vizualni vodič za početnike*. Preuzeto 12. 8 2024 iz Bitcoin store: https://www.bitstore.net/hr/blog/sto-je-blockchain-i-kako-funkcionira/#-to-je-blockchain
5. Calimero. (2024). *Calimero Network*. Preuzeto 16. 8 2024 iz https://www.calimero.network/
6. Canva. (2024). Preuzeto 26. 08 2024 iz Canva: https://www.canva.com/hr_hr/
7. Cardano. (2024). Preuzeto 23. 08 2024 iz Cardano: https://cardano.org/
8. Chain, B. (2024). Preuzeto 22. 08 2024 iz BNB Chain: https://www.bnbchain.org/en/bnb-smart-chain
9. Chainlink. (14. 08 2024). *What Is GameFi?* Preuzeto 23. 08 2024 iz Chainlink: https://chain.link/education-hub/gamefi
10. Chainstack. (2024). Preuzeto 25. 08 2024 iz Chainstack: https://chainstack.com/protocols/quorum/
11. Coinbase. (2024). *What is a crypto wallet?* Preuzeto 26. 08 2024 iz Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-a-crypto-wallet
12. Coinbase. (2024). *What is the difference between a coin and a token?* Preuzeto 25. 08 2024 iz Coinbase: https://www.coinbase.com/learn/crypto-basics/what-is-the-difference-between-a-coin-and-a-token
13. Crypto.com. (02. 02 2022). *What Are Token Standards? An Overview.* Preuzeto 22. 08 2024 iz Crypto.com: https://crypto.com/university/what-are-token-standards#:~:text=Fundamentally%2C%20smart%20contract%20standards%20are,%2C%20and%20library%2Dpackage%20formats
14. CryptoForInnovation. (13. 12 2023). *What is Burning Crypto?* Preuzeto 29. 08 2024 iz Innovation: https://cryptoforinnovation.org/what-is-burning-crypto/
15. Curry, B. (25. 08 2023). *Proof Of Stake Explained.* Preuzeto 20. 08 2024 iz Forbes: https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake/

16. Curry, B. (13. 5 2024). *Proof of Work Explained.* Preuzeto 20. 08 2024 iz Forbes: https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/
17. Cvijović-Gorša, S. (2023). *Mathos Unios.* Preuzeto 19. 08 2024 iz Hash-funkcije u kriptografiji: https://www.mathos.unios.hr/~mdjumic/uploads/diplomski/CVI15.pdf
18. EITCA. (03. 08 2023). *Kako kriptografija eliptične krivulje pruža isti nivo sigurnosti kao tradicionalni kriptografski algoritmi s manjim veličinama ključa?* Preuzeto 16. 08 2024 iz EITCA: https://bs.eitca.org/cybersecurity/eitc-is-acc-advanced-classical-cryptography/elliptic-curve-cryptography/introduction-to-elliptic-curves/examination-review-introduction-to-elliptic-curves/how-does-elliptic-curve-cryptography-provide-the-same-level-of-se
19. Ethereum. (2024). Preuzeto 21. 08 2022 iz Ethereum: https://ethereum.org/en/
20. Filipovic, M. (16. 04 2020). *OSNOVNE ZNAČAJKE I RAZLIKE IZMEĐU PRIVATNOG I JAVNOG BLOCKCHAINA*. Preuzeto 14. 08 2024 iz LinkedIn: https://www.linkedin.com/pulse/osnovne-zna%C4%8Dajke-i-razlike-izme%C4%91u-privatnog-javnog-marko-filipovic
21. GameFi.org. (2024). Preuzeto 23. 08 2024 iz GameFi.org: https://gamefi.org/
22. GeeksForGeeks. (26. 06 2024). *Digital Signature Standard (DSS)*. Preuzeto 16. 08 2024 iz Geeks For Geeks: https://www.geeksforgeeks.org/digital-signature-standard-dss/
23. GeeksForGeeks.org. (06. 04 2023). *Hybrid Blockchain*. Preuzeto 18. 08 2024 iz GeeksForGeeks: https://www.geeksforgeeks.org/hybrid-blockchain/
24. GeeksForGeeks.org. (23. 05 2024). *Smart Contracts in Blockchain.* Preuzeto 22. 08 2024 iz Geeks For Geeks: https://www.geeksforgeeks.org/smart-contracts-in-blockchain/
25. IBM. (2024). *IBM Support*. Preuzeto 24. 08 2024 iz IBM: https://www.ibm.com/support/pages/ibm-blockchain-world-wire-revolutionize-cross-border-payments
26. Kaleido. (2024). *Build on Quorum the Easy Way*. Preuzeto 19. 08 2024 iz Kaleido: https://www.kaleido.io/blockchain-platform/quorum
27. Kerner, S. M. (09 2022). *Proof of stake (PoS).* Preuzeto 20. 08 2024 iz TechTarget: https://www.techtarget.com/whatis/definition/proof-of-stake-PoS
28. Kriptomat. (2024). *Što je privatni ključ?* Preuzeto 13. 08 2024 iz Kriptomat: https://kriptomat.io/hr/blockchain/sto-je-privatni-kljuc/
29. Kriptomat.cash. (2020). *Privatni i javni ključevi*. Preuzeto 14. 08 2024 iz Kriptomat: https://kriptomat.cash/privatepubliccryptokeys/
30. Laurence, T. (2019). *Introduction to Blockchain Technology.* Van Haren Publishing.
31. Ledger. (18. 08 2023). *What Is Proof-of-Stake (PoS)?* Preuzeto 20. 08 2024 iz Ledger: https://www.ledger.com/academy/blockchain/what-is-proof-of-stake
32. Lewis, A. (2018). *The Basics of Bitcoins and Blockchains: An Introduction to.* Mango.

33. Mckinsey&Company. (03. 01 2023). *What is proof of stake?* Preuzeto 20. 08 2024 iz Mckinsey&Company: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-proof-of-stake
34. Microsoft. (2024). *Digitalni potpisi i certifikati*. Preuzeto 14. 08 2024 iz Microsoft: https://support.microsoft.com/hr-hr/office/digitalni-potpisi-i-certifikati-8186cd15-e7ac-4a16-8597-22bd163e8e96#__toc311530578
35. Milosns.eth. (4. 10 2022). *Što je dapp ili decentralizirana aplikacija?* Preuzeto 19. 08 2024 iz Joker.gg: https://www.joker.gg/hr/sto-je-dapp-ili-decentralizirana-aplikacija/#:~:text=Decentralizirana%20aplikacija%20(dapp)%20sli%C4%8Dna%20je,izvan%20ruku%20organizacija%20u%20pozadini
36. Nambiampurath, R. (28. 08 2024). *Polkadot (DOT): Definition, History, and How It Works*. Preuzeto 28. 08 2024 iz Investopedia: https://www.investopedia.com/polkadot-definition-6362436
37. Nevile, S. (17. 5 2024). *What Is Proof of Work (PoW) in Blockchain?* Preuzeto 20. 08 2024 iz Investopedia: https://www.investopedia.com/terms/p/proof-work.asp#:~:text=Proof%20of%20work%20(PoW)%20is%20a%20decentralized%20consensus%20mechanism%20that,a%20reward%20for%20work%20done
38. Nožinić, M. (11. 02 2022). *Što je blockchain tehnologija i kako funkcionira?* Preuzeto 13. 08 2024 iz Mentorica.biz: https://mentorica.biz/aktualno/sto-je-blockchain-tehnologija-i-kako-funkcionira-468/
39. Plavljanić, B. (26. 05 2024). *Uvod u blockchain i kriptovalute*. Preuzeto 13. 08 2024 iz Pcchip: https://pcchip.hr/kriptovalute/uvod-u-blockchain-i-kriptovalute/
40. Polkadot. (2024). Preuzeto 23. 08 2024 iz Polkadot: https://polkadot.com/
41. RapidSSLonline. (2022). *The Difference Between Public Key and Private Key Explained*. Preuzeto 14. 08 2024 iz Rapid SSL online: https://www.rapidsslonline.com/ssl/difference-between-public-and-private-key/
42. Reiff, N. (15. 07 2024). *Decentralized Autonomous Organization (DAO): Definition, Purpose, and Example*. Preuzeto 26. 08 2024 iz Investopedia: https://www.investopedia.com/tech/what-dao/
43. Reiff, N. (30. 08 2024). *What Does It Mean to Burn Crypto? Practical Applications*. Preuzeto 30. 08 2024 iz Investopedia: https://www.investopedia.com/tech/cryptocurrency-burning-can-it-manage-inflation/
44. Reiff, N. (26. 05 2024). *What Is Ether (ETH), the Cryptocurrency of Ethereum Apps?* Preuzeto 21. 08 2024 iz Investopedia: https://www.investopedia.com/tech/what-ether-it-same-ethereum/#:~:text=Ethereum%20is%20a%20blockchain%20and,cap%20of%20about%20%24380%20billion

45. Service, A. W. (2024). Preuzeto 18. 08 2024 iz AWS: https://aws.amazon.com/free/?gclid=EAIaIQobChMI26qd0ZiviAMV3ZeDBx1PMB7iEAAYASAAEgJrDvD_BwE&trk=f17b4b4e-aa1b-4189-b0c4-81a19b53f625&sc_channel=ps&ef_id=EAIaIQobChMI26qd0ZiviAMV3ZeDBx1PMB7iEAAYASAAEgJrDvD_BwE:G:s&s_kwcid=AL!4422!3!645186168166!e!!g!!aws!19
46. Simplilearn. (02. 07 2024). *RSA Algorithm: Secure Your Data with Public-Key Encryption*. Preuzeto 16. 08 2024 iz Simply Learn: https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm#:~:text=The%20RSA%20algorithm%20is%20a,to%20be%20fast%20post%2Ddeployment.
47. Skrill. (2024). *What is the difference between a coin and a token?* Preuzeto 25. 08 2024 iz Skrill: https://www.skrill.com/en/crypto/the-skrill-crypto-academy/beginner/what-is-the-difference-between-a-coin-and-a-token/
48. Srivastav, A. K. (11. 4 2024). *Proof of Stake vs Proof of Work.* Preuzeto 20. 8 2024 iz Well Street Mojo: https://www.wallstreetmojo.com/proof-of-stake-vs-proof-of-work/
49. Svijet-kvalitete. (20. 08 2012). *Razlika između certifikacije i akreditacije*. Preuzeto 17. 08 2024 iz Svijet kvalitete: https://svijet-kvalitete.com/index.php/certifikacija/133-razlika-izmedu-certifikacije-i-akreditacije
50. TheEconomist. (26. 01 2022). *What are DAOs, or decentralised autonomous organisations?* Preuzeto 26. 08 2024 iz The Economist: https://www.economist.com/the-economist-explains/2022/01/26/what-are-daos-or-decentralised-autonomous-organisations?utm_medium=cpc.adword.pd&utm_source=google&ppccampaignID=18151738051&ppcadID=&utm_campaign=a.22brand_pmax&utm_content=conversion.direct-res
51. Zapotochnyi, A. (17. 02 2022). *What Is Quorum Blockchain? A Platform for The Enterprise*. Preuzeto 19. 08 2024 iz Blockgeeks: https://blockgeeks.com/guides/quorum-a-blockchain-platform-for-the-enterprise/

9. Popis slika

Slika 1.Primjer privatnog i javnog ključa 5
Slika 2.Primjer korištenja hash funkcije 10
Slika 3.Primjer mehanizma Proof of Stake.....14
Slika 4.Prikaz Ethereum platforme.....16
Slika 5.Princip rada pametnog ugovora pomoću blockchaina 18
Slika 6.Prikaz Binance Smart Chain mreže 21
Slika 7.Cardano aplikacija 22
Slika 8. Sažetak tržišta Cardano – a.....23
Slika 9. Polkadot (DOT) sustav 24
Slika 10.Spaljivanje kovanica 28
Slika 11.Prikaz sustava plaćanja pomoću IBM WW.....31
Slika 12.Quorum logo.....32
Slika 13.Princip rada Quorum platforme pomoću blockchaina.....33

10. Popis tablica

Tablica 1: Usporedba između Proof of Work (POW) i Proof of Stake (POS) algoritama……15