Blockchain tehnologija

Kralj, Tomislav

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, Faculty of Maritime Studies / Sveučilište u Splitu, Pomorski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:164:726816

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-12-12**

Repository / Repozitorij:

Repository - Faculty of Maritime Studies - Split - Repository - Faculty of Maritime Studies Split for permanent storage and preservation of digital resources of the institution

SVEUČILIŠTE U SPLITU

POMORSKI FAKULTET

TOMISLAV KRALJ

BLOCKCHAIN TEHNOLOGIJA U POMORSTVU

DIPLOMSKI RAD

SPLIT, 2024.

SVEUČILIŠTE U SPLITU

POMORSKI FAKULTET

STUDIJ: POMORSKE ELEKTROTEHNIČKE I INFORMATIČKE TEHNOLOGIJE

BLOCKCHAIN TEHNOLOGIJA U POMORSTVU

DIPLOMSKI RAD

MENTOR:

Prof. dr. sc. Igor Vujović

STUDENT:

Tomislav Kralj (MB: 0023102963)

SPLIT, 2024.

SAŽETAK

Blockchain tehnologija je revolucionirala financijsku industriju svojom sposobnošću da djeluje kao centralni entitet u financijskim transakcijama, ali na posve nov način koji jamči decentraliziranost, sigurnost, privatnost i neograničen pristup informacijama svim akterima transakcije. No nije bilo potrebno dugo da i druge industrije uvide mnoge potencijalne prednosti korištenja takve tehnologije. Pomorska industrija, a posebice grana pomorske trgovine i logistike se također počinje služiti blockchain tehnologijom kako bi unaprijedila radne procese. U ovom radu je dat opsežan osvrt na temeljne principe rada i relevantne koncepte blockchain tehnologije kao takve s posebnim naglaskom na primjenu ove tehnologije u pomorskoj industriji. Prikazano je nekoliko primjera implementacije blockchain tehnologije u pomorskoj industriji na kojima je moguće adekvatnije demonstrirati sve pogodnosti, ali i izazove, korištenja ove tehnologije.

Ključne riječi*:* *blockchain, decentralizacija, pametni ugovori, pomorska trgovina, teretnica*

ABSTRACT

Blockchain technology has revolutionized the financial industry with its ability to act as a central entity in financial transactions, but in a completely new way that guarantees decentralization, security, privacy, and unlimited access to information for all transaction actors. However, other industries did not take long to see the many potential benefits of using such technology. The maritime industry, especially the maritime trade and logistics branch, is also starting to use blockchain technology to improve work processes. This thesis gives an extensive overview of the basic working principles and relevant concepts of blockchain technology, with a special emphasis on the application of this technology in the maritime industry. Several examples of the implementation of blockchain technology in the maritime industry are presented, where it is possible to demonstrate all the benefits more adequately but also the challenges of using this technology.

Keywords: *blockchain, decentralization, smart contracts, maritime trade, bill of lading*

SADRŽAJ

1. UVOD

1.1. PREDMET I PROBLEMATIKA ISTRAŽIVANJA

Predmet istraživanja ovog diplomskog rada je blockchain tehnologija s posebnim naglaskom na utjecaj iste na pomorsku industriju. Osim detaljnog prikaza temeljnih svojstava i načela blockchain tehnologije kao takve, izvršiti će se i temeljiti osvrt na trenutni utjecaj blockchain tehnologije na pomorsku industriju. Spomenuti osvrt će se demonstrirati kroz pomnu analizu više postojećih slučajeva primjene blockchain tehnologije u pomorstvu.

Osim same implementacije blockchain tehnologije, problematika istraživanja se tiče i razvijanja pravne legislative koja bi uopće omogućila ostvarenje takvog projekta. Budući da je pomorska industrija unatoč suvremenim tehnološkim postignućima i dalje veoma tradicionalna i „troma“ u prihvaćanju novih ideja i filozofija, sama implementacija tek jednostavnijih oblika primjene blockchain tehnologije bi se mogla pokazati zahtjevnijom nego očekivano.

1.2. CILJ I SVRHA ISTRAŽIVANJA

Cilj istraživanja ovog rada je detaljno prikazati funkcionalni koncept blockchain tehnologije te jasno prezentirati brojne inovativne prednosti koje donosi pravilna implementacija blockchain tehnologije sa posebnim naglaskom na slučaj pomorske industrije.

1.3. HIPOTEZA RADA

Temeljna hipoteza ovog rada na kojoj autor zasniva daljnje istraživanje je sljedeća:

Pravilna implementacija blockchain tehnologije može značajno unaprijediti kvalitetu i učinkovitost radnih procesa kao i unaprijediti privatnost i sigurnost podataka u pomorskoj industriji.

1.4. ZNANSTVENE METODE

Znanstvene metode korištene prilikom izrađivanja ovog rada su: metoda analize i sinteze, metoda istraživanja, metoda formuliranja, metoda apstrakcije i deskripcije, metoda koja ukazuje na prednosti i nedostatke i metoda konkretizacije.

1.5. KOMPOZICIJSKA STRUKTURA RADA

Diplomski rad je podijeljen u četiri poglavlja. Prvi dio je uvod u kojemu su pojašnjeni predmet i problematika istraživanja, određen je cilj istraživanja, postavljena je hipoteza i navedene su znanstvene metode korištene prilikom izrađivanja rada. Drugo poglavlje rada je opsežan i temeljit osvrt na osnovne principe blockchain tehnologije kao takve. U ovom poglavlju se osim osnovnih principa rada i dizajna blockchaina, pojašnjavaju i koncepti poput rudarenja i pametnih ugovora, a naglasak je na primjenama blockchain tehnologije kao i na njenim nedostacima. Treći dio diplomskog rada se bavi primjenom blockchain tehnologije u pomorskoj industriji. Osim što su nabrojana područja primjene gdje je moguće koristiti blockchain tehnologiju u pomorstvu, data su i tri primjera iz stvarnog života koja jasno prikazuju mogućnosti i mnoge prednosti korištenja blockchain tehnologije u pomorskoj industriji. Četvrto poglavlje rada je zaključak u kojemu je iznesena sažeta poanta ovog istraživanja kao i zaključak o postavljenoj hipotezi.

2. BLOCKCHAIN TEHNOLOGIJA

Digitalna transformacija suvremenog doba i sve popratne „nuspojave“ digitalizacije su zadrle duboko u sve pore civilnog društva, ali i u svijest brojnih industrija koje su praktički primorane prilagoditi se takvom načinu poslovanja žele li ostati kompetitivne na današnjem tržištu. U slučaju industrije, ova pojava se često spominje u kontekstu nove industrijske revolucije pod službenim nazivom Industrija 4.0. Blockchain tehnologija je svakako jedan značajan dio ove nove struje tehnoloških postignuća suvremenog vremena, no još uvijek je dosta nepoznat i gotovo apstraktni koncept, pogotovo kod šire populacije koja nije nužno veoma tehnološki potkovana.

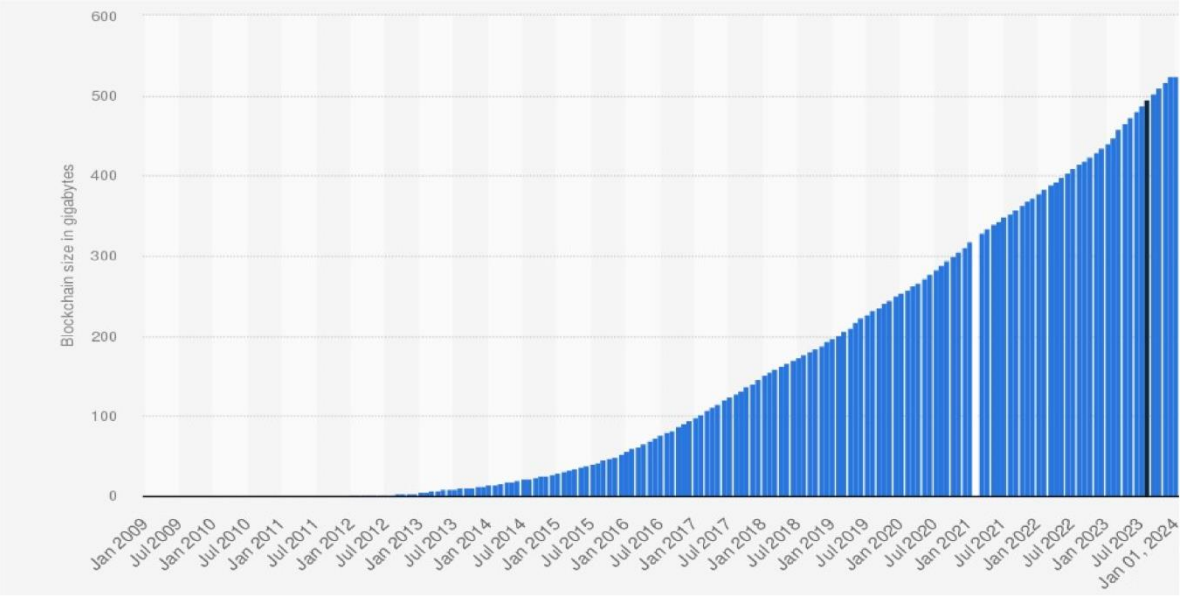
Najjednostavniji opis blockchaina je da je to jedna distribuirana baza podataka u obliku ulančanih blokova podataka (na što ukazuje i doslovni prijevod engleskog termina blockchain) koja korištenjem složene kriptografije sprječava promjenu ili brisanje prije unesenih podataka. Sigurnost podataka je dodatno zagarantirana zbog decentraliziranosti sustava koji se sastoji od distribuirane prostrane mreže velikog broja neovisnih korisnika. Zbog očitih velikih prednosti blockchain tehnologije u području privatnosti i sigurnosti podataka, prva industrija koja je počela sa masovnim prihvaćanjem ove tehnologije je financijska industrija. Tako je postalo moguće izvršavati transakcije bez nadležnosti centralnog entiteta (najčešće banke), već transakcije provjerava decentralizirani sustav računala mreže neovisnih korisnika na različitim lokacijama pomoću specifičnih algoritama. [6]

2.1. POVIJEST BLOCKCHAINA

Povijesna pozadina blockchaina ne seže daleko u povijest. Dovoljno se vratiti tek u 1991. godinu kada su američki kriptograf Stuart Haber i fizičar Wakefield Scott Stornetta pokušali implementirati sustav u kojem će biti nemoguće mijenjati vremenske oznake dokumenata. Nakon samo godinu dana su uz pomoć matematičara Davida Allena Bayera uspješno implementirali vrstu podatkovne konstrukcije pod nazivom Merkle stablo u svoj radni okvir. Merkleova stabla su po strukturi otporna na neovlaštene promjene jer će promjena u bilo kojem listu stabla na putu do korijena promijeniti korijen stabla u potpunosti. Ova preinaka njihovog dizajna je drastično poboljšala učinkovitost što je omogućilo sustavu prikupljanje više različitih certifikata dokumenata koji se potom pohranjuju u jedan blok. [1]

Međutim nakon ovog otkrića nije uslijedila nikakva značajna primjena ove revolucionarne tehnologije, što će se promijeniti tek 2008. godine kada misteriozna osoba ili skupina ljudi pod pseudonimom Satoshi Nakamoto uspijeva konceptualizirati prvi decentralizirani blockchain sustav. Satoshi na svojoj stranici bitcoin.org objavljuje članak pod nazivom „Bitcoin: A Peer-to-Peer Electronic Cash System“ u kojem opisuje decentraliziranu peer-to-peer tehnologiju koja omogućuje novi oblik novca na koji ne utječe nikakva središnja uprava ili posrednik, danas poznat kao kriptovaluta. [10]

Naravno srž tehnologije koja omogućava takvu valutu je upravo blockchain kojeg je Satoshi poboljšao koristeći metodu kriptografskog algoritma za dokaz rada koji se temelji na hash-u i koji zahtijeva određenu količinu rada za izračunavanje, ali se dokaz može učinkovito provjeriti. Takva metoda omogućuje vremensko označavanje blokova bez potrebe da ih potpiše treća strana i uvođenje parametra težine za stabilizaciju brzine dodavanja blokova u lanac. Već sljedeće godine Satoshi objavljuje prvu implementaciju Bitcoina koji će u narednim godinama iz korijena promijeniti svijet financija. U pozadini sve funkcionira upravo na blockchain tehnologiji koja djeluje kao distribuirana glavna knjiga transakcija. Zbog svoje specifične strukture podataka, blockchain prati sasvim pouzdani trag svake transakcije na mreži i u svakom trenutku nudi slobodan uvid svim korisnicima u kompletno računovodstvo. [6] Vrijednosti svih bitcoina 2022. godine je procijenjena na 1.03 trilijuna američkih dolara, a veličina bitcoin blockchain datoteke je danas veća od 500 GB, vidljivo na slici 1.



Slika 1. Graf rasta Bitcoin Blockchain datoteke u gigabajtima

Izvor: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ , pristupljeno : 9.1.2024.

2.2. OSNOVNA TEORIJSKA PODLOGA BLOCKCHAIN TEHNOLOGIJE

Kako je već spomenuto u prethodnim poglavljima Blockchain je zapravo vrsta distribuirane dijeljene knjige (eng. distributed ledger technology, DLT) u koju se pohranjuju podaci. Sama „knjiga“, tj. zapis postoji u obliku ulančanih blokova podataka gdje vrijednosti svakog novog bloka ovise o vrijednosti prethodnog bloka u lancu. Blokovi su povezani sa nekoliko vrsta informacija koji zapravo čine jednu kriptografsku metodu koja sprječava bilo kakvu manipulaciju podacima koji su jednom pohranjeni u blok. Svaki blok tako sadržava kriptografski hash (algoritam koji omogućuje preslikavanje proizvoljnog binarnog niza u binarni niz s fiksnom veličinom od n bitova što ima posebna svojstva poželjna za kriptografsku primjenu) prethodnog bloka, vremensku oznaku transakcije (eng. timestamp) i podatke o samoj transakciji najčešće u obliku Merkleovog stabla, gdje su podatkovni čvorovi predstavljeni listovima stabla. [6]

Posljedica ovakve strukture je to da se blockchain transakcije, nakon što su pohranjene, u bilo kojem bloku ne mogu retroaktivno mijenjati bez izmjene svih sljedećih blokova. To čini blockchain veoma sigurnim, pouzdanim i transparentnim načinom pohrane podataka. Upravljački element ovog sustava je decentralizirana peer-to-peer računalna mreža u kojoj se svi čvorovi (korisnici) kolektivno pridržavaju protokola algoritma za komunikaciju i verifikaciju ispravnosti novih blokova. [10]

2.2.1. Blockchain kao temeljna pozadinska tehnologija kriptovaluta

Danas je gotovo nemoguće raspravljati o blockchainu bez da se pojasne pojedinosti o prvoj pravoj primjeni blockchaina, a to je naravno kriptovaluta bitcoin. Štoviše, upravo elaborirajući temeljne funkcionalne principe bitcoina se čitateljima može jasnije dati „opipljivi“ ili konkretan uvid u funkcioniranje same blockchain tehnologije. Blockchain je temeljna tehnologija svih kriptovaluta današnjice zbog svoje mogućnosti da djeluje kao distribuirana baza podataka bez potrebe za posebnim entitetom koji bi nadzirao transakcije. U tradicionalnim financijskim transakcijama banka je ta koja ima ulogu spomenutog entiteta, odnosno ulogu nadzornika koji bilježi sve transakcije. Potreba za nadzornim entitetom je nastala zbog historijske potrebe za poštenom regulacijom financijskih transakcija, odnosno entiteta koji će osigurati da jedan korisnik neće svjesno prevariti drugoga. Revolucionarnost blockchaina je upravo u tome što nudi alternativu ovakvom sustavu poslovanja, jer nudi potpuno decentraliziran sustav mreže nepoznatih računala čiji korisnici konstantno verificiraju transakcije u mreži na temelju složenog kriptografskog

algoritma. [2] Još veći kredibilitet ovom sustavu daje činjenica je korisnicima u interesu verificirati transakcije, jer su radeći to nagrađeni bitcoinom ili drugom kriptovalutom koju tim procesom „rudare“. Na primjeru bitcoina to funkcionira tako da postoje korisnici i „rudari“. Korisnici generiraju transakcije na kojima „rudari“ mogu zaraditi, a „rudari“ im zauzvrat bilježe transakcije, odnosno održavaju sustav. Ovakav sustav se naziva „Proof-of-Work“ sustav, jer je za verificiranje transakcija potrebno izračunavati zahtjevne matematičke izračune, no postoje i drugi sustavi koji će biti objašnjeni kasnije u radu. [10]

2.2.2. Transakcije kriptovaluta na blockchainu

Konkretan primjer transakcije kriptovaluta između dva korisnika se odvija u nekoliko koraka:

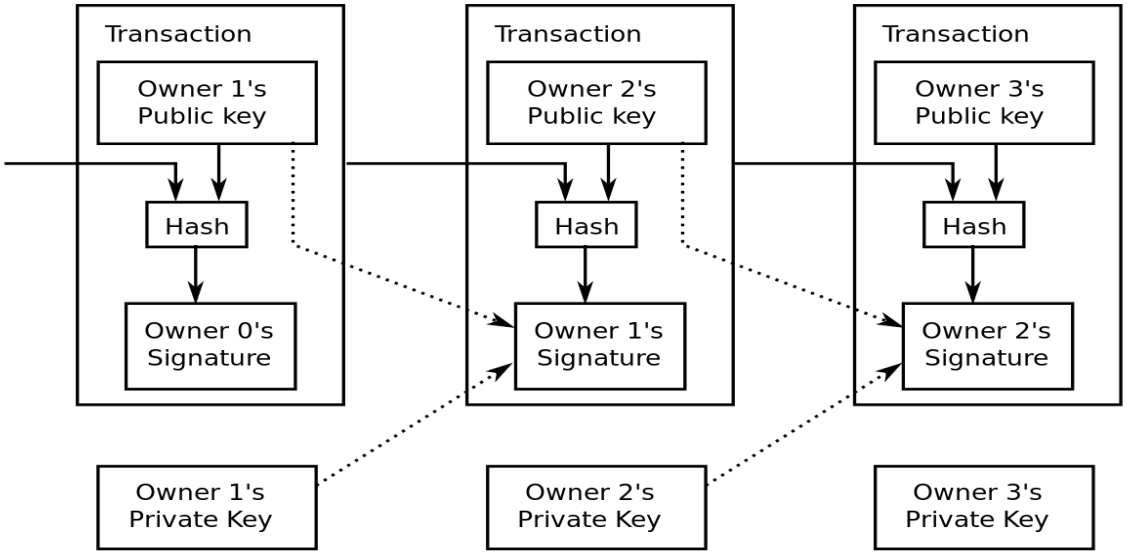
1. korisnik X želi korisniku Y poslati određeni iznos kriptokovanica,
2. korisnik X pomoću softverskog novčanika za kriptovalute objavljuje svoj naum ostatku mreže slanjem posebne kombinacije podataka u specificiranom formatu,
3. „rudari“ pokušavaju verificirati transakciju kako se ona širi mrežom.

Korisnikov novčanik sadrži dva enkripcijska ključa: privatni i javni. Javni ključ ujedno predstavlja i adresu novčanika te ga mogu vidjeti svi na mreži, a privatni ključ vidi samo korisnik kojem dopušta da u svakom trenutku pristupi sredstvima koje kontrolira novčanik. Transakcija koju je korisnik X generirao se automatski kriptira pomoću privatnog ključa, a svi ostali korisnici mreže mogu provjeriti sadržaj transakcije koristeći korisnikov javni ključ. Drugi članovi mreže zapravo koriste javni ključ da bi dekriptirali sadržaj transakcije. Ukoliko neki član mreže pokuša koristiti bilo koji drugi ključ, kriptirani podaci postaju besmisleni što osigurava da samo korisnik X može pristupiti i upravljati svojim kriptovalutama. [10]

Svaka transakcija između dva novčanika je definirana sa ulaznim odnosno izlaznim transakcijama. Prilikom slanja određenog broja kriptokovanica izlazna transakcija se sastoji od nekoliko dijelova. Osnovni dio izlazne transakcije je sam iznos koji korisnik želi poslati sa svog novčanika na novčanik primatelja. Drugi dio izlazne transakcije je naknada za „rudare“ na mreži (eng. miner fee) koja motivira „rudare“ da obrade transakciju. Ovisno o veličini naknade, transakcija će se izvršiti prije ili kasnije. Treći dio izlazne transakcije je iznos koji ostaje u novčaniku korisnika, taj se iznos često naziva UTXO ili Unspent Transaction Output. Kada korisnik pristupa svom novčaniku, preko mreže se automatski provjerava cjelokupna UTXO baza sa svim transakcijama povezanim sa korisnikovim

javnim ključem. Suma svih unosa u bazi predstavlja iznos kriptokovanica kojima korisnik može raspolagati u tom trenutku. [10]

Svi prethodno spomenuti podaci i sve informacije nužne da bi ovakav sustav besprijekorno glatko funkcionirao su pohranjene na blockchainu, što na ovom konkretnom primjeru iz stvarnog života demonstrira kvalitetan uvid u prednosti ove moćne tehnologije. Ako se uz to uzme u obzir i decentraliziranost blockchaina koja nemjerljivo doprinosi privatnosti, sigurnosti i neovisnosti o institucijama jasno je zašto je blockchain tehnologija toliko revolucionarna. Iako isprva djeluje složeno i zamršeno, temeljni funkcionalni koncept ove tehnologije je zapravo veoma logičan i jednostavan. Na slici 2 je prikazan dijagram transakcije kriptovalute gdje je vidljivo koji podaci su potrebni kako bi se izvršila svaka transakcija. [3]



Slika 2. Dijagram transakcije kriptovalute

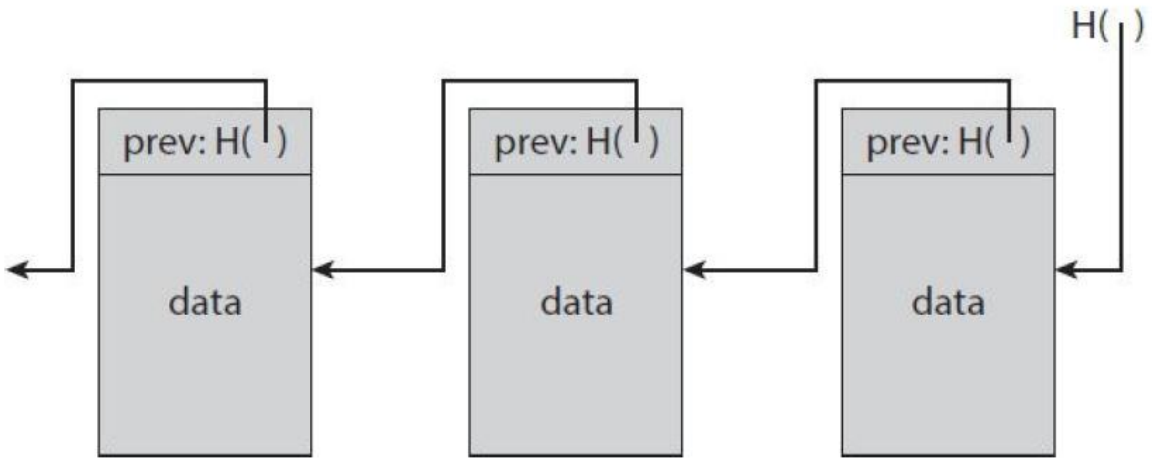
Izvor: https://github.com/graingert/bitcoin-IRP/blob/master/img/Bitcoin_Transaction_Visual.svg , pristupljeno 9.1.2024.

2.3. GRAĐA BLOCKCHAIN TEHNOLOGIJE

Osnovna struktura blockchaina je sastavljena od formiranog lanca blokova u koje se pohranjuju podaci u obliku verificiranih transakcija. Podaci u blokovima su pohranjeni zajedno sa kriptografskim funkcijama koje osiguravaju da je iste podatke nemoguće mijenjati jednom kada su uneseni te da im svaki član mreže može pristupiti u svakom trenutku. Sama blockchain mreža je također decentralizirana i standardizirana što dodatno osigurava sigurnost i lakoću korištenja.

2.3.1. Hash pokazivači

Svaka transakcija na blockchainu je verificirana pomoću kriptografske hash funkcije te sadrži hash pokazivač. Hash pokazivač (eng. hash pointer) je struktura podataka koja pokazuje na mjesto u mreži na kojem su pohranjene informacije zajedno s kriptografskim hashom tih informacija. Dok obični pokazivači pružaju način dohvaćanja informacija, hash pokazivač ujedno omogućuje potvrdu da podaci nisu promijenjeni. Dakle u blockchainu svaki blok osim što govori gdje je bila vrijednost prethodnog bloka, sadrži i sažetak te vrijednosti što omogućuje verifikaciju da vrijednost nije promijenjena. Ovo svojstvo čini blockchain idealnom tehnologijom za bazu podataka koja pohranjuje podatke i omogućuje dodavanje podataka u najnoviju verziju zapisa. Međutim ako bi netko teoretski promijenio podatke koji se pojavljuju ranije u zapisu, to bi se odmah detektiralo. Na slici 3 su prikazani hash pokazivači u blokovima blockchaina. [1]



Slika 3. Prikaz blockchaina sa hash pokazivačima

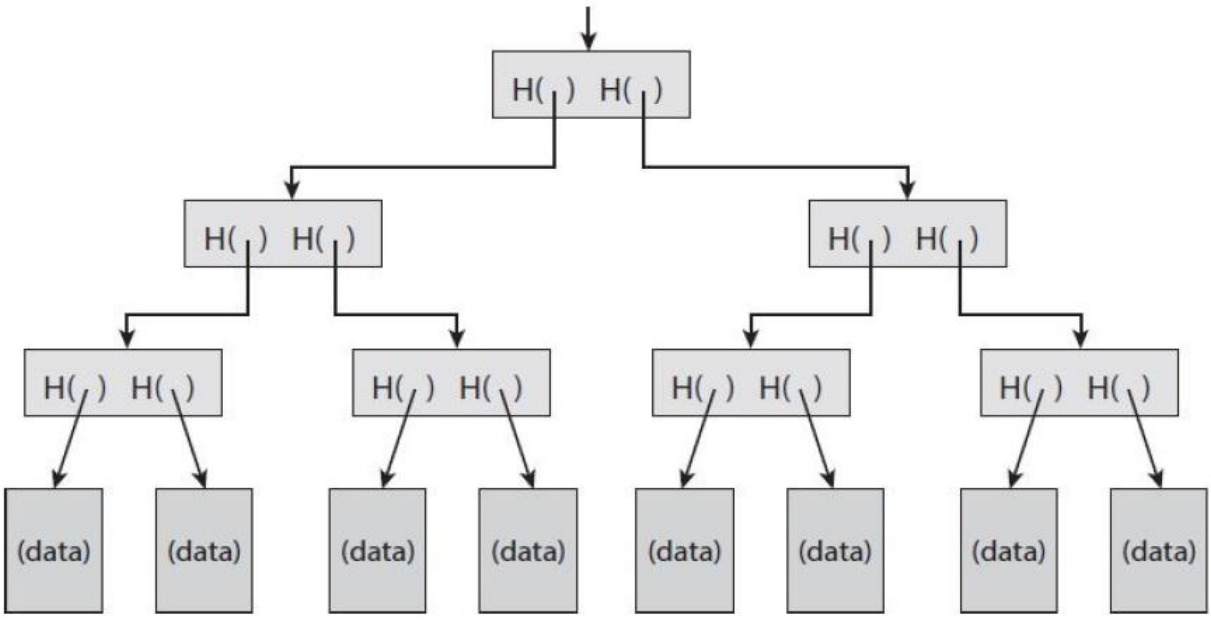
Izvor: Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S.: *Bitcoin and cryptocurrency technologies, A Comprehensive Introduction,* Princeton University, 2016., str. 46.

2.3.2. Merkleovo stablo

Još jedna podatkovna struktura koju je moguće stvoriti koristeći hash pokazivače je Merkleovo stablo. To je binarno stablo sa hash pokazivačima koje je dobilo ime po svom izumitelju, američkom matematičaru Ralphu Merkleu. Stablo se sastoji od „listova“ koje zapravo čine podatkovni blokovi koji su grupirani u grupe od dva bloka. Na slici 4 je prikazano kako izgleda jedno Merkleovo stablo. Za svaki par blokova se stvara nova struktura podataka koja ima dva hash pokazivača, po jedan za svaki od blokova. Ove

strukture podataka čine sljedeću razinu stabla te su ponovo grupirane u grupe od po dvije i za svaki par se kreira nova podatkovna struktura koja sadrži hash svake od njih. To se nastavlja dok se ne dobije jedan blok, korijen stabla čiji je hash pokazivač zapravo jedino bitno zapamtiti. Ovakav dizajn postiže isti učinak kao i u prethodnom slučaju samo sa hash pokazivačima, a to je da ako bi se podaci promijenili u bilo kojem bloku na nekoj nižoj razini, ta bi promjena odmah bila primijećena jer bi se i hash pokazivač korijena također morao promijeniti. Dakle svaki pokušaj mijenjanja podataka u bilo kojem bloku može biti spriječen samo pamćenjem hash pokazivača korijena. [1]

Još jedna prednost Merkleovog stabala je da omogućuju brži način dokaza članstva u mreži (eng. proof of membership). Pretpostavi li se da netko želi dokazati da je određeni blok podataka član Merkleovog stabla, bilo bi potrebno da pomoću hash pokazivača pokaže na taj blok i sve blokove koji vode do korijena. Sve ostale blokove u stablu bi se moglo zanemariti jer nisu relevantni za dokazivanje. Ako u stablu postoji n čvorova, potrebno je prikazati samo približno log(n) stavki. A budući da svaki korak zahtijeva samo izračunavanje hasha podređenog bloka, potrebno je oko log(n) vremena za potvrdu. Čak i ako Merkleovo stablo sadrži velik broj blokova, članstvo je moguće dokazati u relativno kratkom vremenu. [1]



Slika 4. Prikaz Merkle stabla

Izvor: Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S.: Bitcoin and cryptocurrency technologies, A Comprehensive Introduction, Princeton University, 2016., str. 48.

2.3.3. Blokovi

Blok je osnovna jedinica blockchaina u koju se pohranjuju svi podaci odnosno transakcije uz sve kriptografske strukture podataka koje su opisane u poglavljima ranije koje služe kako bi se osigurao integritet bloka i podataka sadržanih u njemu. Prilikom stvaranja novih blokova, ponekad se mogu proizvesti i odvojeni blokovi istovremeno, stvarajući račvanje (eng. fork). Osim kriptografskih podataka za zaštitu integriteta podataka, postoji algoritam koji boduje različite verzije povijesti podataka, tako da se one sa većim rezultatom mogu odabrati u odnosu na one as manjim brojem bodova. Blokovi koji ne budu odabrani za uključivanje u lanac blockchaina postaju blokovi siročad (eng. orphans). Ponekad se može dogoditi da korisnici koji održavaju bazu podataka vide različite verzije povijesti podataka tj. transakcija. U tom slučaju korisnici računaju samo na onu verziju koja ima najveći broj bodova iz prije spomenutog algoritma. U trenutku kad korisnik primi verziju sa više bodova, prepravlja se vlastita baza podataka i prenosi se ista dalje drugim korisnicima. Međutim vjerojatnost zamjene upisa drastično pada na zanemarivu razinu jer blockchain potiče proširenje mreže novim blokovima umjesto prepisivanja starih blokova. [1]

Prosječno vrijeme koje je mreži potrebno da generira jedan blok u blockchainu je vrijeme bloka (eng. block time). U slučaju kriptovaluta, vrijeme bloka je istovjetno sa brzinom kojom se odvija transakcija, tako da kraće vrijeme bloka znači brže transakcije. Prosječno vrijeme bloka za bitcoin je oko 10 minuta, a za ethereum između 14 i 15 sekundi. [4]

2.3.4. Decentralizacija blockchaina

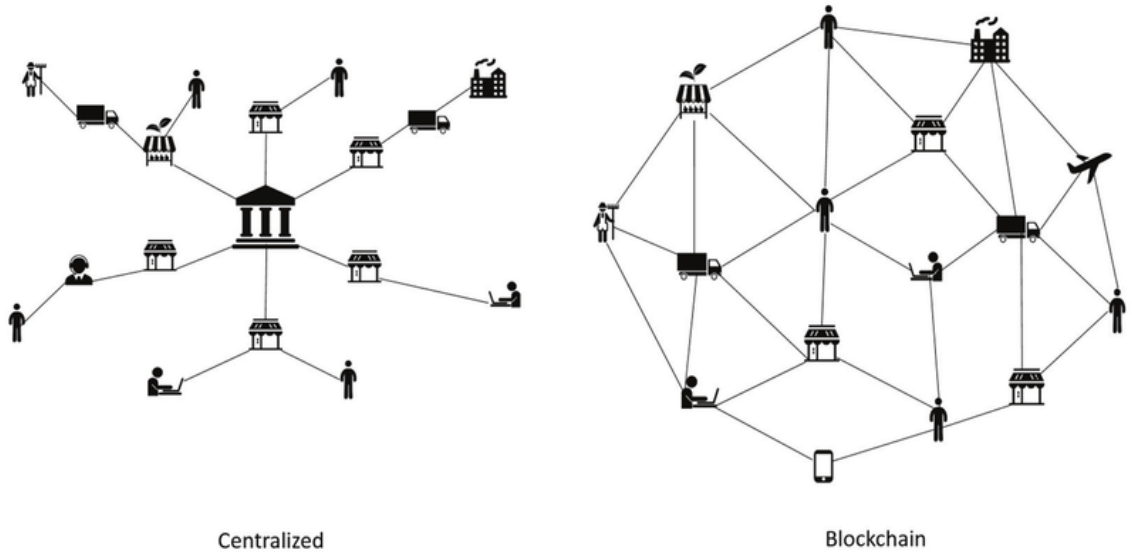
Decentralizacija je raspodjela funkcija, kontrole i informacija umjesto njihove centralizacije u jednom entitetu. Pojam se koristi u brojnim sektorima i industrijama, od informacijske tehnologije do maloprodaje i državne uprave. Također označava sustav koji ima više putova za protok informacija. Centralizirana struktura podrazumijeva kontrolu središnjeg entiteta od strane ljudi koji imaju moć upravljanja, kontrole i nadzora. Jedan primjer bi bila nacionalna valuta kojom upravlja središnja banka. Decentralizacija je suprotno od toga, gdje niti jedna osoba ili entitet ne posjeduje, ne upravlja niti kontrolira mrežu ili strukturu. [11]

U kontekstu blockchain tehnologije decentralizacija je veoma relevantna na primjeni blockchaina za kriptovalute. Nisu sve kriptovalute decentralizirane, iako one najpopularnije poput Bitcoin valute jesu. Za razliku od centraliziranih valuta,

decentralizirane kriptovalute ne reguliraju središnje banke, već njihovim programskim kodom i monetarnom politikom upravlja blockchain mreža svih korisnika. Različiti su načini na koje različite kriptovalute postižu decentraliziranost. Bitcoinov peer-to-peer javni blokchain to postiže koristeći kriptografski protokol koji se zove proof of work. Kako je već utvrđeno u prethodnom poglavljima, blockchain se sastoji od blokova podataka koji sadrže informacije o transakcijama koje se koriste za dokazivanje validnosti sljedećeg bloka. Korisnici bitcoina mogu dodavati blokove u blockchain tako da potvrđuju njihovu validnost putem proof of work protokola. Budući da je blockchain javan, svatko može pristupiti informacijama i dodati blok putem proof of work protokola. [11]

Glavni razlog zašto su blockchaini decentralizirani je izbjegavanje stavljanja kontrole u ruke nekolicine ili središnje banke neke zemlje. To je glavni motiv koji stoji iza prihvaćanja kriptovaluta uopće: isključiti banke iz jednadžbe i ostvariti prave peer-to-peer transakcije.

Nisu sve digitalne valute decentralizirane. Postoje i kriptovalute koje koriste privatne, centralizirane sustave, gdje samo nekoliko odabranih ljudi ima moć dodavanja novih blokova i provjere valjanosti transakcija. Oni se obično koriste u industrijama usmjerenim na privatnost kao što su zdravstvo i financije. Na slici 5 je prikazana grafika koja simbolično prikazuje decentraliziranost blockchaina.



Slika 5. Decentralizacija blockchaina

Izvor: Shash, D., Shay, E.: *How and Why Artificial Intelligence, Mixed Reality and Blockchain Technologies Will Change Marketing We Know Today, Handbook of Advances in Marketing in an Era of Disruptions: Essays in Honour of Jagdish N. Sheth*, New York, 2019., str. 97

Brojne su prednosti decentralizacije blockchaina, uključujući:

- Povjerenje - Povjerenje je zasigurno jedna od najbitnijih predispozicija za uspješno poslovanje. U decentraliziranoj blockchain mreži nitko ne mora poznavati ili vjerovati drugoj strani jer je zagarantirano da su podaci o transakciji zapisani u blokchainu otporni na bilo kakav način manipulacije,
- Povećana točnost podataka - Poduzeća često čuvaju svoje podatke i često ih je potrebno uskladiti na ovaj ili onaj način. Svaki put kad se podacima manipulira, postoji mogućnost neispravnog unosa ili gubitka podataka. U decentraliziranom blockchainu podaci nisu izolirani i kopiraju se iz jedne knjige u drugu, čime se osigurava njihov integritet,
- Smanjena mogućnost kvarova - Decentralizacija može pomoći u ublažavanju kvarova jer ne postoji samo jedna točka kvara. Sve je distribuirano, tako da ako je jedan izvor nedostupan ili postoji usko grlo u sustavu, drugi korisnici mreže mogu preuzeti problem,
- Transparentnost - Decentralizirani blockchaini dostupni su javnosti, stoga su transparentni i svi ih mogu vidjeti,
- Potpuna kontrola - Članovi ili korisnici lanca blokova (a ne bilo kakav središnji entitet) kontroliraju svoje podatke i bilo tko ih može vidjeti ili im pristupiti,
- Nepromjenljivost - Ovo je uobičajeni izraz koji se koristi za opisivanje činjenice da je podatke sadržane u decentraliziranom blockchainu teško mijenjati jer svaku promjenu mora potvrditi svaki čvor u blockchain mreži,
- Sigurnost - Decentralizirani blockchaini su daleko sigurniji od centraliziranih sustava jer koriste sofisticiranu enkripciju za zaštitu podataka. [11]

2.3.5. Pristupačnost i standardizacija

Osim decentralizacije, značajne karakteristike blockchaina koje ga čine veoma učinkovitim i jednostavnim za korištenje su svakako pristupačnost te standardizacija. Budući da su blockchaini najčešće javni kao što je slučaj s bitcoinom, bilo tko na mreži može vidjeti promjene u podacima o transakcijama, čak i ako nema dopuštenje za sudjelovanje u dodavanju novih blokova. Osim toga, blockchain podaci se ne mogu kopirati kao standardne računalne datoteke u koje je zbog toga nemoguće pohraniti ikakvu

vrijednost. Na taj način blockchain pruža efektivan i pristupačan način za pohranu vrijednosti (poput kriptovaluta) široj javnosti. [12]

Kako bi blockchain tehnologija postala široko prihvaćena te kako bi mogla biti korištena interoperabilno s drugim tehnologijama, javila se industrijska potreba za standardizacijom. Tako je Svjetska Organizacija za Standardizaciju (eng. International Organisation for Standardization – ISO) stvorila tehnički odbor 307 (eng. Standards by ISO/TC 307) za blockchain i tehnologije distribuirane knjige. Ovaj tehnički odbor se bavi problematikom terminologije, arhitekture, sigurnosti, privatnosti, identiteta i drugim relevantnim aspektima blockchain tehnologije i tehnologije distribuiranih knjiga. Osim ISO organizacije, standardizacijom blockchain tehnologije se bave i Društvo za svjetsku međubankarsku financijsku telekomunikaciju (eng. Society for Worldwide Interbank Financial Telecommunication - SWIFT), Europska komisija i Ekonomska komisija Ujedinjenih naroda za Europu (UNCE). Mnoga druga nacionalna i javna tijela za standardizaciju također rade na blockchain standardima. To uključuje Nacionalni institut za standarde i tehnologiju (NIST), Europski odbor za elektrotehničku standardizaciju (CENELEC) i Institut inženjera elektrotehnike i elektronike (IEEE). [12]

2.4. VRSTE BLOCKCHAINA

Postoje četiri glavne vrste blockchain mreža: javni blockchaini, privatni blockchaini, hibridni blockchaini i konzorcijski blockchaini. Svaki od ovih tipova ima svoje prednosti, nedostatke i područja primjene.

2.4.1. Javni blockchaini

Kod javnih blockchaina svatko s pristupom internetu se može prijaviti na blockchain platformu kako bi postao validator (tj. sudjelovao u izvršavanju konsenzusnog protokola). Isti korisnik može pristupiti trenutnim i prošlim zapisima i provoditi aktivnosti rudarenja (složeni proračuni koji se koriste za provjeru transakcija i njihovo dodavanje u blockchain). Niti jedan važeći zapis ili transakcija ne može se mijenjati na mreži i svatko može provjeriti transakcije, pronaći greške ili predložiti izmjene jer je izvorni kod obično otvorenog koda.

Jedna od prednosti javnih blockchaina je ta da su potpuno neovisni o organizacijama, pa ako organizacija koja ga je pokrenula prestane postojati, javni blockchain će i dalje moći raditi, sve dok postoje računala povezana s njim. Još jedna

prednost javnih blockchaina je transparentnost mreže. Sve dok korisnici pomno slijede sigurnosne protokole i metode, javni lanci blokova uglavnom su sigurni.

Neki od nedostataka javnog blockchaina uključuju činjenicu da mreža može biti spora, a tvrtke ne mogu ograničiti pristup ili korištenje. Nadalje, ako hakeri osiguraju 51% ili više računalne snage javne blockchain mreže, mogu je jednostrano promijeniti. Javni blockchaini također imaju problem sa skaliranjem, pa se mreža usporava kako se više čvorova pridružuje mreži.

Najčešći slučaj upotrebe javnih lanaca blokova je rudarenje i razmjena kriptovaluta poput Bitcoina. [13]

2.4.2. Privatni blockchaini

Blockchain mreža koja radi u restriktivnom okruženju poput zatvorene mreže ili koja je pod kontrolom jednog entiteta je privatni blockchain. Iako funkcionira kao javna blockchain mreža u smislu da koristi peer-to-peer veze i decentralizaciju, ova vrsta blockchaina je puno manjeg opsega. Umjesto da se svatko može pridružiti i pružiti računalnu snagu, privatnim blockchainima obično se upravlja na maloj mreži unutar tvrtke ili organizacije. Također su poznati kao ovlašteni blockchaini ili enterprise blockchaini.

Kontrolna organizacija postavlja razine dopuštenja, sigurnost, autorizacije i pristupačnost. Na primjer, organizacija koja postavlja privatnu blockchain mrežu može odrediti koji čvorovi mogu pregledavati, dodavati ili mijenjati podatke. Također može spriječiti treće strane u pristupu određenim informacijama. Budući da su ograničene veličine, privatni blockchaini mogu biti vrlo brzi i mogu puno brže obrađivati transakcije od javnih lanaca blokova.

Nedostaci privatnih blockchaina uključuju kontroverznu tvrdnju da oni nisu pravi blockchaini, budući da je temeljna filozofija blockchaina decentralizacija. Također je teže potpuno postići povjerenje u informacije, jer centralizirani čvorovi određuju što je validno. Mali broj čvorova također može značiti manju sigurnost. Ako nekoliko čvorova pokvari, metoda konsenzusa može biti ugrožena.

Brzina privatnih blockchaina čini ih idealnima za slučajeve u kojima blockchain treba biti kriptografski siguran, ali subjekt koji ga kontrolira ne želi da informacijama pristupi javnost. Ostali slučajevi upotrebe za privatni blockchain uključuju upravljanje opskrbnim lancem, vlasništvo nad imovinom i interno glasovanje. [13]

2.4.3. Hibridni blockchaini

Ponekad će organizacije htjeti najbolje od oba svijeta, pa će koristiti hibridni blockchain, vrstu blockchain tehnologije koja kombinira elemente privatnog i javnog blockchaina. Organizacijama omogućuje postavljanje privatnog sustava temeljenog na dopuštenjima uz javni sustav bez dopuštenja, dopuštajući im da kontroliraju tko može pristupiti određenim podacima pohranjenim u blockchainu i koji će podaci biti javno otvoreni. Obično se transakcije i zapisi u hibridnom lancu blokova ne objavljuju, ali se mogu provjeriti kada je to potrebno, primjerice dopuštanjem pristupa putem pametnog ugovora. Povjerljive informacije čuvaju se unutar mreže, ali ih je još uvijek moguće provjeriti. Iako privatni subjekt može posjedovati hibridni blockchain, on ne može mijenjati transakcije. Kada se korisnik pridruži hibridnom blockchainu, ima puni pristup mreži. Identitet korisnika zaštićen je od drugih korisnika, osim ako ne sudjeluju u transakciji. Zatim se njihov identitet otkriva drugoj strani.

Jedna od velikih prednosti hibridnog blockchaina je ta da, budući da radi unutar zatvorenog ekosustava, vanjski hakeri ne mogu izvesti 51% napad na mrežu. Također štiti privatnost, ali dopušta komunikaciju s trećim stranama. Transakcije su jeftine i brze, a nudi bolju skalabilnost od javne blockchain mreže.

Ova vrsta blockchaina nije potpuno transparentna jer informacije mogu biti zaštićene. Nadogradnja također može biti izazov i nema poticaja za korisnike da sudjeluju ili doprinose mreži.

Hibridni blockchain ima veliki broj idealnih slučajeva upotrebe, najčešće za regulaciju administracijske i poslovne dokumentacije u velikim trgovačkim poduzećima. Također je dobar sustav za pohranu medicinske dokumentacije jer zapis ne mogu vidjeti slučajne treće strane, ali korisnici mogu pristupiti svojim podacima putem pametnog ugovora. Vlade bi ga također mogle koristiti za privatno pohranjivanje podataka o građanima, ali za sigurno dijeljenje informacija između institucija. [13]

2.4.4. Konzorcijski blockchaini

Četvrta vrsta blockchaina, konzorcijski blockchain, također poznat kao federalni blockchain, sličan je hibridnom blockchainu po tome što ima privatne i javne značajke blockchaina. Ali razlikuje se po tome što više članova organizacije surađuje na decentraliziranoj mreži. U biti, konzorcijski blockchain je privatni blockchain s ograničenim pristupom određenoj skupini, čime se eliminiraju rizici koji dolaze sa samo jednim entitetom koji kontrolira mrežu na privatnom blockchainu.

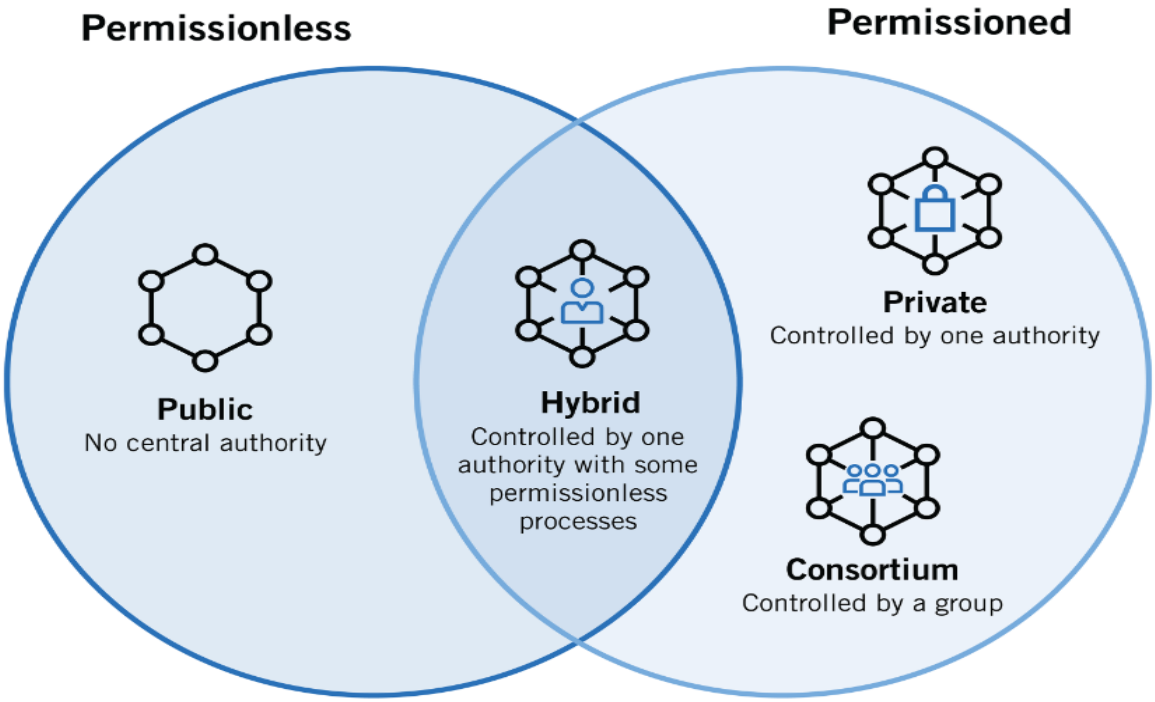
U konzorcijskom blockchainu, procedure konsenzusa kontroliraju unaprijed postavljeni čvorovi. Postoji čvor validatora koji inicira, prima i potvrđuje transakcije. Članovi čvorovi mogu primati ili inicirati transakcije.

Konzorcijski blockchain obično je sigurniji, skalabilniji i učinkovitiji od javne blockchain mreže. Poput privatnog i hibridnog blockchaina, također nudi kontrole pristupa.

Konzorcijski blockchain je također manje transparentan od javnog blockchaina. Još uvijek može biti ugrožen ako je članski čvor probijen, vlastiti propisi blockchaina mogu narušiti funkcionalnost mreže.

Bankarstvo i plaćanja dvije su namjene ove vrste blockchaina. Različite banke mogu se udružiti i formirati konzorcij, odlučujući koji će čvorovi potvrditi transakcije. Istraživačke organizacije mogu stvoriti sličan model, kao i organizacije koje žele pratiti proizvode. Idealan je za opskrbne lance, posebice za aplikacije u hrani i lijekovima. [13]

Na slici 6 je prikazan Vennov dijagram koji prikazuje dva kruga, jedan za blockchaine kojima mogu svi pristupiti (Permissionless) i drugi za blockchaine kod kojih je potrebna dozvola za pristup (Permissioned). Hibridni blockchaini su u presijeku krugova što znači da za njih mogu vrijediti oba slučaja.



Slika 6. Podjela tipova blockchaina

Izvor: obrada autora prema: Wegrzyn W. E., Wang E.: *Types of Blockchain: Public, Private, or Something in Between*, 2021., dostupno na: https://www.foley.com/insights/publications/2021/08/types-of-blockchain-public-private-between/ , pristupljeno 9.1.2024

2.5. VERIFIKACIJA TRANSAKCIJA I RUDARENJE

Verifikacija transakcija u blockchain mreži se provodi prema jednom od dva osnovna principa: dokaz o obavljenom poslu (eng. Proof of Work - PoW) ili dokaz o udjelu (eng. Proof of Stake - PoS). Oba su algoritmi za održavanje sigurnosti blockchaina koji omogućuju da se izvršavaju nove transakcije kriptovaluta. Ključna razlika između ova dva principa je u načinu na koji algoritam blockchaina kvalificira i odabire korisnike za dodavanje transakcija u blockchain.

2.5.1. Dokaz o obavljenom poslu

Dokaz o obavljenom poslu je mehanizam za konsenzus blockchaina kojemu je glavni cilj održavanje integriteta i sigurnosti svih transakcija u mreži. Proof of work blockchaini podržani su kroz mrežu decentraliziranih računala koja se nazivaju čvorovi. Čvorovi imaju dvije zadaće: prihvaćanje serija transakcija od drugih čvorova i potvrđivanje (ili predlaganje) novih blokova transakcija mreži. Ovi se čvorovi također nazivaju rudarima jer troše računalnu snagu i resurse u zamjenu za temeljnu kriptovalutu mreže. Pojam „posla“ u ovom mehanizmu označava računalnu moć čvorova koji moraju doprinijeti potvrđivanju novog bloka transakcija. Ovu snagu predstavlja funkcija kriptografskog raspršivanja SHA-256 i ona ovaj mehanizam konsenzusa čini jedinstvenim. [14]

Algoritam koji se zove prilagodba težine osigurava da će cijeloj mreži trebati određeno vrijeme da potvrdi nove blokove transakcija. Prilagodba težine događa se otprilike svakih 2016 blokova (otprilike jednom svaka dva tjedna) kako bi se održalo ciljno vrijeme bloka od 10 minuta. Rudari koji dolaze i odlaze s mreže na individualnoj osnovi ne čine ništa što bi utjecalo na razinu težine iz minute u minutu ili iz dana u dan.

Rudari osvajaju nagradu kada pogode hash koji padne ispod praga koji daje mreža. Jednom kada rudar pronađe važeći hash bloka, on emitira ovu informaciju drugim rudarima koji mogu brzo potvrditi i dodati novi blok u svoje kopije blockchaina. Ovaj postupak provjere eliminira mogućnost uključivanja rudara u zlonamjerne transakcije, poput pokušaja korisnika da dvostruko potroši novčiće kriptovalute. [14]

Mehanizam dokaza o obavljenom poslu potiče rudare diljem svijeta da potroše računalnu snagu za provjeru valjanosti blokova, ispunjavajući tako ulogu koju obično ima središnji entitet kao što je banka. Još jedna primarna prednost PoW-a je da regulira stvaranje novih kovanica. U slučaju Bitcoina, algoritam uključuje prilagodbu težine

rudarenja koja stabilizira stopu kojom rudari mogu proizvesti nove blokove. Bitcoinov kod određuje cilj od 10 minuta po bloku, s algoritmom dizajniranim da poveća poteškoće u pronalaženju novog hash bloka ako stopa hashiranja naraste do točke u kojoj rudari proizvode blokove brže od prosjeka. Bez prilagodbe poteškoća rudarenja povezane s PoW-om, rudari mogu iscrpiti zalihe BTC-a brže nego što je potrebno za održivo gospodarstvo. [14] [15]

2.5.2. Rudarenje

Mehanizam dokaza o obavljenom poslu je usko povezan s rudarenjem. PoW definira točan proces kroz koji rudari pokazuju kolegama da su izvršili traženo izračunavanje generiranjem hasha koji odgovara cilju za odgovarajući blok. S druge strane, rudarenje se usredotočuje na dodavanje novog bloka u blockchain i primanje pripadajućih nagrada za novčiće kriptovalute. [15]

Razmatranje načina na koji se Bitcoin transakcije obrađuju daje jasan uvid u odnos između PoW-a i rudarenja. Sve korisničke transakcije na Bitcoin mreži završavaju u memorijskom skupu (mempool) iz kojeg rudari odabiru transakcije za dodavanje u sljedeći Bitcoin blok. Svaki rudar ulazi u utrku za stvaranje novog bloka za Bitcoin blockchain, birajući nekoliko transakcija iz spremišta memorije (eng. mempool ili memory pool) i spajajući ih u kandidatski blok. Mempool predstavlja svojevrsnu listu čekanja nepotvrđenih transakcija koje još nisu uključene u blok. Ne postoji jedan globalni mempool, već svaki čvor na mreži održava svoj vlastiti mempool, tako da različiti čvorovi mogu držati različite transakcije u svojim mempoolima. Prije nego što kandidatski blok postane prihvaćen kao važeći, rudar mora izvršiti izračune koji generiraju hash ispod cilja koji je postavio Bitcoin Proof of Work algoritam. Prvi rudar koji proizvede odgovarajući hash za svoj kandidatski blok emitira ga drugim rudarima, koji mogu lako provjeriti i potvrditi njegov dodatak zapisu lanca blokova. [14]

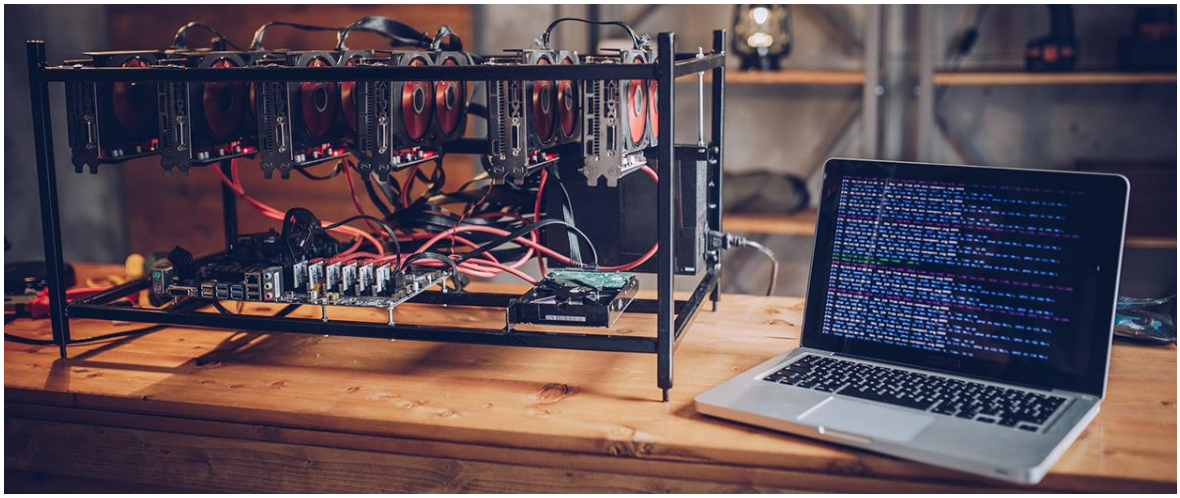
Uspješan rudar prima nagrade za blok i povezane transakcijske naknade, nakon što je dodao novi važeći blok u blockchain. Dakle, veličina Bitcoin blockchaina raste dok počinje utrka za rudarenje sljedećeg bloka.

Rudarenje bitcoina kroz dokaz o obavljenom poslu funkcionira slično kupnji srećki s izvlačenjem nagrada svakih 10 minuta. Svatko može sudjelovati tako da kupi stroj za rudarenje Bitcoina (mining rig) i priključi ga na mrežu. Primjer kako izgleda mining rig je prikazan na slici 7. Iako svi imaju iste šanse da budu izvučeni, kupnja većeg broja listića povećava statističku vjerojatnost dobitka na lutriji. U ovom primjeru srećke predstavljaju

primijenjenu stopu raspršivanja, dok su nagrada za uspješno stvaranje Bitcoin bloka upravo novčići Bitcoin kriptovalute. Brzina raspršivanja je broj raspršivanja u sekundi koje oprema za rudarenje može izvršiti da pronađe gore navedenu kriptografsku funkciju raspršivanja. Što je uređaj za rudarenje učinkovitiji, veće su šanse da rudar osvoji blok nagrade. Na primjer, stroj S19j Pro može izvesti 104 terahasha u sekundi (TH/s), što je ekvivalentno 104 trilijuna pogađanja ili srećki u sekundi.

U međuvremenu, korisnici se mogu pridružiti rudarskim bazenima (eng. mining pool) što povećava njihove šanse za „dobitak na lutriji“, za razliku od solo rudarenja, gdje su izgledi za osvajanje bloka Bitcoina danas izuzetno rijetki. Međutim, svaki dobitak na javnom bazenu za rudarenje dijeli se među članovima proporcionalno njihovom hashrateu.

Poput lutrije, pravila sudjelovanja i potencijalne nagrade kodirani su u Bitcoin softveru. Svatko može provjeriti ova pravila i pristati igrati po njima ako odluči postaviti operaciju rudarenja Bitcoina. [15]



Slika 7. Uređaj za rudarenje Bitcoina (mining rig)

Izvor: Horowitz, D.: *How To Build a GPU Mining Rig*, 2018, dostupno na: https://www.hp.com/gb-en/shop/tech-takes/how-to-build-gpu-mining-rig , pristupljeno 10.1.2024.

2.5.3. Dokaz o udjelu

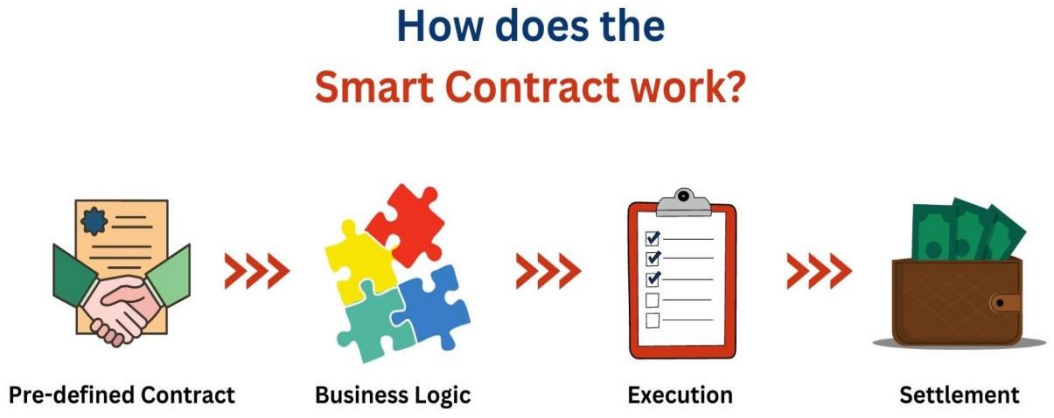
Kod mehanizma dokaza o udjelu rudari obećavaju ulaganje u digitalnu valutu prije potvrđivanja transakcija s dokazom o udjelu. Kako bi potvrdili blokove, rudari moraju staviti ulog vlastitim novčićima. Rudari također pokazuju koliko dugo potvrđuju transakcije. Izbor o tome tko će potvrditi svaku transakciju je nasumičan pomoću težinskog algoritma, koji se regulira na temelju iznosa uloga i iskustva s validacijom.

Nakon što rudar potvrdi blok, on se dodaje u lanac, a rudar prima kriptovalutu za svoju naknadu zajedno sa svojim izvornim ulogom. Ako rudar ne potvrdi ispravno blok, rudarev ulog ili novčići mogu biti izgubljeni. Tjerajući rudare da polože ulog, manja je vjerojatnost da će ukrasti novčiće ili počiniti drugu prijevaru - pružajući još jedan sloj sigurnosti.

Glavni nedostatak mehanizma dokaza o udjelu je potreba za velikim ulaganjem unaprijed za kupnju udjela u mreži. Oni s najviše novca mogu imati najveću kontrolu zbog težine algoritma za odabir validatora. Ako se blockchain račva (eng. fork), validator dobiva duplikat svog uloga jer nema evidencije o uspješnosti. Ako validator pristane na obje strane forka, mogao bi potencijalno dvostruko potrošiti svoje novčiće. [15]

2.6. PAMETNI UGOVORI

Pametni ugovori su digitalni ugovori pohranjeni na blockchainu koji se automatski izvršavaju kada se ispune unaprijed određeni uvjeti Obično se koriste za automatiziranje izvršenja ugovora tako da svi sudionici mogu odmah biti sigurni u ishod, bez uključivanja posrednika ili gubitka vremena. Također mogu automatizirati tijek rada, pokrećući sljedeću radnju kada se ispune uvjeti. Primjer načina na koji funkcionira pametni ugovor je prikazan na slici 8. [16]



Slika 8. Osovni princip rada pametnih ugovora

Izvor: Band A.: *What are Smart Contracts in Blockchain*, 2022, dostupno na: https://www.analyticsvidhya.com/blog/2022/11/what-are-smart-contracts-in-blockchain/, pristupljeno 10.1.2024.

2.6.1. Princip rada pametnih ugovora

Pametni ugovori operiraju kroz jednostavne "if/when...then..." izjave, zapisane u kodu na blockchainu. Kada unaprijed definirani uvjeti budu zadovoljeni i potvrđeni, mreža računala izvršava predviđene radnje, bilo da se radi o oslobađanju sredstava, registraciji vozila, slanju obavijesti ili izdavanju karata. Ažuriranje blockchaina nastupa tek po dovršetku transakcije, čime se osigurava neizmjenjivost transakcija i pristup rezultatima samo onima s odobrenjem.

Pametni ugovori omogućuju postavljanje raznolikog broja uvjeta unutar ugovora kako bi se osiguralo uvjerenje svih sudionika u uspješno izvršenje zadatka. Sudionici, radi postizanja uvjeta, zajedno definiraju način na koji se transakcije i pripadni podaci predstavljaju na blockchainu. Također, usuglašavaju se oko pravila "if/when...then..." koja upravljaju tim transakcijama, istražuju potencijalne iznimke i uspostavljaju okvir za rješavanje sporova. Iako programeri mogu kreirati pametne ugovore, organizacije sve češće pružaju predloške, web sučelja i druge online alate kako bi olakšale proces strukturiranja pametnih ugovora na blockchainu. [16]

2.6.2. Prednosti pametnih ugovora

Neke od prednosti pametnih ugovora su sljedeće:

- Postizanje uvjeta rezultira trenutačnim izvršenjem ugovora, što naglašava brzinu, učinkovitost i preciznost. Digitalna i automatizirana priroda pametnih ugovora eliminira potrebu za procesuiranjem papirnatog materijala i smanjuje vrijeme potrebno za ispravke nastale ručnim ispunjavanjem dokumenata,
- Pouzdanost i transparentnost su zajamčeni jer nema treće strane, a šifrirani zapisi o transakcijama dijele se među sudionicima, eliminirajući potrebu za provjeravanjem eventualnih manipulacija informacijama u osobne svrhe,
- Sigurnost transakcija u blockchainu osigurava njihova minimalna podložnost hakiranju. Povezanost svakog zapisa s prethodnim i sljedećim zapisima u distribuiranoj knjizi zahtijeva od hakera da mijenjaju kompletni lanac kako bi izmijenili samo jedan zapis,
- Pametni ugovori omogućuju uštedu elimininiranjem posrednika u procesu transakcija, čime se istovremeno reduciraju vremenska kašnjenja i pripadajuće naknade. [16]

2.7. PRIMJENA BLOCKCHAIN TEHNOLOGIJE

Blockchain tehnologija, prvotno prepoznata u trgovini virtualnim kriptovalutama, sada ostvaruje uspjeh i izvan financijskog sektora. Njezina primjena proširila se na obrazovanje, zdravstvo, lance opskrbe, trgovinu energijom i druge sektore. Na primjer, financijske usluge blockchain mogu koristiti za pisanje pametnih ugovora između potrošača i njihove bankarske institucije. Slično tome, zdravstvo blockchain može koristiti za pisanje pametnih ugovora između osiguravatelja i bolnica, kao i između pacijenata i bolnica što pokazuje samu širinu mogućnosti primjene ove tehnologije.

2.7.1. Sektor financijske industrije

Financijska industrija također prepoznaje transformativni učinak blockchain tehnologije za stvaranje novih prihoda, postizanje učinkovitosti procesa, poboljšanje iskustva krajnjih korisnika i smanjenje rizika u poslovnim operacijama.

Blockchain tehnologija omogućuje otvorenije, inkluzivnije i sigurnije poslovne mreže, zajedničke operativne modele, učinkovitije procese, smanjene troškove te nove proizvode i usluge u bankarstvu i financijama. Omogućuje izdavanje digitalnih vrijednosnih papira u kraćim vremenskim razdobljima, po nižim jediničnim troškovima, uz više razine prilagodbe. Digitalni financijski instrumenti stoga se mogu prilagoditi zahtjevima ulagača, proširujući tržište za ulagače, smanjujući troškove za izdavatelje i smanjujući rizik druge ugovorne strane. [17]

Tijekom posljednjih pet godina, tehnologija je sazrela za korištenje u poduzećima pokazujući sljedeće prednosti:

- Sigurnost: distribuirana arhitektura blockchain tehnologije temeljena na konsenzusu eliminira pojedinačne točke kvara i smanjuje potrebu za posrednicima kao što su agenti za prijenos, operateri sustava za razmjenu poruka i neučinkovita monopolistička komunalna poduzeća. Blockchain također omogućuje implementaciju sigurnog aplikacijskog koda dizajniranog da bude zaštićen od neovlaštenih promjena protiv prijevara i zlonamjernih trećih strana - čineći ga praktički nemogućim za hakirati ili manipulirati,
- Transparentnost: blockchain koristi zajedničke standarde, protokole i procese, djelujući kao jedinstveni zajednički izvor istine za sudionike mreže,

- Povjerenje: njegova transparentna i nepromjenjiva knjiga olakšava različitim stranama u poslovnoj mreži suradnju, upravljanje podacima i postizanje dogovora,
- Privatnost: pruža alate koji su vodeći na tržištu za privatnost podataka na svakom sloju softverskog skupa, dopuštajući selektivno dijeljenje podataka u poslovnim mrežama. To dramatično poboljšava transparentnost, povjerenje i učinkovitost uz zadržavanje privatnosti i povjerljivosti,
- Visoke performanse: njegove privatne i hibridne mreže osmišljene su za održavanje stotina transakcija u sekundi i povremenih porasta mrežne aktivnosti,
- Skalabilnost: Podržava interoperabilnost između privatnih i javnih blockchaina, nudeći svakom poslovnom rješenju globalni doseg, ogromnu otpornost i visoku cjelovitost glavne mreže.

Prema izvješću Jupiter Researcha, implementacija blockchaina omogućit će bankama da ostvare uštede na prekograničnim transakcijama namire do 27 milijardi USD do kraja 2030., smanjujući troškove za više od 11%. Konkretno, Ethereum je već pokazao disruptivnu ekonomiju, stvarajući preko 10x troškovne prednosti u odnosu na postojeće tehnologije. Financijske institucije priznaju da će tehnologija distribuirane knjige uštedjeti milijarde dolara bankama i velikim financijskim institucijama tijekom sljedećeg desetljeća. [17]

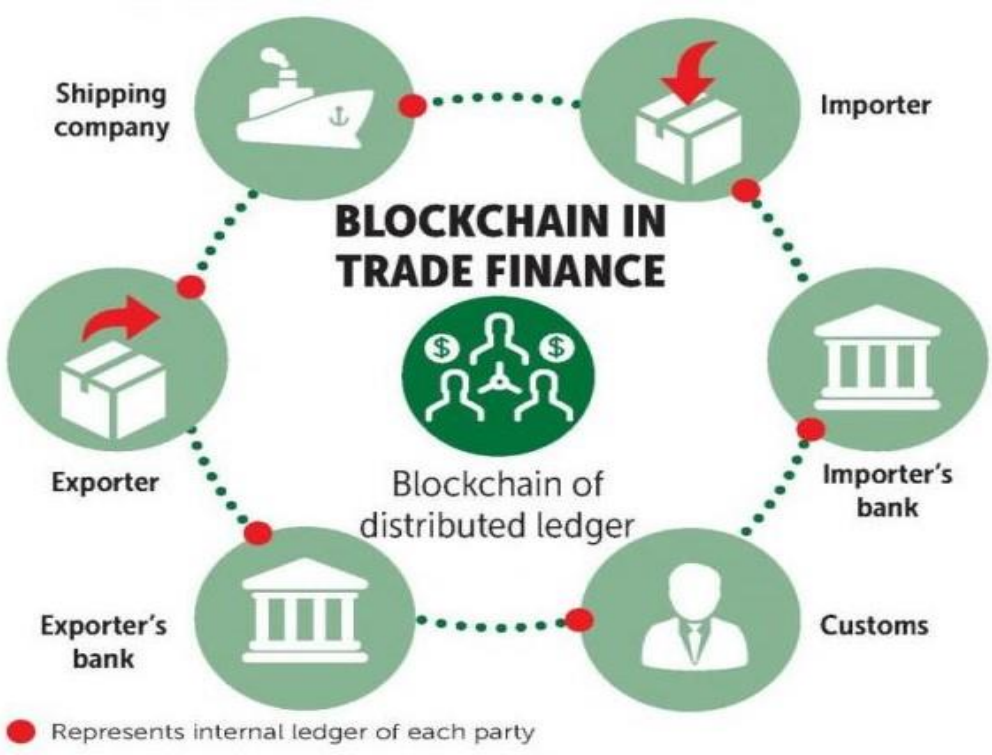
2.7.2. Sektor globalne trgovine

Velike trgovačke tvrtke diljem svijeta prepoznaju transformativni učinak blockchain tehnologije u upravljanju globalnim opskrbnim lancima, upravljanju financiranjem trgovine i otključavanju novih poslovnih modela

Međunarodna trgovina je tržište vrijedno 16 trilijuna dolara koje uključuje razmjenu kapitala, dobara i usluga preko međunarodnih granica ili teritorija. Sa stajališta otpreme i prijevoza, industrija trgovine i financiranja prvenstveno pati od nedostatka povjerenja i koordinacije između izvoznika i uvoznika, osobito na tržištima u razvoju. Osim toga, industrija i dalje sadrži razne operativne neučinkovitosti zbog složene prirode operativnih procesa u međunarodnoj trgovini robom. Na primjer, otprema i trgovina još uvijek se uvelike oslanjaju na ljudske resurse koji se i dalje oslanjaju na ručne i papirnate procese koji su vrlo skupi, spori i skloni pogreškama.

Izvoznici i uvoznici suočavaju se s izazovima financiranja ili jamčenja svojih transakcija, što koči rast i ograničava koristi od globalizacije. Povijesno gledano, ova je industrija vrlo otporna na napredak u tehnologiji i digitalizaciji iako su se neke tehnologije poput rješenja za trgovinu robom i upravljanje rizikom (eng. CTRM - Commodities Trading & Risk Management) pokazale korisnima. [18]

Tijekom proteklih 10-15 godina, mnoge novoosnovane tehnološke tvrtke pokušale su razviti proizvode koji bi se suočili s tim problemima, no s mješovitim uspjehom — sve do pojave blockchain tehnologije za koju je međunarodna trgovina identificirana kao jedan od primarnih slučajeva upotrebe. Potencijalni utjecaj blockchain tehnologije na međunarodno financiranje trgovine potaknuo je mnoge tvrtke i konzorcije da ažuriraju svoju zastarjelu tehnologiju. Osim ulaska u eru digitalizacije, blockchain omogućuje žetonizaciju (tokenizaciju) postojećih dokumenata, akreditiva i ostalih bitnih dokumenata. Pametni ugovori poboljšat će koordinaciju između izvoznika i uvoznika kroz automatizaciju ugovora, poslovnih događaja i drugih ručno intenzivnih procesa. Globalno prihvaćanje blockchain tehnologije stvorit će još veće koristi za prekograničnu koordinaciju, trgovinske nagodbe i standardizaciju. Na slici 9 je prikazano kako mogu teći poslovne transakcije i komunikacija u firmi koja koristi blockchain tehnologiju. [18]



Slika 9. Primjer poslovnog tijeka putem blockchain tehnologije

Izvor: Bangkok Post: *How Blockchain Will Improve International Trade*, 2016, dostupno na: https://www.bangkokpost.com/business/general/1076436, pristupljeno 10.1.2024.

2.7.3. Upravljanje lancima opskrbe

Blockchain tehnologija uz mogućnost programiranja poslovne logike uz korištenje pametnih ugovora omogućuje sljedeće:

- Transparentnost u podrijetlu robe široke potrošnje — od točke izvora do krajnje potrošnje,
- Precizno praćenje imovine,
- Poboljšano licenciranje usluga, proizvoda i softvera.

Čak i u današnjem tehnološki naprednom svijetu, opskrbni lanci mogu dramatično poboljšati učinkovitost i sposobnost praćenja pošiljki i ograničiti izrabljivačko ponašanje. U kontejnerskoj industriji papirologija može predstavljati polovicu troškova prijevoza. Nacionalna studija koju je u SAD-u od 2010. do 2012. provela međunarodna organizacija za zaštitu mora pod nazivom Oceana otkrila je da su plodovi mora krivo označeni do 87% vremena. Tinjac, koji je prisutan u šminki, elektronici i automobilskim bojama, često dolazi iz ilegalnih rudnika gdje se izrabljuju djeca za rad. [19]

Nadalje, roba široke potrošnje, osobito elektronika, lijekovi i luksuzne robne marke, podložna su krivotvorinama i prijevarama. Zapravo, izvješće PwC-a tvrdi da je više od 2% globalne gospodarske proizvodnje rezultat prihoda od krivotvorenja

Blockchain tehnologija se može primijeniti na logistiku kako bi se poslovni procesi učinili učinkovitijima i smanjili troškovi infrastrukture opskrbnog lanca. Blockchain tehnologija može transformirati opskrbni lanac pomoću ova tri slučaja upotrebe:

- Sljedljivost,
- Transparentnost,
- Razmjenljivost.

Sljedljivost poboljšava operativnu učinkovitost mapiranjem i vizualizacijom lanaca opskrbe poduzeća. Sve veći broj potrošača zahtijeva izvor informacija o proizvodima koje kupuju. Blockchain pomaže organizacijama da razumiju svoj lanac opskrbe i angažiraju potrošače stvarnim, provjerljivim i nepromjenjivim podacima.

Transparentnost gradi povjerenje hvatanjem ključnih točaka podataka, kao što su certifikati i zahtjevi, a zatim omogućuje otvoreni pristup tim podacima javno. Nakon što se registrira na blockchain, njegovu autentičnost mogu potvrditi treće strane. Informacije se mogu ažurirati i potvrditi u stvarnom vremenu.

Razmjenljivost je jedinstvena blockchain ponuda koja redefinira koncept konvencionalnog tržišta. Koristeći blockchain, može se "žetonizirati" sredstvo dijeljenjem

objekta na dionice koje digitalno predstavljaju vlasništvo. Slično kao što burza dopušta trgovanje dionicama tvrtke, ovo djelomično vlasništvo dopušta žetonima (tokenima) da predstavljaju vrijednost dioničarevog udjela u određenom objektu. Ovim se žetonima može trgovati, a korisnici mogu prenijeti vlasništvo bez da fizička imovina promijeni vlasnika. [19]

2.7.4. Upravna administracija i javni sektor

Vlade i organizacije javnog sektora koriste blockchain tehnologiju kako bi se udaljili od zatvorenih i neučinkovitih centraliziranih sustava. Trenutačni sustavi sami po sebi su nesigurni i skupi, dok blockchain mreže nude sigurnije, agilnije i troškovno učinkovitije strukture.

Digitalna upravna administracija koja se temelji na blockchainu može zaštititi podatke, pojednostaviti procese i smanjiti prijevare, rasipanje i zlouporabu dok istovremeno povećava povjerenje i odgovornost. Na državnom modelu koji se temelji na blockchainu, pojedinci, tvrtke i vlade dijele resurse preko distribuirane knjige osigurane kriptografijom. Ova struktura minimizira mogućnost pogreški i štiti osjetljive podatke građana i same upravne administracije. [20]

Upravna administracija temeljena na blockchainu ima sljedeće prednosti:

- Sigurno skladištenje vladinih, građanskih i poslovnih podataka,
- Smanjenje radno intenzivnih procesa,
- Smanjenje prekomjernih troškova povezanih s upravljanjem odgovornošću,
- Smanjena mogućnost korupcije i zlouporabe,
- Povećano povjerenje u vladu i online civilne sustave,
- Tehnologija distribuirane knjige može se iskoristiti za podršku nizu aplikacija vladinog i javnog sektora, uključujući digitalnu valutu/plaćanja, registraciju zemljišta, upravljanje identitetom, sljedljivost opskrbnog lanca, zdravstvenu skrb, registraciju poduzeća, oporezivanje, glasovanje i upravljanje pravnim osobama.

2.7.5. Sektor zdravstvene skrbi

Zdravstveni radnici i pružatelji medicinskih usluga u područjima kao što su globalno javno zdravstvo, farmakologija, medicina i zdravstvene znanosti prepoznaju prednosti blockchain tehnologije za pojednostavljenje i osiguranje upravljanja medicinskim podacima, praćenje lijekova i medicinskih uređaja i sl.

Zdravstvena industrija može imati velike koristi od blockchain tehnologije. Tijekom proteklih 30 godina zdravstvena je industrija bila pod utjecajem pojave centraliziranih podatkovnih sustava, regulacije zdravstvenih podataka i mandata da se usredotoči na digitalizaciju medicinskih podataka u partnerstvu s različitim pružateljima usluga elektroničkih medicinskih zapisa (EMR). Većina repozitorija koji obrađuju informacije u vlasništvu pružatelja zdravstvenih usluga, farmaceutskih kompanija i drugih dionika u zdravstvenom i medicinskom ekosustavu ne komuniciraju jedni s drugima. Nedostatak interoperabilnosti među većinom sustava koji sadrže longitudinalne zdravstvene podatke na razini pojedinca (pacijent) i populacije (javno zdravstvo) objašnjava sistemske prepreke koje se često uočavaju u sljedećim situacijama:

- Kada se pacijenti žele konzultirati ili tražiti medicinske usluge od drugih pružatelja zdravstvenih usluga,
- Kada voditelji kliničkog ispitivanja žele potvrditi goleme medicinske podatke njegovih sudionika,
- Kada farmaceutske tvrtke žele osigurati autentičnost lijekova koji kruže globalnim tržištima.

Zbog nemogućnosti sigurnog dijeljenja podataka i izoliranog upravljanja medicinskom dokumentacijom, pacijenti troše dragocjeno vrijeme i resurse tražeći suvišnu medicinsku skrb (npr. provođenje dvostrukih pretraga krvi ili liječničkih pregleda). U hitnim slučajevima liječnici i drugi zdravstveni radnici koji pružaju njegu možda nemaju potpuni uvid u povijest bolesti pacijenta (npr. eksplicitnu dokumentaciju koja naglašava alergije pacijenta, prethodna ili dugotrajna medicinska stanja, davanje kontroliranih tvari itd.) u kojem slučaju riskiraju nepravilno liječenje. [21]

Blockchain tehnologija može pomoći zdravstvenim stručnjacima i cjelokupnoj zdravstvenoj industriji da poboljšaju performanse, transparentnost podataka pacijenata, praćenje i odgovornost, kao i da smanje troškove. To se postiže nizom blockchain mehanizama koji se mogu prilagoditi različitim aplikacijama u zdravstvu, uključujući sljedeće:

- Sigurno upravljanje elektroničkim zdravstvenim zapisima,
- Upravljanje pristankom pacijenata,
- Sljedljivost lijekova,
- Sigurnost podataka u kliničkim ispitivanjima.

Blockchain tehnologija omogućuje sigurno i strukturirano dijeljenje podataka među medicinskom zajednicom putem decentraliziranih baza podataka. Ove strukture rade na zaštiti podataka o pacijentima i privatnosti, omogućuju liječnicima uvid u povijest bolesti svojih pacijenata i osnažuju istraživače da koriste zajedničke podatke za poticanje znanstvenog napretka.

Blockchain rješenja omogućuju strukturirano vlasništvo nad podacima putem slojeva privatnosti i dopuštenja ugrađenih u blockchain. Iako pacijenti ne mogu mijenjati ili brisati određene medicinske informacije koje su liječnici unijeli na svoje profile, oni mogu kontrolirati pristup davanjem pune ili djelomične vidljivosti različitim dionicima u zdravstvenom ekosustavu. Na primjer, pacijenti mogu podijeliti svoju punu evidenciju s medicinskim specijalistom, ali mogu odlučiti podijeliti samo podatke koji se ne mogu identificirati sa znanstveno-istraživačkim tvrtkama ili drugim većim zdravstvenim organizacijama.

Upravljanje lancem opskrbe lijekovima postaje sigurnije i odgovornije uz transparentnost, nepromjenjivost i interoperabilnost koju osigurava blockchain tehnologija. Interoperabilnost između mreža osigurava koherentnu interakciju različitih blockchain aplikacija i sustava duž opskrbnog lanca. Stoga farmaceutske tvrtke mogu registrirati svoje proizvode na blockchainu i pratiti kretanje od izvorišta do krajnjeg potrošača.

Blockchain tehnologija smanjuje rizik od prijevare podataka svojim mehanizmom konsenzusa i decentraliziranom strukturom koja štiti od hakiranja ili manipulacije. Dokumenti mogu dobiti dokaz o postojanju i provjeru autentičnosti na blockchainu. Većina čvorova tada postiže konsenzus za odobravanje novih transakcija i sprječavanje izmjena podataka. To štiti integritet podataka, promiče pouzdane rezultate ispitivanja i potiče suradnju među istraživačkom zajednicom. [21]

2.7.6. Blockchain u ekosustavima interneta stvari

Blockchain tehnologija pojavila se kao kamen temeljac u rješavanju jedinstvenih izazova koje postavlja ekosustav interneta stvari (eng. Internet of Things - IoT). Ekosustav interneta stvari karakterizira ekspanzivna mreža međusobno povezanih uređaja koji komuniciraju i autonomno razmjenjuju podatke. Međutim, ova međusobna povezanost također uvodi ranjivosti povezane sa sigurnošću podataka, integritetom i pouzdanošću transakcija. Blockchain decentralizirana i distribuirana arhitektura glavne knjige predstavlja uvjerljivo rješenje za ove izazove, što je čini posebno korisnom za internet stvari.

Srž problema je pitanje integriteta podataka unutar internata stvari. Ogromna količina podataka koju generiraju IoT uređaji, u rasponu od pametnih kućanskih uređaja do industrijskih senzora, zahtijeva robustan sustav kako bi se osigurala njihova pouzdanost. Blockchain to postiže stvaranjem nepromjenjive i transparentne evidencije transakcija. Svaka transakcija je kriptografski povezana s prethodnom, tvoreći lanac blokova koji je otporan na neovlašteno mijenjanje. U kontekstu interneta stvari, ova značajka štiti integritet podataka koje generiraju uređaji, osiguravajući da ostanu nepromijenjeni tijekom svog putovanja kroz mrežu. [22]

U okviru interneta stvari, sigurnosti se posvećuje posebna briga, jer neovlašteni pristup i zlonamjerni napadi mogu imati teške posljedice. Decentralizirana priroda Blockchaina povećava sigurnost eliminirajući potrebu za središnjim tijelom ili posrednikom. U tradicionalnom centraliziranom sustavu, jedna točka kvara mogla bi ugroziti cijelu mrežu. Uz blockchain, distribuirana priroda glavne knjige osigurava da kompromitiranje jednog čvora ima minimalan utjecaj na cjelokupni sustav. Ova otpornost znatno otežava zlonamjernim akterima manipuliranje ili ometanje IoT mreže.

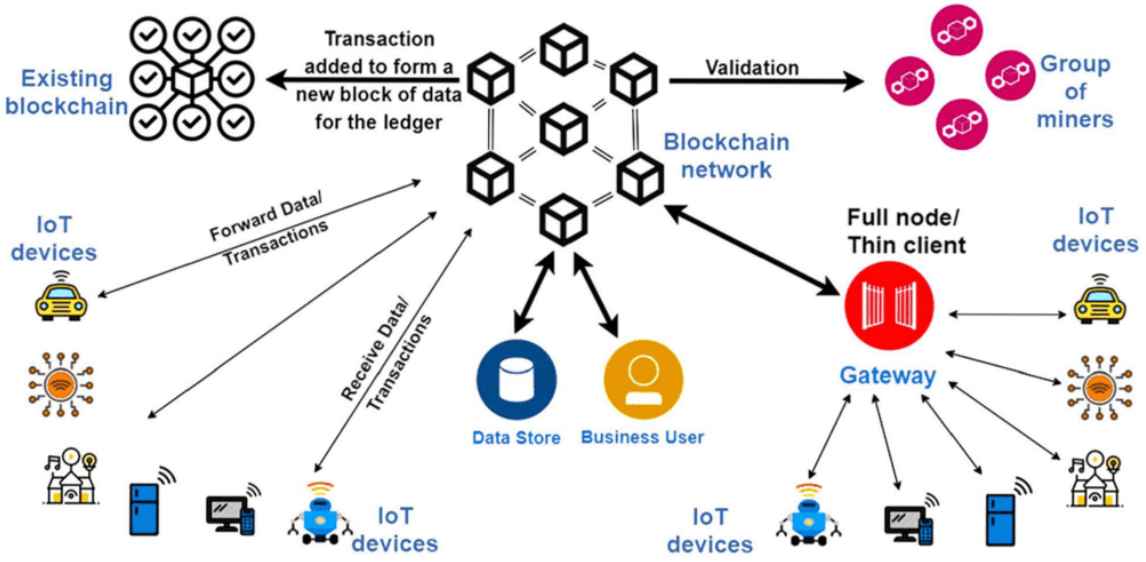
Nadalje, transparentna i zaštićena priroda blockchain transakcija povećava povjerenje među IoT sudionicima. U upravljanju opskrbnim lancem, na primjer, blockchain se može koristiti za stvaranje nezaboravne evidencije o putu robe od proizvođača do krajnjeg korisnika. To osigurava autentičnost proizvoda i pomaže u otkrivanju krivotvorina. Slično, u zdravstvu, gdje IoT uređaji mogu prenositi osjetljive podatke o pacijentima, blockchain pruža sigurnu i sljedljivu metodu upravljanja i dijeljenja tih informacija, održavajući privatnost pacijenata i usklađenost s propisima.

Blockchain se također bavi pitanjem interoperabilnosti unutar raznolikog ekosustava IoT uređaja. Uz uređaje koje proizvode različiti dobavljači i rade na različitim

platformama, postizanje besprijekorne komunikacije i razmjene podataka može biti izazovno. Blockchain pruža standardizirani i sigurni protokol za interakciju uređaja, potičući interoperabilno i kohezivno okruženje interneta stvari.

Dakle, korištenje blockchain tehnologije u internetu stvari nudi specijalizirano i prilagođeno rješenje za jedinstvene izazove koje predstavlja međusobno povezana priroda IoT uređaja. Od osiguravanja integriteta podataka do jačanja sigurnosti i jačanja povjerenja, primjena blockchaina u IoT prostoru omogućava stvaranje otpornijeg, transparentnijeg i učinkovitijeg ekosustava. [22]

Na slici 10 je prikazan primjer arhitekture interneta stvari koja je temeljena na blockchain tehnologiji.



Slika 10. Primjer IoT arhitekture temeljene na blockchainu

Izvor: Academic Library: *Securing IoT and Big Data:Next Generation Intelligence*, dostupno na: https://ebrary.net/194807/computer_science/existing_blockchain_based_security , pristupljeno 10.1.2024.

2.8. NEDOSTACI BLOCKCHAIN TEHNOLOGIJE

Blockchain tehnologija je privukla široku pozornost zbog svog potencijala da revolucionira različite industrije pružanjem decentraliziranog i sigurnog okvira za transakcije. Međutim, kako se prihvaćanje blockchaina ubrzava, osobito s porastom popularnosti kriptovaluta poput Bitcoina i Ethereuma, sve veća pozornost je i na nedostacima ove tehnologije.

2.8.1. Skalabilnost

Blockchain mreže mogu biti spore i neučinkovite zbog visokih računalnih zahtjeva potrebnih za provjeru valjanosti transakcija. Kako se broj korisnika, transakcija i aplikacija povećava, sposobnost blockchain mreža da ih pravodobno obrade i potvrde postaje manja. Zbog toga je blockchain mrežu teško koristiti u aplikacijama koje zahtijevaju velike brzine obrade transakcija. Tradicionalni blockchaini poput Bitcoina oslanjaju se na algoritme konsenzusa kao što su dokaz o obavljenom poslu i dokaz o udjelu, koji mogu biti spori i zahtijevati mnogo resursa. Kao rezultat toga, te se mreže suočavaju s ograničenjima u propusnosti transakcija, što često dovodi do zagušenja i visokih naknada za transakcije.

Predložena su različita rješenja kako bi se pokušali prevladati problemi skalabilnosti, uključujući sustave skaliranja za stvaranje kanala izvan lanca koji omogućuju brže i isplativije transakcije. I dok stručnjaci za blockchain ostvaruju određeni napredak, postizanje skalabilnih, učinkovitih i decentraliziranih blockchain mreža ostaje stalni izazov koji treba dodatno istražiti. [23]

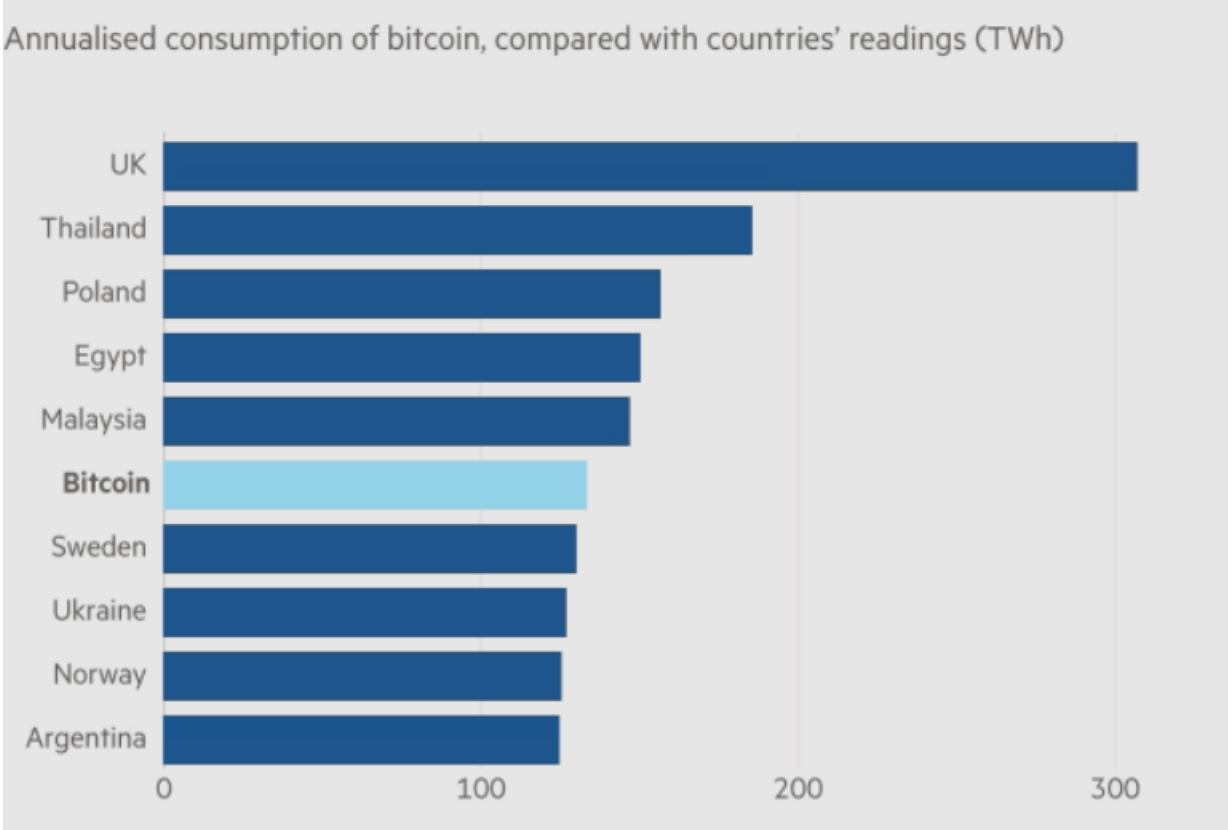
2.8.2. Potrošnja energije

Proces potvrđivanja transakcija na blockchain mreži zahtijeva veliku računalnu snagu, što zauzvrat zahtijeva puno energije, pogotovo kod Proof of Work algoritma koncensusa. To je dovelo do zabrinutosti oko emisija ugljika i utjecaja blockchain tehnologije na okoliš. Rana zabrinutost zbog velike potrošnje energije bila je čimbenik u kasnijim blockchainovima kao što su Cardano (2017.), Solana (2020.) i Polkadot (2020.) koji su prihvatili manje energetski intenzivan Proof of Stake model. Istraživači su procijenili da Bitcoin koji koristi PoW troši 100.000 puta više energije od mreža s PoS modelom.

Godine 2021. studija Sveučilišta Cambridge utvrdila je da Bitcoin (sa 121 TWh godišnje) koristi više električne energije od Argentine (sa 121 TWh) i Nizozemske (109 TWh). Jedna bitcoin transakcija zahtijeva 708 kWh električne energije, količinu koju prosječno američko kućanstvo potroši u 24 dana.

Inicijative poput Ethereuma 2.0 također imaju za cilj smanjiti potrošnju energije mreže Ethereum. Iako su ti napori obećavajući, ključno je da blockchain zajednica nastavi istraživati načine za smanjenje potrošnje energije i razvoj ekološki održivih rješenja. [23]

Na slici 11 je grafički prikaz godišnje potrošnje električne energije potrebne za rudarenje Bitcoina. Vidljivo je da je potrošnja energije potrebna za rudarenje bitcoina veća od godišnje potrošnje električne energije nekih država što pokazuje ozbiljnost problema.



Slika 11. Godišnja potrošnja električne energije za rudarenje bitcoina – usporedba sa nekim državama

Izvor: Martin K., Nauman B.: *Bitcoin's growing energy problem: 'It's a dirty currency'*, 2021, dostupno na https://www.ft.com/content/1aecb2db-8f61-427c-a413-3b929291c8ac , pristupljeno 10.1.2024.

2.8.3. Sigurnost

Sigurnosne mjere blockchaina često su hvaljene kao ključne prednosti tehnologije, no sigurnost blockchain mreža nije bez izazova. Bilo je slučajeva kršenja sigurnosti i hakerskih napada na blockchain mreže, a ti problemi mogu rezultirati novčanim gubicima i oštećenjem integriteta mreže.

Kako bi ublažile rizike, tvrtke rade na poboljšanju sigurnosti blockchain mreža i aplikacija. Njihovi sigurnosni napori uključuju formalnu provjeru pametnih ugovora kako bi se lakše identificirale potencijalne ranjivosti i korištenje novčanika s više potpisa za pohranu i upravljanje digitalnom imovinom.

Kako se blockchain tehnologija nastavlja razvijati, osiguranje sigurnosti korisnika, imovine i transakcija i dalje predstavlja problem. [23]

2.8.4. Složenost

Blockchain je složena tehnologija koja zahtijeva visoku razinu tehničke stručnosti za implementaciju i održavanje. Tehnički izazovi mogu spriječiti široko prihvaćanje blockchain tehnologije i obeshrabriti potencijalne korisnike i programere da se s njome bave. Složenost blockchaina također može dovesti do pogrešaka i neučinkovitosti u implementaciji.

Napori za rješavanje ovog problema uključuju razvoj sučelja prilagođenih korisniku, pojednostavljenih procesa uključivanja i obrazovnih resursa koji pojednostavljuju složenost blockchaina. Povećana suradnja između stručnjaka iz industrije, akademske zajednice i državnih tijela također može promovirati razmjenu znanja i stvaranje standardiziranih protokola i okvira koji smanjuju prepreke ulasku. [23]

2.8.5. Interoperabilnost

Interoperabilnost ili sposobnost različitih blockchain mreža da komuniciraju i međusobno djeluju, još je jedan ključni izazov s kojim se industrija suočava. Trenutačno postoji mnogo različitih blockchain platformi svaka sa svojim vlastitim protokolima i standardima i često ne rade dobro zajedno.

Ovaj nedostatak interoperabilnosti može dovesti do neučinkovitosti, budući da će se pojedinci i tvrtke možda trebati kretati više platformi i koristiti brojne žetone ili kriptovalute za interakciju s različitim mrežama. Ova fragmentacija također može spriječiti suradnju, ugušiti inovacije i spriječiti besprijekornu razmjenu podataka i vrijednosti između različitih blockchain ekosustava.

Kako blockchain industrija nastavlja rasti i diversificirati se, njegovanje interoperabilnosti između različitih mreža bit će ključno za ostvarenje punog potencijala tehnologije. Razbijanjem silosa i promicanjem suradnje između različitih blockchain platformi, industrija može raditi na stvaranju kohezivnog, učinkovitog i uključivog digitalnog krajolika koji koristi korisnicima, programerima i tvrtkama. [23]

3. BLOCKCHAIN TEHNOLOGIJA U POMORSKOJ INDUSTRIJI

Uvođenjem blockchain tehnologije u različite sektore globalnog poslovanja, primjećuju se značajne transformacije koje proizlaze iz njezine inherentne transparentnosti, decentralizacije i sigurnosti. Pomorska industrija, kao ključni stup globalne trgovine, nije izuzetak. Ova revolucionarna tehnologija donosi niz inovacija u pomorski sektor, potičući efikasnost, transparentnost lanca opskrbe, smanjenje rizika od prijevara te poboljšanje sigurnosti i praćenja tereta. U ovom dijelu diplomskog rada istražuju se konkretne primjene blockchain tehnologije u pomorskoj industriji, analizirajući kako je njezino usvajanje unaprijedilo ključne aspekte poslovanja u ovoj grani gospodarstva.

3.1. PODRUČJA POMORSKE INDUSTRIJE POGODNA ZA IMPLEMENTACIJU BLOCKCHAIN TEHNOLOGIJE

Implementacija blockchain tehnologije u okviru pomorskog transporta i lučke logistike nudi niz prednosti koje između ostalog omogućuju lakši prijelaz s papirnatog upravljanja procesima na sigurnije i učinkovitije digitalizirano upravljanje, što podrazumijeva validaciju i pohranjivanje svake radnje ili transakcije u blockchain. Kako bi bilo moguće izvesti digitalizaciju upravljanja procesa pomorske trgovine potrebna je robusna digitalna platforma za razmjenu podataka u stvarnom vremenu. Ovakav način rada osigurava provjerljivost, sljedljivost i nepromjenjivost, što u konačnici dovodi do povećanog povjerenja među različitim akterima u pomorskom prometu. Neka od područja pomorske industrije koje bi blockchain tehnologija mogla unaprijediti su: [7]

- **Plaćanje prijevoza i rješavanje sporova** - Automatizacija plaćanja koja proizlazi iz korištenja pametnih ugovora smanjuje kašnjenja plaćanja i eliminira sporove. Korištenjem pametnih ugovora ostvaruje se automatizirana provjera radnji i transakcija, što dovodi do jače integracije pružatelja financijskih usluga u opskrbni lanac. Osim toga, odobrenje plaćanja transakcija može se automatski pokrenuti u slučaju ispunjenja unaprijed definiranih radnji što rezultira poboljšanjem tijeka financijskih transakcija u opskrbnom lancu,
- **Administrativni troškovi** - Brojni kontejneri koji se prevoze između luka diljem svijeta ne mogu dovršiti svoje putovanje bez dokumenata kao što su teretnice, otpremnice, akreditivi, fakture, sanitarne potvrde, police

osiguranja itd. Tolika količina dokumenata podrazumijeva korištenje mnogo papira i zahtjeva značajan broj radnih sati za obradu istih. Istraživanja Maerska i IBM-a pokazuju da trošak obrade i administracije papirnatih dokumenata doseže čak 20% ukupnih troškova prijevoza, [24]

- **Praćenje tereta i kontrola kvalitete** – Neki od osnovnih izazova u području logistike su kontrola i nadzor kvalitete robe te praćenje fizičkog kretanja robe dok ne dođe do krajnjih korisnika. Sadašnji sustavi nisu uvijek u mogućnosti osigurati praćenje pošiljke u stvarnom vremenu tijekom faze transporta ostavljajući sustav ranjivim na prijevare i manipulacije, što zauzvrat može nanijeti ozbiljne financijske gubitke uključenim stranama. Implementacijom blockchain tehnologije je moguće optimizirati sustav praćenja u opskrbnim lancima gdje bi akteri mogli pratiti kretanja proizvoda od polazišta do odredišta u stvarnom vremenu. Svaka roba ili proizvod bio bi označen jedinstvenim ID-om i skeniran u svakoj fazi transporta. Sudionici uključeni u sporazum o trgovini mogli bi čitati skenirane podatke koji su zabilježeni u distribuiranoj knjizi. Također je moguće zapisati razne podatke o samom proizvodu kao što su npr. temperatura proizvoda u različitim točkama u vremenu ili ostali slični parametri. Stoga blockchain služi kao instrument za provjeru izvornosti robe, sprječavanje rizika krivotvorenja i praćenje kvalitete proizvoda duž transportne rute,[8]
- **Transparentnost i povjerenje -** Teretnice, police osiguranja i fakture su naročito bitni dokumenti koji se koriste u međunarodnoj trgovini kako bi se osiguralo da će financijska sredstva svih transakcija biti uspješno provedena, ali budući da se dokumenti koji se koriste još uvijek često nalaze u papirnatom obliku, podložni su manipulacijama najčešće u obliku krivotvorenja. Osim rizika od krivotvorenja, tradicionalne pomorske tvrtke ranjive su i na širok raspon raznih vrsta kibernetičkih napada. Budući da se blockchain temelji na zajedničkom konsenzusu među različitim stranama, svi dokumenti pohranjeni u njemu su sigurno pohranjeni i samo im ovlaštene osobe mogu pristupiti što uvelike pridonosi povjerenju i povećanju učinkovitosti u zajedničkim procesima više tvrtki,
- **Pomorsko osiguranje** - Potencijalne prednosti blockchain tehnologije za industriju pomorskog osiguranja uključuju obradu šteta i preuzimanje te procjenu rizika. Blockchain tehnologija i pametni ugovori mogli bi se

koristiti kako bi se smanjili troškovi i pogreške povezane s ručnom obradom zahtjeva i kako bi se povećala brzina obrade zahtjeva. Pametni ugovor mogao bi kodirati pravila za omogućavanje prijenosa povrata s tvrtke na osiguranika. Štoviše, mogli bi se smanjiti troškovi vezani uz ručni unos podataka i provjeru novih kupaca. Procjena rizika te prevencija prijevara korištenjem blockchaina omogućuje većem broju certificiranih posrednika (npr. osiguravajućim društvima) da zabilježe podatke koji se odnose na pojedinu osobu. Blockchain bi također mogao riješiti problem prijevare zahvaljujući svom svojstvu koje mu omogućuje pružanje kriptografske provjere autentičnosti i transparentnosti podataka. Pomoću blockchaina osiguravatelji mogu utvrditi dvostruke štete, otkriti obrasce prijevarnog ponašanja i zajednički spriječiti mnoge pokušaje prijevare, [25]

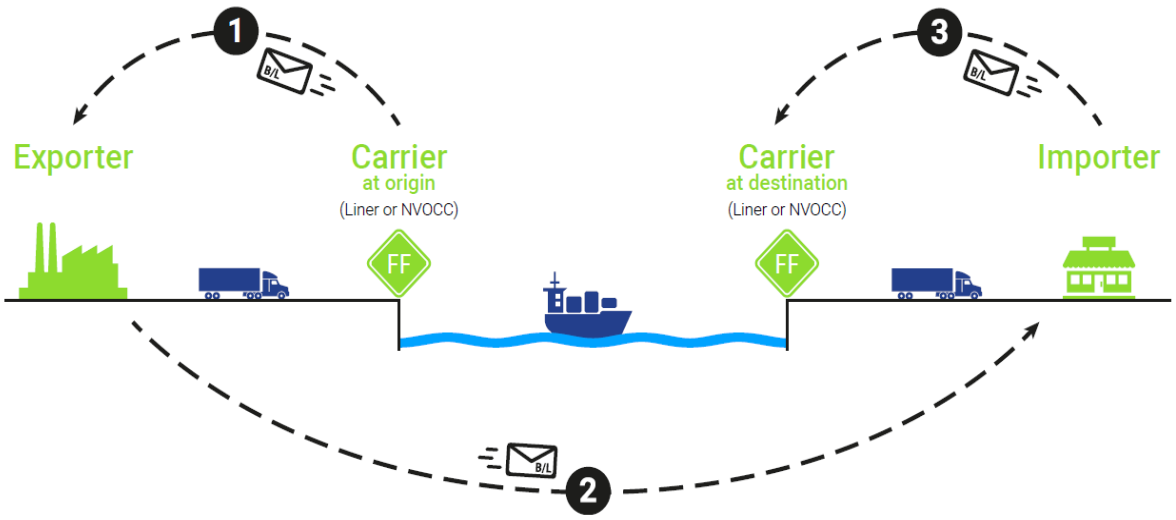
- **Praćenje brodova** - Blockchain se može koristiti za praćenje kretanja i statusa plovila, pomažući u poboljšanju učinkovitosti i točnosti operacija otpreme. Na primjer, položaj plovila, brzina i drugi relevantni podaci mogu se upisati na blockchain u stvarnom vremenu, pružajući transparentan i nepromjenjiv zapis putovanja plovila. To bi se moglo koristiti za poboljšanje točnosti rasporeda otpreme, kao i za praćenje usklađenosti broda s različitim regulatornim zahtjevima,
- **Održavanje brodova** - U pogledu održavanja plovila, blockchain omogućava detaljnu evidenciju o održavanju i popravcima, čime se povećava pouzdanost flote. Pametni ugovori mogu automatski provjeravati ispunjavanje uvjeta održavanja, čime se smanjuje rizik od nepredviđenih kvarova i poboljšava ukupna sigurnost plovidbe.

3.2. STVARNI PRIMJERI KORIŠTENJA BLOCKCHAIN TEHNOLOGIJE U POMORSKOJ INDUSTRIJI

Iako se pomorska industrija može pohvaliti zavidnom razinom tehnološke razvijenosti, ipak se kroz povijest pokazala poprilično spora u ažuriranju operativnih procedura i logistike. Tehnološke inovacije u pomorstvu su najčešće u području inženjerstva dok su se inovacije u sektoru digitalizacije dokumenata i poslovnih procesa tek počele odvijati u bližoj povijesti. Blockchain tehnologija svakako može uvelike doprinijeti još bržem razvoju i modernizaciji poslovnih procesa u pomorstvu. Sljedeći primjeri jasno pokazuju kako blockchain tehnologija pozitivno utječe na pomorstvo.

3.2.1. CargoX

Svaki transfer robe u pomorstvu počinje izdavanjem dokumenta koji se zove teretnica i njime se potvrđuje primitak tereta. Teretnice pružaju detaljan izvještaj o prevezenom teretu te također uključuju datume otpreme i uključene troškove. Ovo je obavezan dokument koji služi kao temeljni dokaz o vlasništvu nad robom u prijenosu. Svatko tko posjeduje teretnicu ima pravo zaprimiti robu u luci, što ju čini najvažnijim dokumentom u brodarskoj industriji. Teretnice su se stoljećima koristile za prijenos vlasničkih prava, omogućujući procvat globalne trgovine, uz održavanje činovničkog reda u složenoj mreži trgovačkih mreža i partnerstava. [5]



Slika 12. Dijagram slanja klasične teretnice

Izvor: obrada autora prema: CargoX Business Overview and Technology Bluepaper - Reshaping the Future of Global Trade with World's First Blockchain-based Bill of Lading, CargoX d.o.o., 2018. god.

Na slici 12 je prikazan proces slanja klasične teretnice koji je praktički nepromijenjen već stoljećima.

Budući da su dokumenti povezani s globalnom pomorskom trgovinom fizički papirnati dokumenti, pojavljuju se svi povezani problemi rukovanja i slanja fizičkih predmeta. Najznačajniji od tih problema su sljedeći: [5]

- usporenost – teretnice u prosjeku putuju s 3 kurirske službe i u tranzitu su od 5 do 10 dana,
- problemi fizičkog dokumenta – teretnica u fizičkom obliku se lako može izgubiti, oštetiti ili čak ukrasti,
- veliki troškovi – svaka se teretnica mora ispisati na papiru i fizički poslati što predstavlja značajne financijske troškove i gubitak dragocjenog vremena. Štoviše u slučaju da se teretnica izgubi može doći do velikih financijskih gubitaka pa se onda i sami paketi osiguravaju što predstavlja dodatni trošak,
- mogućnost prevare – teretnice se obično tiskaju na korporativnom papiru (označenom logotipom izdavatelja). Ovaj korporativni papir može biti ukraden ili izravno krivotvoren i danas služi kao uobičajena baza za prijevare i kriminalne aktivnosti.

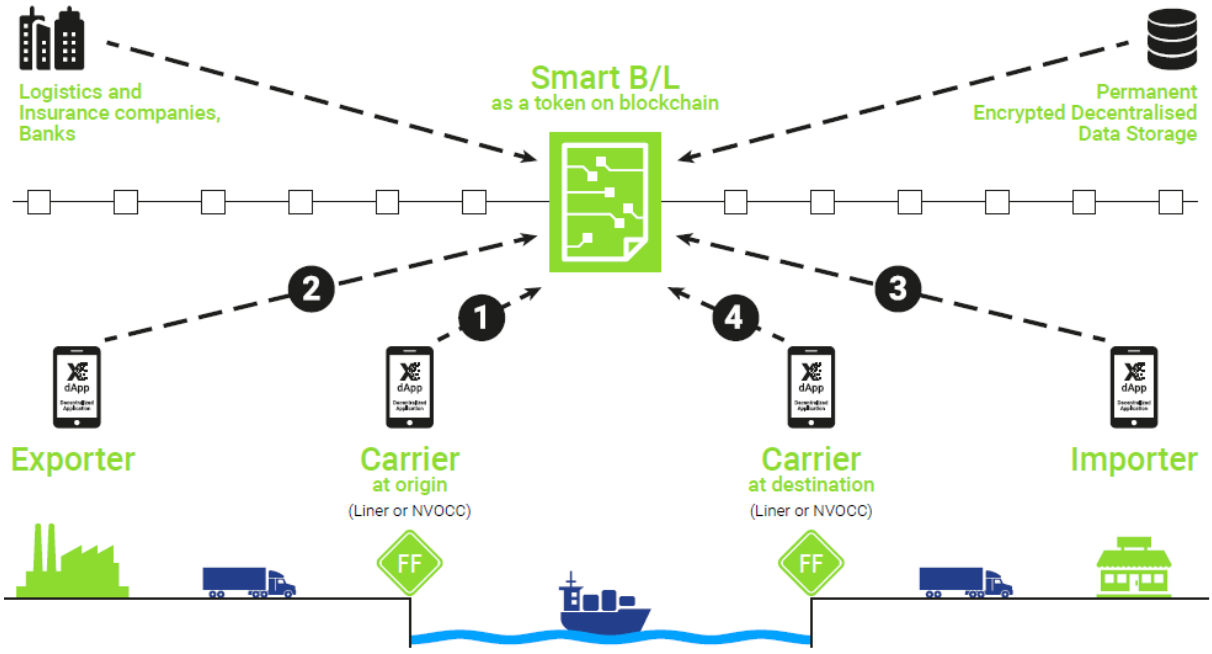
Izumom javnog blockchaina postalo je moguće po prvi put u povijesti povezati sve strane u logističkoj industriji u otvoreni, povjerljivi i decentralizirani ekosustav s transparentno definiranim pravilima rada. Koristeći upravo blockchain tehnologiju CargoX nudi uslugu pametnih teretnica (eng. CargoX Smart B/L). Osnovna svojstva i prednosti pametnih teretnica su sljedeća: [26]

- sigurnost - nema središnje pohrane koja bi bila meta hakera kao ni zajedničkih točaka kvara. Najvažniji dokument u pomorskoj trgovini kriptiran je i sigurno pohranjen na blockchainu, dostupan samo preko vlasnikovih privatnih ključeva tako da se nikada ne može izgubiti ili ukrasti,
- brzina – pametna teretnica se izdaje trenutno i istog trenutka može biti poslana vlasniku robe preko interneta bez posrednika ili kurira, poput slanja e-maila,
- nisu fizički dokument – pametne teretnice sadrže sve informacije kao i klasične papirnate teretnice, čak mogu sadržavati i više bitnih informacija. Budući da je pametna teretnica digitalni dokument pohranjen na

blockchainu nema potrebe za ispisom, pakiranjem, slanjem ili pohranjivanjem papirnatog dokumenta,

- ušteda – budući da pametne teretnice nije potrebno fizički slati raznim kurirskim službama koje mogu biti skupe, stvara se značajna ušteda,
- povjerenje i zaštita od prijevare – klasične papirnate teretnice su podložne manipulacijama jer ne postoji mehanizam za označavanje kada je svaka transakcija potvrđena u stvarnom vremenu. Također ne postoji ni mehanizam za knjiženje sekvenci događaja. Pametne teretnice bilježe svaki unos na blockchainu zajedno s vremenskom oznakom što omogućava sigurniji i transparentniji način rukovanja prijenosom vlasništva nad teretom i sprječava otpuštanje tereta prije nego što se vlasništvo pametne teretnice preda agentu za otpuštanje tereta. Na taj način je lako provjeriti jeli teret prošao carinu ili jeli kontejner stvarno krenuo s terminala u zakazano vrijeme. [5]

Na slici 13 je prikazan proces slanja i primanja CargoX pametne teretnice.



Slika 13. Dijagram slanja i primanja CargoX pametne teretnice

Izvor: obrada autora prema: CargoX Business Overview and Technology Bluepaper - Reshaping the Future of Global Trade with World's First Blockchain-based Bill of Lading, CargoX d.o.o., 2018. god.

3.2.2. Blockshipping

Industrija kontejnerskog pomorskog prijevoza čini značajan udio od približno 60% ukupne svjetske pomorske trgovine, prevozeći godišnje robu u vrijednosti od preko 4 milijarde dolara. Unatoč tome, suočava se s izazovima poput prekapacitiranosti, niskih vozarina, sigurnosnih pitanja i strogih propisa o zaštiti okoliša, postavljajući pritisak na poslovne subjekte da optimiziraju procese i maksimiziraju profit

Inovativni danski start-up Blockshipping razvija prvi svjetski registar teretnih kontejnera, nazvan Global Shared Container Platform (GSCP). Sustav se temelji na blockchainu i osigurat će registar od 27 milijuna kontejnera u stvarnom vremenu koji bi pomorskoj trgovačkoj industriji mogao uštedjeti milijarde svake godine.

GSCP predstavlja prvi potpuni registar svih kontejnera za prijevoz diljem svijeta, istovremeno uvodeći inovativni sustav sigurnih transakcija temeljenih na pametnim ugovorima između ključnih sudionika u industriji, poput prijevoznika, luka i terminala. Prednosti koje bi ovakav sustav donio industriji kontejnera su revolucionarne. Blockshipping procjenjuje da bi implementacija globalnog registra kontejnera mogla rezultirati uštedom od minimalno 5,7 milijardi dolara godišnje u cijelom sektoru. Osim toga, povećana učinkovitost imat će značajan ekološki utjecaj, smanjujući emisiju CO_2 za impresivnih 4,6 milijuna tona godišnje. [28]

Glavni cilj GSCP-a je pružiti informacije pošiljateljima o stvarnoj lokaciji kontejnera. Blockshipping se oslanja na perspektivu primjene pametnih senzora na sve kontejnere, no do tada će koristiti podatkovne točke generirane pri ulasku ili izlasku kontejnera iz depoa, ili prilikom utovara ili istovara s kontejnerskih brodova.

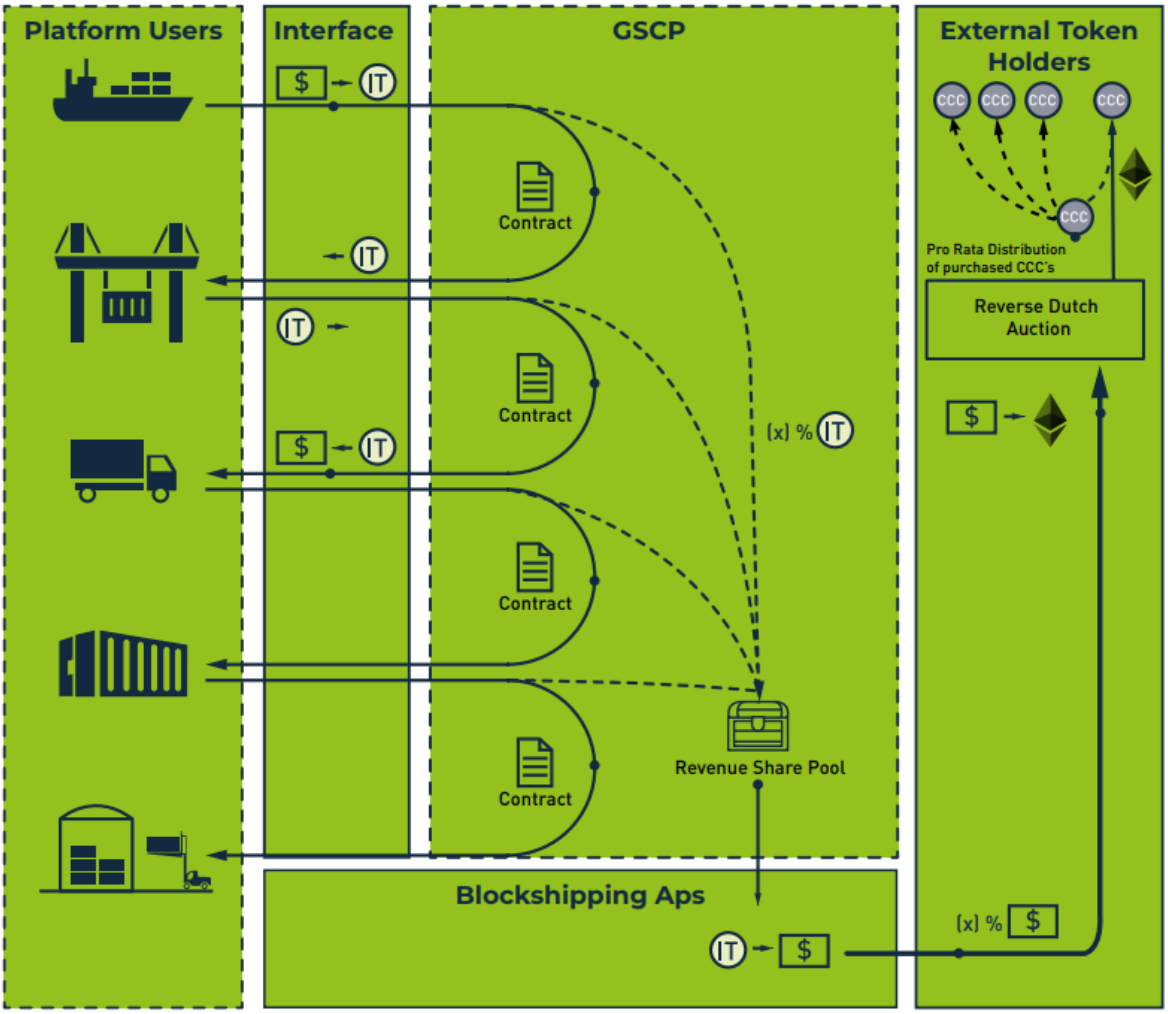
Oko 20% svih kontejnera u svijetu ne može se precizno pratiti u stvarnom vremenu Zbog nedostatka praćenja u stvarnom vremenu i dijeljenja lokacija kontejnera, brodovi koji ih prevoze suočavaju se s prekomjernim zalihama, što bi se pravilnom implementacijom GSCP-a moglo smanjiti za 15% - 20%. Praćenje lokacije kontejnera u stvarnom vremenu pružit će rješenja za dugotrajne probleme industrije, posebno u vezi s premještanjem praznih kontejnera, praksom koja je godišnje stajala brodsku industriju između 15 i 20 milijardi dolara prema procjeni Boston Consulting Grupe 2016. godine. [29]

Ključni dio GSCP-a je njegov mehanizam za premještanje praznih kontejnera (ECR – Empty Container Repositioning), koji stalno izračunava poziciju praznih kontejnera i dostupnih kamiona, a onda te informacije prosljeđuje brodskim linijama, eliminirajući potrebu da to rade sami.

GSCP će stoga omogućiti širenje koncepta „sive kutije“ - ideje da se pošiljateljima pruži zajednički fond kontejnera koji nije povezan s određenom tvrtkom. Premještanje praznih kontejnera može se temeljiti na svim kontejnerima u svijetu, a ne samo na onima u vlasništvu brodarskih kompanija. Šanse da je pravi kontejner dostupan u pravo vrijeme povećavaju se kada postoji zajednički fond kontejnera, umjesto da prijevoznici ovise o specifičnoj tvrtki. [29]

Otvorivši cijelo tržište kontejnera i prateći prazne kontejnere, brodski prijevoznici mogli bi postići značajne uštede na ogromnim troškovima goriva i emisijama koje proizlaze iz kretanja praznih kontejnera, koji trenutno čine 40% ukupnih isporučenih kontejnera širom svijeta.

Na slici 14 je prikazan princip rada GSCP platforme.

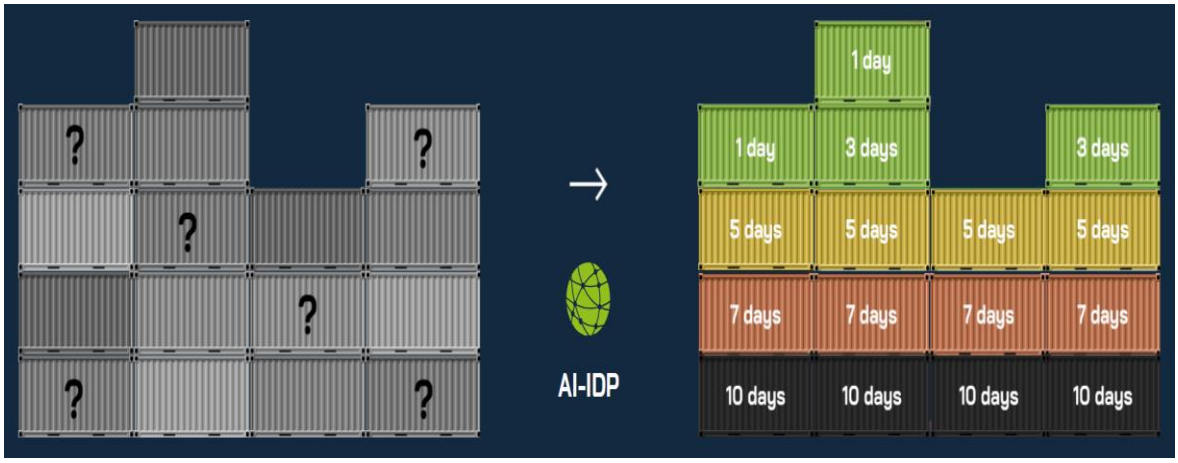


Slika 14. Princip rada GSCP platforme

Izvor: https://urbancrypto.com/wp-content/uploads/2018/08/Blockshipping-flowchart.png , pristupljeno 26.1.2024

Osim što će služiti kao globalni registar za kontejnere, GSCP će također djelovati kao platforma za trgovanje za širok raspon usluga koje se danas razmjenjuju drugim kanalima koji su nerijetko neučinkoviti i skupi. GSCP će djelovati na privatnom blockchainu, koji pruža zajedničku digitalnu knjigu putem koje tvrtke sudionice mogu vidjeti informacije o kontejnerima i sudjelovati u izravnim transakcijama. Na taj način se stvara vrsta „programibilne ekonomije“ u kojoj će transakcije autorizirati autonomni inteligentni softverski agenti (eng. Autonomus Intelligent Software Agents – AISA). Stranke u transakciji daju upute AISA-u da automatski pregovaraju o transakcijama najma kontejnera u njihovo ime – čime se eliminira potreba za trećom stranom i dodatnim troškovima. Sporazumi uspostavljeni između AISA-a (npr. jedan od brodske linije i jedan od iznajmljivača kontejnera) se provode pomoću pametnih ugovora na blockchainu, što jamči maksimalnu transparentnost i sigurnost. [28] [29]

Osim blockchain tehnologije, Blockshipping koristi pogodnosti i umjetne inteligencije (eng. artificial intelligence – AI) nudeći usluge predviđanja vremena zadržavanja (eng. dwell time) uvoznih kontejnera. Prednosti boljeg predviđanja vremena zadržavanja se očituju u manjem broju potrebnih razmještaja kontejnera na pomorskim kontejnerskim terminalima i u povećanom propusnom kapacitetu terminala. [27]



Slika 15. Prikaz metodologije slaganja kontejnera sa AI-IDP umjetnom inteligencijom

Izvor: obrada autora, dostupno na https://blockshipping.net/, pristupljeno 26.1.2024.

Danas većina kontejnerskih terminala ima tradicionalnu i nasumičnu metodu slaganja uvoznih kontejnera na skladištima. Operateri terminala imaju malo saznanja o tome koliko će dugo određeni uvozni kontejner ostati na terminalu i kada će ga netko preuzeti, tako da slaganje nije učinkovito niti troškovno optimizirano. Prosječna cijena

premještanja jednog kontejnera je oko 25 €. Predviđanje vremena zadržavanja putem umjetne inteligencije (eng. AI Import Dwell-time Prediction - AI-IDP) dokazano smanjuje broj poteza za više od 30% i bolje koristi često ograničen prostor dostupan u kontejnerskim terminalima. Nadalje, također se pokazalo da smanjuje vrijeme okretanja kamiona tako da kamioni u prosjeku provode 25% manje vremena na terminalu preuzimajući svoj određeni kontejner, čime se dodatno smanjuju emisije CO_2. [27]

Osim smanjenja troškova poslovanja, AI-IDP također smanjuje emisiju ugljika. Na temelju potencijala, Blockshipping je nedavno dobio sredstva iz Programa razvoja i demonstracije energetskih tehnologija (EUDP). Prema Međunarodnoj pomorskoj organizaciji (IMO), pomorski promet emitira oko 940 milijuna tona CO_2 godišnje i odgovoran je za oko 2,5% emisija stakleničkih plinova. Koristeći AI-IDP, kontejnerski terminali mogu učiniti rad učinkovitijim i smanjiti svoje emisije. Za terminal prosječne veličine to može dovesti do smanjenja od više od 2500 tona CO_2 godišnje, čime rješenje AI-IDP može značajno pridonijeti smanjenju emisija CO_2. [27]

3.2.3. CargoSmart

CargoSmart nudi sveobuhvatan asortiman proizvoda koji pomažu pošiljateljima, primateljima, pružateljima logističkih usluga i špediterima upravljati svojim pošiljkama s više prijevoznika tijekom cijelog ciklusa otpreme. Vidljivost opskrbnog lanca, izvršenje pošiljki, suradnja i rješenja za usklađenost omogućuju korisnicima da automatiziraju i poboljšaju svoje procese upravljanja pošiljkama. Neke od prednosti rješenja koje CargoSmart nudi su:

- niži troškovi upravljanja prijevozom,
- poboljšana učinkovitost upravljanja pošiljkama,
- smanjen rizik od kašnjenja ili pogrešnog upravljanja pošiljkama,
- poboljšana suradnja između sudionika u opskrbnom lancu.

Dostupan u modelu softvera kao usluge (SaaS) i koristeći blockchain tehnologiju, korisnici mogu upravljati isporukama online, offline ili prenositi podatke u interne sustave putem izravne integracije.

CargoSmart rješenja za nadzor lanca opskrbe daju pravovremene informacije o promjenama rasporeda plovidbe, statusu pošiljke, najsuvremenija upozorenja o upravljanju iznimkama i izvješća poslovne inteligencije za mjerenje i optimizaciju performansi lanca opskrbe. [30]

CargoSmart pruža interaktivne rasporede plovidbe i omogućuje pošiljateljima i pružateljima logističkih usluga da točno planiraju pošiljke i izvrše rezervaciju kod svojih prijevoznika. CargoSmart također omogućuje slanje zahtjeva za rezervaciju, automatsko primanje brojeva rezervacija prijevoznika i postavljanje upita za sve podnesene rezervacije online. Moguće je izraditi i dijeliti predloške za rezervacije za učinkovitije slanje rezervacija, uštedu vremena i veću točnost podataka.

Još jedna pogodnost ove platforme je značajno pojednostavljuje upravljane teretnicama i komunikaciju s prijevoznicima na mreži. Prijevoznici učitavaju nacrte teretnica kako bi bilo moguće brzo pregledati sadržaj, zatražiti izmjene i zaprimiti sve potrebne dokumente, smanjujući dodatne troškove telefona i faksa. Zatim je moguće ispisati izvorne teretnice i pomorske tovarne listove eliminirajući nepotrebne kurirske troškove.

CargoSmart omogućuje pošiljateljima, primateljima i pružateljima logističkih usluga pojednostaviti procese upravljanja dokumentima. Kupci mogu elektronički pohranjivati i razmjenjivati svoje dokumente između više pošiljatelja, pružajući jednostavan i centraliziran pristup bilo kojem dokumentu povezanom s pošiljkom na mreži. Pomoću mape za pošiljke (eng. shipment folder) tvrtke mogu nadzirati kritične iznimke dokumenata, smanjiti pogreške u dokumentaciji, poboljšati usklađenost s međunarodnim trgovinskim propisima i smanjiti troškove. [30]

3.3. NEDOSTACI I IZAZOVI KORIŠTENJA BLOCKCHAIN TEHNOLOGIJE U POMORSKOJ INDUSTRIJI

Blockchain tehnologija je uspješno revolucionirala mnoge industrije pa tako uz pravilnu implementaciju u budućnosti ima potencijal da revolucionira i industriju pomorskog prometa kako se može vidjeti u prethodnom poglavlju. Međutim postoji i nekoliko ozbiljnih prepreka koje još uvijek sprječavaju da uporaba ove tehnologije postane ustaljena praksa.

3.3.1. Nedostatak svijesti

Jedan od glavnih izazova za tvrtke koje implementiraju blockchain, a posebno za mala i srednja poduzeća, nedostatak je svijesti o prednostima blockchain tehnologije i široko rasprostranjeno nerazumijevanje kako blockchain funkcionira. Brojne tvrtke ne razumiju u potpunosti što je blockchain ili koje prednosti može ponuditi. To uvelike ima veze s dominacijom „tehničkog“ osoblja na području blockchaina i njihovim pretjerano tehnološkim pristupom, što je menadžerima i ostalom „ne-tehničkom“ osoblju teško razumjeti. Kako bi podigli svijest o blockchainu, menadžeri bi se trebali educirati o toj temi prije implementacije istog u svoju poslovnu strukturu. Ključna pitanja koja bi si menadžeri trebali postaviti prije usvajanja blockchain rješenja vezana su uz samu primjenu blockchaina i kako bi ona promijenila organizaciju i kulturu unutar nje, kako povećati razinu razumijevanja tehnologije na svim razinama i kako bi ona promijenila način na koji ta organizacija komunicira i surađuje s drugima. [9]

3.3.2. Manjak suradnje

Problem s mnogim sadašnjim pristupima implementaciji blockchaina jest taj što organizacije razvijaju vlastite (privatne) blockchaine i aplikacije koje bi radile na njima, a koje trenutno nemaju načina povezivanja s drugim blockchainima. U raznim industrijama različite organizacije koje se pridržavaju različitih standarda razvijaju vlastite blockchaine, što poništava svrhu distribuiranih knjiga te ne uspijeva iskoristiti mrežne učinke i može biti manje učinkovito od kooperativnih pristupa.

Za povećanje razine suradnje među organizacijama rješenje bi mogao biti konzorcij tvrtki. Konzorcij je grupacija tvrtki koje surađuju na razvoju i radu jedne osnovne blockchain infrastrukture i popratnih usluga, koje zatim koriste sudionici za razvoj vlastitog asortimana usluga.

3.3.3. Izazovi sigurnosti i privatnosti

Mnoge aplikacije koje se temelje na blockchainu zahtijevaju da pametne transakcije i ugovori budu nepobitno povezani s poznatim identitetima, što postavlja kritična pitanja o privatnosti i sigurnosti podataka pohranjenih i dostupnih u zajedničkoj knjizi. Iako blockchain nudi veću sigurnost od konvencionalnih računalnih sustava, uz određeni napor, hakeri još uvijek mogu provaliti u aplikacije, sustave i tvrtke izgrađene na blockchainu.

Ključ za rješavanje ovog problema nije samo zaštita privatnosti koju regulira država. Omogućavanje akterima na blockchainu da hvataju i kontroliraju vlastite podatke moglo bi pomoći u sigurnosnim izazovima. [9]

3.3.4. Nedefinirana regulativa

Jedna od velikih prepreka za masovno usvajanje blockchain tehnologije je svakako nedostatak regulativne jasnoće u vezi s blockchain tehnologijom općenito pa tako i sa njenom uporabom u raznim industrijama. Posljedica nepokrivenosti blockchain tehnologije i (za pomorsku industriju veoma bitnih) pametnih ugovora zakonskim propisima mogla bi dovesti do stagniranja u trendu implementacije blockchaina, kao i posustajanje ulagača u daljnja ulaganja u blockchain i srodne tehnologije.

Kako bi prevladali ovaj izazov, vlade i strogo regulirani sektori (kao što su pomorska industrija i prometni sektor) možda će trebati stvoriti propise koji bi mogli pružiti sredstva za kontrolu blockchain ekosustava kako bi se povećala razina sigurnosti i upravljanja, što znači da regulatori moraju razumjeti što je blockchain tehnologija i koji je njezin utjecaj na poduzeća i kupce u njihovom sektoru. [9]

4. ZAKLJUČAK

Pomorski promet je okosnica međunarodne trgovine i globalnog gospodarstva. Preko 80% obujma međunarodne trgovine robom odvija se morem, a postotak je čak i veći za većinu zemalja u razvoju. Stoga je svaki napor da se ova veoma bitna grana industrije unaprijedi u bilo kojem smislu svakako vrijedan i isplativ. Pomorska industrija je tako kroz povijest bila primorana pratiti trendove tehnoloških inovacija kako bi što efikasnije obavljala svoju važnu ulogu u razvoju moderne civilizacije. Spomenute tehničke inovacije su ipak najčešće bile u području inženjerstva dok je po pitanju inovacija u području operativnih procesa i logistike pomorska industrija uvijek bila veoma troma.

Ova tradicionalna industrija ipak sve više počinje implementirati moderna rješenja, pogotovo u zadnjem desetljeću. Tome je svakako doprinio recentni razvoj Industrije 4.0 koji je mnoge prethodno apstraktne tehnološke koncepte približio masama i omogućio njihovu široku upotrebu kroz niz industrija. Još jedan od razloga ove promjene u dinamici industrije pomorskog prometa je i sve veća globalizacija koja nameće tvrtkama žestoku borbu za svaki dio veoma kompetitivnog i surovo kapitalističkog tržišta. Upravo ta kompetitivnost je glavni motiv tvrtkama da maksimalno optimiziraju svoje radne procese kako bi svojim klijentima mogli ponuditi što efikasniju uslugu po prihvatljivim cijenama, plasirajući se tako što bolje na tržištu. Jedan od načina za postizanje takve optimizacije je i korištenje brojnih prednosti blockchain tehnologije što se može vidjeti na stvarnim primjerima u radu.

Optimizacija i unaprjeđenje radnih procesa pomorske industrije nije samo u interesu tvrtkama koje od toga imaju izravnu financijsku dobit već i sveopćoj populaciji. Bilo da se radi o slanju teretnica putem CargoX platforme gdje se one ne moraju slati fizički ili korištenju Blockshippingovog modela umjetne inteligencije koji preslaguje kontejnere tako da štedi broj poteza dizalice i prostor na kontejnerskom terminalu, jasno je da pravilna implementacija ovakvih i sličnih tehnologija može smanjiti ionako prevelike emisije CO2 i drugih štetnih plinova koje pomorska industrija proizvodi.

Blockchain tehnologija kao takva nije bez mana, kao što nisu ni razni primjeri implementacije iste u pomorskoj industriji. Ogroman potencijal da revolucionira ne samo pojedine industrije, nego i čitavo svjetsko gospodarstvo koji blockchain tehnologija posjeduje je samo još veći motivator da se trenutni nedostaci i izazovi blockchaina riješe te da se stvori internacionalna pravna i administrativna legislativa koja bi omogućila što lakšu

primjenu blockchain tehnologije u svim industrijama i civilnim službama koje bi mogla unaprijediti kao što je već unaprijedila i zasigurno će nastaviti unaprjeđivati pomorsku industriju.

Budućnost korištenja blockchain tehnologije u pomorstvu je svijetla, no još je dalek put do toga da bude iskorišten puni potencijal onoga što ona može ponuditi. S obzirom da se pomorska industrija sve više otvara mogućnostima korištenja modernih tehnologija poput blockchaina i umjetne inteligencije, može se zaključiti da će u budućnosti biti sve više tvrtki poput onih koje su obrađene u radu što je svakako pozitivan trend koji treba sačuvati.

Na temelju ovog rada autor zaključuje kako je hipoteza da pravilna implementacija blockchain tehnologije može značajno unaprijediti kvalitetu i učinkovitost radnih procesa kao i unaprijediti privatnost i sigurnost podataka u pomorskoj industriji potvrđena.

LITERATURA

Knjige:

[1] Narayanan, A., Bonneau, J., Felten, E., Mille,r A., Goldfeder, S.: *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, New Jersey, 2016.

[2] Swan, M.: *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Sebastopol, 2015.

[3] Mohiuddin, A.: *Blockchain in Data Analytics*, Cambridge Scholars Publishing, 2020.

[4] Randhir, K., Rakesh, T.: *Implementation of Distributed File Storage and Access Framework using IPFS and Blockchain*, IEEE, 2019.

[5] CagroX Business Overview and Technology Bluepaper, CargoX d.o.o., 2018.

Znanstveni članci:

[6] Roopika, J.: *Blockchain Technology: History, Concepts and Applications,* International Research Journal of Engineering and Technology (IRJET), 2020. URL: https://www.irjet.net/archives/V7/i10/IRJET-V7I10109.pdf pristupljeno 15.10.2023

[7] Phillip, R., Prause, G., Gerlitz, L.: *Blockchain and Smart Contracts for Entrepreneurial Collaboration in Maritime Supply Chains*, TALTECH University, Tallinn, 2019., URL: https://www.researchgate.net/publication/337472180_Blockchain_and_Smart_Contracts_for_Entrepreneurial_Collaboration_in_Maritime_Supply_Chains, pristupljeno 12.11.2023.

[8] Shankar, R., Gupta, R., Pathak, D. K.: *Modeling critical succes factors of traceability for food logistics system,* Transportaton Research Part E: Logistics and Transportation Review, 2018., URL: https://www.researchgate.net/publication/323990024_Modeling_critical_success_factors_of_traceability_for_food_logistics_system, pristupljeno 12.11.2023.

[9] Tijan, E., Aksentijević, S., Ivanić, Jardas, M.: *Blockchain Technology Implementation in Logistics,* Sustainibility, 2019.

Internet Izvori

[10] Arunović, D.: *Što je u stvari blockchain i kako radi?,* URL: https://www.bug.hr/tehnologije/sto-je-u-stvari-blockchain-i-kako-radi-3011 , 2018., pristupljeno 17.10.2023.

[11] Patrizio, A.: *Blockchain Decentralization,* TechTarget, 2023., URL: https://www.techtarget.com/searchcio/definition/blockchain-decentralization, pristupljeno 21.10.2023.

[12] Standards Australia: *Blockchain,* URL: https://www.standards.org.au/flagship-projects/blockchain , pristupljeno 21.10.2023.

[13] Campbell, C.: *What are the 4 different types of blockchain technology?,* TechTarget, 2023., URL: https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology#:~:text=However%2C%20different%20use%20cases%20require,consortium%20blockchains%20and%20hybrid%20blockchains , pristupljeno 23.10.2023.

[14] Quigley, J.L., Gilbert, J.: *What is Proof-of-work (PoW)? All You Need to Know,* Blockworks 2023., URL: https://blockworks.co/news/what-is-proof-of-work , pristupljeno 23.10.2023.

[15] Helter, A.: *Proof of work vs. proof of stake: What's the difference?,* TechTarget, 2023., URL: https://www.techtarget.com/whatis/feature/Proof-of-work-vs-proof-of-stake-Whats-the-difference, pristupljeno 23.10.2023

[16] https://www.ibm.com/topics/smart-contracts, pristupljeno 1.11.2023.

[17] https://consensys.io/blockchain-use-cases/finance, pristupljeno 1.11.2023.

[18] https://consensys.io/blockchain-use-cases/global-trade-and-commerce, pristupljeno 1.11.2023.

[19] https://consensys.io/blockchain-use-cases/supply-chain-management, pristupljeno 1.11.2023.

[20] https://consensys.io/blockchain-use-cases/government-and-the-public-sector, pristupljeno 1.11.2023.

[21] https://consensys.io/blockchain-use-cases/healthcare-and-the-life-sciences, pristupljeno 4.11.2023.

[22] https://www.ibm.com/topics/blockchain-iot, pristupljeno 4.11.2023.

[23] Marr, B.: *The 5 Biggest Problems With Blockchain Technology Everyone Must Know About* , Linkedin, 2023., URL: https://www.linkedin.com/pulse/5-biggest-problems-blockchain-technology-everyone-must-bernard-marr, pristupljeno 9.11.2023.

[24] Solomon, M. B.: *Maersk, IBM launch first blockchain joint venture for trade, transportation*, DC Velocity, 2018., URL: https://www.dcvelocity.com/articles/29429-maersk-ibm-launch-first-blockchain-joint-venture-for-trade-transportation, pristupljeno 12.11.2023.

[25] Garcia, R.: *Will Blockchain Succeed? Cooperation is the Key Factor*, Santander GlobalTech, URL: https://santanderglobaltech.com/en/will-blockchain-succeed/, pristupljeno 25.11.2023.

[26] https://cargox.io/company, pristupljeno 6.1.2024.

[27] https://blockshipping.net/, pristupljeno 6.1.2024.

[28] https://2021.ai/clients/supporting-green-agenda-for-global-container-shipping-industry/, pristupljeno 7.1.2024

[29] Baker, J.: *Will a new blockchain platform change container shipping forever?*, Ship Technology, 2018., URL: https://www.ship-technology.com/features/blockshipping-blockchain-platform/, pristupljeno 7.1.2024.

[30] https://www.cargosmart.com/en-us/solutions, pristupljeno 7.1.2024.

POPIS SLIKA