

Blockchain tehnologija u bankarskom sektoru

Puškaric, Anamarija

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Economics and Business in Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Ekonomski fakultet u Osijeku**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:145:353886>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-03-04**



Repository / Repozitorij:

[EFOS REPOSITORY - Repository of the Faculty of Economics in Osijek](#)



Sveučilište Josipa Jurja Strossmayera u Osijeku

Ekonomski fakultet u Osijeku

Sveučilišni diplomski studij Financijski menadžment

Anamarija Puškarić

BLOCKCHAIN TEHNOLOGIJA U BANKARSKOM SEKTORU

Diplomski rad

Osijek, 2024.

Sveučilište Josipa Jurja Strossmayera u Osijeku
Ekonomski fakultet u Osijeku
Sveučilišni diplomski studij Financijski menadžment

Anamarija Puškarić

BLOCKCHAIN TEHNOLOGIJA U BANKARSKOM SEKTORU

Diplomski rad

Kolegij: ICT u bankarstvu

JMBAG: 0010225424

e-mail: apuskaric@efos.hr

Mentor: prof. dr. sc. Nataša Šarlija

Osijek, 2024.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics and Business in Osijek
University Graduate Study Financial management

Anamarija Puškarić


BLOCKCHAIN TECHNOLOGY IN THE BANKING SECTOR

Graduate paper

Osijek, 2024.

IZJAVA

O AKADEMSKOJ ČESTITOSTI, PRAVU PRIJENOSA INTELEKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat osobnoga rada koji se temelji na vlastitim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.
2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom *Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska*. 
3. Kojom izjavljujem da sam suglasan/suglasna trajnom pohranjivanju i objavljivanju mog rada u Institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, Repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom Repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o visokom obrazovanju i znanstvenoj djelatnosti, NN 119/2022).
4. Izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan s dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta/studentice: Anamarija Puškarić

JMBAG: 0010225424

OIB: 20903170655

e-mail za kontakt: anamarijap44@gmail.com

Naziv studija: Financijski menadžment

Naslov rada: Blockchain tehnologija u bankarskom sektoru

Mentor/mentorica rada: prof. dr. sc. Nataša Šarlija

U Osijeku, 29.5.2024. godine

Potpis 

Sažetak

Ovaj diplomski rad daje kratak opis važnih pojmova u blockchainu kao što su povijesni razvoj, arhitektura blockchaine, funkcioniranje blockchaine, vrste mreže te algoritam blockchaine. Blockchain tehnologija se ističe svojom inovativnom distribuiranom prirodom koja omogućuje verifikaciju transakcija putem decentraliziranog sustava. Sigurnost je jedan od ključnih aspekata, budući da blockchain pruža visoku razinu zaštite transakcija kroz kriptografske tehnike. Transparentnost je također značajna, jer omogućuje svim sudionicima u transakcijama da prate svaki korak transakcije, smanjujući mogućnost prijevara i povećavajući povjerenje. Efikasnost je dodatna prednost, jer transakcije putem blockchain tehnologije obavljaju se brže i bez potrebe za posrednicima, čime se smanjuju troškovi i vrijeme provedeno u financijskim transakcijama. Kroz analizu primjera primjene blockchain tehnologije u bankarstvu na primjerima JP Morgan Chase, HSBC, Santander i Barclays, ovaj rad istražuje konkretne prakse sa svim svojim prednostima i nedostacima. Također, u radu su objašnjeni i izazovi koji proizlaze iz uvođenja ove inovativne tehnologije u bankarski sektor. Rezultati ovog istraživanja pružaju relevantan uvid u potencijalne prednosti i izazove koje donosi integracija blockchain tehnologije u bankarski sektor, nudeći smjernice za buduće strategije implementacije i razvoja u financijskom poslovanju.

Ključne riječi: blockchain, sigurnost, efikasnost, transparentnost

Abstract

This thesis provides a brief description of important concepts in blockchain, including its historical development, blockchain architecture, blockchain functionality, types of networks, and blockchain algorithm. Blockchain technology stands out due to its innovative distributed nature, which enables transaction verification through a decentralized system. Security is one of the key aspects, as blockchain offers a high level of protection for transactions through cryptographic techniques. Transparency is also significant, as it allows all participants in transactions to monitor every step of the transaction, reducing the possibility of fraud and increasing trust. Efficiency is an additional advantage, as transactions via blockchain technology are completed faster and without the need for intermediaries, thereby reducing costs and time spent on financial transactions. Through an analysis of examples of the application of blockchain technology in banking, with case studies such as JP Morgan Chase, HSBC, Santander, and Barclays, this paper explores concrete practices along with their advantages and disadvantages. The paper also explains the challenges that arise from introducing this innovative technology into the banking sector. The results of this research provide a relevant insight into the potential benefits and challenges that the integration of blockchain technology brings to the banking sector, offering guidelines for future implementation and development strategies in financial operations.

Keywords: blockchain, security, efficiency, transparency

Sadržaj

1. Uvod	1
2. Metodologija rada	3
3. Blockchain: Početak nove ere povjerenja i transakcija	4
3.1. Povijesni razvoj Blockchaina	4
3.2. Arhitektura blokchaina	6
3.3. Kako blockchain funkcionira?	10
3.4. Vrste blockchain mreže	12
3.5. Algoritam blockchaina	14
4. Opis istraživanja i rezultati istraživanja	18
4.1. Blockchain u bankarstvu	18
4.2. Implementacija blockchaina u bankarstvu	21
4.3. Sigurnost transakcija	25
4.4. Transparentnost blockchaina	26
4.5. Efikasnost transakcija	27
4.6. Izazovi blockchaina u bankarskom sektoru	29
5. Rasprava	31
6. Zaključak	34
Literatura	36
Popis slika	40
Popis grafikona	40

1. Uvod

U suvremenom digitalnom okruženju, napredak tehnologije igra ključnu ulogu u održavanju konkurentnosti, posebno u bankarskom sektoru koji neprestano prilagođava svoje poslovanje. Integracija blockchain tehnologije u bankarstvo često se opisuje kao revolucionarni pomak koji obećava transformirati načine rada banaka diljem svijeta. Blockchain tehnologija, temeljena na konceptu distribuiranog registra transakcija među mnogim čvorovima umjesto centralizirane pohrane podataka, pruža revolucionaran pristup vođenju transakcija i upravljanju podacima unutar bankarskih sustava.

Ovaj istraživački rad je temeljen na važnoj temi blockchain tehnologije i njezinom potencijalnom utjecaju na bankarski sektor. Cilj istraživanja je analizirati na koji način primjena blockchain tehnologije može transformirati tradicionalne prakse u bankarstvu, posebice s naglaskom na tri ključna područja: sigurnost, transparentnost i efikasnost transakcija.

Rad je podijeljen u nekoliko faza koje će se sustavno baviti prethodno navedenim područjima. Prva faza istraživanja fokusirat će se na pružanje detaljnog pregleda osnovnih principa blockchain tehnologije kao i njezinih karakteristika koje je čine atraktivnom za financijski sektor. Ova faza će pokušati objasniti zašto je blockchain tehnologija relevantna za bankarski sektor te kako se može primijeniti radi unaprjeđenja dosadašnjih praksi.

Nakon toga, istraživanje će prijeći na analizu postojećih primjera implementacije blockchain tehnologije u bankarskom sektoru. Cilj ove faze je identificirati ključne prednosti koje takve inicijative donose, ali i izazove s kojima se suočavaju banke prilikom implementacije. Sljedeća faza istraživanja bit će usmjerena na specifične aspekte sigurnosti transakcija, s ciljem istraživanja novih inovativnih rješenja koje blockchain tehnologija pruža radi zaštite podataka i smanjenja rizika od prijevara. Također će se analizirati kako transparentnost koju blockchain pruža može doprinijeti jačanju povjerenja klijenata u bankarski sektor.

U posljednjoj fazi istraživanja, analizirat će se kako primjena blockchain tehnologije utječe na efikasnost procesa transakcija u bankama. Ovdje će se posebno analizirati ubrzanje transakcijskih vremena, smanjenje troškova transakcija te općenito poboljšanje operativne učinkovitosti.

Kroz navedene faze istraživanja, cilj je napraviti analizu utjecaja blockchain tehnologije na sigurnost, transparentnost i efikasnost transakcija u bankarskom sektoru, ističući ključne prednosti i izazove koje donosi ova digitalna transformacija.

U radu je postavljena sljedeća hipoteza: Implementacija blockchain tehnologije znatno unaprjeđuje integritet i neporecivost transakcijskih zapisa u bankarskom sektoru, čime značajno doprinosi smanjenju incidencija prijevara i neovlaštenih intervencija

2. Metodologija rada

Diplomski rad strukturiran je u šest poglavlja. U uvodnom dijelu detaljno je opisana tema rada, naglašeno je što će biti obuhvaćeno u teorijskom dijelu te objašnjen je pristup izrade empirijskog dijela rada. Drugo poglavlje posvećeno je metodologiji rada gdje je opisan predmet istraživanja, postavljeni su ciljevi, kao i opisane metode koje su korištene. U trećem poglavlju postavljaju se osnovne podloge i karakteristike blockchaina koje služe kao uvodna točka za bolje razumijevanje blockchaina koji je opisan u sljedećem poglavlju kroz njegovu povijest, funkcioniranje, vrste mreža, arhitekturu i algoritme. U empirijskom dijelu, odnosno četvrtom poglavlju, opisane su primjene blockchaina na stvarnim primjerima JP Morgan Chasea, HSBC-a, Barclays i Santander banke, isto kao i ključne prenosti i izazovi primjene blockchain tehnologije u bankarstvu promatrano kroz aspekte sigurnosti, transparentnosti i efikasnosti. Sljedeće poglavlje rezervirano je za raspravu rezultata istraživanja i odbacivanja ili prihvatanja postavljene hipoteze.

Cilj ovog istraživanja je detaljno analizirati utjecaj blockchain tehnologije na sigurnost, transparentnost i efikasnost transakcija u bankama, ističući ključne koristi i izazove ovakvog prelaska u digitalnu eru.

Tijekom istraživanja temeljenog na analizi i sintezi, kao osnovnim metodama istraživanja, korištene su i povijesna metoda, metoda indukcije i dedukcije u procesu donošenja zaključaka, te metoda deskripcije i metoda klasifikacije. Kao izvor informacija korištena je domaća i strana literatura iz koje su prikupljeni sekundarni podaci, a obuhvaćali su stručne knjige kao i razne internetske stranice.

3. Blockchain: Početak nove ere povjerenja i transakcija

Blockchain je koncept izveden iz riječi "Block" (blok) i "Chain" (lanac), opisujući tako sustav povezanih blokova podataka. Blockchain je termin na engleskom jeziku koji se koristi za distribuiranu bazu podataka, koja istovremeno postoji na više računala. U slučaju kriptovaluta, blockchain se često naziva "glavnom ili javnom knjigom" zapisa što bi na engleskom jeziku bilo „public ledger“. Blockchain tehnologija temelji se na sustavu ravnopravnih sudionika (peer-to-peer), oblikujući decentraliziranu mrežu bez potrebe za središnjim autoritetom kao što su banke ili druge financijske institucije (Mataković i Cunjak Mataković, 2018). Ova tehnologija trenutno predstavlja jedan od najsigurnijih načina bilježenja aktivnosti i održavanja aktualnih podataka, omogućujući održavanje transparentne povijesti zapisa bez pogrešaka. Jednom zapisani i potvrđeni podaci postaju dio trajnog bloka koji je gotovo nemoguće izmijeniti ili korumpirati, a brisanje podataka zahtijevalo bi promjenu cijelog blockchain lanca. Povijesni trag podataka i ažuriranja zapisa dostupni su brže nego kod tradicionalnih metoda pohrane (Horvatić, Tafra, 2022). U početku je postojala značajna sumnja prema sudionicima transakcija. No, s napretkom blockchain tehnologije, taj je problem uspješno riješen. Blockchain omogućuje funkcioniranje kao pouzdan posrednik, eliminirajući potrebu za trećom stranom koja bi autentificirala transakcije. Omogućavanjem brzih, ekonomičnih i visoko sigurnosnih kriptiranih informacija, blockchain stvara digitalno povjerenje među sudionicima transakcija. Javne blockchain mreže su otvorene za sve, dok su privatne ograničene na određene sudionike. Različite blockchain platforme koriste različite algoritme i tehnike za postizanje svojih ciljeva. Blockchain tehnologija ima potencijal transformirati mnoge industrije putem transparentnosti, sigurnosti i decentralizacije. Međutim, ključno je temeljito razumjeti i analizirati tehnologiju, kao i njene prednosti i ograničenja, prije nego što se primijeni na određene projekte ili sektore.

3.1. Povijesni razvoj Blockchaina

Blockchain tehnologija postala je široko prepoznata putem pojave digitalne valute Bitcoin, koja se oslanja na principe blockchain tehnologije. Bitcoin je započeo s objavom prvog "Genesis" bloka koji je aktiviran 3. siječnja 2009. godine, a kojega je postavio programer pseudonima Satoshi Nakamoto (Hayes, 2024). Tehnologija blockchain prvi puta je predstavljena javnosti 31. listopada 2008. godine, putem objave na mailing listi fokusiranoj na kriptografiju. U toj

objavi nalazio se link prema članku pod nazivom "Bitcoin: A Peer-to-Peer Electronic Cash System" koji je objavila osoba ili grupa poznata pod pseudonimom Satoshi Nakamoto. (Nakamoto, 2008). Ovaj revolucionarni članak predložio je decentralizirani sustav za razmjenu vrijednosti, koji je postao temelj za razvoj blockchain tehnologije. Nakamoto je osmislio inovativan pristup transakcijama koji je omogućio stvaranje sigurnog, transparentnog i nepromjenjivog registra transakcija. Ideja Satoshija Nakamota dovela je do razvoja Bitcoina, prve digitalne valute koja koristi blockchain tehnologiju. Pokretanjem Bitcoin mreže 2009. godine, uveden je novi model digitalnog povjerenja koji omogućuje transparentne transakcije. Za razvoj Bitcoin mreže. Genesis blok dobio je ime zato što je prvi blok ikada stvoren u blockchainu. Svaki slijedeći blok u blockchainu obično se referira na prethodni blok, dok je Genesis blok poseban jer nema prethodnika. Stoga su početni blokovi često trajno ugrađeni u kod samog blockchaina (Connors i Sarkar, 2023).

3.1.1. Genesis blok

Genesis blok je ključni element svake blockchain mreže jer služi kao temelj cijele strukture. Postoji nekoliko razloga zašto je Genesis blok potreban. Prvo, on inicijalizira mrežu. Pružajući prvi blok u lancu, Genesis blok sadrži hardkodirane podatke koji postavljaju temelje za sve kasnije blokove, uključujući izvorne parametre mreže, prve transakcije i kriptografski hash koji identificira blok. Drugi razlog je osiguranje konsenzusa među sudionicima mreže. Budući da je prvi blok, Genesis blok igra ključnu ulogu u uspostavljanju dogovora među sudionicima o početnom stanju mreže. Ovaj konsenzus je bitan jer blockchain mreže zavise od mehanizma dogovora kako bi se osiguralo da svi sudionici mreže prihvate trenutno stanje mreže. Dodatno, Genesis blok pruža fiksnu početnu točku za blockchain mrežu. To znači da se svi kasniji blokovi mogu provjeravati i pratiti unatrag do prvog bloka, što je ključno za održavanje integriteta blockchaina i sprječavanje bilo kakvih lažnih ili zlonamjernih aktivnosti. Genesis blok također postavlja nagradu za blok u mnogim blockchain mrežama. U pravilu, to je jedini blok koji ima fiksnu nagradu, što motivira rudare da započnu rudarenje i pridonose računalnoj snazi mreže, čime se dodatno osigurava mreža. Naposljetku, Genesis blok ima značajnu povijesnu i kulturnu važnost u svijetu blockchain tehnologije. Predstavlja rođenje jednog novog razdoblja decentraliziranih peer-to-peer mreža. To je simbol potencijala decentraliziranih tehnologija da transformiraju društvo i stvore pravedniji financijski sustav (Sergeenkov, 2024).

Posebnost Genesis bloka je i prisutnost tekstualne poruke unutar bloka koja glasi: „Chancellor on brink of second bailout for banks." (*Chancellor on Brink of Second Bailout for Banks*, 2009). Ova poruka odnosi se na naslov novina The Times istog dana, koji je izvijestio da je tadašnji britanski premijer blizu donošenja drugog paketa pomoći za banke. Ovo događanje povezano je s naporima mnogih centralnih banaka, uključujući i britansku, da spašavaju privatne banke financijskim intervencijama i povećanjem ponude fiat valuta. Sve se ovo dogodilo neposredno nakon globalne financijske krize i recesije 2008. godine, koju su, prema nekima, izazvali propusti privatnih banaka i njihovih partnera. Poruka u Genesis bloku ukazuje na značajnu državnu potrošnju, što mnogi suvremeni ekonomisti tog vremena vjeruju da rezultira devalvacijom fiat valuta poput američkog dolara ili britanske funte. Odluke centralnih banaka i reakcije javnosti dugoročno su se pokazale korisnima za Bitcoin, koji je Satoshi lansirao u pravom trenutku. Ova korist proizlazi iz činjenice da su Bitcoin i ostale digitalne kriptovalute, sa svojom blockchain tehnologijom koja stvara transparentne javne zapise transakcija, viđene kao prava zaštita od brze inflacije od strane mnogih suvremenih ekonomista (*Bitcoin as a hedge against inflation*, 2024), Kriptovalute, kao decentralizirani oblik financijske imovine izvan kontrole elektroničkog bankarskog sustava, mijenjaju obrasce ponašanja na financijskom tržištu, a povjerenje u financijske institucije ustupa mjesto povjerenju u tehnologiju (Wątorrek, Drozd i Kwapien 2021).

3.2. Arhitektura blokchaina

Blockchainovi su distribuirane knjige transakcija bez dozvola u P2P mreži, gdje se informacije bilježe pravodobno, sigurno i otporno na manipulacije. Njihova pouzdanost temelji se na masovnoj suradnji, konsenzusu i kodu, umjesto na tradicionalnim posrednicima. Omogućuju programabilne digitalne resurse za različite oblike vrijednosti. Prvi put u povijesti, subjekti mogu premještati, pohranjivati i upravljati vrijednostima bez oslanjanja na banke i treće strane (Tapscott, 2020).

Postoje različite kategorizacije blockchainova, često proturječne. U ovom poglavlju fokus će biti između blockchainova prema tome zahtijeva li se odobrenje za verifikacijske čvorove i je li pristup podacima javan ili privat. Blockchainovi bez dozvola omogućuju svima sudjelovanje u verifikaciji bez prethodnog odobrenja, dok blockchainovi s dozvolama imaju unaprijed odabrane verifikacijske čvorove. Javni blockchainovi omogućuju svakome čitanje i

slanje transakcija, dok privatni blockchainovi te mogućnosti ograničavaju na korisnike unutar određene organizacije ili grupe (Peters and Panayi, 2018).

U primjeru Bitcoin mreže, koristi se 'permissionless' blockchain. To znači da bilo tko može postati verifikator bez potrebe za prethodnim odobrenjem. Ovi verifikatori su ključni za rad mreže i njihov trud se nagrađuje novom valutom nakon što verificiraju blok transakcija. Permissionless blockchain omogućuje anonimnim korisnicima sudjelovanje i štiti se od napada na identitet. Međutim, potrebno je pažljivo izraditi poticajne mehanizme kako bi se osigurala motivacija verifikatora. U Bitcoinu, verifikatori dobivaju nagrade za verifikaciju transakcija i za objavu blokova transakcija, ali nagrada za blokove je znatno veća. Kako se nagrada za blokove smanjuje, verifikatori će morati povećati naknade za obradu pojedinačnih transakcija, što povećava troškove transakcija u Bitcoinu. Osim Bitcoina, Ethereum je također primjer permissionless blockchainea, koji omogućuje pristup pametnim ugovorima i pruža blockchain kao uslugu (Peters and Panayi, 2018).

U dozvoljenim blockchainovima, verifikaciju provode odabrane pouzdane strane, a dodatne verifikatore se može dodati uz dogovor trenutnih članova ili centralne vlasti. Ova vrsta blockchainea sliči tradicionalnom financijskom sustavu, koji koristi postupke Poznavanja vašeg poslovanja (KYB) ili Poznavanja vašeg klijenta (KYC) za odobravanje korisnika. Swanson (2015) ističe da su blockchainovi bez dozvola i blockchainovi s dozvolama temeljno različiti u načinu rada i mogućnostima koje nude. Dozvoljeni blockchainovi su namjenski izgrađeni kako bi bili kompatibilni s postojećim aplikacijama. Mogu biti potpuno privatni, gdje su prava pisanja ograničena unutar organizacije, ili konzorcijski, gdje proces konsenzusa kontrolira unaprijed odabrani skup čvorova. Pošto su učesnici imenovani, pravno su odgovorni za svoje aktivnosti. Jedna od prednosti dozvoljenog blockchainea je skalabilnost. U blockchainu bez dozvola, svi podaci se pohranjuju na svakom računalu u mreži, a svi čvorovi verificiraju sve transakcije. Kako se broj transakcija povećava, manje korisnika će biti u stanju obraditi sve te verifikacije, što može dovesti do centralizacije. U dozvoljenom blockchainu, manji broj odabranih sudionika obavlja verifikaciju, a velike institucije mogu povećati računalnu snagu u skladu s rastom broja transakcija. Primjeri dozvoljenih blockchainova uključuju Eris, Hyperledger, Ripple i druge (Swanson, 2015).

U tipičnoj blockchain mreži postoje tri vrste čvorova: puni čvor, rudarski čvor i lagani čvor. Puni čvor pohranjuje sve podatke u blockchainu, uključujući zaglavlja blokova i zapise podataka. Rudarski čvor je puni čvor s velikom računalnom snagom, odgovoran za izradu konsenzusnih dokaza. Lagani čvor pohranjuje samo zaglavlja blokova, koja uključuju

konsenzusni dokaz i kriptografske hashove bloka. Važno je napomenuti da zapisi podataka nisu pohranjeni u laganim čvorovima (Zhang i Xu, 2019).

Puni čvorovi su najvažnija vrsta čvorova u Blockchain mreži jer održavaju kompletan primjerak registra Blockchaina. Ovi čvorovi preuzimaju i pohranjuju kopiju svake transakcije i bloka na mreži, što im omogućava neovisnu provjeru cijele povijesti Blockchaina. Međutim, održavanje potpune kopije cijele baze podataka moglo bi biti preskupo za običnog korisnika, budući da zahtijeva značajne resurse za pohranu, računanje i propusnost. Na primjer, minimalni zahtjevi za pokretanje Bitcoin punog čvora uključuju 200 GB slobodnog prostora na disku, neograničenu širokopojasnu vezu s brzinom prijenosa od barem 50 KB po sekundi, te vrijeme rada od 6 sati dnevno. Puni čvorovi djeluju u mreži od čvora do čvora, što znači da komuniciraju s drugim čvorovima kako bi se osiguralo da je Blockchain ažuran i točan (Zhang i Xu, 2019).

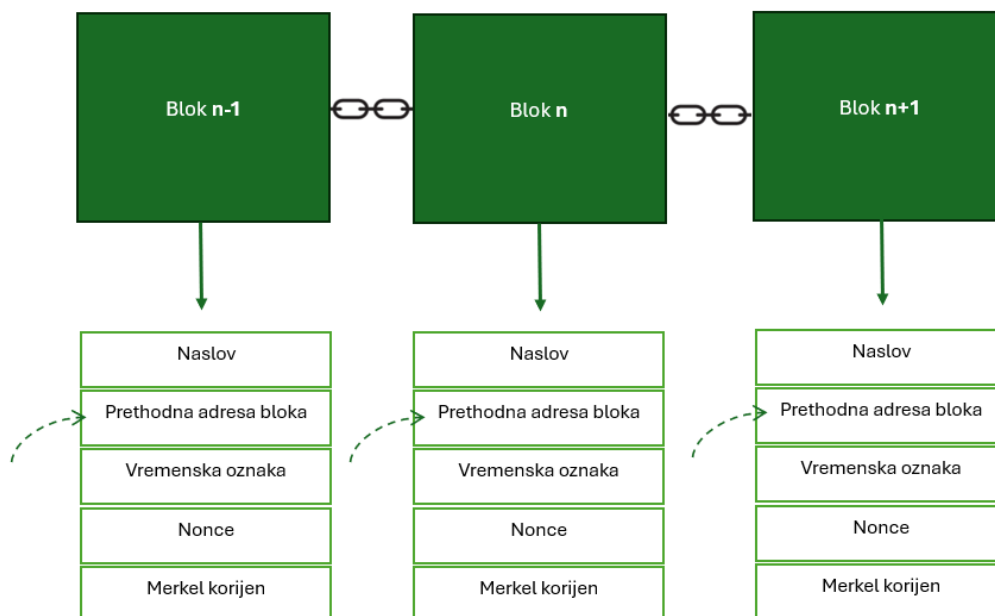
Lagani čvor ne pohranjuje cijeli blockchain, niti provjerava sve transakcije u sustavu. On samo prima podskup transakcija filtriranih od strane povezanih punih čvorova. Takav zahtjev za određenim podacima otkriva informacije o transakcijama povezane s čvorom nenamjerno. Namijenjeni su radu na uređajima s ograničenim prostorom za pohranu i obradom, poput pametnih telefona i tableta. Lagani čvorovi su brži i efikasniji od punih čvorova, ali su također manje sigurni jer se oslanjaju na pune čvorove za validaciju (Ge i Jiang, 2021).

Rudarski čvorovi odgovorni su za provjeru transakcija i dodavanje novih blokova na Blockchain. Proces rješavanja složenih matematičkih krypto zagonetki naziva se rudarenje, a rudari su sudionici koji obavljaju rudarsku aktivnost u mreži kako bi dodali nove blokove. Kada rudar otkrije valjano rješenje, dodaje predloženi blok u blockchain, koji sadrži poveznicu na prethodni blok i popis transakcija. Ove zagonetke su računalno intenzivne i zahtijevaju značajnu računalnu snagu i potrošnju energije za rješavanje. Rudari se natječu jedni s drugima kako bi prvi riješili zagonetku i predložili valjani blok (Nguyen, Truong i Kyungbaek, 2021).

U blockchain mreži, uloge čvorova obuhvaćaju održavanje integriteta, distribuciju konsenzusa te osiguranje sigurnosti mreže. Čvorovi zajedničkim djelovanjem osiguravaju da svi sudionici poštuju pravila protokola te verificiraju svaku transakciju i blok. Decentralizirana priroda blockchaina omogućuje čvorovima da čine mrežu otpornom na napade, čak i ako pojedini čvorovi budu kompromitirani. Oni su ključni elementi blockchain mreže koji osiguravaju njezinu stabilnost, sigurnost te nepromjenjivost podataka. Kroz suradnju i verifikaciju, čvorovi grade decentraliziranu mrežu u kojoj se transakcije mogu sigurno i transparentno provoditi.

Struktura podataka blockchaina nije ravna linija blokova; umjesto toga, zapravo je struktura podataka oblika stabla čije grane predstavljaju sukobljene verzije povijesti transakcijskih podataka. Glavni izazov blockchain algoritma je omogućiti čvorovima distribuiranog sustava da dosljedno odaberu jednu od grana kao autoritativni lanac (Drescher, 2017). Blokovi u blockchainu sastavljeni su od nekoliko elemenata, a oni su prikazani na Slici 1.:

Slika 1. Arihtektura blockchaina



Izvor: Izrada autora prema *Blockchain Structure*, 2022.

<https://www.geeksforgeeks.org/blockchain-structure/>

(pristupljeno 4.5.2024.)

- Naslov bloka: Naslov svakog bloka u blockchainu sadrži *hash* funkciju koja se odnosi na prethodni blok, tako se formira niz *hasheva* sve do prvog bloka. To pomaže u identifikaciji svakog bloka u blockchainu. Rudari koriste *nonce* za mijenjanje vrijednosti i stalno obnavljanje hasha bloka tijekom procesa rudarenja. Na kraju, svaki naslov bloka sadrži tri važna skupa informacija.
- *Hash* prethodnog bloka: Ovi blokovi su kriptografski zapečaćeni u lancu korištenjem *heš* funkcija, vrste kriptografskog sustava koji pretvara ulaz slova i brojeva u šifrirani izlaz fiksne dužine (tzv. "*hash*"), koji se ne može obrnuti kako bi se povratio izvorni ulaz.

- Vremenska oznaka: Bilježi vremensko postojanje određenog elementa zapisa blockchaina u određenom trenutku te verificira podatke u bloku i dodjeljuje vrijeme ili datum stvaranja digitalnih dokumenata.
- *Nonce*: Nasumični broj koji se koristi samo jednom. Ključni je dio dokaza o radu unutar bloka. Uspoređuje se s ciljanom vrijednošću, te ako je manji ili jednak trenutnoj meti, smatra se valjanim.
- Merkelov korijen: Transakcije bloka *hashiraju* se putem Merkle korijena, odnosno *hasha* svih *hasheva* svih transakcija koje su dio bloka u blockchain mreži. To znači da se integritet i sigurnost informacija na blockchainu osiguravaju putem kriptografskih funkcija, a to osigurava nepovratnost zapisa što se veže na visoku pouzdanost i povjerenje jer je nemoguće izbrisati ili urediti ove blokove (Martino, 2021).

3.3. Kako blockchain funkcionira?

U blockchainu se sudionici mreže spajaju i imaju dozvolu za pristup distribuiranoj knjizi. To znači da svaki korisnik može dijeliti i pregledavati ažurirane informacije o transakcijama. Takva transparentnost omogućuje svim korisnicima uvid u povijest transakcija. Povijest transakcija pohranjena je od strane svih sudionika mreže, a pristupna je svima s autoriziranim pristupom. Osim toga, sustav je decentraliziran, što znači da nijedan pojedinačni čvor ne može kontrolirati cijelu mrežu. Umjesto centralnog autoriteta, svi sudionici imaju pristup knjizi. Takav sustav osigurava otpornost jer kvar jednog čvora ne utječe na rad ostalih, čime se održava dostupnost sustava. Što se tiče samog blockchaina, on koristi peer-to-peer tehnologiju koja omogućuje korisnicima izravno povezivanje bez posredničkih autoriteta. Ova tehnologija olakšava decentralizirano procesuiranje transakcija, omogućujući korisnicima direktno slanje informacija unutar mreže. Time je uklonjena potreba za centralnim autoritetom za verifikaciju i prijenos vrijednosti (Martino, 2021). Otisci prstiju su tragovi trenja na prstima ljudske ruke koji se smatraju jedinstvenim za svaku osobu. Koriste se za identifikaciju pojedinaca, kao i u istrazi zločina. Paralela može biti izvučena s konceptom kriptografske *hash*-vrijednosti kao digitalnom ekvivalentu otisaka prstiju. Ova tehnologija se često koristi u blockchainu, stoga je važno razumjeti kriptografsko *hashiranje* za bolje razumijevanje funkcioniranja blockchaina (Drescher, 2017). Svaki sudionik ima jedinstveni par ključeva: privatni ključ, koji čuva tajnim, i javni ključ, koji se otvoreno dijeli. Kada korisnik pokrene transakciju, potpisuje je koristeći

svoj privatni ključ, čime stvara digitalni potpis. Ostali korisnici u mreži zatim mogu provjeriti autentičnost transakcije primjenom javnog ključa pošiljatelja na digitalni potpis. Ovaj pristup osigurava sigurne transakcije jer samo legitimni vlasnik privatnog ključa može autorizirati transakciju, ali svi mogu provjeriti potpise koristeći javni ključ (Casey, Crane i Gensler, 2018). Još jedna značajka blockchaina je njegova transparentnost. Sastoji se od podataka, odnosno blokova, koji su agregirani u lančane blokove označene vremenom koji ne mogu biti promijenjeni ili izbrisani od strane pojedinačnog sudionika; umjesto toga, oni se provjeravaju i upravljaju putem automatizacije i protokola zajedničkog upravljanja. Kao rezultat, blockchain pruža neizbrisiv, transparentan zapis istine. Sve interakcije vlade s dobavljačima, poput zahtjeva za prijedlozima, preporuka i odluka, zabilježene su na blockchainu i vidljive ovlaštenim stranama. Ako je, primjerice, ponuda odbijena, informacije koje su utjecale na tu odluku dostupne su za prigovore i revizije. Transparentnost također omogućuje dobavljačima pristup informacijama u registru o njima, tako da mogu otkriti i prijaviti bilo kakve pogreške. Takozvani dozvoljeni blockchainovi omogućuju upraviteljima distribuirane glavne knjige diskreciju nad tim tko smije pregledavati podatke (Tapscott, 2020).

Tehnologija blockchain-a otvara vrata novim pristupima upravljanju kroz mogućnost decentralizacije različitih procesa, čime se potencijalno omogućava demokratskije i inkluzivnije donošenje odluka. Na tržištu se već počinju razvijati napredne blockchain arhitekture prilagođene specifično za upravljačke odbore, kao i automatizirane sustave za oblikovanje okvira upravljanja u korporativnim okruženjima. Pravi smisao decentralizacije blockchaina manifestira se kada se nova transakcija javi unutar određenog blockchaina. Ovdje se nova transakcija ne odmah pretvara u blok koji se može dodati samom blockchainu. Postupak prvo zahtijeva odobrenje od strane distribuirane mreže računala, osiguravajući time da kontrola i odlučivanje nisu monopolizirani, već su ravnomjerno raspoređeni unutar mreže radi eliminacije bilo kakvih pristranosti ili pogrešnih procjena. Kroz povezanost mreže putem decentraliziranih čvorova koje usklađuju autentičnost novih blokova prije nego što ih uvrste u lanac, osigurava se visoka razina sigurnosti blockchaina za sve korisnike (Peters and Panayi, 2018).

Zbog decentralizacije, transakcije u blockchainu su visoko šifrirane. Ostale prednosti decentraliziranog blockchaina uključuju raspodijeljenu ovlast, čime se brisanje mogućnosti pogreške i pristranosti omogućuje na efikasan način. Decentralizacija također osigurava da upravljanje blockchainom nije pod kontrolom pojedinca, grupe, pa čak ni vlade. Sistematična

digitalna mreža raspodijeljena je tako da nitko ne može manipulirati transakcijama. Ostale sigurnosti upravljaju određene osobe, što potencijalno vodi do mogućnosti ljudske pogreške i pristranosti. Također, decentralizacija sprječava bilo kakvu vrstu internog trgovanja unutar blockchaina. Usklađivanje podataka u stvarnom vremenu omogućava da svi podaci unutar blockchaina budu dostupni u stvarnom vremenu rudarima i investitorima, ostavljajući tako nema prostora za gubitak podataka ili netočnosti. Funkcionira slično kao Google dokumenti, gdje se rad može podijeliti s više ljudi i može se uređivati u isto vrijeme. Optimalna raspodjela resursa osigurava da je cijela mreža blockchaina ravnomjerno raspoređena među različitim čvorovima za optimalno korištenje resursa. Brze transakcije u blockchainu su mnogo brže od tradicionalnih bankovnih transakcija, jer se iz procesa izbacuju mnogi posrednici. Međutim, postoje i ograničenja decentraliziranog blockchaina. S obzirom na to da se cijela valuta koristi u digitalnom obliku, blockchain je često bio preferiran od strane hakera i korisnika dark weba kao sredstvo za transakcije, što je omogućavalo kriminalne aktivnosti (*What is Blockchain security*, 2024).

U svibnju i lipnju 2018. godine, pet kriptovaluta temeljenih na tehnologiji blockchain-a; konkretno Monacoin, Bitcoin Gold, Zencash, Verge i Litecoin Cash, bili su meta 51% napada, što je rezultiralo gubitkom od 5 milijuna američkih dolara. Napadači u svakoj kriptovaluti uspjeli su steći više od 51% *hash* udjela mreže, što su koristili za preuređivanje transakcija i sprječavanje drugih rudara da izračunaju blokove. Kao rezultat toga, uspjeli su preuzeti kontrolu nad blockchain-om i izvršiti dvostruko trošenje kod vrijednih transakcija. (Saad, M., Spaulding, J. and Njilla, L. (2019).

3.4. Vrste blockchain mreže

Javne blockchain platforme eliminiraju potrebu za posrednicima u razmjeni vrijednosti koristeći P2P protokole. Privatni blockchainovi, za razliku od toga ponovno definiraju posrednika. Čvorovi u privatnoj blockchain mreži zahtijevaju pozive i moraju biti potvrđeni od strane administratora mreže ili skupa protokola koji ju reguliraju (Tapscot, 2021). Privatni blockchainovi ograničavaju pristup odabranoj grupi osoba i institucija te obično funkcioniraju u privatnom okruženju koje može uključivati samo ograničenu mrežu ili jednog nadzornog identiteta. Unatoč sličnosti s javnim blockchainom, privatne mreže su obično mnogo manje i često se koriste unutar organizacija ili tvrtki. Ključne prednosti privatnog blockchaina proizlaze iz ekskluzivnosti i sigurnog kontroliranog okruženja gdje su transakcije brže i prilagodljive specifičnim potrebama tvrtki, čineći ga vrlo skalabilnim. Međutim, upravljanje povjerenjem

unutar manje mreže često je izazovno te može izložiti mrežu sigurnosnim prijetnjama. Također, centralizacija koju privatni blockchain donosi može imati negativan utjecaj jer zahtijeva centralizirani sustav za upravljanje identitetom. Na javnim blockchainima, korisnicima se omogućuje pristup povijesnim i trenutačnim podacima te sudjelovanje u svim transakcijama, uključujući rudarenje i provjeru. Ovakva otvorenost omogućuje transparentnost, no istovremeno može izazvati izazove poput niskih brzina transakcija i visoke potrošnje energije. Javni blockchaini su prednosti u pouzdanosti, sigurnosti i transparentnosti, ali također nose izazove poput skalabilnosti. Dok se privatni blockchainovi usredotočuju na kontrolu pristupa i upravljanje povjerenjem unutar zatvorenog sustava, javni blockchainovi se temelje na otvorenosti i transparentnosti za širu publiku (Strehle, 2020).

Organizacije koje žele iskoristiti prednosti oba sustava često se odlučuju za hibridni blockchain, koji spaja karakteristike privatnih i javnih blockchaina. Ovaj pristup omogućava poduzećima da uspostave privatni sustav zasnovan na dozvolama uz paralelni javni sustav bez dozvola. Time se pruža fleksibilnost u odabiru tko može pristupiti određenim podacima na blockchainu i koji će podaci biti javno dostupni. U hibridnom blockchainu, transakcije i zapisnici obično nisu javno dostupni, no moguće ih je validirati kad je to potrebno, omogućavanjem pristupa putem pametnih ugovora. Ovakav pristup nudi veću sigurnost jer se mreža operira unutar zatvorenog okruženja, čime se minimizira rizik od vanjskih napada. Hibridni blockchain također je isplativ jer štiti privatnost, a omogućava interakciju s trećim stranama. Transakcije na ovakvim mrežama su brže i jeftinije, a sustav se bolje skalira u usporedbi s javnim blockchain mrežama. Ipak, hibridni blockchain nije bez nedostataka. Jedan od glavnih izazova je nedostatak potpune transparentnosti, budući da se neke informacije mogu zadržati u privatnosti. Također, korisnici mogu imati manje poticaja za sudjelovanje i doprinos mreži zbog ograničene otvorenosti sustava. Hibridni blockchain nalazi primjenu u različitim industrijskim sektorima. Na primjer, tvrtke iz sektora nekretnina mogu koristiti hibridne mreže za upravljanje svojim sustavima i istovremeno pružanje informacija javnosti. Posebno je prikladan i za visoko regulirane industrije poput bankarstva, gdje regulativa i sigurnosni zahtjevi postavljaju visoke standarde za operativne sustave (*Hybrid Smart Contracts*, 2023).

Blockchain konzorcij, poznat i kao federirani blockchain, sličan je hibridnom blockchainu jer kombinira značajke privatnog i javnog blockchaina. Međutim, razlikuje se po tome što uključuje suradnju različitih organizacijskih članova na decentraliziranoj mreži. Godine 2016., Kanada je pokrenula Peer to Peer sustav plaćanja putem bankarskog konzorcija nazvanog

Interac, gdje se računi mogu povezati s brojem mobilnog telefona ili e-poštom. Kroz Interac, potrošači mogu međusobno obavljati plaćanja gotovo u stvarnom vremenu, ne znajući brojeve računa drugih. Prihvatanje SMS poruke na mobilnom telefonu otpušta sredstva na račun primatelja. Iako su plaćanja za potrošača u stvarnom vremenu, sredstva zapravo kasnije tijekom dana prenose se između banaka putem središnjeg klirinškog sustava (Tapscott, 2020). U konzorcijskom blockchain sustavu, specifični čvorovi vode brigu o metodama konsenzusa, dok postoje validatori čvorovi koji su odgovorni za pokretanje, primanje i verifikaciju transakcija. Sudionici čvorova imaju mogućnost započinjanja ili prihvatanja transakcija. Što se tiče prednosti, konzorcijski blockchain pruža veću sigurnost, skalabilnost i učinkovitost u usporedbi s javnim blockchain mrežama. Kao i kod privatnih i mješovitih blockchain sustava, implementirane su kontrole pristupa koje dodatno čuvaju mrežu. Međutim, jedan od izazova konzorcijskih blockchain sustava jest ograničena transparentnost. U slučaju neovlaštenog pristupa jednom od sudioničkih čvorova, postoji rizik od hakerskog napada, a određena pravila blockchaine mogu uzrokovati nefunkcionalnost mreže. Konzorcijski blockchain nalazi primjenu u raznim sektorima. Na primjer, u financijskom sektoru, skupina financijskih institucija može formirati konzorcij koji upravlja odabirom čvorova za validaciju transakcija. Također, ovakav sustav je koristan u istraživačkim aktivnostima jer omogućava dijeljenje podataka i rezultata istraživanja između različitih organizacija. Na konzorcijskim blockchainovima, korištenje prilagođenog algoritma konsenzusa omogućava "konačnost bloka": jednom kada je blok validiran, ostaje na glavnom lancu. To smanjuje vrijeme čekanja za potvrde (Dib, Broumische i Durand, 2018).

3.5. Algoritam blockchaine

Temeljne karakteristike blockchain tehnologije uključuju upotrebu protokola suglasnosti kako bi se stvorio niz zapisa koji se mogu samo dodavati (na primjer, Bitcoinov zapis transakcija) čime se omogućuje stvaranje revizibilne baze podataka (primjerice, evidencija o vlasništvu novčića). Ova baza podataka oblikovana je od strane različitih, ponekad nepovjerljivih sudionika, te je osigurana kriptografskim metodama kako bi svaki unos mogao biti pregledan i potvrđen. Odgovornost algoritama je očuvanje integriteta blockchaine, sprječavajući potencijalne pokušaje manipulacije mrežom od strane pojedinačnih ili grupa čvorova. Kroz

osiguravanje sigurnosti, oni sprečavaju neovlašten pristup mreži, osiguravajući time valjane transakcije i stabilno funkcioniranje sustava (Casey, Crane i Gensler, 2018).

Nakamoto je 2008. godine predstavio najpoznatiji algoritam konsenzusa koji je postao temelj Bitcoin mreže. U ovom sustavu, sudjelujuća računala moraju riješiti matematičku zagonetku kroz složene računalne operacije koristeći unaprijed definiranu *hash* funkciju (Nakamoto, 2008). Ovaj postupak omogućava postizanje suglasnosti među svim strankama o tome kako će se pečatirati transakcije i dodati novi blok u lanac. Svaki blok, osim popisa transakcija, sadrži ključne informacije poput *hasha*, *noncea*, te *hash* vrijednost prethodnog bloka - sve to kako bi se osigurala integritet i kontinuitet lanca. Proof of Work (PoW), ili Dokaz o radu, je metoda konsenzusa koju primjenjuju mnogi blockchain sustavi kako bi osigurali vjerodostojnost transakcija i dodavanje novih blokova u lanac. Satoshi Nakamoto je ovaj mehanizam prvi put uveo s ciljem osiguravanja mreže i sprječavanja višestrukog trošenja sredstava. Rudari se natječu u rješavanju zahtjevnih matematičkih problema ili *hash-ova* kako bi odobrili transakcije i integrirali nove blokove u lanac. Ovaj proces zahtijeva velike količine računalne snage jer su zadaci *hash* funkcije namjerno postavljeni kao računski zahtjevni. Iako PoW pruža visoku sigurnosti zahvaljujući složenosti *hash* problema i zahtjevnosti za preuzimanje kontrole nad mrežom, kritizira se zbog visoke potrošnje energije. Međutim, zagovornici ovog sustava tvrde da je energetska potrošnja opravdana jer pruža neophodnu sigurnost i štite od potencijalnih napada koji bi mogli ugroziti integritet mreže (Khan, Syed i Hammad, 2022).

Dokaz udjela predstavlja alternativu dokazu rada, dijeleći iste osnovne mehanizme kada je u pitanju kibernetička sigurnost kriptovaluta. PoS i PoW koriste blockchain mehanizam za olakšavanje i verifikaciju transakcija digitalne imovine. Blockchain, kao digitalna knjiga računa, služi kao digitalni registar za bilježenje javnih transakcija digitalne imovine. Osobitost dokaza udjela je sustav kazni, gdje se tvorac sljedećeg bloka odabire na temelju uložene količine kriptovalute od strane određenog korisnika. Bilo kakav pokušaj prijevare u rudarenju kriptovaluta može rezultirati gubitkom uloga kao kaznom. Sustav postavlja kazne od stotina do tisuća dolara, potičući time ispravno trgovačko ponašanje te olakšavajući praćenje rizičnih osoba za kibernetičku sigurnost kriptovalute. Važno je naglasiti da odabir tvorca sljedećeg bloka ovisi o iznosu uloga, prema kojem vlasništvo nad kriptovalutom odgovara glasu. Dodatno, sustav PoS ne nagrađuje rad na rješavanju problema, već slučajnim odabirom "validatora" te motivira ispravno ponašanje kako bi se izbjegle prijevare. Za razliku od dokaza rada gdje rudari troše energiju na rješavanje zadatka, sustav PoS se oslanja na validatore. Oni

moraju posjedovati određenu količinu kriptovalute za potvrđivanje transakcija i dodavanje novih blokova. PoS također nudi nisku energetska potrošnju u poredbi s PoW, uz ekološku osviještenost i financijsku učinkovitost. Unatoč nekim slabostima, poput mogućnosti centralizacije među većim posjednicima kriptovalute, PoS pruža poticaj za decentralizaciju i manju ekološku i financijsku opterećenost (Lin, 2023).

Delegirani dokaz o udjelu (DPoS) je varijacija dokaza o udjelu (PoS) koja se koristi u određenim blockchain sustavima za verifikaciju transakcija i dodavanje novih segmenata u lanac. U DPoS sustavima, delegate ili svjedoci, ograničena skupina validatora, obavljaju verifikaciju transakcija i dodavanje blokova na lanac. Vlasnici tokena glasaju za delegate koji ih predstavljaju tijekom procesa validacije, a delegati su odgovorni za ispravnu provjeru transakcija. Oni koji krše pravila ili destabiliziraju mrežu mogu biti smijenjeni i izgubiti nagrade. Osim brze obrade transakcija, DPoS podržava decentralizaciju jer daje vlasnicima tokena pravo glasa u odabiru delegata, umanjujući rizik od centralizacije. DPoS u sustavima blockchaine prekida ciklus natjecanja za računalne resurse za generiranje blokova implementiranjem glasanja temeljenog na PoS-u i smanjuje vrijeme generiranja blokova na 3 sekunde. Svjedoci, delegati i radnici su tri kategorije čvorova u DPoS sustavu. Svjedoci su glavni sudionici i biraju se glasanjem svih čvorova, s najviše glasova postaju svjedoci koji naizmjenično generiraju blokove. Delegati mogu pokrenuti ažuriranje lanca, dok radnici mogu predložiti projekte i biti nagrađeni. Svjedoci zadržava pravo generiranja blokova dugoročno, no mogu biti smijenjeni u konkretnim situacijama, što zbog centralizacije u DPoS-u može predstavljati sigurnosni rizik. Iako DPoS donosi brojne prednosti poput brže obrade transakcija i veće participacije vlasnika tokena u donošenju odluka, postoji i nekoliko izazova koji dolaze s ovim modelom. Centralizacija moći među malom skupinom svjedoka ili delegata može dovesti do potencijalnog zloupotrebljavanja te manipulacije mrežom. Ukoliko mala grupa delegata kontrolira većinu glasova, postoji rizik da će udruženjem moći narušiti integritet mreže. Radi suzbijanja ovakvih problema, neke DPoS mreže razvile su strategije poput ograničenja na maksimalan broj delegata koje pojedini subjekt može kontrolirati ili uvođenja dodatnih procedura za sprečavanje zloupotrebe (Yang, Zhou i Wu, 2017).

Najamni dokaz o udjelu je metoda konsenzusa upotrebljena u određenim blockchain mrežama za provjeru transakcija i ubacivanje novih blokova u lanac. LPoS je inačica tradicionalnog dokaza o udjelu (PoS) koja dopušta posjednicima manjeg broja tokena da se uključe u proces validacije iznajmljujući svoje tokene većim validatorima. U okviru mreže LPoS, vlasnici tokena

iznajmljuju svoje tokene validatorima, koji ih koriste za povećanje svojeg udjela i bolje šanse u procesu odabira za potvrđivanje transakcija i dodavanje novih blokova. Vlasnik tokena i dalje zadržava vlasništvo nad svojim tokenima i dobiva dio dobitka koji validator ostvari, proporcionalno iznosu iznajmljenih tokena. Prednost LPoS-a jest što omogućava vlasnicima manjeg broja tokena da se angažiraju u procesu validacije i ostvare dobit bez potrebe za posjedovanjem velike količine tokena. To doprinosi decentralizaciji i omogućava širi spektar sudionika u mreži. Osim toga, LPoS može povećati sigurnost mreže jer omogućavanjem šireg kruga posjednika tokena da sudjeluje u validaciji, teže je da jedan validator ili grupa validatora dominira mrežom i upravlja transakcijama. Ipak, jedan od potencijalnih nedostataka LPoS-a je veća složenost u odnosu na druge algoritme konsenzusa. Vlasnici tokena trebaju biti upoznati s rizicima i prednostima iznajmljivanja svojih tokena validatorima, dok validatori moraju odgovorno upravljati iznajmljenim tokenima (*Liquid Proof Of Stake*, 2023).

4. Opis istraživanja i rezultati istraživanja

Istraživački proces ovog diplomskog rada analizira primjenu tehnologije blockchain u bankarskom sektoru. Proučavanje primjene blockchain tehnologije u bankarstvu istražuje se na primjerima JP Morgan Chasea, HSBC-a, Santander banke i Barclays banke. Takva implementacija blockchaina u bankarstvu analizira strategije koje banke koriste za integraciju ove tehnologije u svoje poslovanje. Važna tema istraživanja je sigurnost transakcija u bankarskom sektoru putem blockchain tehnologije, gdje se istražuje kako blockchain pruža sigurniji okvir za financijske transakcije. Transparentnost blockchaina istražuje kako tehnologija omogućuje transparentnost i povjerenje u bankarske transakcije, dok se učinkovitost transakcija usredotočuje na brzinu i troškovnu učinkovitost transakcija unutar blockchain sustava.

Također, istraživanje identificira izazove s kojima se bankarski sektor suočava prilikom implementacije blockchain tehnologije, uključujući pitanja regulacije i nedostatke jasnih pravnih okvira, zabrinutosti oko sigurnosti i privatnosti te nedostatak razumijevanja o samoj tehnologiji između organizacije, ali i pojedinaca.

4.1. Blockchain u bankarstvu

Tradicionalno bankarstvo seže duboko u povijest financijskog svijeta i svoj početak ima u praksi posuđivanja novca u drevnim civilizacijama. Vremenom je evoluiralo u složene financijske institucije koje nude različite usluge pojedincima, tvrtkama i vladama. Uloga tradicionalnih banaka obuhvaća zaštitu novčanih sredstava, pružanje raznovrsnih kreditnih usluga te olakšavanje plaćanja između različitih strana. Međutim, u današnje vrijeme, tradicionalno bankarstvo suočava se s brojnim izazovima uslijed tehnološkog napretka i promjena u očekivanjima korisnika. Centralizirana priroda tradicionalnih banaka može voditi do ranjivosti na kibernetičke prijetnje, dok dugotrajni procesi međunarodnih transakcija rezultiraju neefikasnostima i visokim troškovima. Financijski sektor, s tradicionalnim bankama kao njegovim stupovima, igra vitalnu ulogu u globalnoj ekonomiji, pri čemu se svakodnevno prenose značajni iznosi novca širom svijeta. Uprkos integraciji inovacija poput kreditnih kartica i mobilnih aplikacija, banke su suočene s izazovima koji uključuju sporije, neefikasne i skuplje transakcije te velike sigurnosne rizike. Ovisnost o višestrukim posrednicima povezana s IT

sustavima stvara visoke troškove i administrativne izazove te produljuje vrijeme obrade transakcija za klijente (Neyigapula, 2021).

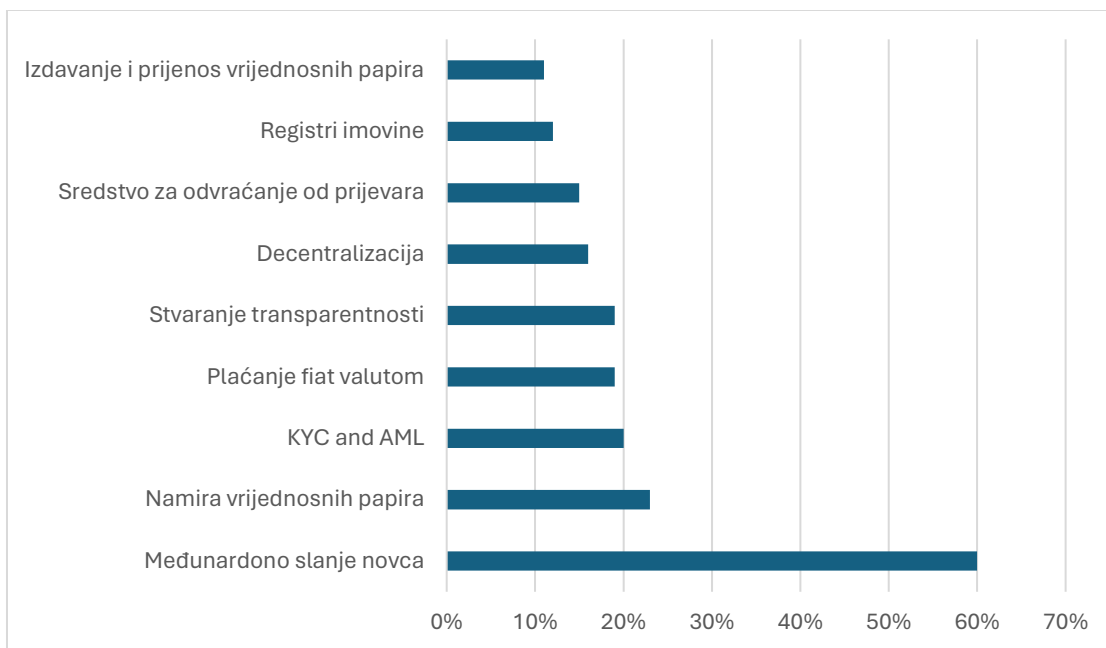
Banke imaju ključnu ulogu u transakcijskim procesima, stoga čak i najmanje pogreške u njihovom radu mogu imati ozbiljne posljedice ne samo za banke same, već i za sve uključene sudionike. Centralizirani sustavi često postaju mete cyber napada koje provode zlonamjerne skupine ili pojedinci, što rezultira velikim gubicima i oštećenjem ugleda financijskih institucija. Implementacija cyber sigurnosnih mjera je izazovna zbog visokih troškova uzrokovanih složenim sustavima. Primjerice, u energetske sektoru je lakše upravljati centraliziranim kontrolnim sustavom koji nadzire energetske opskrbnu mrežu, no istovremeno predstavlja primarnu metu za cyber napade zbog svoje vidljivosti (Pourmirza, 2023). (Podaci pokazuju da gotovo polovica korisnika banaka diljem svijeta bila izložena pokušajima prijevara i kriminalnih aktivnosti tijekom obavljanja operacija, kao što su transakcije s burzama, platnim vratima ili agencijama za prijenos novca. Jedan od ključnih problema u financijskom sektoru je nedostatak pristupa bankovnim uslugama za polovicu svjetske populacije, što ih prisiljava na korištenje alternativnih platnih sustava. Na primjer, u zemljama poput Kenije, velik broj ljudi nema pristup bankovnim računima (Naheem, 2019).

Blockchain tehnologija pruža niz prednosti u području AML/KYC (Anti-Money Laundering/Know Your Customer) uključujući veću transparentnost, poboljšanu usklađenost i mogućnost dijeljenja podataka. Kroz upotrebu blockchain tehnologije, provjere i verifikacije AML-a i KYC-a mogu se izvršavati učinkovito putem zajedničke baze identiteta radi automatizacije analize ponašanja i provjere subjekata te podrške analitičkim procesima i donošenju odluka. Očekuje se da će smanjenje troškova povezano s primjenom blockchain tehnologije proizaći iz ušteda na radnoj snazi/ resursima i povezanosti s listom za praćenje. U SAD-u se očekuje smanjenje troškova od 52%, dok u Europi i Aziji iznosi 74% odnosno 33%. Banke sve više koriste blockchain tehnologiju kako bi unaprijedile svoje operacije, osigurale sigurnost i povećale učinkovitost. Najznačajnije prednosti uključuju ubrzanje i smanjenje troškova međunarodnih transakcija putem eliminacije posrednika, što rezultira većom sigurnošću i brzinom transakcija (*Blockchain and the impact on fund distribution, 2018*).

Blockchain tehnologija, uz vođenje evidencije o trajnim prijenosima valute, može pouzdano bilježiti i druge vrste vremenski slijedećih podataka. To uključuje obradu koraka potrebnih za izvršavanje programa poznatih kao 'pametni ugovori', koji digitalno olakšavaju i provode prijenos digitalne imovine prema uvjetima definiranim softverom. Primjerice, kompanija

može koristiti pametni ugovor na blockchainu kako bi platila korisniku digitalnu imovinu tek kada je aktivirana određena programska klauzula zbog međusobno priznatih promjena stanja. Ključna prednost pametnih ugovora leži u činjenici da ne zahtijevaju povjerenje u treću stranu poput skrbnika ili agenta za odvjetničko jamstvo; umjesto toga, mreža blockchaina samostalno provodi izvršenje ugovora. Ovo smanjuje trenje tijekom prijenosa vrijednosti između entiteta i otvara vrata većoj automatizaciji transakcija (Casey, Crane i Gensler, 2018). Na grafikonu 1. može se vidjeti za što banke najviše koriste blockchain.

Grafikon 1. Prikaz usluga za koje banke najviše koriste blockchain tehnologiju



Izvor: Izrada autora prema *Blockchain in Banking – Key Opportunities and Challenges for Businesses*, 2024. Dostupno na:

<https://appinventiv.com/blog/blockchain-in-banking/>

(pristupljeno 4.5.2024.)

Graf prikazuje razne usluge za koje banke najviše koriste blockchain tehnologiju, raspoređene po učestalosti uporabe. Najveći postotak, 60%, odnosi se na međunarodno slanje novca. To pokazuje da banke primarno koriste blockchain kako bi poboljšale brzinu, sigurnost i troškovnu učinkovitost prekograničnih transakcija. Sljedeća najčešća upotreba je namira vrijednosnih papira, koja čini 23%. Korištenje blockchaina smanjuje vrijeme i troškove povezane s

namirama, istovremeno povećavajući sigurnost. KYC (Know Your Customer) i AML (Anti-Money Laundering) procesi također značajan udio s 20%. Blockchain omogućuje sigurnu pohranu i transparentnost vezanu za identifikaciju i provjeru klijenata, što pomaže u smanjenju prijevare i usklađivanju s regulatornim zahtjevima. Usluge plaćanja fiat valutom i stvaranja transparentnosti obje su na 19%. Blockchain povećava učinkovitost i sigurnost fiat transakcija, dok istovremeno osigurava veću transparentnost u poslovnim procesima. Decentralizacija, na 16%, pokazuje da banke koriste blockchain za reduciranje ovisnosti o centraliziranim sustavima, čime povećavaju robustnost i otpornost sustava na napade. Kao sredstvo za odvratanje od prijevare, blockchain ima udio od 15%. Njegova nepromjenjivost i transparentnost čine ga snažnim alatom za sprečavanje i otkrivanje prijevare. Registri imovine koriste blockchain tehnologiju u 12% slučajeva, čime se osigurava transparentno i sigurno praćenje vlasničkih prava. Konačno, izdavanje i prijenos vrijednosnih papira čine 11%, koristeći blockchain za poboljšanje učinkovitosti i sigurnosti u ciklusima izdavanja i prijena. Ovi podaci jasno pokazuju širok raspon primjena blockchain tehnologije u bankarskom sektoru, s naglaskom na njejoj sposobnosti da poboljša sigurnost, učinkovitost i transparentnost u različitim financijskim i uslužnim domenama.

4.2. Implementacija blockchaine u bankarstvu

Više vodećih banaka i financijskih institucija diljem svijeta već istražuje i primjenjuje blockchain tehnologiju u svojim operacijama. U nastavku će kroz primjere JP Morgan Chasea, HSBC-a, Santander banke i Barclays banke biti objašnjena upotreba blockchaina zbog svoje sposobnosti omogućavanja sigurnih, transparentnih i efikasnih financijskih transakcija. Također, uz prednosti koje blockchain nosi, razradit će se i nedostaci.

4.2.1. JP Morgan Chase

JPMorgan Chase, kao pionir u blockchain tehnologijama, posjeduje tim s globalnim fokusom koji istražuje potencijalne primjene u poslovanju, s naglaskom na kreativne strategije za korisnike. Chase je iskoristio Ethereum mrežu za izgradnju Quorum projekta, svog pionirskog proizvoda digitalne valute. Quorum, kao privatna blockchain platforma izgrađena 2016. godine na temelju Ethereum mreže, osmišljen je za povećanje sigurnosti i učinkovitosti financijskih

transakcija. Quorum je posebno prilagođen za korporativne potrebe, omogućavajući zaštitu privatnosti transakcija, upravljanje pristupom podacima i povećanu efikasnost. Funkcionira slično kao druge blockchain platforme, ali s naglaskom na poslovne svrhe i specifične korporativne potrebe. Omogućava privatne transakcije dostupne samo ovlaštenim korisnicima, čime se štite povjerljivi podaci. Quorum projekt koristi JPM Coin za trenutno izvršenje plaćanja, što znači da, čim je uplata izvršena na drugi bankovni račun, novac se odmah reflektira na računu primatelja. Ovaj sustav omogućuje brže i efikasnije poslovne transakcije, stvarajući značajnu fleksibilnost. JPMorgan Chase razmatra dugoročnu mogućnost digitalizacije mnogih svojih teško automatizirajućih procesa kako bi pojednostavila strukture troškova. Koristeći Quorum platformu, banka upravlja međubankarskim sporazumima i imovinom, osiguravajući sigurno i efikasno evidenciranje i provjeru transakcija bez potrebe za centralnim autoritetom. Osim toga, Quorum nudi napredne sigurnosne značajke poput visoke kriptografije, ovlaštenih čvorova i decentraliziranog sustava upravljanja ključevima, što dodatno unapređuje sigurnost i povjerljivost u korporativnom okruženju (Shevchenko i Lunsford, 2022).

Quorum je značajno brži od Bitcoina i Ethereum, omogućavajući više od 150 transakcija u sekundi zahvaljujući jednostavnom mehanizmu konsenzusa. Quorum se može koristiti za međunarodne plaćanja i druge financijske transakcije. Zbog mogućnosti privatnosti, omogućava suradnicima da trguju bez otkrivanja osjetljivih podataka kao što su iznosi transakcija ili identiteti uključenih strana. Sposobnost Quoruma da prati i verificira transakcije čini ga korisnim alatom za upravljanje lancem opskrbe. Primjenom blockchain tehnologije za praćenje proizvoda kroz lanac opskrbe, tvrtke mogu osigurati autentičnost proizvoda te otkriti i eliminirati prijevare (*Quorum Blockchain*, 2023).

Najveće prednosti Quoruma leže u njegovoj privatnosti, sigurnosti i fleksibilnosti. Funkcije privatnosti u Quorumu omogućuju strankama da obavljaju transakcije međusobno ne otkrivajući osjetljive informacije. To je posebno korisno u financijskim transakcijama gdje strane mogu željeti zadržati privatnost identiteta ili iznosa transakcija. Quorum koristi konsenzusni mehanizam nazvan "QuorumChain", koji je osmišljen za sprječavanje zlonamjernih napada i osiguravanje sigurnosti mreže. QuorumChain je također brži od mehanizama konsenzusa korištenih na drugim blockchain platformama, poput Proof of Work-a ili Proof of Stake-a. Quorum je izgrađen na Ethereum blockchain-u, što znači da može podržavati pametne ugovore i decentralizirane aplikacije. Ovo čini Quorum vrlo prilagodljivom platformom koja se može koristiti za različite namjene. S druge strane, Quorum je još uvijek relativno nova platforma, te je do sada njezina upotreba bila ograničena. Razlog tome

djelomično je činjenica da je platforma dizajnirana specifično za financijske institucije, što znači da možda nije prikladna za druge industrije ili različite slučajeve upotrebe. Potrebne su kontinuirane brige i ažuriranja za Quorum kako bi se osigurala sigurnost i performanse. Taj proces može biti skup i zahtijevati puno vremena, što može predstavljati prepreku za neke tvrtke koje razmišljaju o prihvaćanju ove platforme (*Smart Contracts and Transactions*, 2023).

Quorum Blockchain je snažna platforma za blockchain namijenjena poslovnim korisnicima, prilagođena njihovim specifičnim potrebama. Njegova fokus na privatnost, strukturirane dozvole i visoku učinkovitost čine ga atraktivnim izborom za tvrtke koje žele iskoristiti prednosti tehnologije blockchajna. Razvojem i sve većom prihvaćenošću, Quorum će imati dugoročan utjecaj na područje decentraliziranih aplikacija i poslovnih rješenja.

4.1.2. HSBC

HSBC koristi blockchain za smanjenje troškova i vremena potrebnog za obavljanje trgovinskih financija. HSBC koristi tehnologiju blockchain u raznim područjima poslovanja, kao što su podrška trgovini, međunarodna plaćanja, provjera digitalnog identiteta i upravljanje lancem opskrbe. Korištenjem blockchain tehnologije, HSBC može unaprijediti procese, smanjiti mogućnost prijave te povećati povjerenje između sudionika u mreži. Također, implementacija pametnih ugovora na blockchainu omogućuje automatsko obavljanje unaprijed definiranih akcija nakon ispunjenja određenih uvjeta, što dodatno poboljšava učinkovitost i smanjuje mogućnost ljudskih grešaka (*Transforming the future of trade finance*, 2024).

4.1.3. Santander

Santander je jedna od prvih velikih banaka koja je lansirala blockchain baziran platni sustav pod nazivom One Pay FX. Sustav koristi Ripple blockchain tehnologiju za omogućavanje brzih i jeftinijih međunarodnih transakcija koja je dostupna u četiri zemlje. Nova usluga omogućuje korisnicima da u većini slučajeva obave međunarodne prijenose istog dana ili najkasnije sljedećeg dana (Santander, 2018).

Ovo je dio Ripple pristupa protiv zastarjelih bankarskih sustava, koji prisiljava pružatelje usluga plaćanja da drže velike količine kapitala kao likvidnost u inozemstvu. Aplikacija OnePay FX

pokazuje prelazak banaka na moderne sustave kako bi omogućile brže i učinkovitije plaćanje diljem svijeta. Kroz aplikaciju korisnici mogu vidjeti ukupan trošak slanja njihovih plaćanja, kao i bankovne naknade i tečajeve razmjene. Uspjeh ove usluge ne leži samo u transparentnosti, već i u jednostavnom iskustvu za mobilne korisnike. To može biti slanje sigurne poruke prijatelju, pozivanje dijeljenja vožnje ili slanje novca preko granica. Uz mobilno korisničko sučelje infrastrukturu i blockchain tehnologiju, aplikacija One Pay FX nudi korisnicima prijenos sredstava uz značajke kao što su: prikaz ukupnog troška pošiljke, uključujući bankovne naknade i tečajne razlike, procjenu vremena isporuke za dodatnu transparentnost te potvrdu plaćanja za potpunu sigurnost transakcije (*Santander uses Ripple technology to offer international payment*, 2018).

4.1.4. Barclays

Barclays je, zajedno s inovativnom start-up tvrtkom Wave, postao prvom organizacijom koja je izvršila globalnu trgovinsku transakciju koristeći blockchain tehnologiju. Transakcija akreditiva između Ornué i Seychelles Trading Company prva je koja je koristila Wave platformu za obradu trgovinskih dokumenata, dok su sredstva prenesena putem Swift-a. Ova značajna transakcija mogla bi označiti početak nove ere jednostavnijeg, sigurnijeg i bržeg financiranja trgovine. Trenutno trgovinske transakcije te vrste često uključuju velik broj sudionika u različitim zemljama diljem svijeta, što zahtijeva značajnu količinu papirologije, potpisivanja i slanja kurirskih pošiljki. Novi sustav temeljen na blockchainu, koji je razvila tvrtka Wave, koristi tehnologiju distribuirane knjige kako bi sve strane mogle vidjeti, prenijeti vlasništvo i poslati druge originalne trgovinske dokumente kroz sigurnu decentraliziranu mrežu, čime se eliminiraju mnoge trenutne neefikasnosti u međunarodnoj trgovini. Ovaj sustav ubrzava trgovinske transakcije, smanjuje troškove za tvrtke širom svijeta te smanjuje rizik od dokumentarne prijevare. Tvrtke diljem svijeta mogle bi ostvariti značajne uštede u vremenu i troškovima, posebno u broderskoj industriji i financijskim institucijama. Barclays je identificirao značajne uštede na kurirskim troškovima samo korištenjem Wave sustava (*Barclays and fintech start-up Wave pioneer blockchain trade finance transaction*, 2016).

4.3. Sigurnost transakcija

Od kada su kriptovalute uvedene prije deset godina i postale široko prihvaćene kao zamjena za tradicionalne metode plaćanja, broj njihovih korisnika naglo je porastao. Iako su kriptovalute vrlo popularne, većina organizacija i vlada oklijeva da ih prihvati kao standardni oblik plaćanja. Ovo nepovjerenje je posljedica njihove decentralizirane prirode, anonimnosti i nestabilnosti, što ih čini glavnim ciljem za razne kibernetičke zločine, uključujući pranje novca, pružanje rizičnih ili ilegalnih usluga i podržavanje terorističkih grupa. U digitalnom dobu, krađa identiteta i lažni korisnički računi predstavljaju značajan izazov za tvrtke. Blockchain tehnologija može ponuditi rješenja za ove probleme kroz napredne metode provjere identiteta i autentifikacije. Primjenom blockchaina, organizacije mogu uspostaviti decentralizirani sustav za upravljanje identitetima koji sigurno pohranjuje i provjerava korisničke podatke. Ova strategija izbjegava uporabu tradicionalnih centraliziranih baza podataka osobnih informacija, značajno smanjujući rizik od krađe podataka i identiteta (Tripathy, Balabantaray Parida, 2024).

4.3.1. Kako blockchain omogućuje otkrivanje prijevара

Blockchain tehnologija se odlikuje ključnom osobinom nemogućnosti izmjene zapisa transakcija. Jednom kada je transakcija dodana na blockchain, ne može se izmijeniti ili obrisati. Ova trajnost osigurava da su sve transakcije transparentne i lako dostupne za praćenje, pružajući jasan auditni trag za otkrivanje i istraživanje prijevара. Implementacija blockchain rješenja osigurava nepromjenjivost financijskih zapisa i smanjuje mogućnost unosa prijevernih transakcija ili falsificiranja informacija. Korištenje kriptografski povezanih blokova dodatno jamči da nitko ne može izmijeniti ili izbrisati zapise bez da to bude otkriveno (Tapscott, 2020).

Pametni ugovori, koji se sami izvršavaju, sadrže uvjete sporazuma unutar linija koda. Ovi ugovori su pohranjeni i izvršavaju se na blockchainu, što osigurava transparentnost i uklanja potrebu za posrednicima. Pametni ugovori mogu biti programirani da automatski pokreću određene akcije na temelju unaprijed definiranih uvjeta, poput nastupa određenog događaja ili ispunjenja obveza. Korištenjem pametnih ugovora, tvrtke mogu automatizirati procese otkrivanja prijevара, omogućujući stalno praćenje i brzo reagiranje na sumnjive aktivnosti (*What is Blockchain security*, 2024).

Sigurnost podataka i zaštita privatnosti ključni su elementi u sprječavanju i otkrivanju prijevara. Tradicionalne baze podataka, koje centralizirano pohranjuju osjetljive informacije, izložene su riziku povrede podataka i neovlaštenom pristupu. Blockchain nudi sigurniju alternativu šifriranjem i distribucijom podataka kroz više čvorova, čime se osigurava zaštita i dostupnost podataka samo za ovlaštene osobe. Osim toga, blockchain omogućuje pohranu podataka s dozvolama, gdje se kontrola pristupa može provoditi na različitim razinama, što osigurava da samo pouzdane strane mogu vidjeti ili mijenjati određene podatke (Pehar, 2024).

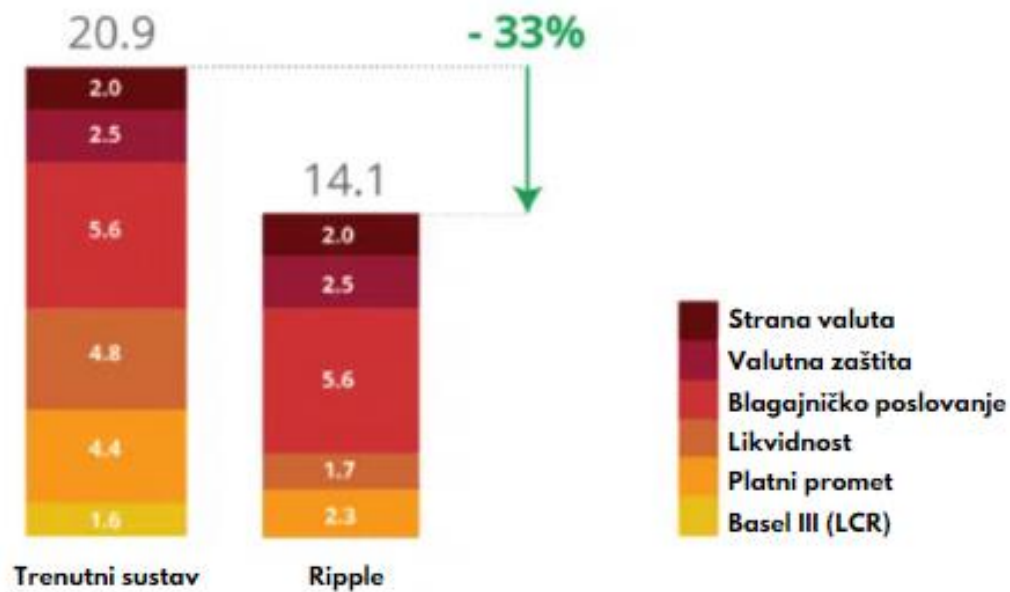
4.4. Transparentnost blockchainta

Transparentnost u blockchainu definira sposobnost pregledavanja javnih adresa gdje se može pristupiti povijesti transakcija, imovini itd. bez ograničenja. Ovaj stupanj transparentnosti nikada nije postojao unutar financijskog sustava ili poslovanja prije, što je dovelo do sumnji i zabrinutosti u nekim industrijama. Transparentnost blockchainta u bankarskom sektoru doprinosi jačanju povjerenja klijenata na nekoliko načina. Prednost je u tome što svaka transakcija koja se jednom dogodi i zabilježi na blockchainu postaje trajni i neizbrisivi zapis, koji je dostupan za pregled i provjeru svim sudionicima u mreži (*What is Blockchain security*, 2024). Ova transparentnost stvara jasan i provjerljiv pregled svih transakcija, što povećava povjerenje klijenata u banku. Kroz blockchain tehnologiju, klijenti mogu imati uvid u detalje svojih transakcija u stvarnom vremenu, prateći svaki korak putem distribuirane knjige. Nedostatak transparentnosti blockchainta može se pojaviti u slučaju kada se privatnost klijenata ili osjetljivi podaci moraju očuvati. S obzirom na prirodu javne distribucije podataka na blockchainu, rizik od otkrivanja osjetljivih informacija postoji. Osim toga, razumijevanje i interpretacija podataka na blockchainu mogu biti izazovni, jer blockchain tehnologija zahtijeva određenu razinu tehničkog znanja da bi se potpuno shvatila. U konačnici, pravilno korištenje transparentnosti blockchainta u bankarskom sektoru može pridonijeti jačanju povjerenja klijenata putem transparentnih i provjerljivih transakcija. Međutim, važno je uzeti u obzir potrebu zaštite privatnosti i osjetljivih podataka te pravilno upravljanje interpretacijom i razumijevanjem informacija kako bi se izbjegli nedostaci transparentnosti blockchainta (Petrov, 2019).

4.5. Efikasnost transakcija

Od samih početaka novčanih transakcija, banke su imale važnu ulogu u međunarodnim plaćanjima. Pojavom FinTech tvrtki poput PayPal-a i TransferWise-a, banke su doživjele značajan pad udjela na tržištu platnih usluga. Ove tvrtke su se istaknule nadmašujući banke po brzini, troškovima, fleksibilnosti i transparentnosti, predstavljajući ozbiljnu konkurenciju za bankovne usluge plaćanja. Banke se oslanjaju na SWIFT (Society for Worldwide Interbank Financial Telecommunications) mrežu za slanje i primanje međunarodnih plaćanja. Iako je SWIFT najsigurniji način za međunarodna plaćanja, proces je dugotrajan i skup. Na primjer, prosječno trajanje prijenosa je od 1 do 5 radnih dana, dok su troškovi u prosjeku između 40 i 50 dolara (*What is an international wire transfer*, 2023). Danas, prijenos vrijednosti na konačan način zahtijeva dugotrajan proces s brojnim sudionicima (npr. klijentima, bankama, klirinškim sustavima, sustavima za poravnavanje i sl.) koji rade na SWIFT mreži, koju banke koriste za prijenos svih vrsta financijskih informacija. Da bi se novac efikasno premjestio, nekoliko centraliziranih sustava djeluje kao javni bilježnik transakcije, čineći postupak vrlo dugim i složenim. Putem blockchaina, u suradnji s Bitcoinom i drugim kriptovalutama, ovaj proces može se odvijati na izravan, siguran i konačan način bez sudjelovanja spomenutih sudionika. Konkretno, zahvaljujući ključnim karakteristikama tehnologije distribuirane glavne knjige blockchain povezan s kriptovalutama omogućava dvjema osobama koje se ne poznaju međusobno izravnu razmjenu digitalne imovine na siguran i konačan način. To znači da na kraju transakcije dolazi do učinkovitog prijenosa vlasništva (Martino, 2021).

Slika 2. Troškovi infrastrukture međunarodnih plaćanja



Izvor: Izrada autora prema *SWIFT vs Ripple – the fight for better, faster, cheaper bank transactions*, 2022.

<https://www.penser.co.uk/article/swift-vs-ripple/>

(pristupljeno 5.5.2024.)

Prema Rippleu, banke koje mogu smanjiti kašnjenja u poravnanju i smanjiti operativne troškove obrade međunarodnih plaćanja mogu ostvariti uštedu od 33% u troškovima. Fokusirajući se na izazove transfera novca, Ripple koristi mrežu baziranu na blockchain tehnologiji radi poboljšanja procesa transfera. Ripple predstavlja sustav za brzu obradu u stvarnom vremenu (RTGS), mrežu za razmjenu valuta i plaćanja, namijenjenu direktnom prijenosu sredstava. Blockchain tehnologija može pomoći financijskim institucijama da brže i jeftinije obrade međunarodna plaćanja. Sustavi temeljeni na blockchainu mogu ukloniti potrebu za posrednicima, što omogućuje direktnije i sigurnije transakcije. Nadalje, blockchain rješenja mogu ubrzati procesiranje, smanjiti mogućnost grešaka i poboljšati transparentnost procesa plaćanja. Ripple je dobar primjer blockchain platforme dizajnirane za olakšavanje međunarodnih plaćanja i transakcija (Casey, Crane i Gensler, 2018).

4.6. Izazovi blockchaina u bankarskom sektoru

Puno ljudi još uvijek miješa Blockchain s Bitcoinom; međutim, nisu isti. Bitcoin je samo jedna od mnogih aplikacija koje koriste tehnologiju Blockchain. Blockchain tehnologija nosi sa sobom nekoliko potencijalnih izazova u svojoj primjeni. Neki od tih izazova uključuju pitanja regulacije i nedostatak jasnih pravnih okvira, zabrinutosti oko sigurnosti i privatnosti podataka, nedostatak razumijevanja o samoj tehnologiji među organizacijama i pojedincima, te troškove i efikasnost vezane uz različite vrste blockchaina i sudionike u mreži. Sve ove prepreke zahtijevaju pažljivo razmatranje prilikom implementacije blockchain tehnologije kako bi se uspješno prevladale i iskoristio njen puni potencijal (Tasatanattakool i Techapanupreeda, 2018).

4.6.1. Regulacije i sigurnost kao glavni izazovi blockchaina

Regulacija predstavlja jedan od ključnih izazova povezanih s tehnologijom blockchain. S obzirom na to da se blockchain zasniva na principu decentralizacije, način njegove regulacije postao je važna tema diskusije među regulatornim tijelima. U potpunosti decentraliziran sustav je u praksi gotovo neostvariv i nužno je postojanje određenog autoriteta koji bi u određenoj mjeri nadzirao financijske institucije. Trenutačno ne postoje univerzalni nacionalni ili međunarodni propisi za blockchain. Iako države istražuju mogućnosti kako regulirati ovu tehnologiju, pravni okviri koji bi regulirali blockchain još uvijek su nejasni. Dodatno, postavlja se pitanje tko će preuzeti ulogu autoriteta u kriznim situacijama. Odsutnost autoriteta znači da nema tko ublažiti negativne učinke tijekom teških vremena, što može rezultirati ekonomskim poteškoćama. Stoga je esencijalno da regulatorna tijela imaju potpuni uvid u sve aspekte prije nego što se odluče na implementaciju. Također, bez jasnih regulativa, ostaje nejasno kako riješiti sporove između dviju financijskih institucija, što može otežati brzu prihvaćenost ove tehnologije (Petrov 2019).

4.6.2. Razumijevanje i edukacija blockchain tehnologije

Unatoč velikom potencijalu, nedostaje adekvatno razumijevanje blockchain tehnologije i njezinih mehanizama. Dok organizacije i pojedinci nisu potpuno informirani o značaju i funkciji blockchaina, teško je očekivati progres u novim inicijativama i investicijama. Veliki

troškovi i pitanja učinkovitosti su također prevladavajući problemi blockchain tehnologije. Troškovi i učinkovitost uvelike ovise o vrsti blockchaine koja se koristi i o sudionicima unutar mreže. Neefikasnost se javlja zato što svi čvorovi u mreži moraju provjeriti svaku transakciju. Iako veći broj čvorova povećava sigurnost, to istovremeno smanjuje brzinu transakcija (Guo & Liang 2016). Prema istraživanjima tvrtke Deloitte iz 2016. godine, implementacija blockchain tehnologije za poslovne i osobne međunarodne transakcije mogla bi rezultirati značajnim smanjenjem troškova transakcija od 40 do 80%. Osim toga, očekuje se da bi takve transakcije mogle biti finalizirane u prosjeku za četiri do šest sekundi, što je znatno brže od standardnog procesa prijenosa koji obično traje od dva do tri dana. Primjerice, u travnju 2018. godine, Banco Santander pokrenuo je prvu uslugu međunarodnih novčanih transfera temeljenu na tehnologiji blockchain, što je omogućilo korisnicima da izvrše međunarodne prijenose istog ili sljedećeg dana. Uz to, korisnicima se prikazuje precizan iznos koji će primiti u ciljanoj valuti prije nego što izvrše sam transfer (*Cross-border payments on blockchain, 2016*).

5. Rasprava

Glavni fokus ovog istraživačkog procesa orijentiran je na pregled implementacije blockchaina u bankarskom sektoru promatran na stvarnim primjerima JP Morgan Chasea, HSBC-a, Barclays i Santander banke. Također, promatrana je sigurnost kroz traženje rješenja zaštite podataka i smanjenja rizika od prijevara. Transparentnost je promatrana kroz jačanje povjerenja klijenata u bankarski sektor. U posljednjoj fazi, istraživanje je procijenilo kako primjena blockchaina utječe na efikasnost procesa transakcija u bankama.

U najvećem postotku banke koriste blockchain za međunarodno slanje novca. Ključan je to pokazatelj da banke prvenstveno koriste blockchain za poboljšanje brzine, sigurnost i troškovne učinkovitosti međunarodnih transakcija. U podjednakoj mjeri banke koriste blockchain za namiru vrijednosnih papira, za KYC (Know Your Customer) i AML (Anti-Money Laundering) procese te za usluge plaćanja fiat valutom i stvaranja transparentnosti čime se zapravo omogućuje sigurna pohrana i transparentnost vezana za identifikaciju i provjeru klijenata. U najmanjoj mjeri blockchain u bankarskom sektoru koriste za izdavanje i prijenos vrijednosnih papira što se koristi za poboljšanje učinkovitosti i sigurnosti u ciklusima izdavanja i prijenosa.

Na temelju informacija o blockchain platformi Quorum razvijenoj od strane JPMorgan Chasea, možemo zaključiti sljedeće: Quorum je stvoren s ciljem unaprjeđenja sigurnosti i efikasnosti financijskih transakcija, posebice ističući se po brzini u usporedbi s Bitcoinom i Ethereumom. Platforma omogućuje obavljanje transakcija bez otkrivanja osjetljivih informacija zahvaljujući značajkama privatnosti. Korištenje QuorumChain konsenzusnog mehanizma osigurava sigurnost mreže i sprječava zlonamjerne napade. Unatoč tim prednostima, Quorum je još uvijek relativno nova platforma, ograničena u primjeni do sada. Njegova specifična namjena za financijske institucije može predstavljati izazov kod prihvaćanja u drugim sektorima. Redovito održavanje i aktualizacija Quoruma imperativni su za očuvanje sigurnosti i performansi platforme, no taj proces može biti skup i dugotrajan, što može predstavljati prepreku za tvrtke koje razmatraju implementaciju ove tehnologije. U konačnici, Quorum nudi znatne beneficije, no zahtijeva pažljivo vođenje i stalno praćenje kako bi se iskoristile sve prednosti blockchain tehnologije u financijskom sektoru.

HSBC koristi blockchain za optimizaciju poslovnih procesa, smanjenje troškova te vrijeme potrebno za trgovinske financije. Osim toga, implementacija pametnih ugovora pridonosi povećanju učinkovitosti i smanjenju mogućnosti ljudskih grešaka u različitim područjima poslovanja poput međunarodnih plaćanja i upravljanja lancem opskrbe. Time HSBC unapređuje procese, smanjuje rizike od prijevara te izgrađuje povjerenje među sudionicima u mreži.

Santanderova blockchain bazirana usluga One Pay FX omogućuje brze, jeftine međunarodne transakcije koristeći Ripple tehnologiju. Ova inovativna usluga naglašava prelazak banaka na moderne sustave koji podupiru učinkovitija plaćanja diljem svijeta. Transparentan pristup i mobilno korisničko sučelje čine ovu uslugu jednostavnom i sigurnom za korisnike, olakšavajući prijenos sredstava preko granica.

Barclays i start-up tvrtka Wave su prva organizacija koja je izvršila globalnu trgovinsku transakciju koristeći blockchain tehnologiju, što bi moglo označiti početak novog, pojednostavljenijeg i sigurnijeg načina financiranja trgovine. Novi sustav baziran na blockchainu omogućuje brže, sigurnije i efikasnije trgovinske transakcije, eliminirajući papirologiju i potrebu za slanjem dokumenata putem kurirskih usluga. Ova inovativna platforma ubrzava procese trgovine, smanjuje troškove te minimizira rizik od prijevara, donoseći potencijalne uštede u vremenu i financijskim resursima tvrtkama diljem svijeta, posebice u broderskoj industriji i financijskim sektorima.

Gore navedeni primjeri prikazuju upotrebu blockchaine u bankarskom sektoru kao novu i ne toliko istraženu tehnologiju koja će zasigurno pronaći mjesto i u ostalim bankarskim sustavima. Osim implementacije blockchaine na primjerima realnih bankarskih suatava, u radu je istražen utjecaj sigurnosti, transparentnosti i efikasnosti blockchaine na same transakcije. Na temelju navedenih informacija, zaključak je sljedeći: Blockchain tehnologija pruža neizbrisivu i transparentnu evidenciju transakcija te eliminira rizik od centralne točke otkaza, pružajući sigurniji način za pohranu i prijenos podataka putem decentralizirane strukture. Korištenje pametnih ugovora omogućuje automatizaciju procesa otkrivanja prijevara te ubrzava reakciju na sumnjive aktivnosti. Također, implementacija blockchain tehnologije pridonosi sigurnosti podataka kroz šifriranje i distribuciju putem više čvorova, čime se osigurava zaštita i dostupnost podataka samo za ovlaštene osobe.

S druge strane, uvođenje blockchain tehnologije u bankarski sektor predstavlja revoluciju s brojnim koristima, ali i izazovima koje treba riješiti. Regulacija je ključni izazov, budući da decentralizirana priroda blockchaine zahtijeva jasne smjernice i autoritete za nadzor nad

financijskim institucijama. Nedostatak regulacije može dovesti do nejasnoća u rješavanju sporova i upravljanju u kriznim situacijama. Sigurnost i privatnost podataka su zabrinutosti u javnim blockchainima, te naglašava važnost privatnih blockchain mreža za veću sigurnost. Također, nedostatak razumijevanja tehnologije te troškovi i učinkovitost predstavljaju prepreke koje treba prevladati prije šire primjene blockchain tehnologije. Važno je pravilno istražiti i razumjeti tehnologiju kako bi se iskoristile njezine prednosti uz minimalne rizike i komplikacije.

Na temelju gore navedenog, hipoteza „Implementacija blockchain tehnologije znatno unaprjeđuje integritet i neporecivost transakcijskih zapisa u bankarskom sektoru, pridonoseći značajnom smanjenju incidencija prijevare i neovlaštenih intervencija“ se prihvaća.

6. Zaključak

Analiza primjene blockchain tehnologije u bankarskom sektoru kroz primjere JP Morgan Chasea, HSBC-a, Barclays i Santander banke ukazuje na ključne prednosti poput sigurnosti, transparentnosti i efikasnosti. Informacije o Quorum platformi JPMorgan Chasea, HSBC-ovoj optimizaciji poslovnih procesa te Santanderovoj One Pay FX usluzi naglašavaju prednosti blockchaine u financijskim transakcijama. Također, implementacija blockchaine olakšava automatizaciju, smanjenje prijevара te jača povjerenje među sudionicima. Očekuje se da će blockchain tehnologija donijeti značajne promjene u bankarskom sektoru s ubrzavanjem transakcija, smanjenjem troškova i povećanjem transparentnosti.

Primjena blockchain tehnologije u bankarskom sektoru donosi temeljne promjene i ključne prednosti koje poboljšavaju sigurnost, transparentnost i efikasnost financijskih usluga. Kroz implementaciju blockchaine u stvarne primjere kao što su JP Morgan Chase, HSBC, Barclays i Santander banke, tehnologija se pokazala kao korisna za kreiranje trajnog i neporecivog zapisa transakcija. Ova svojstva omogućuju praćenje svih transakcija i pružaju jasan auditni trag koji olakšava otkrivanje i istraživanje prijevара.

Ključni pozitivni aspekt blockchain tehnologije je decentralizirana i distribuirana struktura koja elimira rizik od centralne točke otkaza. Tradicionalne centralizirane baze podataka često su mete hakera, dok blockchain oslanja na validaciju i verifikaciju transakcija putem mreže računala, što značajno smanjuje rizik od neovlaštenog pristupa podacima. Implementacija pametnih ugovora omogućuje automatizaciju procesa otkrivanja prijevара, omogućujući kontinuirano praćenje i brzu reakciju na sumnjive aktivnosti. Ova tehnologija postiže transparentnost i eliminira potrebu za posrednicima, čime se olakšava učinkovitost poslovanja. Pored toga, blockchain osigurava zaštitu privatnosti i sigurnost podataka putem šifriranja i distribucije podataka kroz više čvorova. Ova metoda osigurava dostupnost podataka samo za ovlaštene osobe te smanjuje rizik od krađe identiteta i podataka.

Ukratko, primjena blockchain tehnologije u bankarskom sektoru pruža niz koristi koje obuhvaćaju poboljšanje sigurnosti, smanjenje rizika od prijevара, veću transparentnost, učinkovitije transakcije te zaštitu podataka i privatnosti. Ova tehnologija predstavlja napredak koji doprinosi transformaciji bankarske industrije prema sigurnijem, bržem i pouzdanijem poslovanju. Budući da je ovo još uvijek relativno nova tehnologija, najveći nedostatak i izazovi

predstavljaju razumijevanje blockchaina zbog čega je važno pravilno istražiti i osjetiti tehnologiju kako bi se maksimalno iskoristili benefiti uz minimalne rizike i komplikacije.

Prihvaćena hipoteza koja potvrđuje da implementacija blockchain tehnologije pridonosi integritetu i sigurnosti bankarskih transakcija te smanjuje incidencije prijevara i neovlaštenih intervencija ističe ključnu ulogu ove tehnologije u transformaciji bankarskog sektora. Kroz korištenje blockchaina, banke dobivaju alat koji omogućuje neporecive zapise transakcija, smanjuje rizik od manipulacije podataka i pruža veću transparentnost poslovanja. Ovaj koncept učvršćuje povjerenje klijenata u bankarske institucije, osiguravajući im pouzdanije i sigurnije bankarsko iskustvo. Uz smanjenje mogućnosti prijevara i neovlaštenih pristupa, implementacija blockchain tehnologije može znatno unaprijediti integritet bankarskih transakcija te pomoći sektoru u suočavanju s brojnim izazovima današnjeg digitalnog doba, postavljajući temelje za efikasnije, sigurnije i transparentnije bankarsko poslovanje u budućnosti.

Literatura

Knjige, članci i radovi

1. Casey, M. Crane, J. and Gensler, G. (2018). *The Impact of Blockchain Technology on Finance: A Catalyst for Change*. Geneva: International Center for Monetary and Banking Studies.
2. Casey, M., Crane, J. And Gensler, G. (2018). *The Impact of Blockchain Technology on Finance: A Catalyst for Change*. Geneva: CEPR Press.
3. Connors, C., Sarkar, D. (2023). *PBL: System for Creating and Maintaining Personal Blockchain Ledgers*. Str. 1-15.
4. Dib, O., Brousmiche K. L., and Durand, A. (2018). *Consortium Blockchains: Overview, Applications and Challenges*. International Journal on Advances in Telecommunications, vol 11 no 1 & 2. Str. 51-64.
5. Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Frankfurt am Main: Apress.
6. Ge, L., Jiang, T. (2021). A Privacy Protection Method of Lightweight Nodes in Blockchain. Vol 2021. Str. 1-17.
7. Guo, Y., Liang, C. (2016). *Blockchain application and outlook in the banking industry*. Volume 2, Article number: 24. Str. 1-12.
8. Khan, S., Syed, M.H., Hammad, R. (2022). *Blockchain Technology and Computational Excellence for Society 5.0*
9. Lin, S. (2023). *Proof of Work vs. Proof of Stake in Cryptocurrency*. Highlights in Science, Engineering and Technology CMLAI 2023 Volume 39 (2023). Str. 953-961.
10. Martino, P. (2021). *Blockchain and Banking How Technological Innovations Are Shaping the Banking Industry*. Pisa: Palgrave Macmillan.
11. Mataković, H. i Cunjak Mataković, I. (2018). International Journal of Digital Technology & Economy, Vol. 3. No. 1., 2018. Str. 23-37.
12. Naheem, M.A. (2019). *Exploring the links between AML, digital currencies and blockchain technology*. Journal of Money Laundering Control. vol. 22(3) .Str. 515-526.
13. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Dostupno na: <https://bitcoin.org/bitcoin.pdf> (pristupljeno 6.5.2024.)

14. Neyigapula, B. (2021). Reshaping Banking through Blockchain: Exploring the Future of Financial Transactions. *Authorea*. Str. 1-16.
15. Nguyen, A., Truong D., and Kyungbaek K. (2018). *A Survey about Consensus Algorithms Used in Blockchain*. Journal of Information Processing Systems , vol. 14, no. 1, Str. 101–128.
16. Peters, G. and Panyi E. (2018). *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Mone*. University College London Str. 239-278.
17. Petrov, D. (2019). The impact of blockchain and distributed ledger technology on financial services. *Industry 4.0* Vol. 4 (2019), Issue 2, Str. 88-91.
18. Pourmirza, Z. (2023). *Cybersecurity in centralised vs decentralised energy systems*. Str. 1-5.
19. Saad, M., Spaulding, J. and Njilla, L. (2019). Overview of Attack Surfaces in Blockchain. *Blockchain for Distributed Systems Security*. Str 51–66.
20. Shevchenko, E. and Lunsford, R. (2022). *Blockchain Disruption in Finance: JPMorgan Chase’s Success Story and the Transfer of Quorum to ConsenSys*. Journal of Finance and Accountancy Volume 32. Str. 1-12.
21. Strehle E. (2020). *Public Versus Private Blockchains*. BRL Working Paper Series No. 14. Str. 1-8.
22. Swanson, T. (2015). *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems*. Str. 1-66.
23. Tapscott, A. (2020). *Financial Services Revolution*. Barlow Publishing.
24. Tasatanattakool, P. and Techapanupreeda, C. (2018). Blockchain: Challenges and applications. International Conference on Information Networking (ICOIN). Str. 1-4.
25. Tripathy, N.M., Balabantaray, S. K. And Parida, S.(2024). Cryptocurrency fraud detection through classification techniques. *International Journal of Electrical and Computer Engineering*, Vol. 14, No. 3. Str. 2918-2926.
26. Wątorek, M., Drozd. and S., Kwapien (2021). Multiscale characteristics of the emerging global cryptocurrency market. *Physics Reports*, 901(20), Str. 1-82.
27. Yang, F., Zhou, W., Wu, Q. (2017). Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm with Downgrade Mechanism. *IEEE Access*. Str. 1-15.

28. Zhang, C., and Xu, J. (2019). Enabling Verifiable Boolean Range Queries over Blockchain Databases. Str. 141-158.

Internetski izvori:

29. Bybit Learn. (2023). *santandof Of Stake*. Dostupno na: <https://learn.bybit.com/glossary/definition-liquid-proof-of-stake-lpos/> (pristupljeno 30.4.2024.)
30. Chainlink. (2023). *Hybrid Smart Contracts*. Dostupno na: <https://chain.link/education-hub/hybrid-smart-contracts> (pristupljeno 7.5.2024.)
31. Computer Weekly. (2018). *Santander uses Ripple technology to offer international payments*. Dostupno na: <https://www.computerweekly.com/news/252439085/Santander-uses-Ripple-technology-to-offer-international-payments> (pristupljeno 3.5.2024.)
32. Deloitte. (2016). *Cross-border payments on blockchain*. Dostupno na: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/grid/cross-border-payments.pdf> (pristupljeno 7.5.2024.)
33. Deloitte. (2018). *Blockchain and the impact on fund distribution*. Dostupno na: <https://www.deloitte.com/lu/en/Industries/technology/research/impacts-blockchain-fund-distribution.html> (pristupljeno 7.5.2024.)
34. Demos, T. (2016). J.P. Morgan Has a New Twist on Blockchain. Dostupno na: <https://www.wsj.com/articles/j-p-morgan-has-a-new-twist-on-blockchain-1475537138> (pristupljeno 1.5.2024.)
35. FinTech Future. (2016). *Barclays and fintech start-up Wave pioneer blockchain trade finance transaction*. Dostupno na: <https://www.fintechfutures.com/2016/09/barclays-and-fintech-start-up-wave-pioneer-blockchain-trade-finance-transaction/> (pristupljeno 6.5.2024.)
36. GeeksForGeeks. (2023). *Quorum Blockchain*. Dostupno na: <https://www.geeksforgeeks.org/quorum-blockchain/> (pristupljeno 1.5.2024.)

37. Genesis Block Newspaper - Copies of The Times Jan 3 2009. (n.d.). Bitcoin Genesis Block Newspaper - *The Times 03 Jan 2009*. Dostupno na: <https://www.thetimes03jan2009.com/> (pristupljeno 2.5.2024.)
38. HSBC UAE. (2024). *Transformin the future of trade finance*. Dostupno na: <https://www.business.hsbc.ae/en-gb/campaigns/blockchain> (pristupljeno 8.5.2024.)
39. IBM. (2024). *What is Blockchain security*. Dostupno na: <https://www.ibm.com/topics/blockchain-security> (pristupljeno 4.5.2024.)
40. Intellipaat. (2023). *Quorum Blockchain: A Complete Guide*. Dostupno na: <https://intellipaat.com/blog/quorum-blockchain/> (pristupljeno 1.5.2024.)
41. Investopedia. (2023). *What is the SWIFT Banking system*. Dostupno na: <https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp> (pristupljeno 30.4.2024.)
42. Pehar, D. (2024). Forbes. *How Blockchain Revolutionizes Data Integrity And Cybersecurity*. Dostupno na: <https://www.forbes.com/sites/forbestechcouncil/2024/01/17/how-blockchain-revolutionizes-data-integrity-and-cybersecurity/?sh=2ca490425b9a> (pristupljeno 7.5.2024.)
43. Santander. (2018). *Santander launches the first blockchain-bases international money transfer service across four countries*. Dostupno na: <https://www.santander.com/content/dam/santander-com/en/documentos/historico-notas-de-prensa/2018/04/NP-2018-04-12-Santander%20launches%20the%20first%20blockchain-based%20international%20money%20transfer%20service%20across%20-en.pdf> (pristupljeno 3.5.2024.)
44. Seergenkov, A. (2024). Cointelegraph. *What is the genesis block, explained*. Dostupno na: <https://cointelegraph.com/explained/what-is-the-genesis-block-explained> (pristupljeno 4.5.2024.)
45. Tardi, C. (2024). *Genesis Block: Bitcoin Definiton, Mysteries, and Secret Message*. Dostupno na: <https://www.investopedia.com/terms/g/genesis-block.asp> (pristupljeno 5.5.2024.)
46. Tipalti. (2023). *What is an international wire transfer?* Dostupno na: <https://tipalti.com/mass-payments-hub/international-wire-transfer/> (pristupljeno 7.5.2024.)

Popis slika

Slika 1. Arihtektura blockchaina

Slika 2. Troškovi infrastrukture međunarodnih plaćanja

Popis grafikona

Grafikon 1. Prikaz usluga za koje banke najviše koriste blockchain tehnologiju