Tehnologija ulančanih blokova kao novi način pohrane podataka

Kolarić, Luka

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2022./2023.

Luka Kolarić

Tehnologija ulančanih blokova kao novi način pohrane podataka

Završni rad

Mentor: izv.prof.dr.sc. Vedran Juričić

Zagreb, lipanj 2023.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Sadržaj

Sadržaj iv

1. Uvod 1

2. Decentralizirana arhitektura i funkcionalnost tehnologije ulančanih blokova 3

2.1. Tehnologija distribuiranog knjigovodstva 3

2.2. Kriptografija 4

2.2.1. Simetrična kriptografija 4

2.2.2. Asimetrična kriptografija 4

2.2.3. Hash funkcije 5

2.3. Distribuirani konsenzus 5

2.3.1. Dokaz rada 6

2.3.2. Dokaz o udjelu 6

2.4. Pametni ugovori 7

3. Proces pohrane podataka na blockchain 9

3.1. Šifriranje 9

3.2. Fragmentiranje podataka 10

3.3. Paritetni fragmenti 10

3.4. Verifikacija datoteka 11

4. Prednosti pohrane podataka pomoću tehnologije ulančanih blokova 12

4.1. Decentralizacija 12

4.2. Nepromjenjivost podataka 13

4.3. Transparentnost 14

5. Nedostatci pohrane podataka pomoću tehnologije ulančanih blokova 16

5.1. Ograničena skalabilnost i visoki troškovi transakcija 16

5.2. Nedostatak regulacije i standardizacije 17

5.3. Složenost i nedostatak razumijevanja tehnologije 18

6. Primjena pohrane podataka pomoću tehnologije ulančanih blokova 21

7. Zaključak 22
8. Literatura 24
Popis slika 26
Sažetak 27
Summary 28

1. Uvod

Već duže vrijeme kao glavni način pohrane podataka koristimo računalni oblak zbog njegove brzine i jednostavnosti pristupa različitim vrstama podataka. Korisnici imaju pristup svojim podacima s bilo kojeg mjesta ako imaju Internet, što im omogućuje da ih brzo i lako preuzmu ili izmijene. Osim toga, računalni oblak pruža visoku razinu skalabilnosti i dostupnosti, što znači da se kapacitet pohrane može lako povećati ili smanjiti prema potrebama korisnika. To je posebno korisno za male i srednje velike tvrtke koje mogu iskoristiti prednosti računalnog oblaka bez potrebe da ulaze u velike investicije u IT opremu i održavanje.

Međutim, unatoč mnogim prednostima, postoje i značajni nedostatci vezani za sigurnost i privatnost podataka pohranjenih u računalnom oblaku. U zadnje vrijeme, dokumentirano je mnogo slučajeva u kojima su hakeri (engl. *hackers*) uspjeli neovlašteno doći do osjetljivih podataka upravo jer je sigurnost računalnog oblaka zakazala. Osim toga, postoji i pitanje vlasništva i kontrole podataka, budući da korisnici moraju povjeriti svoje podatke trećim stranama koje pružaju usluge pohrane u oblaku. Kada korisnici pohrane svoje podatke u oblak, oni gube kontrolu nad njima i moraju se osloniti na pouzdanost i sigurnost treće strane. Iako većina tvrtki koje pružaju takve usluge imaju određene mjere sigurnosti u mjestu, postoji rizik od kompromitiranja ili neovlaštenog pristupa podacima, što može imati ozbiljne posljedice za korisnike.

Tu u igru ulazi tehnologija ulančanih blokova (engl. *blockchain technology*). Tehnologija ulančanih blokova može riješiti brojne probleme vezane za sigurnost i privatnost podataka pohranjenih u računalnom oblaku. Ulančani blok je decentralizirani, raspodijeljeni registar koji se sastoji od lančanih blokova koji sadrže podatke. Svaki blok je povezan s prethodnim blokom pomoću kriptografskih algoritama, što onemogućuje izmjenu ili brisanje podataka bez promjene svih prethodno spojenih blokova. Tehnologija ulančanih blokova je također decentralizirana, što znači da nije kontrolirana od strane jedne jedinice, već je održavana od strane mreže računala koja su povezana putem Interneta. Svako računalo (engl. *node*) u ovoj mreži ima kopiju cijelog ulančanog bloka. Ako se pokuša izmijeniti bilo koji podatak u jednom bloku, sva ostala računala u mreži će to detektirati i odbaciti promjenu kao nevažeću. To čini tehnologiju ulančanih blokova iznimno sigurnom i otpornom na hakiranje (engl. *hacking*).

U ovom radu usporedit će se pohrana podataka s i bez tehnologije ulančanih blokova. Istražit će se prednosti i nedostatci računalnog oblaka i tehnologije ulančanih blokova kao načina

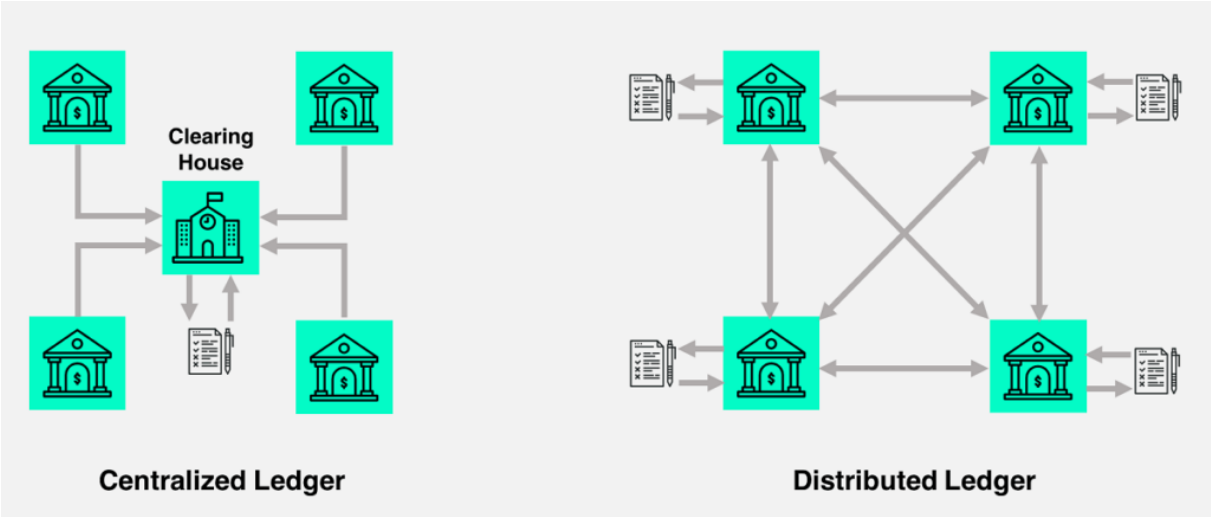
pohrane podataka. Analizirat će se ključne razlike između ovih metoda pohrane i proučiti u kojim se situacijama koja od njih može najbolje primijeniti. Detaljno će se opisati decentralizirana arhitektura i funkcionalnost tehnologije ulančanih blokova, te razmotriti njena različita područja primjene. Proučit će se kako se tehnologija ulančanih blokova koristi za pohranu podataka u različitim sektorima, uključujući financije, zdravstvo i lanac opskrbe. Objasnit će se kako se decentralizirana arhitektura tehnologije ulančanih blokova odražava u njenoj funkcionalnosti i kako se razlikuje od tradicionalnih metoda pohrane podataka. Također će se objasniti način na koji se podaci pohranjuju na ulančanom bloku te navesti razlozi zbog kojih je ovo sigurniji i održiviji način pohrane podataka u odnosu na tradicionalni računalni oblak. Proučit će se kriptografski mehanizmi koji se koriste za zaštitu podataka na ulančanom bloku, te kako se sprječava neovlašteni pristup i promjena podataka. Na kraju rada razmotrit će se mogućnosti i izazovi budućeg razvoja tehnologije ulančanih blokova i njene primjene u različitim industrijama.

2. Decentralizirana arhitektura i funkcionalnost tehnologije ulančanih blokova

Merriam-Webster objašnjava da je tehnologija ulančanih blokova decentralizirana arhitektura koja sadrži informacije (poput zapisa financijskih transakcija) koje se mogu istovremeno koristiti i dijeliti unutar velike decentralizirane, javno dostupne mreže. U toj mreži, transakcije se grupiraju u blokove i dodaju se na blockchain u linearnom i kronološkom redoslijedu. Svaki blok sadrži jedinstveni kod (eng. *hash*) koji ga povezuje s prethodnim blokom u lancu tako da su na kraju svi blokovi međusobno povezani. To stvara trajni i neizbrisivi zapis svih transakcija, što onemogućuje manipulaciju i brisanje podataka. Decentralizirana priroda blockchaina znači da mrežu ne kontrolira jedna centralizirana strana, i svi korisnici imaju jednak pristup istim informacijama. To čini blockchain tehnologiju idealnom za širok raspon primjena, uključujući pohranu podataka, digitalnu valutu, sustave glasanja, itd.

2.1. Tehnologija distribuiranog knjigovodstva

Tehnologija distribuiranog knjigovodstva (engl. *Distributed ledger technology*) je glavni razlog zašto je blockchain dobio svoj naziv. Gates (2017) navodi da se „svake sekunde na blockchainu dogodi mnogo transakcija u isto vrijeme pa se te transakcije zatim grupiraju i dodaju u novi blok. Ovaj novi blok dodaje se na vrh prethodnog bloka, povezujući ih zajedno. Povezivanjem ovih blokova, stvara se lanac blokova, od kuda i naziv "blockchain". Svaki novi blok odnosi se na prethodni blok, a taj blok se odnosi na blok prije njega, i tako sve do početka. Blokovi dodani u blockchain ne mogu se mijenjati niti obrisati.“ Ova tehnologija predstavlja vrstu arhitekture u kojoj se kopija baze podataka održava na svakom računalu u mreži, a ne na jednom centraliziranom mjestu. Na slici 1 prikazana je razlika između centraliziranog i distribuiranog knjigovodstva. Ta decentralizirana struktura je temeljna ideja većine blockchainova. Činjenica da je knjigovodstvo replicirano na više računala u mreži omogućuje poboljšanu sigurnost, jer ne postoji centralna točka koja može biti meta napadača. Osim toga, budući da svako računalo ima kopiju knjigovodstva, nema potrebe za centralnom vlasti za potvrđivanje transakcija i održavanje integriteta baze podataka. Još jedan važan aspekt DLT-a je da je omogućeno samo dodavanje podataka, što znači da jednom kada su podaci dodani u knjigovodstvo, oni se ne mogu mijenjati ili izbrisati. Ovo stvara neizbrisive zapise transakcija, što omogućuje veću transparentnost i sigurnost. DLT, uz distribuirani konsenzus mreže računala (engl. *distributed consensus*) i kriptografiju (engl. *cryptography*), stvara temeljnu tehnologiju iza blockchainova.



Slika 1. Razlika između centraliziranog i distribuiranog knjigovodstva (Shaker, M., Aliee, F.S. i Fotohi, R., 2021)

2.2. Kriptografija

Kriptografija ima ključnu ulogu u osiguravanju sigurnosti i integriteta podataka unutar blockchain tehnologije. Merriam-Webster navodi da kriptografija označava šifriranje i dešifriranje poruka. Upotrebom različitih kriptografskih tehnika, blockchainovi osiguravaju nepromjenjivost podataka (engl. *immutability*) i samim time visoku razinu povjerenja. Glavne vrste kriptografije korištene na blockchainu su: simetrična kriptografija, asimetrična kriptografija i hash funkcije.

2.2.1. Simetrična kriptografija

Jedna od temeljnih vrsta kriptografije koja se koristi u blockchainovima je simetrična kriptografija. Sahu (2022) objašnjava da „simetrična kriptografija uključuje upotrebu jednog ključa za procese šifriranja i dešifriranja. Taj ključ, također poznat kao tajni ključ (engl. *secret-key*), zajedno dijele pošiljatelj i primatelj.“ Simetrična kriptografija osigurava povjerljivost i integritet podataka koji se razmjenjuju. Sahu (2022) nadalje predstavlja dva pojma, niz šifri (engl. *stream ciphers*) i blokovske šifre (engl. *block ciphers*) kao dvije varijacije simetrične kriptografije. Nizovi šifri rade tako da mijenjaju ključeve ponavljajući postupak za svaki pojedini bit, dok blokovske šifre šifriraju jedan blok informacija odjednom.“ Važno je napomenuti da sigurno prenošenje tajnog ključa između sudionika ostaje izazov u simetričnoj kriptografiji.

2.2.2. Asimetrična kriptografija

Još jedna bitna kriptografska tehnika koja se koristi u blockchainovima je asimetrična kriptografija, također poznata kao kriptografija s javnim ključem. Prema Sahu-u (2022),

asimetrična kriptografija koristi par ključeva: javni ključ za šifriranje (engl. *public key*) i privatni ključ za dešifriranje (engl. *private key*). Par ključeva generira se koristeći isti algoritam, pri čemu se javni ključ dijeli javno, dok se privatni ključ čuva tajno. Ova vrsta kriptografije pruža nekoliko prednosti. Ona omogućuje sigurnu razmjenu ključeva između različitih komunikacijskih partnera te osigurava autentičnost javnog ključa. Međutim, kako Sahu (2022) napominje, provjera autentičnosti javnog ključa može predstavljati izazov jer može biti podložna napadima. Kako bi se riješio taj problem, Sahu predlaže korištenje infrastrukture s javnim ključem (PKI) koja koristi treću stranu zvanu certifikacijsko tijelo (engl. *certificate authority*) koje provjerava vlasništvo ključeva.

2.2.3. Hash funkcije

Hash funkcije su funkcije koje ne koriste ključeve, već generiraju hash vrijednost (engl. *hash value*) iz koje neće biti moguće dešifrirati izvorni tekst, kako je istaknuo Sahu (2022). Za razliku od simetrične i asimetrične kriptografije, hash funkcije ne zahtijevaju ključeve za svoje djelovanje. One se primarno koriste za integritet i identifikaciju podataka. Svaki sadržaj u blockchainu predstavljen je jedinstvenom hash vrijednošću, koja služi kao digitalni otisak prsta. Sahu (2022) ističe da je gotovo nemoguće rekonstruirati izvorni tekst iz hash vrijednosti, čime se osigurava integritet podataka.

2.3. Distribuirani konsenzus

Da bi se novi blok dodao u lanac i zapisao u knjigovodstvo, mora dobiti potvrdu od strane mreže računala. Ova računala rade zajedno kako bi postigla konsenzus o valjanosti transakcija unutar bloka. Jednom kada je blok potvrđen, on se dodaje u lanac i transakcije koje sadrži postaju dio trajnog zapisa. Gates (2017) ovdje uvodi pojam „distribuirani konsenzus“ te objašnjava kako se „većina računala na mreži treba složiti da je transakcija valjana da bi se mogla izvršiti. Kod većine blockchainova prag konsenzusa je preko 50%. To znači da ako se više od 50% računala na mreži slože da je transakcija valjana, tada se ona prihvaća i potvrđuje. Ovo je način na koji decentralizirani blockchainovi najčešće rade za odobravanje transakcija i upravljanje mrežom. Umjesto da jedan entitet odobrava sve transakcije i održava bazu podataka točnom, ta dužnost se dijeli među mrežom računala. Sva računala spojena na mrežu mogu odlučiti treba li transakcija biti prihvaćena u blockchain ili ne.“ Mehanizmi distribuiranog konsenzusa su zapravo algoritmi koji se koriste za potvrđivanje transakcija i održavanje integriteta distribuiranog knjigovodstva u mreži blockchaina. Najčešći mehanizmi konsenzusa su dokaz rada (engl. *proof of work*) i dokaz o udjelu (engl. *proof of stake*). Oba

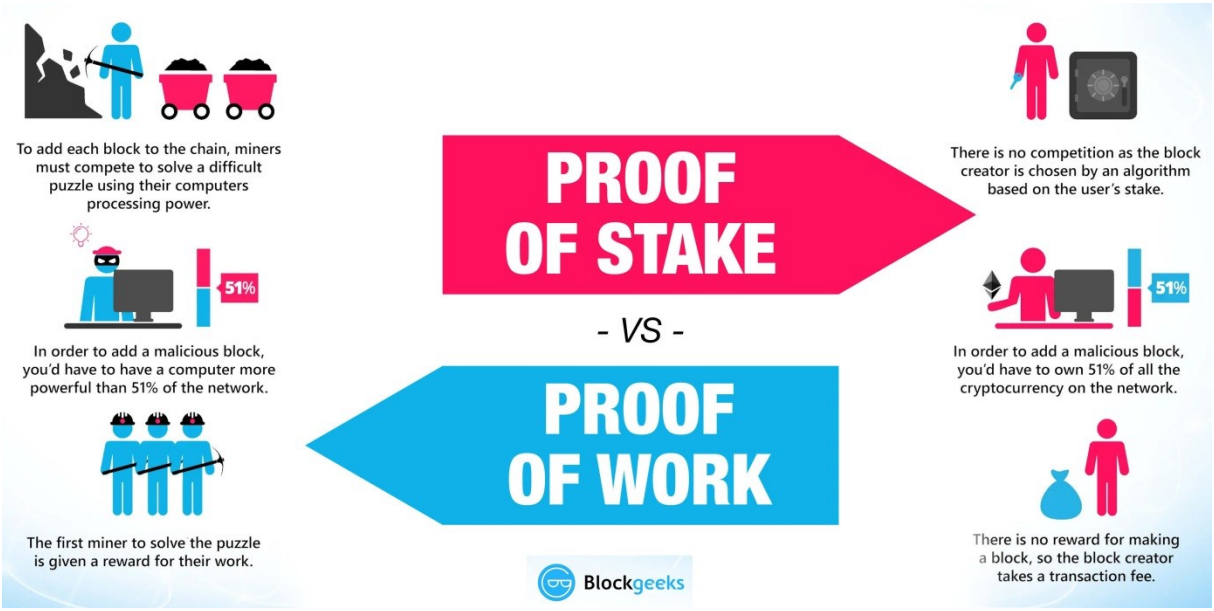
mehanizma se koriste za postizanje konsenzusa i potvrđivanje transakcija na mreži, ali to postižu na različite načine koji su prikazani na slici 2.

2.3.1. Dokaz rada

Dokaz rada je originalni mehanizam konsenzusa koji se koristi na najpopularnijem blockchainu Bitcoinu. Taj mehanizam uključuje intenzivan proces zvan rudarenje (engl. *mining*) koji zahtijeva računala, poznata i kao rudari (engl. *miners*), da koriste značajnu energiju za rješavanje složenih matematičkih problema. Antonopoulos (2015) na jednostavan način opisuje rudarenje govoreći kako „rudarenje u kriptovalutama možemo opisati kao veliku igru sudokua koja se resetira svaki put kada se pronađe rješenje. Težina slagalice, ili procesa rudarenja, se prilagođava tako da je potrebno oko 10 minuta da se pronađe rješenje. Slagalica koja se koristi u rudarenju temelji se na kriptografiji i ima slične karakteristike kao sudoku slagalica - teško je riješiti, ali lako je provjeriti.“ Računala se natječu te ono koje prvo riješi slagalicu potvrđuje transakciju i dodaje ju u blok. Rudarenje je vrlo popularno jer računala koja rudare automatski primaju nagradu u određenoj valuti, npr. Bitcoinu.

2.3.2. Dokaz o udjelu

Dokaz o udjelu je noviji mehanizam konsenzusa koji je predstavljen kao alternativa dokazu rada. Cilj mu je riješiti neke od problema povezanih s dokazom rada, kao što je visoka potrošnja energije. Frankenfield (2023) navodi da problem visoke potrošnje energije uspijeva riješiti tako da se umjesto korištenja rudarenja, koristi mehanizam temeljen na držanju zaključanog udjela izvorne valute mreže (engl. *staking*). Umjesto rudara koji rješavaju složene matematičke probleme, potvrđivanje se obavlja računalima koja drže određenu količinu izvorne valute mreže zaključanom. Računala se nasumično odabiru za potvrđivanje transakcija na temelju udjela valute koju drže. Što više valute računalo drži, to su veće šanse da će biti izabrano. Kada je računalo izabrano, ono dodaje blok u lanac te prima nagradu temeljenu na trošku transakcije. Možemo primijetiti da oba ova mehanizma konsenzusa nude nagrade računalima u svojim mrežama, što je glavni poticaj ljudima da sudjeluju u održavanju blockchaina.



Slika 2. Razlika između dokaza rada i dokaza o udjelu (Rosic, A., 2022)

2.4. Pametni ugovori

Da bismo shvatili ogroman potencijal decentralizirane arhitekture tehnologije ulančanih blokova, moramo se upoznati s pametnim ugovorima (engl. *smart contracts*). Pametni ugovori su zapravo automatizirani programi s uvjetima napisanima direktno u kodu. Oni su ključna značajka blockchain tehnologije koja omogućuje automatizaciju različitih vrsta transakcija i programa.

Glavna prednost pametnih ugovora je sposobnost automatskog izvršenja, bez potrebe za posrednicima. Ovo može značajno povećati učinkovitost i smanjiti trošak transakcija. Swan (2015) objašnjava da „postoje tri elementa pametnih ugovora koji ih čine jedinstvenima, a to su autonomija, samodostatnost i decentralizacija. Kao prvo, autonomija znači da nakon pokretanja ugovora, njegov inicijator ne mora biti u daljnjem kontaktu s ugovorom, već ugovor radi sam od sebe. Drugo, pametni ugovori su samodostatni u svojoj sposobnosti organiziranja resursa—to jest, prikupljanja sredstava pružanjem usluge ili izdavanjem vlasničkog kapitala i njihovo trošenje na potrebne resurse, kao što je obrada, napajanje ili skladištenje. Treće, pametni ugovori su decentralizirani utoliko što nisu zapisani na jednom centraliziranom poslužitelju, nego su raspoređeni i sami se izvršavaju preko cijele mreže računala.“

Na primjer, u tradicionalnoj transakciji nekretnina, pametni ugovor se može koristiti za automatizaciju prijenosa vlasništva nekretnine kada se ispune svi uvjeti ugovora, poput

plaćanja dogovorene cijene. Ovo eliminira potrebu za pravnikom ili tvrtkom za prijenos vlasništva, što smanjuje vrijeme i troškove cijelog procesa. Pametni ugovori se također mogu koristiti za stvaranje kompleksnih transakcija koje bi bile teško izvesti ručno. Na primjer, u sustavu upravljanja lancem opskrbe, pametni ugovor se može koristiti za automatizaciju isplate dobavljačima nakon što se roba primi i pregleda. Ovo osigurava da se plaćanja izvršavaju samo za robu koja zadovoljava određene standarde kvalitete, što smanjuje rizik od prijevare.

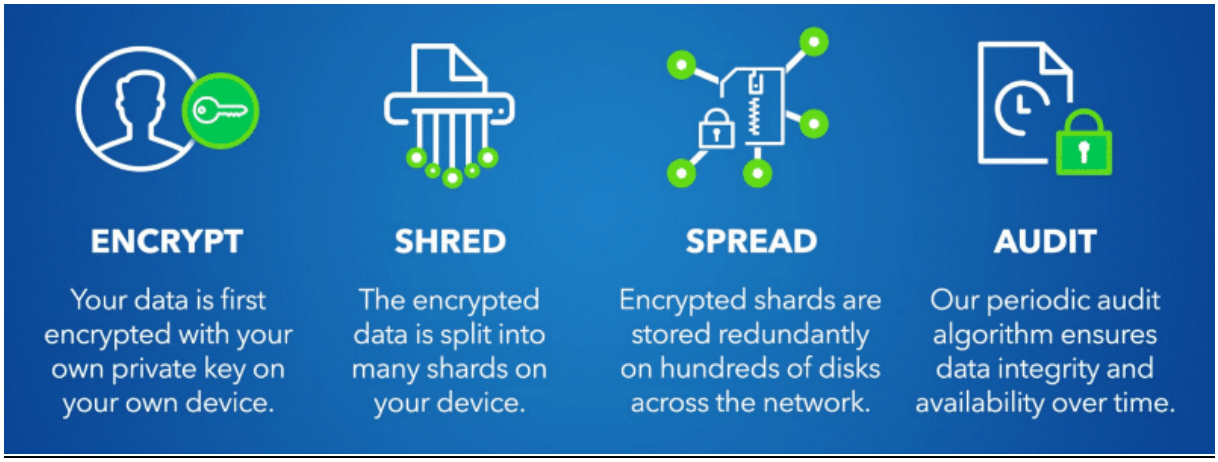
Pametni ugovori su također vrlo prilagodljivi, što omogućuje stvaranje jedinstvenih i specijaliziranih ugovora za širok raspon industrija. Ovo bi moglo uključivati financijske usluge, zdravstvo i logistiku. Još jedan aspekt koji treba uzeti u obzir je da su pametni ugovori neizmjenjivi, što znači da jednom kada se zapišu na blockchain, njihov kod se ne može mijenjati i manipulirati. Ovo čini pametne ugovore vrlo sigurnima, ali također znači da će bilo kakve pogreške u kodu biti trajne i neće se moći popraviti. Zato je važno temeljito testirati i revidirati sve pametne ugovore prije nego što se zapišu na blockchain.

3. Proces pohrane podataka na blockchain

Sada znamo kako tehnologija ulančanih blokova funkcionira i možemo se upoznati sa samim procesom pohrane podataka na blockchain. Kao primjer, prikazat ću proces pohrane podataka preko Storja. Garner (2018) opisuje Storj kao decentralizirano rješenje za pohranu datoteka koje koristi enkripciju, fragmentiranje datoteka i hash tablicu temeljenu na blockchainu za pohranu datoteka na peer-to-peer mreži. Cilj je učiniti pohranu datoteka bržom, jeftinijom i privatnijom. Storj vaše podatke šifrira, zatim fragmentira te na kraju šalje fragmentirane dijelove na mnogo računala u svojoj decentraliziranoj mreži.

Garner naglašava da se taj postupak sastoji od 4 koraka koji su naznačeni na slici 3:

1. Šifriranje
2. Fragmentiranje podataka
3. Stvaranje i slanje paritetnih fragmenata
4. Verifikacija datoteka



Slika 3. Proces pohrane podataka na Storj (Garner, 2018)

3.1. Šifriranje

Šifriranje je snažna sigurnosna mjera koja osigurava privatnost podataka poslanih s uređaja pošiljatelja na uređaj primatelja, čineći ih nedostupnima bilo kakvim posrednicima, uključujući pružatelje usluga. Kako Garner (2018) ističe u svom članku, šifriranje ima ključnu ulogu u zaštiti osjetljivih podataka. U kontekstu Storja, korisnici koji šalju ili pohranjuju svoje

datoteke, automatski ih šifriraju prije fragmentacije. Taj postupak šifriranja generira jedan ključ koji ostaje isključivo u posjedu vlasnika datoteke. Kao rezultat toga, samo vlasnik ključa za šifriranje može dešifrirati i pristupiti datoteci. Čak i ako bi domaćin podataka presreo neki fragment, bio bi beskoristan bez svih ostalih fragmenata i ključa za šifriranje. Vlasništvo nad ključem za šifriranje, u kombinaciji s distribuiranom prirodom sustava fragmentacije, čini izuzetno izazovnim za bilo koju neovlaštenu osobu da pristupi datoteci. Ovakva vrsta šifriranja pruža snažnu zaštitu od neovlaštenog pristupa, osiguravajući privatnost i povjerljivost osjetljivih informacija tijekom prijenosa i pohrane.

3.2. Fragmentiranje podataka

Fragmentiranje podataka je metoda koja dijeli datoteke na brojne manje dijelove. Prema Garneru (2018), ova metoda ima dva cilja. Prvo, omogućuje paralelno slanje i preuzimanje dijelova datoteka, što rezultira bržim prijenosom podataka. Drugo, osigurava da nijedan pojedinac ne posjeduje cijelu datoteku, što poboljšava privatnost korisnika. Storj ovdje naglašava privatnost korisnika. Samo vlasnik datoteke zna gdje se nalaze svi dijelovi. Kako bi olakšao preuzimanje dijelova, Storj koristi distribuiranu hash tablicu koja se oslanja na blockchain i kriptografiju. Ova hash tablica zahtijeva privatni ključ za točno lociranje dijelova datoteke. Bez privatnog ključa, gotovo je nemoguće dešifrirati lokacije dijelova. Sveukupno, fragmentiranje podataka u Storju kombinira prednosti paralelnog prijenosa datoteka, poboljšane privatnosti i sigurnog preuzimanja putem distribuirane hash tablice i kriptografije.

3.3. Paritetni fragmenti

Garner (2018) nadalje raspravlja o konceptu paritetnih fragmenata u kontekstu Storjovog sustava pohrane podataka govoreći da se prilikom korištenja Storja, pojedinačni fragmenti datoteka raspoređuju na običnim računalima u mreži. Ti paritetni fragmenti pružaju dodatni sloj zaštite podataka, smanjujući vjerojatnost gubitka bilo kojeg specifičnog fragmenta. Prilikom prenošenja datoteka, korisnici mogu odabrati željeni stupanj redundancije ili koristiti Storjove preporučene postavke. Međutim, s vremenom se povećava vjerojatnost gubitka fragmenata. Garner (2018) objašnjava da „kako bi se ta vjerojatnost minimalizirala, Storj provodi redovite provjere i metode verifikacije kako bi se osigurao integritet podataka.“ S druge strane, pretjerana redundancija može negativno utjecati na performanse mreže. Kako bi optimizirao sustav, Storj primjenjuje određena pravila koja identificiraju duplicirane fragmente i smanjuju njihovu redundanciju. Istovremeno, ta pravila pomažu identificirati jedinstvene podatke koji zahtijevaju povećanu redundanciju radi poboljšane zaštite.

Postizanjem ravnoteže između redundancije i učinkovitosti mreže, Storj osigurava brzinu prijenosa i dostupnost podataka pohranjenih unutar svoje mreže.

3.4. Verifikacija datoteka

Verifikacija datoteka je ključan aspekt osiguravanja cjelovitosti i dostupnosti datoteka pohranjenih na Storj mreži. Garner (2018) navodi da kako bi se riješile zabrinutosti u vezi postojanja datoteka i potencijalnih zlonamjernih radnji računala koja sadrže dijelove vaših podataka, Storj implementira provjeru datoteka svakog sata. U ovom procesu, računala su dužna pružiti dokaz da posjeduju određene fragmente koji su im dodijeljeni. Storj inicira zahtjev za provjerom prema računalima, i ako je računalo manipuliralo ili izbrisalo šifrirani fragment, ono neće moći pravilno odgovoriti. Međutim, ako računalo još uvijek posjeduje datoteku, ono može pravilno odgovoriti na zahtjev za provjerom. Kao nagradu za svoj doprinos, računala primaju plaćanja preko „STORJ“ tokena.

4. Prednosti pohrane podataka pomoću tehnologije ulančanih blokova

Blockchain tehnologija nudi mnoge prednosti za pohranu podataka, što je čini privlačnom opcijom za mnoge tvrtke i organizacije. Kao prvo, nudi decentralizaciju. To znači da nema centralne vlasti koja kontrolira cijeli sustav, čineći ga sigurnijim i otpornijim na pokušaje hakiranja. Drugo, blockchain tehnologija pruža nepromjenjivost podataka, osiguravajući da podaci ne mogu biti promijenjeni ili izbrisani bez suglasnosti cijele mreže. Ovo je važan aspekt tehnologije jer je čini idealnim rješenjem za pohranu osjetljivih informacija. Treće, blockchain tehnologija promovira transparentnost. Sve transakcije su zabilježene i vidljive svima na mreži, što je posebno korisno u industrijama poput upravljanja lancem opskrbe. Četvrto, korištenje blockchain tehnologije za pohranu podataka je ekonomično jer eliminira posrednike poput banaka ili drugih financijskih institucija. Zbog decentraliziranog konsenzusa, ne trebamo banke prilikom izvršenja bilo kakvih transakcija. Naposljetku, blockchain tehnologija osigurava sigurnost podataka korištenjem naprednih algoritama šifriranja i hashiranja, zbog čega je gotovo nemoguće hakirati ili manipulirati podatke na mreži. Sveukupno, blockchain tehnologija nudi brojne prednosti za pohranu podataka i odlično je rješenje za bilo koga tko traži siguran i učinkovit način za upravljanje i pohranu svojih podataka.

4.1. Decentralizacija

Jedna od ključnih prednosti korištenja blockchain tehnologije za pohranu podataka je njezina decentralizirana priroda. Za razliku od tradicionalnih sustava u kojima se podaci pohranjuju u centraliziranoj bazi ili poslužitelju pod kontrolom jednog entiteta, blockchain koristi već spomenutu tehnologiju distribuiranog knjigovodstva koja pohranjuje podatke preko mreže računala, što znači da nema centralne vlasti koja upravlja sustavom. To ga čini sigurnijim i otpornijim na pokušaje hakiranja, jer ne postoji jedna točka kvara koju hakeri mogu ciljati. Upotreba distribuiranog knjigovodstva znači da svako računalo u mreži ima kopiju lanca blokova, osiguravajući da su podaci uvijek dostupni, čak i ako neka računala zakažu ili su kompromitirana. To čini tehnologiju ulančanih blokova idealnom za pohranu povjerljivih podataka. Osim toga, decentralizirana priroda blockchain tehnologije osigurava da nijedan pojedinac ne kontrolira podatke. Svako računalo u mreži sudjeluje u procesu validacije i verifikacije, osiguravajući da su sve transakcije legitimne i smanjujući rizik od korupcije ili manipulacije. To je posebno važno u industriji financija, gdje su povjerenje i odgovornost

ključni. Gates (2017) ističe da bi „korištenje blockchain tehnologije za transakcije između banaka značajno pojednostavilo proces, jer bi banke samo trebale uskladiti transakcije na jednoj zajedničkoj knjizi kojoj bi sve banke imale pristup i na kojoj bi se složile oko točnog zapisa transakcija.“ Ovime bi banke povećale povjerenje korisnika i u isto vrijeme poboljšale međusobnu suradnju. Ako korisnici ne žele koristiti banke za transakcije, blockchain rješava i taj problem. Eliminiranjem potrebe za posrednicima poput banaka ili drugih financijskih institucija, blockchain tehnologija otvara nove mogućnosti za transakcije između pojedinaca i tvrtki, omogućujući im da izravno posluju jedni s drugima. To ne samo da smanjuje troškove, već omogućuje i nastanak novih poslovnih modela. Osim toga, decentralizirana priroda tehnologije ulančanih blokova čini je otpornijom na cenzuru i kontrolu vlade. U zemljama u kojima je cenzura učestala, tehnologija ulančanih blokova pruža način pojedincima da sigurno pohranjuju i dijele informacije, bez straha od intervencije ili cenzure vlade. Blockchain tehnologija bi se mogla koristiti i prilikom glasanja na raznim izborima jer bi bilo gotovo nemoguće falsificirati glasove.

4.2. Nepromjenjivost podataka

Još jedna ključna prednost blockchain tehnologije za pohranu podataka je njena sposobnost pružanja nepromjenjivosti, što znači da podaci pohranjeni na blockchainu ne mogu biti promijenjeni ili izbrisani bez suglasnosti cijele mreže. Doubleday (2018) objašnjava da je nepromjenjivost blockchaina „sposobnost koja omogućuje glavnoj knjizi blockchaina da postane trajna, neizbrisiva i nepromjenjiva povijest transakcija.“ To je idealno rješenje za pohranu osjetljivih informacija, kao što su financijski zapisi, medicinski zapisi i pravni dokumenti. Nepromjenjivost se postiže korištenjem kriptografskih algoritama koji stvaraju jedinstveni digitalni potpis za svaki blok podataka pohranjen na blockchainu. Taj se potpis zatim koristi za provjeru integriteta podataka, osiguravajući da podaci nisu izmijenjeni. Nepromjenjivost blockchain tehnologije posebno je važna u industrijama poput financija i zdravstva. Na primjer, u financijskoj industriji, blockchain tehnologija može se koristiti za pohranu financijskih zapisa poput plaćanja, koje je potrebno redovito provjeravati i revidirati. U zdravstvenoj industriji, blockchain tehnologija može se koristiti za pohranu medicinskih zapisa poput informacija o pacijentu i povijesti liječenja. Nepromjenjivost blockchaina osigurava da se nitko ne može naštetiti zloupotrebom tih podataka, pružajući siguran i pouzdan izvor informacija za zdravstvene stručnjake. Nepromjenjivost blockchain tehnologije ovime također promovira povjerenje i transparentnost. Doubleday (2018) naglašava da „implementacija blockchaina u postojeće industrije može donijeti neviđenu razinu povjerenja

u podatke i informacije koje poduzeća koriste svakodnevno.“ Pružajući siguran i pouzdan izvor informacija, blockchain tehnologija omogućuje pojedincima i organizacijama provjeru autentičnosti i točnosti podataka pohranjenih na blockchainu. To je posebno važno u industrijama poput upravljanja lancem opskrbe, gdje su transparentnost i odgovornost ključni. Osim toga, nepromjenjivost blockchain tehnologije također štiti od prijevare i kibernetičkog kriminala (engl. *cybercrime*) koji postaje sve veći problem u današnjem svijetu.

4.3. Transparentnost

Za razliku od tradicionalnih sustava u kojima se promjene u knjizi mogu mijenjati ili skrivati, transparentnost blockchaina osigurava da su promjene vidljive svima u mreži i kao što je već spomenuto ranije u radu, jednom unesene na blockchain, transakcije se ne mogu mijenjati ili izbrisati. Upravo ova transparentnost sprječava da slučajevi prijevare prođu neotkriveno, što je čest problem kod tradicionalnih knjiga.

Mnogo je primjera gdje je nedostatak transparentnosti u postojećim sustavima omogućio ljudima da manipuliraju podacima, što je dovelo do slučajeva masovnih prijevara. Samo neki od tih primjera uključuju manipulaciju financijskih izvješća, provođenje neovlaštenih transakcija i unutarnje trgovanje. Manipulacija financijskih izvješća događa se u financijskim sustavima gdje pojedinci s pristupom glavnoj knjizi izvješća mogu manipulirati unosima i mijenjati brojke. Skrivanjem gubitaka i obveza te prikazivanjem prihoda koji ne postoje mogu stvoriti lažan dojam o financijskom zdravlju organizacije. Bez transparentnosti, takve manipulacije mogu proći nezapaženo tijekom internih i vanjskih revizija. Kod provođenja neovlaštenih transakcija, pojedinci s privilegiranim pristupom mogu pokrenuti takve transakcije bez odgovarajućeg nadzora ili odobrenja. Oni mogu prebacivati sredstva na osobne račune ili preusmjeravati plaćanja na lažne račune. Nedostatak transparentnosti otežava drugim ljudima u tvrtki otkrivanje tih neovlaštenih aktivnosti, povećavajući rizik od financijskih gubitaka. Unutarnjim trgovanjem, prevaranti mogu ostvariti profitabilne transakcije na štetu drugih sudionika na tržištu koji nemaju iste informacije. Ovo su samo neki primjeri koji ilustriraju kako nedostatak transparentnosti u tradicionalnim sustavima omogućuje prijevare. Odsutnost javno provjerljive glavne knjige i mogućnost manipuliranja ili prikrivanja podataka stvara prilike za prevarante da iskoriste sustav radi osobne koristi.

Blockchain tehnologija rješava taj problem pružajući transparentnost svim sudionicima u mreži, s transakcijama vidljivim svim povezanim računalima. Ta transparentnost postiže se već spomenutim mehanizmom distribuiranog konsenzusa, gdje većina računala povezanih s

blockchainom mora odobriti transakcije ili promjene, sprječavajući da se transakcije skrivaju ili manipuliraju.

Gates (2017) ističe da „blockchain tehnologija omogućuje gotovo trenutačnu vidljivost transakcija koje se dodaju na blockchain.“ To znači da se financijske transakcije, na primjer, mogu pratiti u stvarnom vremenu na blockchainu, što eliminira nesigurnost vezanu uz status transakcija u tradicionalnim sustavima.

Osim toga, Gates (2017) još objašnjava da transparentnost koju pruža blockchain tehnologija ide dalje od financijskih transakcija. Sve vrijedne informacije zabilježene na blockchainu mogu imati koristi od iste razine transparentnosti. Ta transparentnost u različitim industrijama ključna je kako za kupce tako i za tvrtke, jer potiče povjerenje i sigurnost.

5. Nedostatci pohrane podataka pomoću tehnologije ulančanih blokova

Uz sve svoje prednosti, blockchain tehnologija također ima određene nedostatke kada se primjenjuje na pohranu podataka. Jedni od značajnih nedostataka su ograničena skalabilnost i visoki troškovi transakcija. Iako blockchain osigurava sigurnost i decentralizaciju, suočava se s poteškoćama u brzoj obradi velikog broja transakcija. Distribuirani konsenzus može dovesti do sporije obrade transakcija, čime postaje nepraktičan za potrebe pohrane i dohvaćanja podataka u stvarnom vremenu. Osim toga, s povećanjem broja transakcija, potrebna računalna snaga za provjeru i bilježenje također se povećava, što rezultira visokim troškovima transakcija. Još jedan izazov je nedostatak regulacije i standardizacije. Odsutnost jasnih regulatornih okvira i općeprihvaćenih standarda predstavlja značajne prepreke organizacijama i vladama koje žele implementirati blockchain za pohranu podataka. Nedostatak odgovarajućih propisa stvara neizvjesnost u vezi s pravnim i usklađenim aspektima, što znatno otežava implementaciju blockchainova u bilo kakve organizacije.

Kompleksnost i ograničeno razumijevanje blockchain tehnologije također predstavljaju izazove. Sama tehnologija nije jednostavna za razumjeti i zahtijeva mnogo znanja da bi se učinkovito implementirala u sadašnje industrije. Blockchain tehnologija je također još uvijek u vrlo ranoj fazi razvoja te zato možemo vidjeti nedostatak stručnjaka i ograničene obrazovne resurse u tom području.

Naposljetku, ovisnost o energetski intenzivnim postupcima rudarenja stvara brige za okoliš. Blockchain mreže koje koriste mehanizme konsenzusa dokaza o radu zahtijevaju značajnu računalnu snagu i potrošnju energije za rudarenje novih blokova. Ova energetski intenzivna ovisnost postavlja pitanja o održivosti blockchain tehnologije. Priznavanje i rješavanje ovih ograničenja ključno je za informirano donošenje odluka i realna očekivanja u vezi s implementacijom blockchaina u sustave pohrane podataka.

5.1. Ograničena skalabilnost i visoki troškovi transakcija

Ograničena skalabilnost i visoki troškovi transakcija jedni su od glavnih nedostataka blockchain tehnologije. Ograničenja skalabilnosti nastaju prvenstveno zbog decentralizirane prirode blockchaina, u kojoj svako računalo u mreži mora obraditi i potvrditi svaku transakciju. Ako dođe do naglog povećanja broja sudionika i transakcija, procesiranje se može usporiti i moguće je rušenje cijelog sustava. Nedostatak skalabilnosti postaje očit prilikom

usporedbe obrade transakcija na blockchainu s tradicionalnim sustavima plaćanja poput Vise. Na primjer, Bitcoin trenutno obrađuje oko sedam transakcija u sekundi, dok Visa može obraditi preko dvadeset tisuća transakcija u sekundi. Međutim, postoje drugi blockchainovi poput Solane koji mogu obraditi 5 do 10 tisuća transakcija u sekundi.

Dodatno, visoki troškovi transakcija povezani s blockchain tehnologijom predstavljaju značajan izazov. Računalni resursi potrebni za rudarenje i održavanje blockchaina zajedno s decentraliziranim procesom validacije su glavni razlozi tih troškova. Proces rudarenja zahtijeva značajne računalne resurse i potrošnju električne energije, što može biti vrlo skupo. Rudari moraju ulagati u specijaliziranu opremu i snositi pripadajuće troškove električne energije, što sudjelovanje u mreži čini ekonomski opterećujućim. Stoll (2018) naglašava kako je prosjek godišnjih emisija ugljika koje proizvodi Bitcoin u rangu emisija koje proizvode države Bolivija i Portugal.

Blockchainovi naplaćuju naknade za sve transakcije koje distribuiraju rudarima kako bi potaknuli rudarenje. Kada potražnja za transakcijama premaši kapacitet mreže, naknade za transakcije mogu dramatično porasti, čineći pohranu podataka na blockchainu neprofitabilnom. To postavlja izazove za mikro transakcije ili aplikacije u kojima je minimaliziranje troška svake transakcije ključno. Brojne transakcije malih vrijednosti mogu brzo akumulirati visoke troškove transakcija, čineći pohranu podataka na blockchainu financijski neodrživom.

Aplikacije koje zahtijevaju brzu obradu podataka također se suočavaju s preprekama zbog sporijih brzina transakcija blockchaina. Takve aplikacije se oslanjaju na infrastrukture koje mogu obraditi veliki broj transakcija brzo i efikasno, nešto što tradicionalne baze podataka trenutno mogu pružiti učinkovitije.

Međutim, važno je napomenuti da se provode mnoga istraživanja i razvojni napori kako bi se riješila ova ograničenja. Sve više blockchainova koristi alternativne mehanizme konsenzusa poput dokaza o udjelu kako bi se poboljšala skalabilnost i energetska učinkovitost. Marr (2023) naglašava da ako želimo da blockchainovi postanu svakodnevna opcija za pohranu podataka, moramo nastaviti istraživati načine za smanjenje potrošnje energije i razvijati ekološki održiva rješenja.

5.2. Nedostatak regulacije i standardizacije

Nedostatak propisa i nejasnoće vezane uz vlasništvo podataka ističu potrebu za jasnijim pravnim okvirom vezanim uz blockchain tehnologiju. Nedostatak jasnih pravnih okvira

predstavlja izazove jer blockchain djeluje preko granica, te uključuje pohranu i obradu osjetljivih podataka. Nedostatak zakonski određenih pravila često dovodi do nejasnoća u vezi s vlasništvom podataka, privatnošću i sigurnošću. Nejasan pravni status blockchaina i njegovih primjena često odbije tvrtke i organizacije od prihvaćanja ove tehnologije za pohranu podataka. Bez jasnih smjernica, potencijalni rizici i odgovornosti povezani s pohranom podataka na blockchainu postaju prepreka za njegovu implementaciju. Nedostatak standardiziranih pravila može dovesti do nepotrebnih pravnih sporova i dodatne brige za organizacije koje pokušavaju koristiti blockchain. Jasni i dobro definirani propisi nužni su kako bi se ojačalo povjerenje i osigurala usklađenost s propisima o zaštiti podataka i privatnosti. Uspostavljanjem regulacija koje se bave pitanjima poput vlasništva podataka, privatnosti i sigurnosti, organizacije bi mogle lakše usvojiti ovu novu tehnologiju jer se ne bi previše trebali zamarati pravnim rizicima. Jasne smjernice i standardizirane prakse potrebne su kako bi se stvorilo okruženje koje potiče ulaganja, suradnju i kontinuirani razvoj blockchaina. George (2023) objašnjava da je regulacija kripto valuta i blockchainova spori kontinuirani proces i da je teško predvidjeti kako će svaka zemlja reagirati prilikom uspostavljanja novih zakona i pravila. Uglavnom, dok se pravne regulacije ne uspostave, većina radnji koje koriste tehnologiju ulančanih blokova ostaju u sivoj zoni. Decentralizirana priroda blockchain tehnologije također postavlja pitanja o vlasništvu i kontroli podataka. Tradicionalni modeli pohrane podataka obično se oslanjaju na centralne autoritete ili posrednike koji mogu biti odgovorni za kršenje podataka ili neovlašteni pristup. Međutim, u decentraliziranoj blockchain mreži, podaci su raspoređeni na više računala, što otežava određivanje tko posjeduje podatke i tko je odgovoran za njihovu sigurnost. Nedostatak jasnoće može izazvati pravne i etičke brige, kao i ometati rješavanje sporova vezanih za vlasništvo podataka na blockchainu.

5.3. Složenost i nedostatak razumijevanja tehnologije

Razumijevanje kompleksnosti blockchaina i snalaženje u toj kompleksnosti zahtijeva specijalizirano znanje i stručnost, što dovodi do mnogo izazova u različitim fazama usvajanja ove tehnologije. Prvi i najkompliciraniji problem je kriptografija. Ispravna implementacija kriptografskih tehnika poput hashiranja, digitalnih potpisa i šifriranja zahtijeva duboko razumijevanje blockchain tehnologije, koje nije lako za usvojiti. Osim toga, koncepti poput mehanizama konsenzusa, pametnih ugovora i modela decentralizirane uprave dodaju dodatne slojeve kompleksnosti koji zahtijevaju stručnost u distribuiranim sustavima i programiranju.

Ta kompleksnost predstavlja izazove tijekom razvoja i implementacije blockchain aplikacija. Stručnjaci koji su vješti u kriptografiji, distribuiranim sustavima i razvoju softvera ključni su za učinkovito iskorištavanje potencijala blockchaina za pohranu podataka. Rijetkost takvih stručnjaka usporava napredak i ograničuje široko usvajanje blockchain tehnologije.

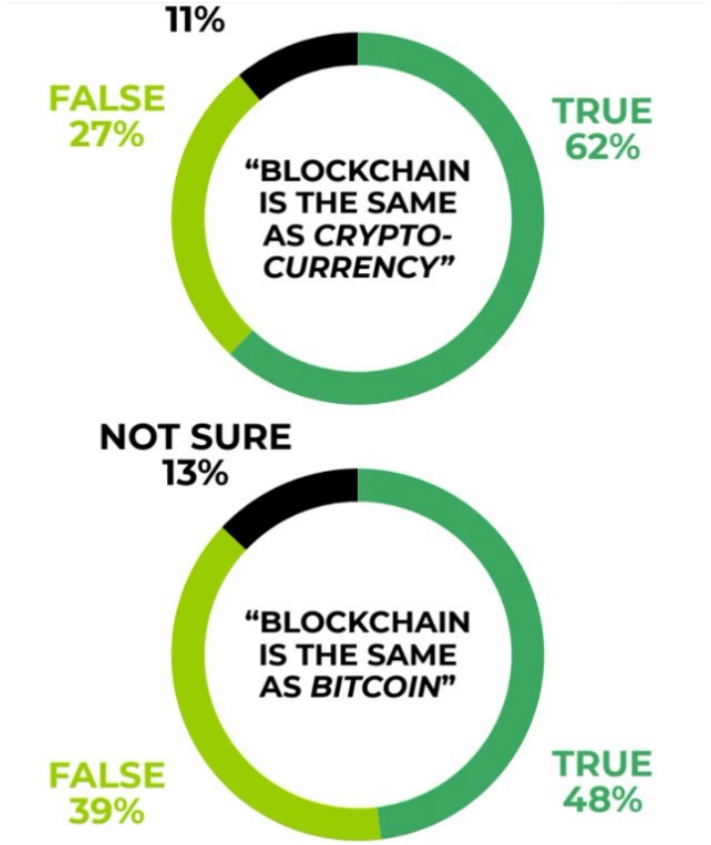
Nadalje, nepromjenjivost blockchaina također znači da je iznimno teško ispraviti bilo kakve pogreške. Čak i mala pogreška u kodu ili konfiguraciji neke blockchain aplikacije može imati opasne posljedice, ugrožavajući integritet podataka ili dovodeći do značajnih financijskih gubitaka. Kompleksnost tehnologije zahtijeva iznimnu preciznost i mnogo testiranja kako bi se osigurala sigurnost i pouzdanost cijelog sustava.

Da bi se riješili ti izazovi, potrebni su usklađeni napori u obrazovanju i širenju znanja. Lichtigstein (2018) navodi više načina na koje bi se ljudi mogli bolje obrazovati o blockchain tehnologiji:

1. Pokretanje kolegija u obrazovnim ustanovama
2. Pokretanje posebnih online tečajeva
3. Održavanje konferencija od strana tvrtki koje rade na blockchainovima

Nadalje naglašava kako neke institucije i organizacije poput IBM-a i Princetona već nude tečajeve o blockchain tehnologiji, ali da ima još mnogo prostora za napredak.

O nedostatku razumijevanja blockchain tehnologije govori i Brown (2021) koja je provela anketu u lipnju 2020. godine provedenu na 2000 ljudi iz Sjedinjenih Američkih Država. Anketa je pokazala da 1 u 4 ispitanika praktički ne zna ništa o blockchainu, a od onih koji prepoznaju taj termin, većina ga ne razumije. Na slici 4. možemo vidjeti da 62% ispitanika misli da je blockchain isto što i kriptovaluta (engl. cryptocurrency), što naravno nije točno jer termin kriptovaluta samo opisuje vrstu digitalnog novca koja se nalazi na nekom blockchainu, dok blockchain opisuje cijelu tehnologiju. 27% ispitanika je odgovorilo da blockchain nije isto što i kriptovaluta, dok je 11% njih reklo da nisu sigurni. Na pitanje je li blockchain isto što i Bitcoin, 14% ispitanika nije bilo sigurno, 48% njih je mislilo da je to točno, a samo 39% je reklo da je to netočno. Odgovor na pitanje je naravno također ne jer je Bitcoin samo jedna od kriptovaluta.



Slika 4. Odgovori ankete o razumijevanju blockchaina (Brown 2021)

6. Primjena pohrane podataka pomoću tehnologije ulančanih blokova

Pohrana podataka putem blockchain tehnologije ima potencijala za donijeti promjenu u brojne industrije, redefinirajući način na koji se podaci pohranjuju i dijele. Jedna industrija koja može doživjeti značajnu transformaciju je upravljanje lancem opskrbe. S blockchainom, cijeli lanac opskrbe postaje transparentan i moguće ga je lako pratiti. Svaki korak procesa može se zabilježiti i provjeriti, osiguravajući autentičnost robe. Singh (2022) navodi da bi transparentnost bila znatno bolja s blockchain tehnologijom jer bi „svi sudionici u lancu opskrbe bili dužni ispuniti uvjete pametnog ugovora prije nego bi se proizvod poslao/prodao drugom sudioniku. Nakon ispune uvjeta, glavna knjiga transakcija bi se odmah ažurirala i informacije o transakciji bi bile dostupne svima."

Industrija zdravstva također svjedoči potencijalu pohrane podataka putem blockchain tehnologije. Daley (2022) navodi da bi blockchain tehnologija olakšala siguran prijenos medicinske dokumentacije pacijenata te ojačala sigurnost opskrbe lijekova i obranu zdravstvenih podataka." Osim toga, blockchain omogućava lakšu i bolju suradnju, omogućavajući različitim zdravstvenim sustavima međusobnu razmjenu podataka.

Upravljanje intelektualnim vlasništvom predstavlja još jedno područje gdje pohrana podataka putem blockchain tehnologije može pokazati svoju vrijednost. Blockchain pruža neizbrisiv zapis vlasništva i dokaze o autorstvu. Budući da je zaštita prava intelektualnog vlasništva vrlo važna, na ovaj način može se pravilno zaštititi. Autori mogu zaštititi svoje intelektualno vlasništvo, upravljati autorskim pravima te olakšati licenciranje i plaćanja autorskih naknada putem blockchaina.

Pohrana podataka putem blockchain tehnologije također nalazi primjenu u sustavima glasanja. Iskorištavanjem nepromjenjivosti i kriptografske sigurnosti blockchaina, procesi glasanja postaju transparentniji i sigurniji. Blockchain pruža sustave glasanja koji su transparentni i otporni na manipulaciju, osiguravajući integritet izbora i upravnih procesa. Time se povećava povjerenje birača, smanjuju se prijevare i povećava se dostupnost putem mogućnosti daljinskog ili internetskog glasanja. Decentralizirana priroda blockchaina također smanjuje ovisnost o centraliziranim autoritetima i time promovira demokratsko upravljanje.

7. Zaključak

Blockchain tehnologija je još uvijek u svojim ranim fazama, ali već možemo uočiti mnoge prednosti u vezi pohrane podataka. Glavne prednosti koje nam pruža blockchain tehnologija u odnosu na tradicionalne oblike pohrane podataka su decentralizacija, nepromjenjivost podataka i transparentnost. Decentralizirana priroda blockchaina eliminira potrebu za centralnim autoritetom i omogućava izravne transakcije među korisnicima. To je iznimno važno jer nam osigurava da nijedan pojedinačni entitet nema potpunu kontrolu nad podacima. Nepromjenjivost podataka na blockchainu pruža visoku razinu integriteta podataka i čini neovlaštene promjene nemogućim. Ta nepromjenjivost osigurava sigurnost tehnologije ulančanih blokova. Također, transparentnost blockchaina omogućava povećano povjerenje u različitim primjenama, poput upravljanja lancima opskrbe, financijskim transakcijama i pohrani podataka.

Međutim, važno je prepoznati i ograničenja blockchain tehnologije. Ograničena skalabilnost blockchain mreže otežava učinkovito procesiranje velikog broja transakcija. S naglim povećanjem broja sudionika i transakcija, mreža se znatno uspori, a i može doći do kompletnog rušenja cijelog sustava. Ovo ograničenje predstavlja značajnu prepreku širokom usvajanju blockchain tehnologije u industrijama s velikim brojem svakodnevnih transakcija. Još jedan nedostatak je potreba za regulatornim okvirom koji će se baviti pravnim pitanjima povezanim s blockchainom. Svaka država bi trebala uvesti zakone povezane s korištenjem blockchain tehnologije. Nadalje, sama složenost blockchain tehnologije predstavlja veliku prepreku za mnoge pojedince i organizacije. Tehnička stručnost potrebna za implementaciju i održavanje blockchain sustava može biti zastrašujuća za korisnike koji nemaju dovoljno tehničko znanje.

Da bismo prevladali ova ograničenja, možemo razmotriti nekoliko prijedloga za poboljšanje. Prije svega, ključno je rješavanje pitanja skalabilnosti. Istraživanje i razvoj treba usmjeriti na optimizaciju blockchain protokola i ispitivanje alternativnih mehanizama konsenzusa koji mogu poboljšati skalabilnost bez ugrožavanja sigurnosti i decentralizacije. Također je potrebna suradnja između akademskih institucija i regulatornih tijela kako bi se uspostavili čvrsti okviri i standardi za implementaciju blockchaina u postojeće industrije. Na blockchain tehnologiju ne bismo trebali gledati kao zamjenu tradicionalnih sustava pohrane podataka, već kao njihovu alternativu. Nema razloga zašto ne bismo koristili oboje te iskoristili prednosti svih sustava pohrane i nadomjestili njihove nedostatke. Bez napora i suradnje nikada nećemo

moći iskoristiti puni potencijal ove nove tehnologije koja zaista ima potencijala unijeti kvalitetne promjene u razne postojeće industrije.

8. Literatura

1. Antonopoulos, A.M. (2015) *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly.

2. blockchain. (n.d.). U: Merriam-Webster. Dostupno na: https://www.merriam-webster.com/dictionary/blockchain

3. Brown, E. (2021) *Consumers don't understand blockchain but covet what it enables, survey reveals*. ZDNet. Dostupno na: https://www.zdnet.com/finance/blockchain/consumers-dont-understand-blockchain-but-covet-what-it-enables-survey-reveals

4. cryptography. (n.d.). U: Merriam-Webster. Dostupno na: https://www.merriam-webster.com/dictionary/cryptography

5. Daley, S. (2022) *Blockchain Voting: The Future of Elections?*. Builtin. Dostupno na: https://builtin.com/blockchain/blockchain-voting-future-elections

6. Doubleday, K. (2018) *Blockchain Immutability — Why does it matter?*. Medium. Dostupno na: https://medium.com/fluree/immutability-and-the-enterprise-an-immense-value-proposition-98cd3bf900b1

7. Frankenfield, J. (2023) *What Does Proof-of-Stake (PoS) Mean in Crypto*. Investopedia. Dostupno na: https://www.investopedia.com/terms/p/proof-stake-pos.asp.

8. Garner, B. (2018) *What is storj?: Beginner's guide*. CoinCentral. Dostupno na: https://coincentral.com/storj-beginners-guide/

9. Gates, M. (2017) *Blockchain: Ultimate Guide to understanding blockchain, Bitcoin, cryptocurrencies, smart contracts and the future of money*. Wise Fox Publishing.

10. George, K. (2023) *Cryptocurrency Regulations Around the World*. Investopedia. Dostupno na: https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122

11. Lichtigstein, A. (2018) *Blockchain Education- The Key To Economic Growth*. 101Blockchains. Dostupno na: https://101blockchains.com/blockchain-education-the-key-to-growth

12. Marr, B. (2023) *The 5 biggest problems with blockchain technology everyone must know about*. Bernard Marr Co. Dostupno na: https://bernardmarr.com/the-5-biggest-problems-with-blockchain-technology-everyone-must-know-about/

13. Rosic, A. (2022) *Proof of Work vs Proof of Stake: Basic Mining Guide*. Blockgeeks. Dostupno na: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

14. Sahu, M. (2022) *Cryptography in Blockchain: Types & Applications [2023]*. upGrad. Dostupno na: https://www.upgrad.com/blog/cryptography-in-blockchain/

15. Shaker, M., Aliee, F.S. i Fotohi, R. (2021) *Online rating system development using blockchain-based distributed ledger technology*. ResearchGate. Dostupno na: https://www.researchgate.net/publication/348426918_Online_rating_system_development_using_blockchain-based_distributed_ledger_technology

16. Singh, O. (2022) *How blockchain technology is used in supply chain management?*. Cointelegraph. Dostupno na: https://cointelegraph.com/explained/how-blockchain-technology-is-used-in-supply-chain-management

17. Stoll, C., Klaassen, L. i Gallersdörfer, U. (2018) *The Carbon Footprint of Bitcoin*. JSTOR. Dostupno na: https://www.jstor.org/stable/resrep34616?seq=3

18. Swan, M. (2015) *Blockchain: Blueprint for a new economy*. O'Reilly.

Popis slika

Slika 1. Razlika između centraliziranog i distribuiranog knjigovodstva.....4
Slika 2. Razlika između dokaza rada i dokaza o udjelu 7
Slika 3. Proces pohrane podataka na Storj.....9
Slika 4. Odgovori ankete o razumijevanju blockchaina.....20

Tehnologija ulančanih blokova kao novi način pohrane podataka

Sažetak

Tehnologija ulančanih blokova (engl. *blockchain technology*) jedno je od novijih rješenja za pohranu podataka. Ova tehnologija radi na temelju distribuiranog knjigovodstva, kriptografije i distribuiranog konsenzusa. Pomoću pametnih ugovora tj. programa zapisanih na blockchainu služi kao novi sustav pohrane i dijeljenja podataka. Konkurira tradicionalnim vrstama pohrane podataka poput pohranjivanja na računalni oblak jer nudi decentralizaciju, nepromjenjivost podataka i transparentnost. Međutim, blockchain ima i svoje mane, poput ograničene skalabilnosti, visokog troška transakcija, nedostatka regulacije i standardizacije te same kompleksnosti tehnologije. Neke od potencijalnih primjena blockchain tehnologije za pohranu podataka možemo naći u lancu opskrbe, zdravstvenoj industriji i financijskom sektoru. Iako je blockchain tehnologija još u ranim fazama razvoja, već nam nudi brojna rješenja za određene probleme na koje nailazimo prilikom tradicionalne pohrane podataka. Na nama je da zajedničkim naporima i međusobnom suradnjom nastavimo unaprjeđivati blockchain tehnologiju kako bismo u budućnosti mogli iskoristiti njen puni potencijal te unijeti kvalitetne promjene u razne postojeće industrije.

Ključne riječi: blockchain, kriptografija, tehnologija, distribuirano knjigovodstvo, distribuirani konsenzus

Blockchain as a new way of storing data

Summary

Blockchain technology is one of the newer solutions for data storage. This technology is based on a distributed ledger, cryptography, and distributed consensus. Using smart contracts or programs deployed on the blockchain, it serves as a new system for storing and sharing data. It competes with traditional data storage methods such as cloud storage because it offers decentralization, data immutability, and transparency. However, blockchain also has its drawbacks, such as limited scalability, high transaction costs, lack of regulation and standardization, and the complexity of the technology itself. Some potential applications of blockchain technology for data storage can be found in supply chains, the healthcare industry, and the financial sector. Although blockchain technology is still in its early stages of development, it already provides us with numerous solutions to certain problems encountered in traditional data storage. It is up to us to continue improving blockchain technology through collaborative efforts and cooperation so that we can fully harness its potential and bring about meaningful changes in various existing industries.

Keywords: blockchain, cryptography, technology, distributed ledger, distributed consensus