Tehnologija ulančanih blokova

Lipošćak, Antonio

SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET

Antonio Lipošćak

TEHNOLOGIJA ULANČANIH BLOKOVA

ZAVRŠNI RAD

Rijeka, 2023.

SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET

TEHNOLOGIJA ULANČANIH BLOKOVA

BLOCKCHAIN TECHNOLOGIES

ZAVRŠNI RAD

Kolegij: Baze podataka

Mentor: izv. prof. dr. sc. Jasmin Ćelić

Student: Antonio Lipošćak

Studijski smjer: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112069585

Rijeka, 2023.

Student: Antonio Lipošćak

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112069585

IZJAVA O SAMOSTALNOJ IZRADI ZAVRŠNOG RADA

Kojom izjavljujem da sam završni rad s naslovom TEHNOLOGIJA ULANČANIH BLOKOVA izradio samostalno pod mentorstvom izv. prof. dr. Sc. Jasmina Ćelića.

U radu sam primijenio metodologiju izrade stručnog/znanstvenog rada i koristio literaturu koja je navedena na kraju završnog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući naveo u završnom radu na uobičajen, standardan način citirao sam i povezao s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Student

A.L

(potpis)

Student: Antonio Lipošćak

Studijski program: Elektroničke i informatičke tehnologije u pomorstvu

JMBAG: 0112069585

IZJAVA STUDENTA – AUTORA
O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Izjavljujem da kao student – autor završnog rada dozvoljavam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskog fakulteta.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskog fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/

Student

A.L

(potpis)

Antonio Lipošćak

SAŽETAK

U ovome radu se opisuje detaljan pregled ulančanih blokova, njihovih aplikacija, prednosti i nedostataka u usporedbi sa tradicionalnim bazama podataka.

Ulančani blokovi su dio inovativne tehnologije koja donosi privatnost, sigurnost, anonimnost, decentralizaciju i nepromjenjivost što ima široku primjenu u raznim područjima. Također će se naglasiti izazovi poput skalabilnosti, sigurnosti i regulacije koji se moraju riješiti kako bi se iskoristile sve prednosti ove tehnologije. Prikazujući primjere primjene u financijama, zdravstvu, upravljanju opskrbnim lancem i glasačkim sustavima, istražuje se kako ulančani blokovi imaju potencijal transformiranja različitih industrija.

Konačno, razmotrit će se budućnost ulančanih blokova te potreba za daljnjim radom i istraživanjem kako bi se ostvario puni potencijal ove tehnologije.

Ključne riječi: ulančani podaci, decentralizacija, baze podataka, skalabilnost, sigurnost, regulativa.

SUMMARY

This paper describes a detailed overview of chain technologies, it's applications, advantages and disadvantages compared to traditional databases.

Blockchains are part of an innovative technology that brings privacy, security, anonymity, decentralization and immutability, which has wide applications in various fields. Likewise, challenges will be emphasized regarding scalability, security, and regulations that must be addressed in order to take full advantage of this technology. Showing examples of applications in finance, healthcare, supply chain managment and voting systems, it explores how blockchains have the potential to transform various industries.

Finally, the future of blockchains and the need for further work and research to realize the full potential of this technology will be considered.

Keywords: Blockchain, decentralization, database, scalability, safety, regulation.

Sadržaj

1. UVOD

Ulančani blokovi predstavljaju revolucionarnu tehnologiju koja se ističe po svojoj decentralizaciji, sigurnosti, transparentnosti u pohrani i upravljanju podacima. Korištenjem distribuiranih knjiga, mehanizama konsenzusa, kriptografije i pametnih ugovora, ulančani blokovi pružaju nepromjenjive zapise koji su otporni na manipulaciju, zlonamjerne računalne aktivnosti i prijevaru.

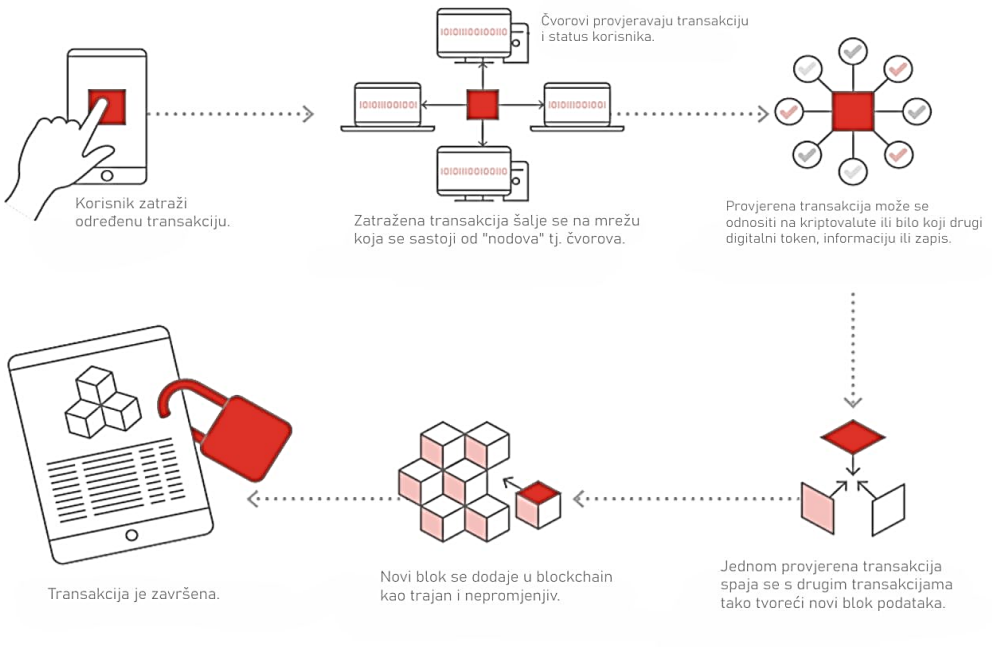
Ova tehnologija ima potencijal da transformira razne industrije, uključujući financije, zdravstvo, upravljanje opskrbnim lancem i glasačke sustave. Međutim, kako bi se u potpunosti iskoristili potencijali ulančanih blokova, potrebno je suočiti se s izazovima poput skalabilnosti, interoperabilnosti i regulatornih okvira.

Daljnja istraživanja i razvoj su neophodni kako bi se riješili ovi problemi te omogućili široko usvajanje i primjenu ulančanih blokova.

2. ULANČANI BLOKOVI

2.1. OPIS ULANČANIH BLOKOVA

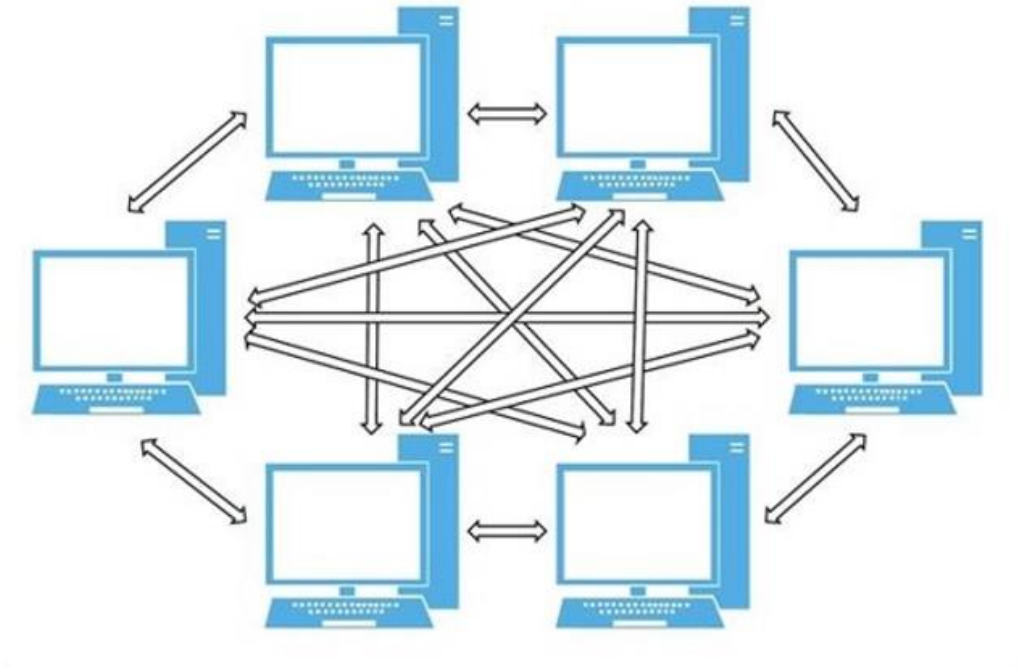
Početak razvoja ulančanih podataka može se povezati sa tzv. „Open sourced Bitcoin whitepaper“, dokumentom kojeg je objavila osoba pod pseudonimom Satoshi Nakamoto 09. siječnja 2009. U tom dokumentu se navodi da ulančani blokovi pružaju korisnicima povjerenje u digitalne transakcije zbog načina na koji rade. Ulančani blokovi su baze podataka koje se lako mogu dijeliti između svih korisnika mreže. Podaci se pohranjuju u blokove kronološkim redom te se nikada ne mogu mijenjati što jamči sigurnost svim korisnicima. Svaki novi blok je povezan (ulančan) sa prethodnim. Svaki blok sadrži kriptografski matematički izračun koji provjerava slijed i verifikaciju prijašnjeg bloka. Svaki čvor (računalo u mreži) verificira transakciju kako bi se stvorila dijeljena digitalna glavna knjiga (eng. ledger) između korisnika. Ta knjiga sadrži sve bitne informacije o transakcijama (na primjer, tko je sudjelovao u transakciji, koji je iznos transakcije, da li je ona bila uspješna, itd.). Što znači da se bilo koju transakciju u bilo kojem trenutku može verificirati ne samo od jednog centralnog autoriteta već od više njih čime knjiga stječe transparentnost [1, 2].



Slika 1. Transakcija blokova

Izvor: https://pcchip.hr/wp-content/uploads/2022/02/blockchain-dijagram.jpg (08.11.2022)

Prethodno navedenim načinom ukida se potreba za korištenjem dodatnih potvrda za autorizaciju putem posrednika i ona se prenosi na elektronički sustav plaćanja temeljen na kriptografskom dokazu umjesto na povjerenju, eng. peer-to-peer (isti s istim ili svaki sa svakim) načinom rada.



Slika 2. Peer to peer mreža

Izvor: *https://www.c-sharpcorner.com/article/building-a-blockchain-in-net-core-p2p-network/* (08.11.2022)

Vremenska oznaka je važna radi označavanja blokova i njome se dokazuje da su podaci postojali u trenutku kad se transakcija odvijala. Svako zaglavlje bloka sadrži raspršivanje prethodnog bloka, funkciju koja ispunjava šifrirane zahtjeve potrebne za zaštitu informacija, što osigurava nepromjenjivost za vrijeme dodavanja novih blokova [3].

Slika 3. Vremenska oznaka

Izvor: prilagođeno iz *https://www.researchgate.net/figure/Blockchain-timestamps-and-immutability_fig1_330972635* (10.11.2022)

Postupak formiranja mreže čvorova:

1. svaka transakcija se prenosi na sve čvorove (eng. nod),
2. svaki čvor prikuplja informacije u blok,
3. svaki čvor radi na pronalaženju dokaza o radu (eng. Proof of work) na svom bloku,
4. kada čvor pronađe dokaz o radu, prenosi ga na sve čvorove,
5. čvor prihvaća blok samo ako su sve transakcije u njemu verificirane i ako već nisu iskorištene,
6. čvor prihvaća blok radeći na način da stvara slijedeći blok u lancu koristeći enkripciju prihvaćenog bloka kao prethodni podatak.

2.2. VRSTE ULANČANIH BLOKOVA

Postoje četiri vrste ulančanih blokova: javni, privatni, konzorcijski i hibridni. U nastavku se opisuju karakteristike prethodno navedenih blokova vezano uz pristup.

2.2.1. Javni ulančani blokovi

Javni ulančani blokovi nemaju ograničenja u pristupu. Svi koji imaju pristup internetu mogu se prijaviti na ulančanu blok platformu kako bi time postali ovlašteni korisnici jednog čvorišta i dijela mreže ulančanih blokova. Time pristupaju trenutnim i prijašnjim knjigama

transakcija. Najveća korist ovakve mreže je da se ona koristi za provjeru dolaznih blokova za rudarenje i razmjenu kripto valuta kao što su Bitcoin i Litecoin.

2.2.2. Privatni ulančani blokovi

Privatni ulančani blokovi sadrže ograničenje operativnosti samo u zatvorenoj mreži. Obično se koriste unutar organizacija ili poduzeća gdje samo odabrani i odobreni članovi od strane administratora imaju dopuštenje pristupiti takvoj mreži. Razina sigurnosti, ovlaštenja, i pristupačnosti su u rukama organizacije koja ih kontrolira. Upotreba je slična kao i kod javnih mreža. Koriste se za glasovanje, digitalne identitete, popise nekretnina i vlasništva, medicinsku dokumentaciju i slično.

2.2.3. Konzorcijski ulančani blokovi

Konzorcijski ulančani blokovi su polu-decentralizirani tip gdje više organizacija može upravljati ulančanom blok mrežom. Kako bi se osigurala odgovarajuća funkcionalnost, svaka od uključenih organizacija može kreirati čvor za verifikaciju radi obavljanja funkcija provjeravanja, pokretanja ili primanja transakcija. Konzorcijski ulančani blokovi sadrže sve značajke privatnih ulančanih blokova koje uključuju privatnost, transparentnost, učinkovitost i njihovi administratori dozvoljavaju uvid nad ograničenim brojem pouzdanih čvorova.

2.2.4. Hibridni ulančani blokovi

Hibridni ulančani blokovi su kombinacija privatnih i javnih ulančanih blokova, odnosno funkcioniraju u privatnim sustavima koji su temeljeni na dopuštenjima za rad, kao i javnim sustavima bez dopuštenja. S takvim hibridnim mrežama korisnici mogu kontrolirati tko pristupa određenim podatcima koji su spremljeni u sustavu. Samo odabrani dio podataka je otvoren pristupu javnosti. Transakcija u privatnoj mreži hibridnog sustava se obično provjerava unutar te mreže. Javni ulančani blokovi povećavaju brzinu te broj čvorova kojima se može pristupiti. S obzirom da se uključuje više blokova koji se mogu provjeriti, povećava se sigurnost i transparentnost ovakve ulančane blok mreže [4].

2.3. SVOJSTVA ULANČANIH BLOKOVA

2.3.1. Transparentnost

Ulančani blokovi (eng. blockchain) su dostupni svim sudionicima ili unaprijed definiranom skupom korisnika. Dok se kod privatnih ili zatvorenih ulančanih blokova pristup zapisima može ograničiti na određene korisnike, u javnim ili otvorenim ulančanim blokovima svi koji imaju pristup internetu imaju ista prava na pristup ili ažuriranje glavne knjige transakcija (eng. ledger). Sve transakcije su transparentne i vidljive što može povećati povjerenje u mrežu.

2.3.2. Otpornost na neovlaštene izmjene

Jako bitna značajka ulančanog bloka je da je vrlo teško izmijeniti ili obrisati zapis snimljene transakcije. Svaka modifikacija ulančanog bloka je vidljiva svim korisnicima. Kriptografski potpisi osiguravaju integritet i verifikaciju transakcije.

2.3.3. Sigurnost

Čuvanje i provjeravanje podataka u sigurnom načinu rada jedna je od ključnih prednosti ulančanih blokova. Sve transakcije imaju vremenski pečat, odnosno podatke kao što su detalji o plaćanju, ugovoru, prijenosu vlasništva itd. Podatci su pohranjeni kronološkim redom što znači da ih nitko ne može modificirati. Ovo je vrlo korisna značajka stoga što korisnici mogu provjeriti kada je izvršena transakcija i njena verifikacija. Sudionici imaju poseban identitet temeljen na kombinaciji privatnoga i javnoga ključa. Javni ključevi se dijele s ostalima u mreži dok se privatni čuvaju u tajnosti. Transakcije šifrirane privatnim ključem mogu otvoriti samo primatelji sa odgovarajućim javnim ključem, ili ako je poruka šifrirana javnim ključem, mogu ga jedino otključati samo određeni primatelji koristeći njezin privatni ključ.

2.3.4. Decentralizacija

Ulančani blokovi funkcioniraju kroz distribuiranu mrežu sudionika koji ne moraju imati povjerenje jedni u druge. Provjera među sudionicima je utemeljen skup protokola, (eng. The Blockchain consensus), kojeg se korisnici pridržavaju za provjeru, validaciju i dodavanje transakcija. Najpoznatiji mehanizam konsenzusa je dokaz o radu (eng. Proof of work) koji se oslanja na računsku ili procesorsku snagu računala da bi se riješili složeni matematički algoritmi u što kraćem vremenu. S obzirom da ne postoji središnji subjekt koji bi kontrolirao taj cijeli sustav i središnja točka neuspjeha, vrlo je teško napasti takvu vrstu mreže. Postoje i različiti problemi ovakvog sustava kao što su limiti transakcija i performanse.

2.3.5. Otvorenost

Ulančani blokovi su otvoreni i pristupačni svima što znači da svatko može sudjelovati u razvoju i održavanju ulančanih blokova, pokretanju svojih blokova, potvrđivanju transakcija ili jednostavno se koristi za pohranu podataka u mreži. Prethodno navedeno podrazumijeva da bilo tko na mreži može vidjeti promjene u dijeljenoj glavnoj knjizi transakcija (eng. ledgeru) [5].

2.4. TOLERANCIJA BIZANTINSKIH GREŠAKA

Tolerancija Bizantinskih grešaka (eng. Byzantine Fault Tolerance), kraće BFT, je faktor tolerancije na pogreške ulančanih blokova koji se odnosi na sposobnost mreže da nastavi funkcionirati čak i ako neki čvorovi ili sudionici zakažu ili djeluju zlonamjerno.

Tehnologija ulančanih blokova postiže toleranciju na pogreške kroz svoju decentraliziranu i distribuiranu prirodu. U ulančanoj blok mreži transakcije su provjerene i zabilježene na mreži čvorova od kojih svaki sadržava kopiju glavne knjige što znači da čak i ako neki čvorovi zakažu ili postanu ugroženi, mreža može nastaviti funkcionirati sve dok postoji dovoljno čvorova koji su ispravni i operativni.

Ulančani blokovi mreže koriste mehanizme konsenzusa kako bi se osiguralo da se svi čvorovi slažu oko stanja glavne knjige. Ovi mehanizmi konsenzusa zahtijevaju da čvorovi

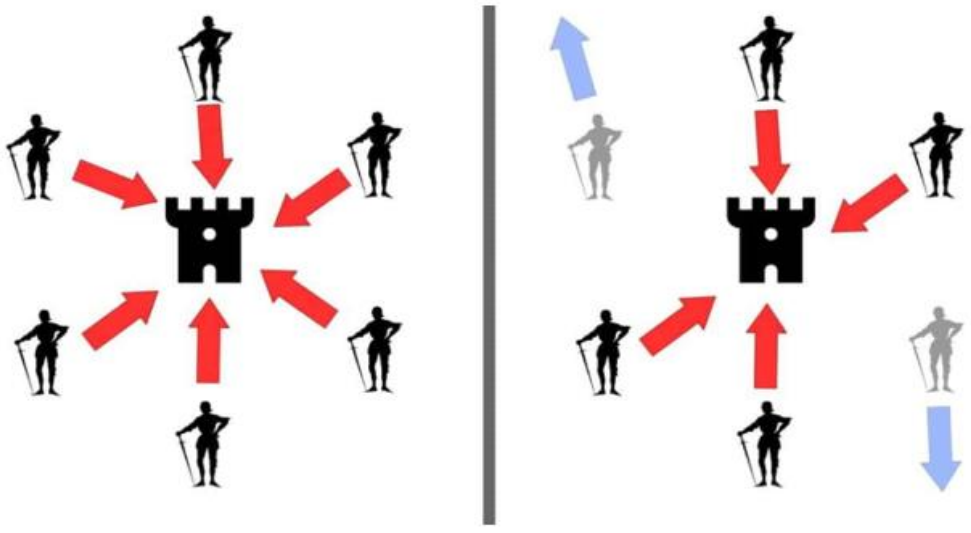
postignu dogovor kroz niz protokola čime se onemogućava bilo kojem pojedinačnom čvoru ili grupi čvorova da manipulira s glavnom knjigom. Prethodno navedeno pomaže da se osigura očuvanje integriteta glavne knjige, čak i uz prisutnost zlonamjernih osoba.

Općenito, faktor tolerancije na greške ulančanih blokova jedna je od njegovih ključnih prednosti i čini ga pouzdanom i sigurnom tehnologijom za provođenje transakcija i pohranu podataka.

Osnovni pregled funkcioniranja praktične tolerancije Bizantinskih grešaka:

1. klijent postavlja zahtjev primarnom čvoru,
2. primarni čvor šalje taj zahtjev sekundarnim čvorovima,
3. čvorovi obrađuju zahtjev, pružaju uslugu i odgovaraju klijentu,
4. klijent čeka dok ne dobije isti odgovor od m+1 čvorova, pri čemu je m najveći broj neispravnih/zlonamjernih čvorova koji sustav dopušta.

U praktičnom sustavu tolerancije Bizantinskih grešaka, maksimalan broj neispravnih ili zlonamjernih čvorova ne može biti jednak ili veći od jedne trećine ukupnog broja čvorova sustava.



Slika 4. Tolerancija Bizantinskih grešaka

Izvor: *https://cryptopotato.com/byzantine-fault-tolerance-in-blockchain-a-closer-look* (15.12.2022)

Postoji nekoliko vrijednih prednosti praktične tolerancije Bizantinskih grešaka kao na primjer da ona ne zahtijeva značajnu računalnu snagu ili potrošnju energije. To se čini ekološki prihvatljivijim u usporedbi sa dokazom o radu (eng. Proof of work). Osim toga, transakcije ne zahtijevaju višestruke potvrde. Ako se čvorovi slažu oko bloka, transakcije se odmah i potvrđuju.

Niti jedno rješenje nije savršeno, a praktična BFT ima neke značajne mane kao podložnost na napade poput Sybil, vrste napada na računalnu uslužnu mrežu, gdje jedna strana može preuzeti kontrolu nad velikim dijelom čvorova. Što je više čvorova, to je teže pokrenuti Sybil napad stoga što BFT zahtijeva komunikaciju između čvorova u svakom koraku procesa čime se troši vrijeme te uzrokuje problem sa stajališta skalabilnosti odnosno sposobnosti sustava da se prilagodi povećanom radnom opterećenju.

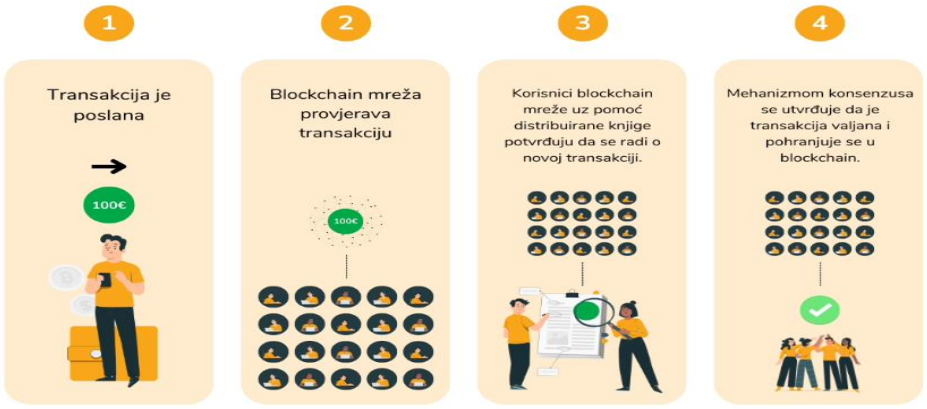
Ulančani blok možda neće uvijek imati svaki čvor koji ispravno radi i uvijek će biti zlonamjernih osoba koji pokušavaju manipulirati transakcijama. Svaka kripto valuta ima konsenzusni algoritam osmišljen kako bi joj pomogao postići određeni stupanj tolerancije Bizantinskih grešaka. Kao opće pravilo, ovi algoritmi omogućuju normalan rad kripto valuta sve dok najmanje dvije trećine njezinih čvorova ispravno funkcionira [6, 7].

2.5. DOKAZ O UDJELU (eng. PROOF OF STAKE)

Dokaz o udjelu, kraće POS (eng. Proof of stake), je noviji mehanizam konsenzusa koji pokreće novije kripto valute kao što su Ethereum 2.0, Cardano, i sl. Koristi se algoritmom koji nasumično odabire sudionike nazvani „validatori“ za stvaranje blokova temeljem iznosa uloženog broja tokena odnosno digitalne valute. Vlasnici s većom količinom tokena imaju veće šanse da budu odabrani. POS ne zahtijeva ulaganje u skupu računalnu opremu te je stoga pristupačan većem broju sudionika, posljedično transakcije postaju puno brže, mreža snažnija, a cijeli proces jeftiniji. Nedostaci ovakvog mehanizma su utjecaji na stabilnost i integritet poput centralizacije u manjim mrežama, pitanje sigurnosti i pristupačnosti [8].

2.6. DOKAZ O RADU

Dokaz o radu je mehanizam konsenzusa koji se koristi za provjeru točnosti transakcija u ulančanoj mreži. Mehanizam potvrđuje transakcije, dodaje nove blokove transakcija u „lanac“, osigurava normalan rad mreže i sprječava potencijalne probleme kao što je dupliranje tj. slanje istog tokena iz jedne transakcije više puta različitim osobama. Nakon što se blok doda u postojeći lanac, računalo koje uspije pogoditi kombinaciju kriptogramske slagalice, dobiva nagradu za svoj rad [9].

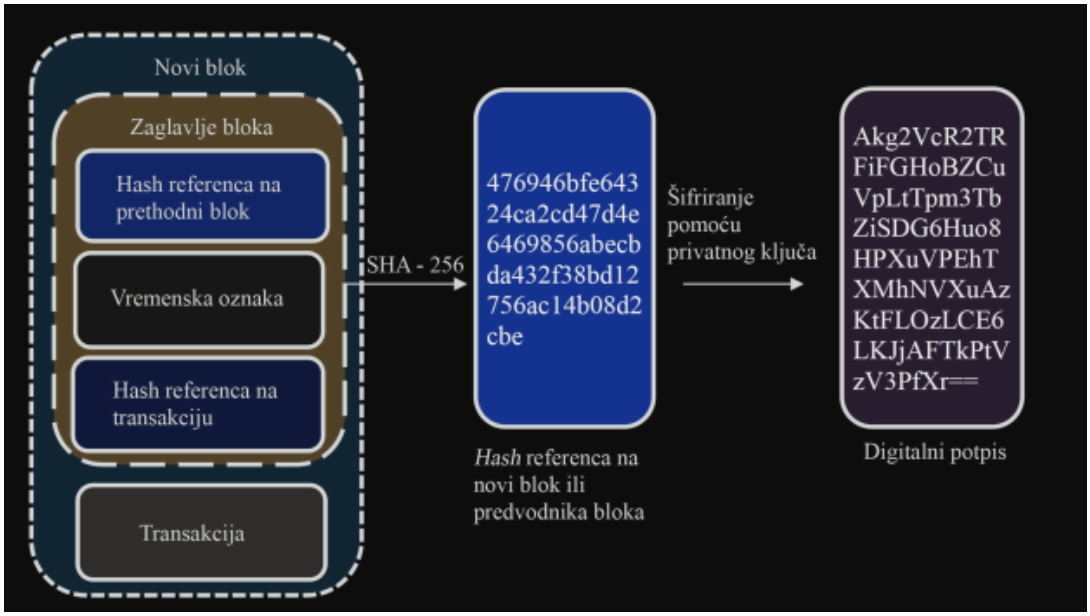


Slika 5. Opis udjela rada

Izvor: *https://www.bitcoin-store.hr/blog/sto-je-proof-of-work/* (15.01.2023)

2.7. KRIPTIRANI PODATAK (eng. HASH)

Kriptirani podatak je izlazna vrijednost funkcije koja pretvara ulazne podatke u poseban kod fiksne veličine. To je digitalni otisak kojeg je relativno lako proizvesti iz podataka kao što je bitcoin blok, ali je teško ili gotovo nemoguće otkriti početne podatke iz samog kriptiranog podatka. U ulančanoj blok tehnologiji, kriptirane funkcije su ključne jer onemogućavaju stvaranje digitalnih otisaka za blokove transakcija i osiguravaju integritet podataka. Koriste se za generiranje jedinstvenog koda za svaki blok, a taj kod se onda povezuje sa sljedećim blokom te stvara ulančani blok. Kriptirane funkcije su bitne za informacijsku sigurnost, koriste se za enkripciju podataka i digitalno potpisivanje kako bi se osigurala sigurna komunikacija putem interneta, brzo pretraživanje i provjera integriteta podataka [10].



Slika 6. Stvaranje novog bloka sa kriptiranim podatkom

Izvor: *https://hrcak.srce.hr/file/385765* (03.02.2023)

3. RAZLIKE IZMEĐU ULANČANIH BLOKOVA I OSTALIH BAZA PODATAKA

3.1. TEHNOLOGIJA RADA

Tehnologija rada ulančanih blokova distribuirane digitalne glavne knjige (eng. ledgera) omogućuje skupu čvorova da rade zajedno kako bi stvorili jedinstvenu, decentraliziranu mrežu. Također, oni mogu komunicirati i razmjenjivati informacije ili podatke i potvrđivati ih uz pomoć algoritama konsenzusa. U navedenom se slučaju koristi dokaz o radu (eng. Proof of work) koji osigurava da se u ulančanim blokovima ne koriste nevažeće transakcije. Blokovi se koriste za pohranu transakcija i drugih važnih informacija potrebnih za uspješno funkcioniranje ulančanih blokova te nema potrebe za centraliziranim tijelom što čini mrežu pouzdanom u usporedbi s drugim mrežama. Stvaraju se vremenske oznake kako bi se osiguralo da bilo tko može pratiti, podržavati i provjeravati svaku transakciju. Ovakav sustav doprinosi sigurnosti, transparentnosti i nepromjenjivosti.

Općenito baze podataka predstavljaju centralizirane knjige koje vode administratori. One pokazuju jedinstvene značajke koje uključuju sposobnost čitanja i pisanja podataka gdje samo strane s odgovarajućim pristupom mogu obavljati ove radnje. Nadalje, one omogućuju pohranu kopija podataka i njihove povijesti. Centralizacija donosi prednost brzog i jednostavnog pristupa podatcima, ali se pojavljuju i nedostatci. Jedan od nedostataka je mogućnost oštećenja podataka. Kako bi se prevladao taj nedostatak izrađuje se više sigurnosnih kopija. Drugi nedostatak je da podatke može izmijeniti svatko tko kontrolira samu bazu podataka, s obzirom da je baza podataka centralizirana.

Ulančani blokovi rade na decentralizaciji dok su baze podataka centralizirane. Decentralizacija omogućuje mrežama da rade neovisno i uklanja potrebu za centraliziranom kontrolom [11].

Baze podataka ne bi mogle biti funkcionalne bez administratora koji njime upravlja, izmjenjuje ih i kontrolira.

Kod tehnologije hibridnih ulančanih blokova administrator organizacijama daje punu mogućnost prilagodbe postavki prema zahtjevima korisnika.

3.1.1. Arhitektura

Baze podataka temelje se na arhitekturi klijent/poslužitelj. To je vrlo uspješna tehnologija koja može raditi i u malim i u velikim okruženjima. Ovdje su klijenti primatelji, dok poslužitelji djeluju kao centralizirana procesorska jedinica. Komunikacija između klijenta i poslužitelja održava se putem sigurne veze.

Ulančani blokovi koriste distribuiranu mrežnu arhitekturu glavne knjige (eng. ledgera) što omogućuje ravnopravnu komunikaciju gdje se svaki ravnopravni uređaj može povezati s drugim pomoću kriptografskih protokola. Kako ne postoji centralizirani čvor, čvorovi tj. blokovi mogu zajedno sudjelovati u algoritmu konsenzusa. Jedan od najpoznatijih takvih principa, dokaz o radu (eng. proof of work), koriste rudari kripto valuta od kojih se traži da nađu rješenje vrlo složenih matematičkih jednadžbi za provjeru valjanosti transakcija.

	Baze podataka	Hibridni ulančani blok	Javni ulančani blok
Tip	Dozvoljena	Dozvoljena	Javna
Kontrola	Centralizirano	Hibridna sa značajkama centraliziranog	Javna "peer to peer"
Arhitektura	Klijent-server	Zatvorena "peer to peer"	Javna "peer to peer"
Postojanost podataka	Nepostojanost	Nepromjenjiv	Nepromjenjiv
Mogućnost neuspjeha	Da	Ne	Ne
Performansa	Izuzetno brza	Srednja brzina	Spora

Slika 7. Arhitektura

Izvor: prilagođeno iz *https://101blockchains.com/blockchain-vs-database-the-difference/* (10.02.2023)

3.1.2. Manipulacija podatcima te transparentnost

Ulančani blokovi se baziraju na nepromjenjivosti što znači da se upisani podatak ne može obrisati niti zamijeniti čime se pospješuje sigurnost i transparentnost podataka. Upravo je transparentnost jedna od najvećih prednosti ulančanih blokova. Svaki korisnik može biti siguran da su podatci koje ima nekorumpirani od trenutka kada su zabilježeni. Radi svoje karakteristike nepromjenjivosti, integritet ulančanog bloka je osiguran. Jednom pohranjeni podaci ne mogu se oštetiti niti promijeniti na bilo koji način.

Baze podataka se bave kreiranjem, čitanjem, ažuriranjem i brisanjem podataka te su podložne manipulaciji podataka od strane zlonamjernih korisnika. Korisnici ne mogu provjeriti podatke, no administrator može skup podataka učiniti javnim iako verifikacija podataka ne može biti ostvarena samo od jednog korisnika.

3.1.3. Cijena, brzina i performansa

Baze podataka su ekonomičnije od ulančanih blokova kada se promatraju troškovi. održavanja i upravljanja, dok su ulančani blokovi nova tehnologija u koju se još uvijek ulaže radi razvoja i istraživanja. Tradicionalne baze podataka je jednostavnije postaviti i skalirati jer rade s već postojećim procesima i sustavima. Baze podataka su poznate po bržem vremenu obrade milijuna podataka u bilo kojem trenutku.

Ulančani blokovi su znatno sporiji u usporedbi s bazama podataka. Kada se transakcija izvrši u ulančanome bloku, ona se provodi na isti način kao i u tradicionalnoj bazi podataka, ali se usporava zbog izvođenja više operacija kao što su: provjera potpisa, mehanizmi konsenzusa te redundancija.

3.1.4. Prednosti ulančanih blokova pred klasičnim bazama podataka

Baze podataka su prilagođene korisnicima i podržavaju ih mnogi popularni sustavi upravljanja za programere i administratore. Sustavi poput burzi koji se oslanjaju na brzo poslovanje moraju koristiti baze podataka radi boljeg protoka podataka.

Baze podataka koriste aplikacije za kontinuirani unos podataka, mrežne obrade transakcija koje moraju biti brze, aplikacije ili sustave kojima nije potrebna provjera podataka i relacijski podaci.

Tehnologija ulančanih blokova se danas smatra svestranom tehnologijom, odnosno svestranim alatom jer nudi mogućnost pohrane različitih oblika informacija pa je tako pronašla primjenu u pohranjivanju financijskih transakcija, službenih dokumenata, medicinskih zapisa, glasova, razmjeni dobara ili imovine.

Baze podataka imaju prednost u brzini, korisnosti i točnosti, no ulančani blokovi su bolji u vezi inovacije, provjere podataka i automatizacije. Ulančani blokovi gube svoju brzinu zbog metode provjere no zato pružaju osjećaj sigurnosti i povjerenja te transparentnosti dok su baze podataka idealne za aplikacije ili usluge visokih performansi te za aplikacije koje zahtijevaju skalabilnost [12].

3.2. UPRAVLJANJE PODATCIMA

Relacijske baze podataka su preferirana tehnologija za pohranu podataka. Imaju mogućnost osiguravanja integriteta podataka i pružanja sigurnog pristupa različitim korisnicima. Bazama upravljaju odabrani administratori koji su istovremeno i vlasnici baze podataka. Ovo centralizirano tijelo održava bazu podataka čime osigurava administrativne aktivnosti poput redovitih sigurnosnih kopija, upravljanje podatcima te rješavanje samih problema baze podataka. Tradicionalne baze podataka se koriste za stvaranje, čitanje, ažuriranje i brisanje podataka, dok se kod ulančanih blokova jedino mogu dodavati novi podaci, što znači da je vidljiva povijest svih do tada upisanih podataka [13].

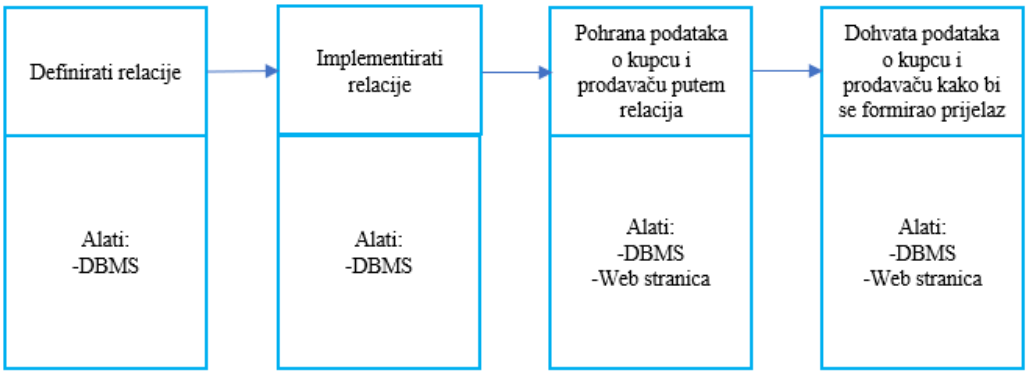
S druge strane, tehnologija distribuirane digitalne glavne knjige (javne) sve se više prepoznaje kao decentralizirana pohrana podataka i kao alternativa tradicionalnim sustavima za pohranu podataka. Njezina obilježja su distribuirani konsenzus, neovisnost o centraliziranoj vlasti, izgrađeno povjerenje, poprilično jednostavan pristup za pridruživanje mreži te stoga privlači mnoge različite domene na primjenu ove tehnologije. U ulančanim blokovima, bilo koji čvor koji ima pristup knjigama ima mogućnost potvrde i provjere te ako dođe do bilo kakve izmjene transakcije u bilo kojem bloku, izvršava se izračun kriptiranog podatka (eng. hash) koji se uspoređuje s prethodnim blokom.

Obje tehnologije koriste na isti način definiranje strukture podataka upotrebljavajući podatke o imenima, adresi, lokaciji kao što su zemljopisna dužina i širina, podatke o kontaktu, kao i preferencije o tome kako se želi trgovati. Dohvaćanje pohranjenih podataka za obavljanje transakcija se također obavlja kod obje tehnologije, podaci se dohvaćaju kako bi formirali transakcije između prodavača i kupaca.

Kod ulančanih blokova transakcije se formiraju putem algoritma za trgovinu, dok se kod baza podataka nakon trgovinskih transakcija podaci vraćaju u bazu.

3.2.1. Implementacija sa MySQL „bazom podataka"

Kao i u svakoj relacijskoj bazi podataka, strukture podataka u MySQL (eng. Structured Query Language)-u trebaju biti predstavljene putem relacija tj. tablica u bazi podataka. Kao što je prikazano na slici broj 8, proces počinje sa definiranjem tablica i odnosa među njima što zahtijeva da podaci moraju budu normalizirani i povezani. Normalizacija je uklanjanje redundancije u podacima što dovodi do sigurnosti kohezija među entitetima i povećane dosljednosti. Nakon normalizacije podaci se raspoređuju u skup povezanih entiteta nazvanih relacije u tablice.



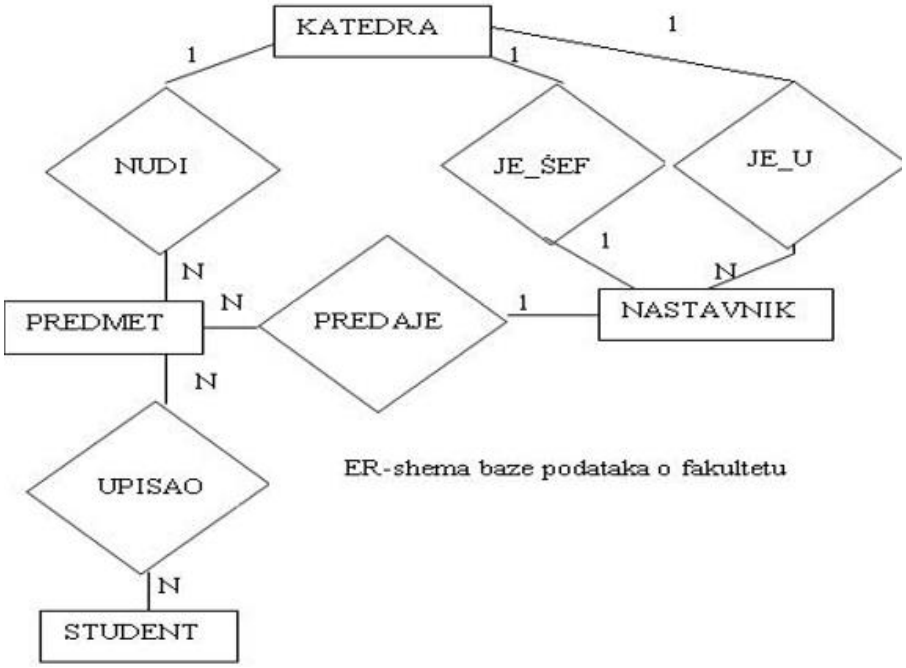
Slika 85. Pohranjivanje i dohvaćanje podataka pomoću MySQL-a

Izvor: prilagođeno iz

https://towardsdatascience.com/blockchains-versus-traditional- databasese (02.03.2023)

Jedinstveni identifikatori zvani ključevi definirani su za svaki zapis te se pozivaju u drugim zapisima kada se treba uspostaviti veza između dva dijela podataka.

Upotreba takvih ključeva osigurava referentni integritet između entiteta tj. osigurava očuvanje integriteta podataka kada se dva ili više dijelova podataka moraju odnositi jedni na druge.



Slika 9. Entiteti i odnosi identificiranja nakon normalizacije

Izvor: *https://www.znanje.org/abc/tutorials/accessmmx/01/relacije.htm* (03.03.2023)

Uz MySQL, svi koraci (tj. definicija relacije, implementacija, pohrana podataka i dohvaćanje) u potpunosti su podržani od strane samog sustava za upravljanje bazom podataka, gdje se naredbeni redak mjesto web sučelja može koristiti za izvođenje svih potrebnih radnji.

Postavljanje relacija svodi se na naredbu CREATE TABLE unutar, RDBMS (npr. za korisničku tablicu:

```
CREATE TABLE IF NOT EXIST korisnik (
korisnik_id          VARCHAR(255)          NOT NULL,
korisnicko_ime       VARCHAR(255)          NOT NULL,
adresa               VARCHAR(255)          NOT NULL,
postanski_broj       INT                   NOT NULL,
email_adresa         VARCHAR(255)          NOT NULL,
broj_mobitela        VARCHAR(255)          NOT NULL,
geografska_duzina    FLOAT                 NOT NULL,
geografska_sirina    FLOAT                 NOT NULL,
PRIMARY KEY (korisnik_id)
);
```

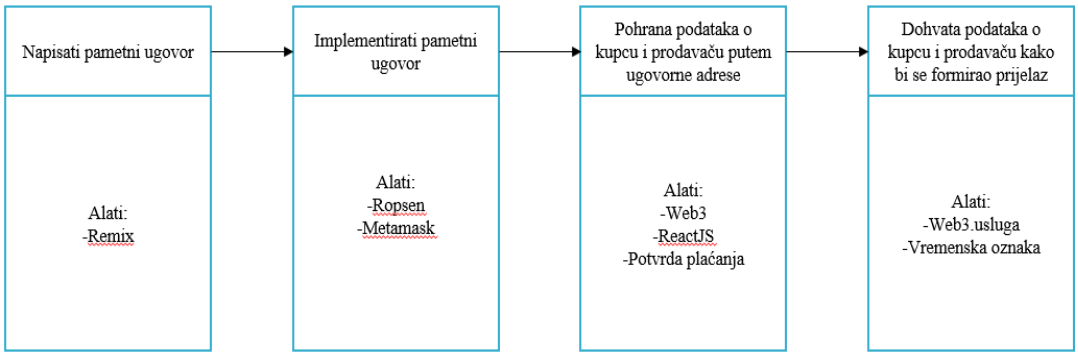
Pohranjivanje podataka se bazira na naredbu INSERT s osvrtom na specifično ime tablice, a novi redak zapisa je umetnut i pohranjen u referenciranoj tablici npr:

INSERT INTO korisnik (korisnik_id)

VALUES (12345);

Dohvaćanje pojedinih zapisa vrši se naredbom SELECT referenciranjem jedinstvenih ključeva unutar svakog zapisa podataka, pri čemu se povezani podaci identificiraju ponovljenom upotrebom istog ključa u drugim tablicama [14].

3.2.2. Implementacija sa ulančanim blokom



Slika 10. Pohranjivanje i dohvaćanje podataka uz ulančanog bloka

Izvor: prilagođeno iz

https://towardsdatascience.com/blockchains-versus-traditional-databasese (09.03.2023)

Na primjeru Ethereuma, koji je najraširenija platforma ulančanih blokova, definiranje podatkovnih struktura provodi se kroz izradu pametnog (eng. smart) ugovora kao što je prikazano na slici broj 10, i koji sadržava podatke za pohranu u ulančanome bloku. Stoga su za ovu svrhu pametni ugovori ekvivalentni tablicama u RDBMS-u.

Ethereum omogućuje uklanjanje dupliciranja (slično normalizaciji podataka u RDBMS-u) koji se provodi razbijanjem struktura podataka u više ugovora. Budući da ugovori mogu uključivati reference na druge ugovore putem svojih ugovornih adresa, a ne na pojedinačne zapise, može se usporediti s nekom vrstom stranog ključa.

Međutim, ove reference upućuju na cijeli ugovor (i njegove cjelokupne podatke), a ne pojedinačne zapise te je to razlika u odnosu na pojedinačna referenciranja zapisa RDBMS-ova.

Ugovori također mogu prikazati događaje. Događaj povezan s ugovorom definiran je za indeksiranje brzog filtriranja podataka ugovora izvan ulančanog blok pristupa [15].

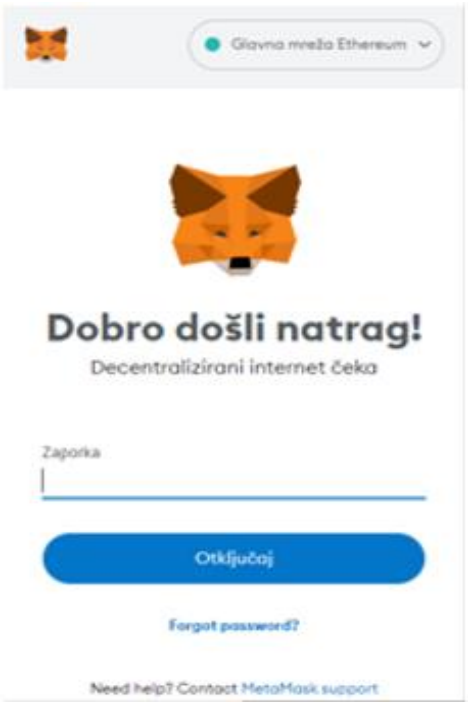
3.2.3. Interakcija ulančanog bloka

Interakcija s ulančanim blokovima je podijeljena u dvije kategorije. Prva kategorija su pozivi, interakcije s pametnim ugovorima koji samo čitaju podatke ali ne mijenjaju stanje ulančanih blokova. Kada se izvrši poziv pametnog ugovora, dobit će se odgovor s povratnim informacijama na trenutnom stanju pametnog ugovora. Pozivi dolaze izravno iz ulančanih blok čvorova i stoga ne zahtijevaju uključivanje druge strane u mreži.

Druga kategorija su transakcije, interakcije s pametnim ugovorima koje mijenjaju stanje ulančanih blokova. Moraju biti prikazane, obrađene i uključene unutar distribuirane glavne knjige. Na račun ove obrade zahtjeva se pohrana drugih čvorova u mreži, transakcije moraju biti potpisane vanjskim računom. Ovaj vanjski račun mora imati dovoljno sredstava za plaćanje troškova mreže.

Stoga se implementacija pametnog ugovora mora odvijati putem transakcije na ulančanoj blok mreži koja će ga zabilježiti u trajni registar (lanac) i potvrditi da se slaže s očekivanim formatima i pravilima (npr. koje je postavio protokol konsenzusa).

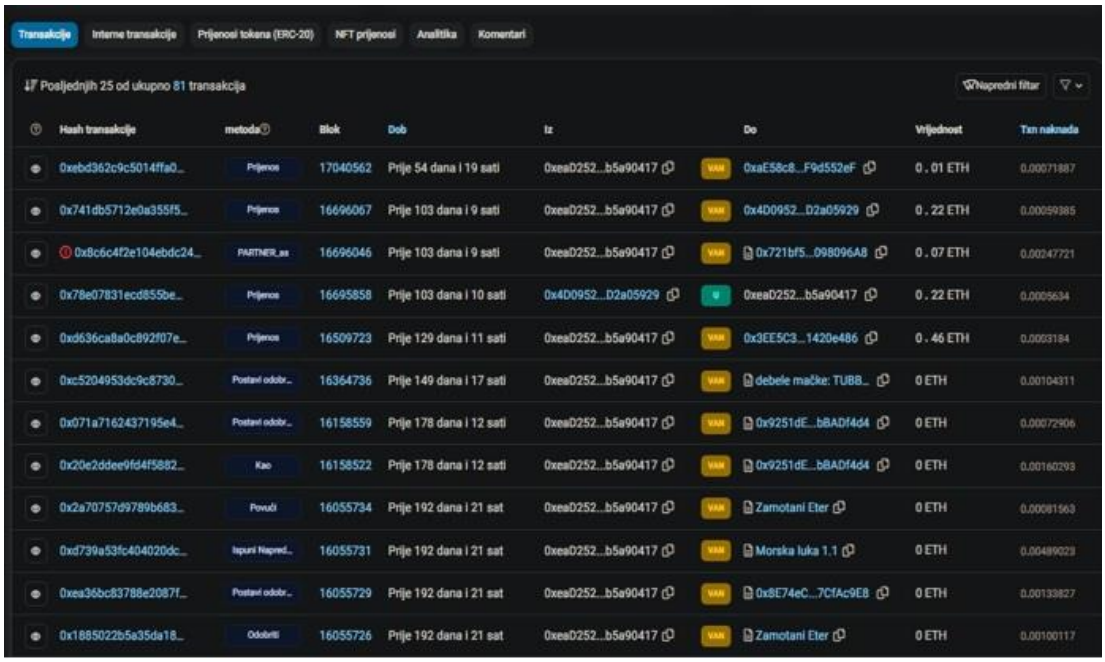
Najkorištenija aplikacija koju koristimo za pametne ugovore (smart contract) je Metamask koji nije ništa drugo nego obični chrome nastavak.



Slika 11. Metamask

Izvor: *https://metamask.io/* (13.03.2023)

Pomoću te aplikacije stvara se vlastita kontaktna adresa pomoću koje se radi identifikacija na mreži. Da bi se transakcija stvorila na mreži prethodno je potrebno napraviti običnu transakciju prijenosa sredstava s jednog računa na drugi. Jedini problem je to što se naplaćuje naknada nakon svake transakcije koja ovisi o vrsti mreže koju koristimo.



Slika 12. Transakcije

Izvor: *https://etherscan.io/address/0xead25279ac65b25b4e32dd0eacd97b98b5a90417* (13.03.2023)

Podaci se dohvaćaju iz ulančanog bloka pomoću adrese pametnog ugovora u kojem su podaci pohranjeni, što omogućuje izravni pristup pomoću poziva za čitanje varijabli unutar ugovora. Metoda dohvaćanja ovih podataka ovisi o vrsti pohrane koja se koristi unutar pametnog ugovora.

Ako pametni ugovor prikazuje događaje u mreži, mogu se postaviti upiti o tim događajima pomoću filtera na bilo kojem indeksiranom parametru (slično SELECT naredbama u SQL-u). Ovi filteri su prilično ograničeni, sa samo tri parametra koja se mogu indeksirati po događaju.

Događaji mogu također biti filtrirani prema broju bloka čime ograničuju prostor pretraživanja, ali to zahtijeva određeno znanje o pohranjenim podacima kako bi se mogli učinkovito koristiti [16] [17].

3.2.4. Usporedba karakteristika i primjene

Ulančani blokovi i MySQL su dvije tehnologije s različitim načinima upotreba i prednostima. Evo nekih zapažanja o korištenju ulančanih blokova i MySQL-a:

- sigurnost: ulančani blokovi su poznati po svojoj snažnoj sigurnosti, zahvaljujući svojoj decentraliziranoj i nepromjenjivoj prirodi. To ih čini idealnim izborom za aplikacije koje zahtijevaju visoku razinu sigurnosti, kao što su financijske transakcije, upravljanje opskrbnim lancem i sustavima glasovanja. Suprotno tome, MySQL je centralizirani sustav baze podataka koji se oslanja na sigurnosne mjere,

- performanse: MySQL je sustav baze podataka visokih performansi koji može brzo obraditi velike količine podataka i transakcija. S druge strane, ulančane blok transakcije mogu biti sporije zbog distribuirane prirode mreže i potrebe za konsenzusom među sudionicima mreže,

- skalabilnost: decentralizirana priroda ulančanih blokova omogućuje jednostavnu skalabilnost, budući da se novi čvorovi mogu dodavati mreži prema potrebi. MySQL, s druge strane, može biti zahtjevniji za skaliranje kako veličina baze podataka raste,

- trošak: postavljanje i održavanje ulančanih blokova mreže može biti skupo zbog potrebe za specijaliziranim hardverom i softverom. MySQL se, s druge strane, široko koristi i može se pokrenuti na standardnom poslužiteljskom hardveru,

- slučajevi upotrebe: ulančani blokovi se obično koriste za aplikacije koje zahtijevaju transparentnost, sigurnost i decentraliziranu kontrolu, kao što su kripto valute, pametni ugovori i upravljanje opskrbnim lancem. Dok je MySQL sustav baze podataka opće namjene koji se može koristiti za širok raspon aplikacija.

Ukratko, izbor između ulančanih blokova i MySQL-a ovisit će o specifičnim zahtjevima aplikacije. Ako su sigurnost i decentralizacija ključni, onda bi ulančani blok mogao biti najbolji izbor. Međutim, ako su performanse i skalabilnost primarni problemi, MySQL bi mogao biti bolja opcija [14] [15].

4. PRIMJENA TEHNOLOGIJE ULANČANIH BLOKOVA

4.1. PRIMJENA TEHNOLOGIJE ULANČANIH BLOKOVA U POMORSTVU

Korištenje ulančane blok tehnologije u pomorstvu bi imalo značajan utjecaj na pomorsku industriju. Na primjer, svakom plovilu iznad 100 bruto tona se izdaje jedinstveni sedmoznamenkasti međunarodni identifikacijski broj (IMO-kod) prema Međunarodnoj pomorskoj organizaciji (IMO). Česta potreba razmjena podataka između više stranaka i duga povijest različitih tipova skladišta koja se odnose na brodski IMO kod, su činjenice koje indiciraju da je potrebna svojevrsna baza podataka. Svaki podatak je različite vrste i pohranjen je u različitim fizičkim i digitalnim formatima. Također, podaci su u vlasništvu različitih organizacija čije poslovanje ovisi o razmjeni podataka. Pomorstvo stoga pruža jasni primjer industrije kojoj je potrebno zajedničko korištenje baze podataka koja se temelji na ulančanom bloku za sprječavanje nedosljednosti podataka.

„Svaki put kada učine nešto u vezi registra, bilo da je ovdje na danskom pomorstvu nadležno tijelo ili njegova brodska poduzeća, ili posrednici, ili agenti itd. šalje se putem ulančanog bloka pa se sve ažurira odjednom“[1] [18].

Pomorske tvrtke sve više ostvaruju potencijal ovakve tehnologije koja služi za održavanje certificirane povijesti informacija te sposobnost automatizacije izvršenja i izvješćivanja o transakcijama između sudionika. Implementiranje ovakvog sustava ima prednosti u smanjenju svakodnevnih troškova poslovanja u industriji i vremenskoj učinkovitosti. Pomorske tvrtke bi mogle brže i efikasnije dijeliti svoje podatke o svom održavanju i programu isporuke, statusu svojih isporuka, statusu i stanju plovila, promjena posade itd. S obzirom da se teretnice moraju izdati za svaki zaseban teret, broj vitalnih papirnatih dokumenata bi bio uvelike smanjen.

[1] Project Manager and Nautical Advisor, Danish Maritime Authority p.103, 2017.

4.1.1. Cargo X

Cargo X je digitalna kurirska služba. Ulančani blok pruža spoznaju o tome koji su digitalni dokumenti izvorni te tko ih posjeduje. Samo vlasnik dokumenta može prenijeti posjed tog dokumenta na primatelja. Slanje digitalnih podataka diljem svijeta traje nekoliko sekundi i mnogo je sigurnije i jeftinije. S ovakvim načinom pristupa rada se smanjuje šteta na okoliš, te ogromna količina papira i ugovora vezano uz korištenje zračnih, kopnenih ili brodskih vozila radi prijevoza dokumenata čime se smanjuje i korištenje fosilnih goriva. Na slici 13. prikazuje se trošak teretnog prijevoza po godinama, lokacijama i težini tereta, te se vidi značajna razlika cijene ovisno o korištenju tehnologije ulančanih blokova ili ne.

Freight market	2014	2015	2016	2017	Future with blockchain	Future without blockchain
Trans-Pacific	**(Dollars per 40-foot equivalent unit)**					
Shanghai–United States West Coast	1 970	1 506	1 272	1 485	1458.25	**1558.25**
Far East–Europe	**(Dollars per 20-foot equivalent unit)**					
Shanghai–Northern Europe	1 161	629	690	876	739	839
Shanghai–Mediterranean	1 253	739	684	817	773.25	873.25
North–South	**(Dollars per 20-foot equivalent unit)**					
Shanghai–South America (Santos)	1 103	455	1 647	2 679	1371	1471
Shanghai–Australia/ New Zealand (Melbourne)	678	492	526	677	493.25	593.25
Shanghai–West Africa (Lagos)	1 838	1 449	1 181	1 770	1459.5	1559.5
Shanghai–South Africa (Durban)	760	693	584	1 155	698	798
Intra-Asian	**(Dollars per 20-foot equivalent unit)**					
Shanghai–South-East Asia (Singapore)	233	187	70	148	59.5	159.5
Shanghai–East Japan	273	146	185	215	104.75	204.75
Shanghai–Republic of Korea	187	160	104	141	48	148
Shanghai–Hong Kong SAR	65	56	55	—	*	*
Shanghai–Persian Gulf/ Red Sea	820	525	399	618	490.5	590.5

Slika 13. Trenutna implementacija teretnice (eng. bill of landing)

Izvor: *https://unctad.org/system/files/official-document/rmt2018_en.pdf* (17.04.2023)

	Traditional Bill of Lading	CargoX Bill of Lading
Time to prepare the documents	120 – 170 minutes	N/A
Transit time	Up to 10 days, dependable on conditions	Instant, as soon as uploaded on the Blockchain
Courier costs	USD 35 – 100	USD 0
Cargo costs		
General cargo	USD 350	USD 15 for all types of Cargo
Refrigerated Cargo	USD 500	USD 15
Hazardous Cargo	USD 500	USD 15
All Other Cargo	USD 350	USD 15

Slika 14. Komparacija tradicionalne teretnice (eng. bill of landing) i Cargo x teretnice

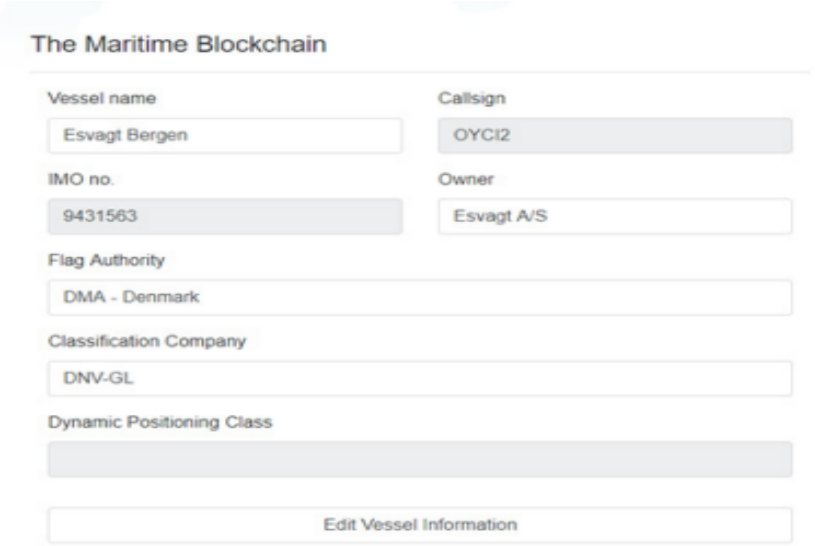
Izvor: preuzeto iz članka **Scientific Journal of Maritime Research 34 (2020) 178-184** (17.04.2023)

Na slici 14. prikazana je tablica koja uspoređuje tradicionalnu papirnatu teretnicu s Cargo x teretnicom koja predstavlja pametni ugovor. U tablici su dani parametri vezani uz vrijeme potrebno za pripremu i prijevoz dokumenata te općeniti troškovi prijevoza ovisno o potrebama vrsta tereta (hladnjača, opasan teret i sav ostali teret). Vrijeme potrebno za pripremu normalne teretnice traje oko 120-170 minuta. Vrijeme isporuke traje do 10 dana te se mora platiti dostava. Kurirski troškovi kod Cargo x teretnice ne postoje jer se može odmah izdati i predati zakonitom vlasniku. Cijena raznoraznih tereta ima trošak od 350 do 500 USD, dok je kod Cargo x ta cijena 15 USD neovisno o vrsti tereta [19].

4.1.2. Problemi koji mogu nastati te kako ih spriječiti

Javljaju se tehnički problemi, kvarovi vezani uz mrežu koji onemogućavaju pristup podacima ili izvršavanju transakcija, sigurnosni rizici poput zlonamjernih napada te neovlaštenog pristupa i promjena podataka, skalabilnosti koja se javlja u slučaju naglog porasta broja korisnika što za posljedicu ima usporavanje mreže, pravni i regulatorni izazovi, prihvaćanje i sudjelovanje relevantnih sudionika.

Korištenjem hibridnog modela omogućuje se transparentnost i pouzdanost u interakcijama između javnog i privatnog sektora u kojem dio podataka može biti javno dostupan i transparentan, omogućavajući korisnicima pristup određenim informacijama kao što su tip tereta, lokacija ili tip broda, dok drugi podatci mogu biti privatni i dostupni samo određenim sudionicima.



Slika 15. Informacije o brodu

Izvor: *https://www.researchgate.net/publication/333545589* (21.04.2024)

U privatnome sektoru ulančanog bloka postoji mogućnost administratorskog prava s kojim se dodjeljuju raznorazne privilegije/pristup podacima koji trebaju biti nepromjenjivi. IMO organizacija (eng. International Maritime Organisation) je odgovorna za reguliranje pomorskog prometa i jedna od ključnih funkcija joj je dodjela jedinstvenog koda za brodove. Organizacija usko surađuje s pomorskim autoritetima koji su odgovorni za održavanje registra, provođenje inspekcija i certificiranje brodova kako bi osigurali da brodovi udovoljavaju međunarodnim standardima sigurnosti, zaštite okoliša i radnih uvjeta.

Različita prava različitih sudionika u upravljačkome sustavu nisu jedinstvena, što dokazuje da bi korištenje ulančanog blok sustava bilo vrlo korisno [20].

4.2. PRIMJENA TEHNOLOGIJE ULANČANIH BLOKOVA U MEDICINI

4.2.1. Prednosti i problemi ulančanog bloka u medicini

Prednosti ovakve tehnologije omogućuju otpornost na neovlaštene izmjene, decentraliziranu prirodu digitalnih glavnih knjiga (ledgera), te nemogućnost naknadne promjene obavljenih transakcija unutar korisničke zajednice koja dijeli tu knjigu. Takva tehnologija se naziva tehnologija digitalne glavne knjige (DLT). Korištenjem navedene tehnologije omogućuje se nepromjenjiva baza podataka s kojom se dolazi do dostupnosti podataka bilo kojem ovlaštenom korisniku, zajedno sa zabranom korištenja od strane neovlaštenih korisnika radi enkripcije koja ovisi o privatnome ključu pacijenta.

Ulančani blok omogućuje da se stvori jedinstveni sustav za pohranjivanje podataka koji su stalno ažurirani, čime zdravstveni zapisi postaju sigurni i vrlo jednostavni za dohvaćanje i od strane ovlaštenih korisnika. Ovakav sustav nudi izbjegavanje pogrešne komunikacije između različitih zdravstvenih djelatnika što omogućuje bržu dijagnozu te intervenciju, a zdravstvena njega je personalizirana za svakog pacijenta.

Problemi koji nastaju korištenjem ovakve tehnologije su skalabilnost, povjerljivost podataka (osjetljivi medicinski podatci moraju biti zaštićeni i pravilno upravljani kako bi se osigurala sigurnost i usklađenost s propisima o zaštiti podataka), integracija s postojećim sustavima, tehničke poteškoće (zahtijevaju napredne računalne infrastrukture i složene algoritme za održavanje i sigurnost mreže), zakonski i regulatorni aspekti jer implementacija ulančanog bloka mora biti usklađena sa propisima o zaštiti podataka, pravima pacijenata i drugim relevantnim propisima [21].

4.2.2. Područja primjene

Područja primjene ulančanih blokova u medicini omogućuju:

1. upravljanje podacima elektroničke medicinske dokumentacije,
2. zaštitu zdravstvenih podataka,
3. zdravstveno osiguranje pomoću pametnog ugovora,
4. zaštitu podataka o genomu.

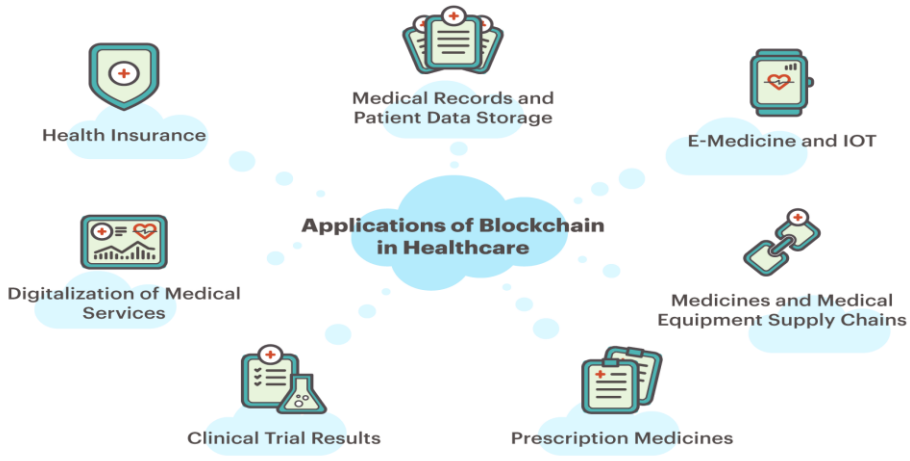
Trenutno, elektronički zdravstveni zapisi dopuštaju automatsko ažuriranje i razmjenu medicinskih podataka o određenom pacijentu samo unutar organizacije ili mreže organizacija. Postoji mogućnost proširenja ako bi informacije bile organizirane na način da su u skupu informacija na najvišem sloju ulančanog bloka samo oni podaci za osobnu identifikaciju. Navedeno bi omogućilo istraživačima i drugim organizacijama pristup ovom širokom spektru podataka koji sadrže podatke stotina tisuća pacijenata. Dostupnost takve količine podataka proizveo bi značajan razvoj kliničkih istraživanja, prijavljivanje i identifikaciju sigurnosnih događaja i štetnih događaja te izvješćivanje o javnom zdravlju.

Jedna od karakteristika trenutnih elektroničkih zdravstvenih zapisa je brzo prebacivanje pacijenata između različitih pružatelja usluga. Isti podatci u ulančanome bloku omogućuju različitim pacijentima jednostavno otključavanje i dijeljenje zdravstvenih podataka različitim pružateljima usluga ili organizacijama putem privatnog ključa. Takav sustav bi pomogao zdravstvenoj informacijskoj tehnologiji skraćeno HIT-u (eng. Health Information Technology) da postane kompatibilna i surađuje između različitih korisnika.

Od 2009. do 2017. dogodilo se više od 176 milijuna proboja podataka koji su u vezi sa zdravstvenom dokumentacijom. Sigurnosne značajke ulančanog bloka mogu puno bolje zaštititi zdravstvene podatke. Svaki pojedinac ima javni identifikator ili ključ i privatni ključ, kojim se mogu otključati podatci u onoj mjeri u kojoj su zatraženi. Svaki zlonamjerni proboj zahtijeva pojedinačni napad. Kad se takav proboj dogodi u normalnom sustavu, odjednom su vidljive sve moguće informacije o svim pacijentima.

Jedinstvena mogućnost ulančanog bloka je da pomaže u izvješćivanju o bolestima u stvarnom vremenu i istraživanju bolesti u vezi s identificiranjem podrijetla bolesti i parametara prijenosa [21] [22].

Na slici 16. prikazane su aplikacije ulančanih blokova u zdravstvenom sektoru koje se sastoje od zdravstvenog osiguranja (eng. health insurance), medicinskih podataka i medicinskih kartona pacijenata (eng. medical records and patient data storage), internet medicini i kolekciji medicinskih aplikacija (eng. E-medicine and IOT), opskrbnih lanaca lijekova i medicinske opreme (eng. medicines and medical equipment supply chains), lijekova na recept (eng. prescription medicines), rezultata kliničkih istraživanja (eng. clinical trial results) i digitalizacije medicinskih usluga (eng. digitalization of medical services).



Slika 16. Ulančani blok u medicini

Izvor: *https://medium.com/@pixelplex/blockchain-implementation-in-healthcareand-medicine-ece699e7a5bb* (07.05.2023)

4.2.3. Primjer kompanija koje koriste ulančane blokove u medicini

U nastavku se navode neke od kompanija koje koriste tehnologiju ulančanih blokova u medicini:

- Akiri Foster, grad Kalifornija: Akiri upravlja mrežom kao uslugom optimiziranom posebno za zdravstvenu industriju, pomažući u zaštiti zdravstvenih podataka pacijenata prilikom njihovog prijenosa. Mreža funkcionira kao protokol za postavljanje politika i konfiguracija slojeva podataka uz provjeru izvora i odredišta podataka u stvarnom vremenu. Kompanija osigurava da zdravstveni podaci ostanu zaštićeni i djeljivi samo sa stranama ovlaštenima za pristup u trenucima kad im zatrebaju.

- BurstIQ, Kolorado Springs: kompanija koristi ulančani blok za poboljšanje načina dijeljenja i korištenja medicinskih podataka. Uključuje potpune i ažurirane informacije o zdravlju i zdravstvenoj aktivnosti pacijenata, mogli bi pomoći iskorijeniti zloupotrebu opioida ili drugih lijekova na recept.

- Medicalchain, London: održavaju integritet zdravstvenih kartona dok uspostavljaju jedinstvenu vezu između pacijenta i doktora. Liječnici, bolnice i laboratoriji mogu zahtijevati sve podatke o pacijentima koji imaju zapis o podrijetlu i štite identitet pacijenta iz vanjskih izvora. U svibnju 2018. Medicalchain je objavio svoju stranicu Myclinic.com, platforma za

telemedicinu koja omogućuje pacijentima da se savjetuju sa svojim liječnicima putem videa i plaćaju konzultacije sa kripto valutom nazvanom „medtokens“.

- ProCrexEx, Tampa Florida: platforma koristi vlasničke mehanizme za provjeru valjanosti i ograničava članstvo samo na provjerene i odabrane organizacije kako bi zdravstveni sustavi mogli brzo steći provjerene certifikate i promovirati sigurnost pacijenata i kvalitetu njege.

- Embleema, New York: virtualna platforma za ispitivanje i regularnu analizu koja je dizajnirana za ubrzanje razvoja lijekova. Korisnici koji su prijavljeni digitalno pristaju na sigurnu, nepromjenjivu bazu medicinskih podataka, koja se pohranjuje na bloku Embleema i analiziraju. Platforma omogućuje pacijentima da pomognu u ubrzavanju dostupnosti liječenja i poboljšanju sigurnosti putem virtualnih studija tvrtke [23].

4.3. OSTALA PODRUČJA PRIMJENE TEHNOLOGIJE ULANČANIH BLOKOVA

4.3.1. Automobili/mobiteli

Postoje primitivni oblici pametnog vlasništva. Ključ automobila, na primjer, može biti opremljen imobilizatorom, pri čemu se automobil može aktivirati jedino kada se dodirne pravi protokol na ključu, a pametni telefon će funkcionirati tek nakon što je unesen ispravan PIN kod. Oboje rade na kriptografiji kako bi zaštitili vlasništvo. Problem s primitivnim oblicima pametnog vlasništva kao što su fizički ključevi i kartice je taj da imaju ograničenja u pogledu prenosivosti i kopiranja što može uzrokovati probleme i ograničenja u upravljanju vlasništvom i pristupom. Ulančana blok tehnologija rješava navedeni problem tako da pruža siguran način pohrane vlasničkih podataka i omogućuje njihovu prenosivost putem digitalnih ključeva.

4.3.2. Putovnice

Prva digitalna putovnica pokrenuta je na internetskoj platformi za upravljanje izvornim kodom tzv. „Githubu“ godine 2014. Digitalna putovnica je temeljena na tehnologiji ulančanog bloka te je kombinirala prednosti digitalne putovnice s karakteristikama sigurnosti, transparentnosti i neporecivosti. Podatci o putniku kao što su osobni podatci, biometrijski podaci i povijest putovanja, mogli su se pohraniti kao digitalni zapisi u blokovima. Ti zapisi se kriptiraju i digitalno potpisuju kako bi se osigurao njihov integritet i autentičnost. Svi relevantni sudionici, kao što su vlasti za izdavanje putovnica, granične kontrole ili putničke agencije, mogu imati pristup relevantnim informacija putem distribuirane knjige. To pruža transparentnost i smanjuje mogućnost manipulacije ili krivotvorenje podataka.

4.3.3. Pametna imovina

Svi entiteti/imovina kao što su kuća, zemljište, automobili, dionice itd. mogu biti predstavljeni u tehnologiji glavne knjige i ulančanih blokova koji se mogu koristiti za praćenje svih operacija i evidencija imovine.

Nakon što su zapisi pohranjeni u ulančanome bloku, oni se dijele sa svim zainteresiranim stranama ili sudionicima stranke koje se lako mogu koristiti za sklapanje ugovora i njihovu provjeru. Dakle, s decentraliziranim knjigama, bilo koji izgubljeni zapis se može duplicirati s mreže i odmah se može koristiti za oporavak.

4.3.4. Pametni uređaji

Pametni uređaji su elektronički uređaji potpomognuti kibernetičkim sustavom tako da kibernetički dio može razmjenjivati informacije o okolini oko uređaja i samom uređaju.

Moguće je koristiti ulančani blok za kodiranje pametnih uređaja kao pametnih vlasništva jer pruža sigurnu i transparentnu platformu za evidenciju vlasništva i praćenje promjena u vlasništvu pametnih uređaja. Kada se pametni uređaj registrira u ulančani blok, generira se jedinstveni digitalni identitet za taj uređaj. Taj identitet se zatim povezuje s vlasnikom uređaja putem digitalnog potpisa ili drugih kriptografskih mehanizama.

Informacije o vlasništvu, povijesti prijenosa vlasništva i drugih relevantnih podataka se zatim pohranjuju kao transakcije u blokove ulančanih blokova.

4.3.5. Donacije i transparentnost

Ulančani blok pruža mogućnost poboljšanja transparentnosti u procesu donacija. Koristi se za evidentiranje svake donacije kao transakcije koja sadrži informacije o donatoru, primatelju, iznosu donacije i vremenu transakcije. Pruža preglednost raspodjele sredstava, odnosno svi sudionici mreže mogu provjeriti i pratiti kako su donirana sredstva raspoređena i koriste li se u skladu s namjerom donacije. Time se osigurava autentičnost donacija te se prati napredak projekata ili inicijativa koje se financiraju.

4.3.6. Glasovanje

Glasovanje putem ulančanog bloka pruža mogućnost transparentnog, sigurnog i neporecivog procesa glasanja. Funkcionira na sljedeći način:

- identifikacija birača: svaki birač ima svoj jedinstveni identitet koji je povezan s njegovim biometrijskim podacima ili drugim identifikacijskim podacima koji mogu biti provjereni kroz postojeće sustave ili putem biometrija ili digitalnih potpisa.

- kreiranje blokova glasova: svaki glas se bilježi kao transakcija koja sadrži informacije o biraču, izborima na koji se glasa, vremenu glasanja i drugim relevantnim podacima. Ove se transakcije kriptografski potpisuju.

- validacija i potvrda glasova: ulančani blok koristi konsenzusni mehanizam kako bi se osiguralo da samo valjani glasovi ulaze u blokove. Validatori mreže provjeravaju i potvrđuju glasove.

- transparentnost: svi sudionici imaju pristup blokovima i mogu provjeriti rezultate glasanja. Blokovi su transparentni i neizmjenjivi.

- anonimnost: identitet birača može biti kriptografski zaštićen, a samo relevantne informacije potrebne za provjeru valjanosti glasa su dostupne.

- rezultati i deklariranje pobjednika: po završetku glasanja, rezultati se mogu automatski izračunati temeljem broja glasova zabilježenih u blokovima ulančanih blokova [24].

5. ZAKLJUČAK

Tehnologija ulančanih blokova je koncept koji se još uvijek razvija, ali već privlači veliku pozornost i prihvaćanje od strane tvrtki i vlada diljem svijeta. Iako se tehnologija nalazi u ranim fazama, njeno napredovanje je brzo, a različite industrije istražuju njezine mogućnosti te je sve više u upotrebi.

Usprkos brojnim prednostima tehnologije ulančanih blokova postoje izazovi i ograničenja koja se moraju riješiti kako bi se postiglo šire usvajanje. Neki od tih izazova uključuju skalabilnost, interoperabilnost i usklađenost s propisima.

Uspjeh tehnologije ulančanih blokova u konačnici će sve ovisiti o njenom usvajanju i integraciji u svijetu. Tvrtke i pojedinci moraju biti spremni prilagoditi svoje poslovne modele i infrastrukturu kako bi iskoristili puni potencijal ove tehnologije. Uvođenje tehnologije ulančanih blokova zahtijeva suradnju različitih dionika, uključujući tvrtke, vladu, regulatorna tijela i korisnike. Važno je stvoriti okruženje koje potiče inovacije i podržava usvajanje ove tehnologije.

U konačnici tehnologija ulančanih blokova predstavlja obećavajući alat koji će utjecati na različite sektore te će promijeniti način na koji se obavljaju transakcije i upravljanje podacima. Unatoč izazovima koji se moraju riješiti, očekuje se da će tehnologija ulančanih blokova imati značajan utjecaj na budućnost.

LITERATURA

[1] L. Popovski, i G. Soussou „A Brief History of Blockchain“ 2018. dostupno na: https://bit.ly/2FbJrg2, (pristupljeno 08.11.2022).

[2] S. Nakamoto 2008. "A peer-to-peer electronic cash system" https://bitcoin.org/bitcoin.pdf, (pristupljeno 8.11.2022).

[3] A. Hughes "Blockchain timestamps and immutability" https://www.researchgate.net/figure/Blockchain-timestamps-and-immutability_fig1_330972635, (pristupljeno 10.11.2022).

[4] "What is blockchain", types of blockchains https://www.oracle.com/middleeast/blockchain/what-is-blockchain/. (pristupljeno 12.12.2022).

[5] "Features of blockchain", Data-flair.training https://data-flair.training/blogs/features-of-blockchain/ (pristupljeno 13.12.2022).

[6] M. Castro, B. Liskov, "Practical Byzantine fault tolerance In Proceedings of the Third Symposium on Operating Systems Design and Implementation", 1999.

[7] „Byzantine fault tolerance explained“, academy.binance https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained. (pristupljeno 15.12.2022).

[8] "What is proof of stake", Investopedia.com https://www.investopedia.com/terms/p/proof-stake-pos.asp (pristupljeno 15.01.2023).

[9] "Što je Proof of Work?", Bitcoin-store.hr https://www.bitcoin-store.hr/blog/sto-je-proof-of-work/ (pristupljeno 15.01.2023).

[10] NIST (2015a), “Secure hash standard”, doi: 10.6028/NIST.FIPS.180-4, dostupno na: www.nist.gov/publications/secure-hash-standard (pristupljeno 03.02.2023).

[11] B. Imran, "Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained" 2018.

[12] "Blockchain vs Database"- Understanding the difference, 101blockchains.com https://101blockchains.com/blockchain-vs-database-the-difference/ (pristupljeno 10.02.2023).

[13] B. Imran "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications" 2022.

[14] C. Andrew, B. Stephen, "MySQL Explained: Your Step-by-Step Guide" 2015.

[15] "How to store data on ethereum blockchain", geeksforgeeks.org
https://www.geeksforgeeks.org/how-to-store-data-on-ethereum-blockchain/
(pristupljeno 09.03.2023).

[16] "How to use metamask to deploy a smart contract in solidity blockchain“, geeksforgeeks.org
https://www.geeksforgeeks.org/how-to-use-metamask-to-deploy-a-smart-contract-in-solidity-blockchain/
(pristupljeno 13.03.2023).

[17] "How does MetaMask connect to a blockchain network", support.metamask.io
https://support.metamask.io/hc/en-us/articles/5378119120667-How-does-MetaMask-connect-to-a-blockchain-network-
(pristupljeno 13.03.2023).

[18] Project Manager and Nautical Advisor, Danish
Maritime Authority p.103, 2017.

[19] Scientific Journal of Maritime Research 34 (2020) 178-184 (pristupljeno 17.04.2023)

[20] "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies", researchgate.net.
https://www.researchgate.net/publication/333545589_A_Ten-Step_Decision_Path_to_Determine_When_to_Use_Blockchain_Technologies.
(pristupljeno 21.04.2023).

[21] Khezr, S. et al. (2019). „Blockchain technology in healthcare: a comprehensive review and directions for future research Applied Sciences“. Dostupno na
https://doi.org/10.3390/app9091736.
(pristupljeno 07.05.2023).

[22] "Blockchain Applications in Healthcare", news-medical.net
https://www.news-medical.net/health/Blockchain-Applications-in-Healthcare.aspx
(pristupljeno 07.05.2023).

[23] "Blockchain in Healthcare", builtin.com
https://builtin.com/blockchain/blockchain-healthcare-applications-companies
(pristupljeno 07.05.2023).

[24] J. Cybersecur. Priv. 2021, 1(1), 4-18;
dostupno na https://doi.org/10.3390/jcp1010002.

KAZALO KRATICA

Kratica	Značenje na engleskom	Hrvatski prijevod
DLT	Digital Ledger Technology	Tehnologija digitalne knjige
HIT	Health Information Technology	Zdravstvena informacijska tehnologija
IMO	International Maritime Organization	Međunarodna pomorska organizacija
RDBMS	Relational Database Management System	Sustav upravljanja relacijskom bazom podataka
BFT	Byzantine Fault Tolerance	Tolerancija bizantinskih grešaka
POS	Proof of Stake	Dokaz o udjelu
POW	Proof of Work	Dokaz o radu

POPIS SLIKA