UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

UVEDBA TEHNOLOGIJE VERIŽENJA BLOKOV NA PODROČJU TRGOVANJA Z ELEKTRIČNO ENERGIJO

Ljubljana, maj 2020 METKA BAŠELJ

IZJAVA O AVTORSTVU

Podpisana Metka Bašelj, študentka Ekonomske fakultete Univerze v Ljubljani, avtorica predloženega dela z naslovom Uvedba tehnologije veriženja blokov na področju trgovanja z električno energijo, pripravljenega v sodelovanju s svetovalcem prof. dr. Alešem Popovičem

I Z J A V L J A M

1. da sem predloženo delo pripravila samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbela, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobila vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označila;

7. da sem pri pripravi predloženega dela ravnala v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobila soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Ljubljani, dne 20. maja 2020. Podpis študentke: _____

KAZALO

KAZALO TABEL

KAZALO SLIK

SEZNAM KRATIC

angl. – angleško

ETRM – (angl. Energy Trading and Risk Management); programska oprema za trgovanje in analizo energetskih sredstev

SHA256 – (angl. Secure Hash Algorithm); zgoščevalna funkcija, imenovana SHA256

H – (angl. Hash); zgoščevalna funkcija

N – (angl. Nonce); naključno arbitrarno število

Tx – (angl. Transaction); transakcija

PBFT – (angl. practical byzantine fault tolerance); praktično bizantinsko soglasje

BFT – (angl. byzantine fault tolerance); bizantinsko soglasje

F – konstanta

No – (angl. Nodes); vozlišče

ICO – (angl. Initial Coin Offering); način zbiranja zagonskih sredstev

DAO – (angl. Decentralized Autonomous Organization); decentralizirana avtonomna organizacija

GDPR – (angl. General Data Protection Regulation); Uredba o varstvu osebnih podatkov

IP – (angl. Internet Protocol); internetni protokol

REST – (angl. Representational State Transfer); predstavitveni prenos stanja

API – (angl. Application Program Interface); aplikacijski programski vmesnik

SDK – (angl. Software Development Kit); zbirka programskih orodij za razvijanje programske opreme

kWh – (angl. kilowatt-hour); kilovatna ura

UVOD

Energetski sektor je v zadnjih letih težil predvsem k čim večji decentralizaciji, digitalizaciji in liberalizaciji trga z električno energijo. Decentralizacija spodbuja v glavnem proizvajalce električne energije iz obnovljivih virov, ki so v zdajšnjem sistemu majhni deležniki na trgu. V Evropski uniji obstajajo regulacijske spodbude, ki poudarjajo predvsem lokalnost. Tako nastajajo lokalna energetska omrežja, ki lahko delujejo samostojno ali pa so povezana z večjimi omrežji. Poleg neodvisnosti lokalnega energetskega omrežja takšne mikromreže znižujejo izgube v omrežju, ki nastanejo s prenosom elektrike. Posledica sprostitve trga je, da se elektrika obravnava kot tržno blago, zato je z njo mogoče trgovati. Od finančnih storitev se energetski sektor razlikuje po tem, da ima dejanski fizični proizvod (energijo), ki ga je treba dostaviti. Transakcije ne vključujejo samo informacij, ampak tudi trgovanje z energijo, ki jo je treba dostaviti po omrežni infrastrukturi. Pomembno je, da se trguje, še preden se dostavi energija, za to pa je potrebno zaupanje. Ker je energijo izredno težko shraniti, je glavni izziv imeti pravo ravnotežje med nakupno in prodajno stranjo. Ponudba in povpraševanje morata biti uravnotežena, saj je potrebna vedno enaka napetost v omrežju. Da se izogne deviacijam, je treba strogo načrtovati in predvideti vedenje potrošnikov in proizvajalcev. Zaradi večje decentralizacije postaja sistem vedno bolj zapleten. Povečuje se število igralcev v igri na strani ponudbe, ki bi radi enakovredno sodelovali v sistemu. Z ustreznimi digitalnimi orodji in sodobno tehnologijo, na primer s tehnologijo veriženja blokov, se lahko omenjene težave rešijo.

Tehnologija veriženja blokov je seznam kriptografsko podpisanih zapisov transakcij, ki so znane in vidne vsem udeležencem v omrežju. Vsak zapis vsebuje časovno oznako in referenčno povezavo na predhodno transakcijo. S pomočjo referenčne povezave se lahko preveri vse pretekle transakcije. Vsak s pravicami lahko izsledi transakcije in vidi vso zgodovino, ki pripada kateremu koli udeležencu (Kandaswamy & Furlonger, 2018). Tehnologija veriženja blokov zagotavlja enoten sistem zapisovanja transakcij, čeprav si udeleženci v omrežju ne zaupajo. Tehnologija veriženja blokov za delovanje uporablja koncept algoritmov soglasja, ki je jedro tehnologije veriženja blokov. Funkcija algoritmov soglasja je, da zapisi oziroma transakcije predstavljajo edino resnico, hkrati pa varuje omrežje pred zlonamernimi uporabniki in kontradiktornimi vplivi.

Tehnologija veriženja blokov je pritegnila pozornost številnih podjetij v različnih panogah. Na področju energetike je največ zanimanja v trgovanju z energenti. Za trgovanje z energenti je treba imeti borzno platformo, ki v osnovi združi trgovce na eni strani in prodajalce na drugi. Glavna naloga je zagotoviti poštene in pregledne transakcije med kupci in prodajalci. V magistrski nalogi bom analizirala trgovalno platformo na podlagi tehnologije veriženja blokov. Aplikacija deluje v razvojnem okolju Hyperledger Fabric in orodju Hyperledger Composer. Glede na to, da se orodje uporablja v nekaterih pilotnih projektih, je zanimivo proučiti predvsem delovanje aplikacije. Namen aplikacije je omogočiti neposredno in decentralizirano trgovanje z električno energijo prek trgovalne platforme, zgrajene na

podlagi tehnologije veriženja blokov. Aplikacija temelji na ideji, da se bo v prihodnosti vzpostavil liberaliziran mikrotrg. Mali proizvajalci bi tako lahko svojo energijo prodali po dogovorjeni ceni v distribucijskem omrežju. Želja po trgovanju in plačevanju mikrokoličine električne energije po določenih cenah in zagotovitev zanesljive oskrbe bi bili lahko dober primer uporabe tehnologije veriženja blokov. Namen aplikacije je udeležencem v sistemu omogočiti dejavno vlogo, kar pomeni, da so hkrati porabniki in proizvajalci električne energije. Dejavni uporabniki oskrbujejo svoja gospodinjstva z električno energijo, proizvedeno iz lastnih virov energije (na primer fotovoltaičnih sistemov), hkrati pa odvečno elektriko oddajajo v omrežje. Če nimajo dovolj lastnih zmogljivosti, tudi sami sodelujejo kot odjemalci elektrike. Dejavni udeleženec v sistemu lahko ponudi elektriko odjemalcem. To bi bila priložnost za opredelitev decentralizirane narave trgovanja z električno energijo.

Zavedati se je treba, da je pred tehnologijo veriženja blokov še vedno veliko izzivov, ki so predvsem zakonodajne in varnostne narave. Varnostne ovire se pojavljajo zato, ker upravljanje omrežja na podlagi veriženja blokov pomeni usklajevanje pravil in procesov, s katerimi se nadzoruje omrežje. Varnostne ovire nastanejo zaradi hitrega uvajanja aplikacij veriženja blokov, ki lahko vsebujejo šibke točke, te pa napadalci izkoriščajo. Na drugi strani obstajajo zakonodajne ovire, ki predstavljajo predvsem interpretacijo zakonov. Ker je tehnologija vedno korak pred regulativo in zakoni, bo v prihodnosti potrebnih še veliko usklajevanj in sprememb trenutne zakonodaje.

Namen magistrske naloge je osvetliti področje praktične uporabe tehnologije veriženja blokov na področju trgovanja z električno energijo, ki bi lahko spremenilo delovanje celotnega energetskega trga.

Osnovni cilj magistrske naloge je prikazati glavne spremembe in izzive, ki jih bo tehnologija veriženja blokov prinesla na področju trgovanja z energenti. Zato bom v teoretičnem delu opisala osnovne principe in značilnosti, ki jih ima tehnologija veriženja blokov. Opisan bo tudi zdajšnji sistem trgovanja z energenti. Ker se energetski sektor in trgovanje z energenti pomikata k vedno večji decentralizaciji, je ena izmed tehnologij, ki bo omogočila lažjo transformacijo sektorja, lahko ravno tehnologija veriženja blokov. Praktičen primer uporabe bo razložen v empiričnem delu, kjer bom simulirala trgovalno platformo, zgrajeno na podlagi tehnologije veriženja blokov, ki deluje v razvojnem okolju Hyperledger Fabric.

Vodilna nit magistrske naloge temelji na vprašanjih:

- Kakšne spremembe bi prinesla uvedba tehnologije veriženja blokov na področje trgovanja z električno energijo?
- Katere lastnosti in koncepti dodajo vrednost tehnologiji veriženja blokov na področju trgovanja z električno energijo in zakaj?
- Katere specifikacije je treba proučiti pred uvedbo tehnologije veriženja blokov na področju trgovanja z električno energijo?

– Kakšni so trenutni problemi in omejitve (zakonodajne in varnostne) pri uporabi tehnologije veriženja blokov na področju trgovanja z električno energijo?

Magistrska naloga bo temeljila tako na znanstvenoraziskovalnem pristopu teoretičnega raziskovanja kot tudi na praktični predstavitvi aplikacije neposrednega trgovanja. Prvi del magistrske naloge bo temeljil na deskriptivni metodi. S pomočjo različne literature bodo opisani osnovni koncepti tehnologije veriženja blokov in trgovanja z električno energijo. Najprej bom razložila trenutni potek trgovanja z električno energijo in spremembe, ki se lahko pričakujejo v prihodnosti. S tem bom podala širšo sliko o tem, kako bi lahko tehnologija veriženja blokov izboljšala trgovanje z električno energijo. Ker je tematika razmeroma nova, bo večina literature povzeta iz tujih virov. Ko bo s pomočjo sekundarnih virov omogočen širši vpogled, bom primerjala različne tipe algoritmov soglasja, ki so jedro tehnologije veriženja blokov. Med algoritmi soglasij bo narejena primerjava glede na različne specifikacije, ki so pomembne za področje trgovanja. Na koncu teoretičnega dela bom opisala glavne pomanjkljivosti trenutnih aplikacij, ki temeljijo na tehnologiji veriženja blokov.

Opisane koncepte tehnologije veriženja blokov bom nato praktično pokazala v drugem delu magistrske naloge. V empiričnem delu bom naredila preslikavo iz teorije v prakso. Postavljena bo trgovalna platforma, ki temelji na tehnologiji veriženja blokov. Pri tem bom uporabila razvojno okolje Hyperledger Fabric, ki bo pomagalo simulirati aplikacijo. Na podlagi aplikacije bom proučila, kako deluje tehnologija, in predstavila namen njene uporabe.

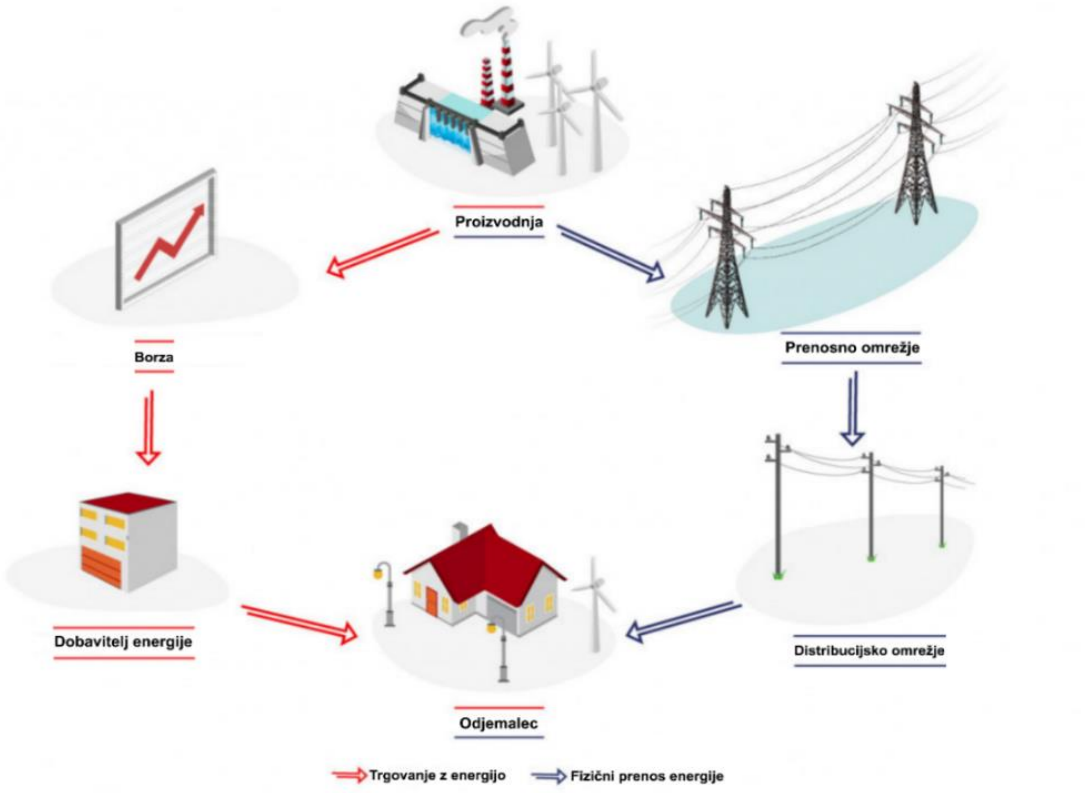
1 TRGOVANJE Z ELEKTRIČNO ENERGIJO

Energetski trg se je začel razvijati z energetsko tranzicijo, predtem je bil trg z električno energijo vertikalno integriran. S popolno vertikalno decentralizacijo so se ločili proizvodnja, prenos in distribucija energije. Slovenija je morala deregulirati elektroenergetski sistem zaradi vstopa v Evropsko unijo. V preteklosti so elektriko prodajali le pooblaščeni monopolni trgovci, zdaj pa lahko kupci izberejo dobavitelja električne energije. Z liberalizacijo elektrogospodarstva je postala elektrika tržno blago, ki jo lahko prodajajo vsi z ustrezno licenco.

Spodnja slika 1 prikazuje elektroenergetski sistem, ki je sestavljen iz fizične infrastrukture in iz organiziranega trga električne energije. Po fizičnem omrežju se pretaka električna energija, na sliki je to označeno z modro barvo. Elektriko proizvajajo elektrarne, ki lahko za vir uporabljajo vodo, biomaso, sonce, veter, premog, plin ... Proizvedena energija se sprva prenese na prenosno omrežje in se nato v večini primerov porazdeli po distribucijskem omrežju do končnih odjemalcev. Večji odjemalci električne energije so neposredno povezani v prenosni sistem omrežja. Dejavnost prenosa in distribucije električne energije je netržna dejavnost in ima značilnosti naravnega monopola. Tržna dejavnost obsega proizvodnjo in dobavo električne energije. Zato mora proizvajalec električne energije sam

poskrbeti za prodajo proizvedene elektrike. Z rdečo barvo je na sliki 1 označeno, kako poteka trgovanje z energijo. Elektrarne pošljejo podatke o proizvedeni energiji na organiziran trg električne energije ali pa prodajo elektriko z bilateralnimi oziroma dvostranskimi pogodbami. V bistvu se ločita veleprodajni in maloprodajni trg z električno energijo. Na veleprodajnem trgu se trguje med trgovci in dobavitelji, medtem ko na maloprodajnem trgu nastopajo dobavitelji, ki prodajajo energijo končnim odjemalcem.

Slika 1: Elektroenergetski sistem



Prirejeno po Augstsprieguma tikls AS, 2019

Trgovanje z električno energijo je zelo zapleteno in vključuje veliko udeležencev, ki aktivno sodelujejo med seboj. Glavni akterji, ki so vključeni v trgovanje z električno energijo, so (Merz, 2019):

- proizvajalci oziroma elektrarne, ki dovajajo električno energijo v omrežje;
- dobavitelj električne energije, ki kupuje električno energijo od proizvajalcev in jo prodaja odjemalcem;
- odjemalec, ki porablja električno energijo in jo potem plača dobaviteljem;
- trgovec, ki kupuje energijo od proizvajalcev na veleprodajnih trgih in proda energijo drugim trgovcem ali dobaviteljem;
- borze, organizacije, ki ponujajo trg z električno energijo in so pod nadzorom državnih regulatorjev;

- posrednik (angl. broker), ki pomaga trgovcem, da lažje uskladijo ceno s prodajalci. Namesto da trgovci trgujejo neposredno na borzi, je mogoče trgovati tudi prek posrednikov;
- klirinška hiša, ki izvaja finančno ali fizično poravnavo energetskih transakcij, kar pomeni, da prevzame vsa tveganja, dokler niso obveznosti posla izpolnjene. Ob morebitnem neplačilu udeležencev klirinška hiša posreduje in zagotovi neuspele dobave ali nadomesti neplačila;
- operater prenosnega omrežja, ki dobi plačilo za prenos električne energije na dolge razdalje, hkrati pa zagotavlja stabilnost sistema;
- operater distribucijskega omrežja, ki je plačan za dobavo električne energije končnim odjemalcem;
- regulator, ki določa pravila in nadzira delovanje energetskega trga na državni in evropski ravni. Agencija za energijo in agencija za sodelovanje energetskih regulatorjev sta dve izmed institucij, ki skrbita za zakonodajo.

Trgovanje z električno energijo je specifično in se razlikuje od trgovanja s finančnimi sredstvi, na primer z delnicami, obveznicami in surovinami. Najpomembnejša razlika trgovanja z električno energijo je, da se mora električna energija porabiti skoraj v istem trenutku, kot se proizvede. Ker elektrike trenutno še ni mogoče shraniti v velikih količinah, je to velik izziv. Pričakuje se lahko, da bo razvoj baterij, ki omogočajo shranjevanje elektrike, prinesel še večjo prilagodljivost trga. Ker morata biti ponudba in povpraševanje vedno uravnotežena, je mogoče, da je cena električne energije negativna. Torej plačilo nekomu, da porabi elektriko. Včasih pride do okvar v prenosnem sistemu ali do nepričakovanih vremenskih razmer, kar povzroči pomanjkanje ponudbe in zato cenovne dvige. Elektrika je izredno homogeno blago, ki ga je izredno težko razlikovati. Ne glede na to, da je elektrika homogeno blago, pa cena elektrike zaradi transporta elektrike in s tem povezanih prenosnih omejitev ni enotna za vse regije (Jakovac, 2010).

Vsak udeleženec, ki želi trgovati z električno energijo ali jo dobavljati, mora pridobiti licenco za opravljanje energetske dejavnosti, ki jo izda Agencija za energijo. Pravila za delovanje trga z elektriko zahtevajo, da je vsak trgovec ali dobavitelj elektrike tudi član bilančne sheme. Člani bilančne sheme so odgovorni bilančni skupini, ki mora pred trgovanjem vplačati bančno garancijo. Namen bančne garancije je zaščita sistemskih operaterjev omrežja, ki skrbijo za izravnavanje omrežja. Ker mora biti omrežje vedno v ravnovesju, sistemski operater pred dobavo energije preveri ravnotežje med porabo in proizvodnjo ter v primeru odstopanja sam kupi energijo. Energija pred neposredno nabavo je najdražja energija, zato se v primeru odstopanj sistemski operater finančno zaščititi z bančnimi garancijami (Agencija za energijo, 2017).

Eden izmed načinov trgovanja z električno energijo je trgovanje na organiziranem trgu oziroma trgovanje na borzni platformi. Borzna platforma pomeni prostor, kjer so združeni trgovci na eni strani in prodajalci na drugi. Borza mora zagotoviti poštene in varne transakcije med kupci in prodajalci. Če katera od strank ne more izpolniti svojih obveznosti,

borza prevzame finančno tveganje. Za učinkovit trg z električno energijo je pomembna predvsem likvidnost na borzah, kar pomeni, da je dovolj ponudbe električne energije in povpraševanja po njej. Večinoma se na borzah trguje s standardiziranimi terminskimi pogodbami (angl. futures). To je pogodba med dvema strankama za nakup ali prodajo določene dobrine, standardizirane količine in kakovosti na določen datum v prihodnosti po ceni, sklenjeni danes.

V ozadju trgovanja poteka veliko procesov, ki so med seboj soodvisni. Sprva se sklene posel in s tem ustvari transakcija med kupcem in prodajalcem elektrike. Podatki o poslih se ločeno zbirajo pri kupcu in prodajalcu v informacijskem sistemu, imenovanem ETRM (angl. Energy Trading and Risk Management). Nato zaledne pisarne od kupca in prodajalca pridobijo podatke o transakciji iz sistema ETRM in se med seboj uskladijo glede trgovanja. Ta korak je lahko dosežen avtomatizirano ali s tradicionalnimi komunikacijskimi kanali, na primer telefonskim klicem ali elektronsko pošto. Ko je posel usklajen na obeh straneh, je treba podrobnosti transakcije sporočiti ustreznim regulatorjem. Pred fizično dobavo elektrike se pošljejo vozni redi o dobavi energije operaterju omrežja. Po dostavi elektrike sledi poravnava bilančne sheme, v kateri se vsa odstopanja od voznih redov plačajo sistemskemu operaterju. Na koncu se finančne obveznosti po navadi poravnajo prek klirinške hiše oziroma banke (Besnainou, 2017).

Energetski sektor se počasi, a vztrajno spreminja, in to z vidika proizvodnje, distribucije in vloge uporabnikov. Zavedanje o podnebnih spremembah je vse večje, zato Evropska unija s svojo politiko podpira smernice, ki bodo pripomogle k večji energetski učinkovitosti in hkrati manjši onesnaženosti. Razumevanje smernic je ključnega pomena za doseganje ciljev energetske politike. Glavne smernice, ki bodo ključne do leta 2030, so dekarbonizacija, digitalizacija, decentralizacija in dejavna udeleženost uporabnikov.

Dekarbonizacija (razogljičenje) je prva smernica, ki bo zaznamovala prihodnost našega planeta. Ljudje so po vsem svetu že začeli doživljati vplive podnebnih sprememb, kot so poplave, suše, izumiranje nekaterih živalskih in rastlinskih vrst. Leta 2015 je bil sprejet Pariški podnebni sporazum, kjer se je več kot 190 držav zavzelo za boj proti podnebnim spremembam. Vsaka država po svoje usmerja politiko za doseganje enakega cilja, ki bo vodil v čistejši planet. S spreminjanjem politike se spodbuja predvsem proizvodnja energije iz obnovljivih virov, na primer vetrna in sončna energija, ki vse bolj izpodrivata konvencionalne vire energije, kot so premog, zemeljski plin in jedrska energija. V zadnjih letih so se stroški električne energije, ustvarjene iz obnovljivih virov, drastično znižali. Kmalu bodo cene gradnje vetrnih in sončnih projektov cenejše od obratovanja obstoječih elektrarn na fosilna goriva. Poleg pocenitve proizvodnje elektrike iz obnovljivih virov se cenijo tudi baterije za shranjevanje elektrike. Energetska tranzicija temelji na tehnologijah, na primer baterijah in elektrarnah iz obnovljivih virov, kjer so potrebni visok investicijski vložek in nizki stroški obratovanja. Nizki obratovalni stroški elektrarn predstavljajo velik izziv na konvencionalnih trgih z električno energijo. V splošnem velja, da proizvajalci ponujajo elektriko po variabilnih proizvodnih stroških in upajo, da bodo na trgu prodali svojo

elektriko po višji ceni. Cena električne energije je zasnovana tako, da se vsako uro izmed vseh proizvajalcev izbere niz elektrarn, ki imajo za to uro predvidene najnižje obratovalne stroške proizvodnje. Glede na izbrani niz elektrarn se končna tržna cena določi na podlagi najvišjih obratovalnih stroškov, ki jih imajo izbrane elektrarne. Na trgih, kjer je veliko elektrarn z obnovljivimi viri, je cena električne energije v nekaterih urah dneva blizu nič, kar znižuje ceno električne energije na veleprodajnih trgih. Vse napovedi kažejo na to, da je energetski sistem, ki temelji na čisti energiji, vedno bolj dosegljiv (Buck, Graf & Graichen, 2019).

V tradicionalnem poslovnem modelu je na trgu malo velikih podjetji, ki delujejo kot monopol. To pomeni, da je načrtovanje elektroenergetskega sistema potekalo od vrha navzdol. Prenos energije je potekal od lastnih elektrarn po lastnem omrežju do končnih odjemalcev, kar je pomenilo, da je bil celoten sistem vertikalno integriran. Liberalizacija trga z električno energijo je v Evropi prinesla veliko obnovljivih virov energije in s tem decentraliziran model prihodnosti. V tem segmentu se je razvil nov koncept, imenovan aktivni uporabnik, ki lahko neposredno porabi energijo ali jo proda drugim udeležencem v omrežju. Aktivni uporabniki so pomemben dejavnik pri energetski tranziciji, saj bodo imeli veliko vlogo pri načrtovanju infrastrukture. Zavedati se je treba, da vedno več mikroenot pomeni tudi vedno več operativnega dela, zato bi nam lahko nove tehnologije pomagale pri zmanjševanju količine dela (Buck, Graf & Graichen, 2019).

Digitalizacija in s tem sodobne digitalne tehnologije omogočajo nove poslovne modele, ki spreminjajo energetsko industrijo. Digitalizacija je ključen dejavnik, ki bo omogočil usklajevanje ponudbe in povpraševanja v realnem času. Uspeh energetske tranzicije bo odvisen od pripravljenosti sprejemanja novih tehnologij in storitev, ki bodo pripomogle k spreminjanju energetske infrastrukture (Buck, Graf & Graichen, 2019).

Raziskovalna in svetovalna institucija Gartner je navedla tehnologijo veriženja blokov kot eno izmed najzanimivejših nastajajočih digitalnih tehnologij. Predvidevajo, da bo tehnologija zaživela v petih do desetih letih (Levy, 2018). Vendar je za uporabo tehnologije bistveno eksperimentiranje oziroma raziskovanje in osredotočenost na poslovni problem, in ne na tehnološko rešitev. Tehnologija veriženja blokov ponuja novo paradigmo poslovanja med podjetji in posamezniki.

2 ARHITEKTURA TEHNOLOGIJE VERIŽENJA BLOKOV

Na kratko bi lahko tehnologijo veriženja blokov opredelila kot digitalno tehnologijo, ki združuje kriptografijo, upravljanje podatkov in mehanizem, ki spodbuja preverljivost, izvajanje in zapis transakcij med večjim številom udeležencev. Poenostavljeno je tehnologija veriženja blokov (angl. blockchain) knjiga, ki vsebuje seznam (angl. chain) skupin (angl. block), v katerih so zapisane transakcije. Subjekti predlagajo transakcijo, nato vozlišča transakcijo preverijo in jo zapišejo v nov blok. Vsebina verige blokov je replicirana

na številna distribuirana vozlišča. Omenjena vozlišča upravljajo sistem veriženja blokov brez osrednjega nadzora oziroma katere koli potrebe po zaupanju tretji osebi. Torej, namesto da se zaupa tretji osebi, se rajši zaupa kolektivnemu upravljanju. Tehnologija veriženja blokov odpravlja težavo zaupanja in težavo koncentracije moči (Murray, 2018).

2.1 Lastnosti

Ko se govori o tehnologiji veriženja blokov, so lahko v mislih zelo različne vrste tehnologije veriženja blokov, ki se med seboj razlikujejo po logiki delovanja in uporabi kriptografije. Ker je prvi uspešen model uporabe tehnologije veriženja blokov kriptovaluta bitcoin, večina lastnosti izhaja ravno iz njegove logike. V tem sklopu bodo razložene osnovne lastnosti tehnologije veriženja blokov na podlagi kriptovalute bitcoin.

2.1.1 Celovitost omrežja

Pri uporabi digitalnih sredstev, na primer denarne valute, vedno obstaja tveganje, da se bo isti denar zapravil dvakrat, oziroma povedano drugače, težava dvojnega trošenja. Za zaupanje med deležniki skrbijo posredniki, ki dražijo transakcije, saj posredniki vzamejo določeno provizijo, hkrati pa to tudi podaljša čas izvedbe transakcije. Ustanovitelj bitcoina Satoshi Nakomoto je želel izločiti posrednike iz sistema. Izkoristil je distribuirano omrežje skupaj z uporabo kriptografije in algoritma soglasja. V sistemu bitcoina so transakcije javno objavljene in časovno ožigosane, zato ne pride do dvojne porabe (angl. double spending problem). Vsako transakcijo preverijo in potrdijo drugi deležniki v sistemu na podlagi distribuiranega algoritma soglasja. Tehnologija veriženja blokov omogoča, da si uporabniki med seboj neposredno pošiljajo digitalna sredstva in pri tem zaupajo samo sistemu, ki temelji na matematični osnovi. Zasnovana je tako, da je praktično nemogoče oziroma stane preveč časa, denarja, energije ali ugleda, da bi kdor koli deloval proti njej. Tehnologija veriženja blokov omogoča varno in zanesljivo množično sodelovanje različnih deležnikov (Tapscott & Tapscott, 2018).

2.1.2 Porazdeljena moč

V obdobju informacijske tehnologije organizacije operirajo z veliko količino podatkov in podatkovnimi bazami, kjer hranijo podatke o svojih uporabnikih. Obstaja veliko primerov, kjer so bili osebni podatki shranjeni in uporabljeni brez privolitve uporabnikov. Tehnologija veriženja blokov bi lahko izboljšala legitimnost današnjih institucij in resnično preusmerila moč uporabnikom in s tem vsem zagotovila udeležbo v družbi in blaginjo. Tehnologija veriženja blokov deluje na konceptu, kjer se razdeljuje moč omrežja med enakovredne deležnike brez enotne točke nadzora. Noben deležnik v omrežju ne more izklopiti sistema in nihče ni tako pomemben, da sistem ne bi mogel delovati brez njega (Tapscott & Tapscott, 2018).

2.1.3 Kibernetska varnost

Vsak dan se dogajajo veliki hekerski vdori, kjer prihaja do nepooblaščenih dostopov do osebnih podatkov. Kraja identitete, nezaželena pošta, goljufije, zlonamerna programska oprema itd. Vse to so načini, ki spodkopavajo varnost posameznika. Trenutno je povprečen uporabnik medmrežja v večini primerov primoran uporabljati samo uporabniško ime in geslo za uporabo določene storitve. Predvideva se, da se bo medmrežje razvijalo v smeri prenašanja vrednosti med strankami brez posrednikov, zato mora biti komunikacija med strankami varnostno na najvišji mogoči ravni. V prihodnosti se lahko pričakuje potreba po zagotavljanju močnejših varnostnih rešitev (Tapscott & Tapscott, 2018).

Tehnologija veriženja blokov dodaja varnost sistemu, saj so varnostni ukrepi vgrajeni v delovanje omrežja. Vsi udeleženci v omrežju imajo vzpostavljeno varno platformo, ki uporablja asimetrično kriptografijo. Z asimetrično kriptografijo se lahko varno shranjujejo in pošiljajo digitalna sredstva in tudi zaupne informacije (Tapscott & Tapscott, 2018).

V digitalni dobi je kibernetska varnost pogoj za varnost človeka v družbi. Glede na to, da se vedno bolj zanaša na digitalna orodja, se je treba podučiti tudi o grožnjah, ki se pri tem pojavijo. S tehnologijo veriženja blokov se lahko povečata varnost in preglednost ter s tem zaščita podatkov.

2.1.4 Zasebnost

V zadnjih dvajsetih letih svetovnega spleta so se zbirale vse vrste zaupnih podatkov posameznikov in institucij, pogosto tudi brez posameznikove vednosti. Zasebnost je temeljna človekova pravica, ki temelji na sodobni družbi. Ljudje bi morali nadzorovati svoje podatke. Vsak posameznik bi moral imeti pravico odločati, kdaj, kako, kaj in koliko o svoji identiteti želi deliti z nekom drugim (Tapscott & Tapscott, 2018).

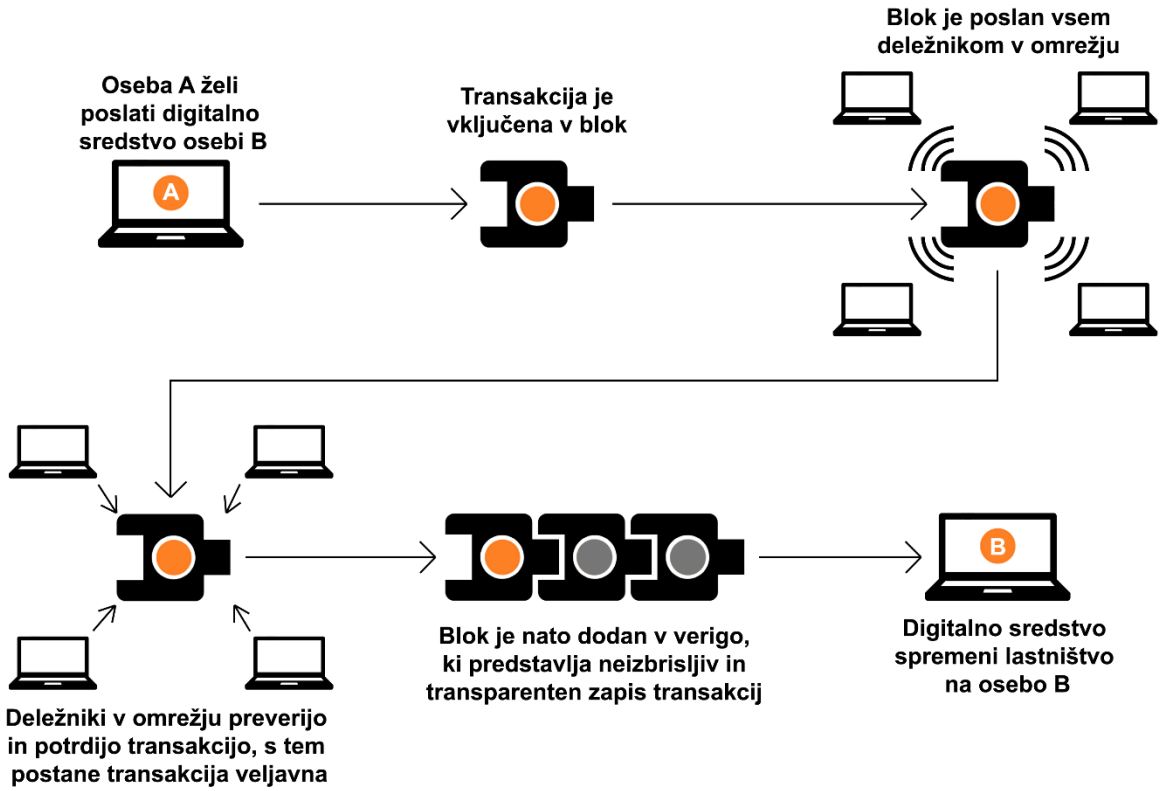
Tehnologija veriženja blokov je zasnovana tako, da ima identifikacijsko raven ločeno od transakcijske ravni. Udeleženci odločajo in ohranijo določeno stopnjo osebne anonimnosti, tako da jim ni treba izdati identitete in je shraniti v centralno podatkovno bazo. Tehnologija veriženja blokov nam omogoča, da se izbere raven zasebnosti in s tem pomaga bolje obvladovati identiteta posameznika. Zagotovo tehnologija veriženja blokov ponuja priložnost, kjer bodo imeli uporabniki večji pregled nad svojimi podatki, dostop do njih jim bo omogočala asimetrična kriptografija (Tapscott & Tapscott, 2018).

2.2 Temeljni koncepti in princip delovanja

Temeljni koncept delovanja tehnologije veriženja blokov je narediti varno transakcijo med dvema subjektoma, ki si med seboj ne zaupata. Slika 2 prikazuje premikanje digitalnega sredstva (na sliki oranžni krog) s pomočjo tehnologije veriženja blokov od osebe A k osebi B. Dostop do digitalnega sredstva in nadzor nad njim ima samo njegov lastnik z zasebnim

ključem. Oseba A potrebuje zasebni ključ za dostop do svojih digitalnih sredstev ter njihovo pošiljanje in javni ključ osebe B, ki ji želi poslati sredstva. Transakcija se pošlje v omrežje in doda v blok, kjer čaka na potrditev omrežja. Ker ni osrednjega subjekta, ki bi potrjeval transakcije, so transakcije potrjene na podlagi algoritma soglasja. Blok z zapisanimi transakcijami se pošlje v distribuirano omrežje, kjer drugi subjekti v omrežju, ki se imenujejo vozlišča, dosežejo soglasje. Vozlišča se morajo strinjati z vsemi transakcijami v bloku, ki je dodan v verigo blokov. Blok s transakcijami nato omrežje preveri in potrdi. Preveri se količina sredstev osebe A, zato da vidi, ali jih ima dovolj in ali jih ni že predtem poslala nekomu drugemu. Ko je blok potrjen in zapisan v verigo blokov, ga ni mogoče spreminjati, torej je dokončen in ni vrnitve. Končni rezultat premika digitalnega sredstva je sprememba lastnika digitalnega sredstva na osebo B.

Slika 2: Delovanje tehnologije veriženja blokov

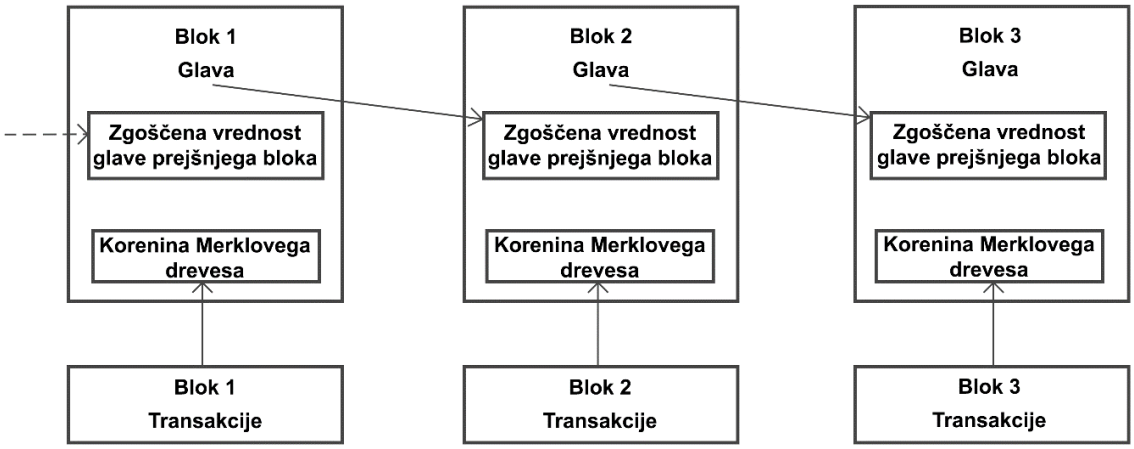


Vir: Thomson Reuters (2019).

Arhitektura tehnologije veriženja blokov temelji na povezovanju med bloki. Povedano drugače, veriga blokov je podatkovna struktura, ki vsebuje bloke, v katerih so shranjene transakcije. Na spodnji sliki 3 lahko vidimo povezave med bloki, ki tvorijo verigo blokov. Vsak blok je povezan s prejšnjim blokom prek reference oziroma zgoščene vrednosti glave bloka. Posamezen blok ima samo enega otroka, to je naslednji blok v verigi, in enega starša, kar je predhodni blok v verigi. Razen prvi generirani blok (angl. genesis block), ki nima staršev (Zheng, Xie, Dai, Chen & Wang, 2017). Tako imenovana zgoščena vrednost glave bloka je povezana s prejšnjim blokom, ta referenca se imenuje tudi zgoščeni kazalec (angl.

hash pointer). To pomeni, da zgoščena vrednost bloka ne vsebuje samo podatkov prejšnjega bloka, ampak podatke o vseh prejšnjih blokih. Ta lastnost dodaja zanesljivost, varnost in sledljivost verigi blokov. Recimo, da se poskuša spremeniti blok številka 1. Zaradi reference zgoščene vrednosti glave bloka 1 v bloku 2 bi bilo treba spremeniti vse zgoščene vrednosti glave bloka od prvega do zadnjega bloka (Rosic, 2017a).

Slika 3: Povezava med bloki



Vir: Nakamoto (2008).

Slika 4 prikazuje strukturo bloka, ki je sestavljen iz glave bloka (angl. block header) in telesa bloka (angl. block body).

V telesu bloka so zapisani naslednji podatki (Bashir, 2017):

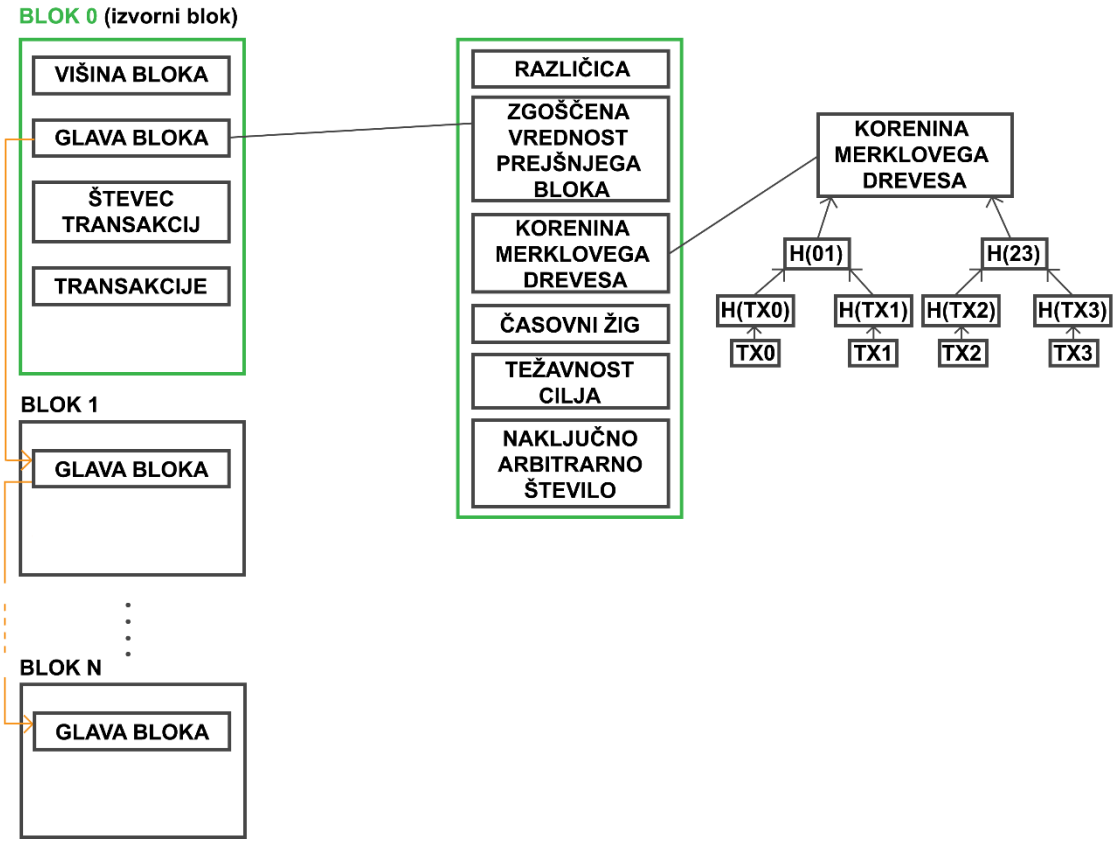
- višina bloka (angl. block size), ki se ga opredeli kot število blokov, ki so pred določenim blokom v nizu. Prvi blok ima višino bloka 0, saj pred njim ni nobenega bloka;
- glava bloka se uporablja za identifikacijo določenega bloka in je povezava med bloki;
- števec transakcij, v katerem je število transakcij, ki so zapisane v bloku;
- transakcije so vse transakcij, ki so zapisane v bloku.

Glava bloka vsebuje naslednje podatke (Bashir, 2017):

- različico oziroma verzijo bloka;
- zgoščeno vrednost prejšnjega bloka (angl. previous block header hash) – podatek, ki zagotavlja pravilno sosledje blokov in se uporablja kot referenca;
- korenino Merklovega drevesa – predstavlja zgoščeno vrednost vseh v paru zgoščenih vrednosti;
- časovni žig (angl. time stamp) – čas, kdaj se je ustvaril blok;
- težavnost cilja (angl. difficulty) – težavnost algoritma dokazovanja dela za ta blok;

– naključno arbitrarno število (angl. nonce) – rešitev, ki jo iščejo rudarji in je rezultat uganke. Naključno arbitrarno število je edina vrednost, ki jo lahko rudarji spreminjajo pri računanju zgoščene vrednosti bloka.

Slika 4: Glava in telo bloka



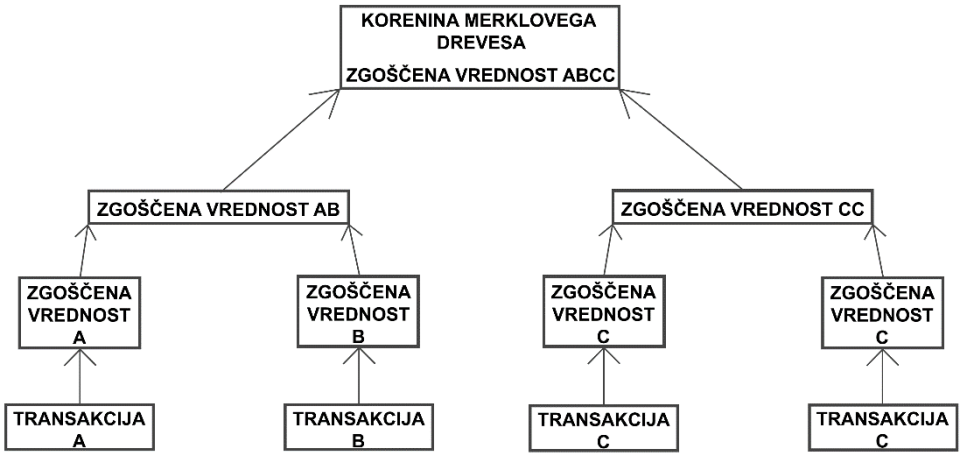
Vir: Bashir (2017, str. 128).

2.3 Merklovo drevo

Koncept je imenovan po R. Merklu, ki je leta 1979 patentiral Merklovo drevo. Merkle je v patentu oblikoval postopek za preverjanje podatkov, ki bi računalnikom omogočil, da opravijo svoje delo hitreje in učinkoviteje kot kdaj koli prej.

Pri tehnologiji veriženja blokov je želja, da bi uporabili čim manj podatkov pri preverjanju transakcij. Na eni strani se zmanjša čas procesorske obdelave, na drugi stran se zagotovi višja raven varnosti. Transakcije niso razporejene po zaporednem vrstnem redu, vendar imajo drevesno strukturo, imenovano Merklovo drevo. Postopek poteka tako, da ima vsaka transakcija, ki se zapiše v omrežju, zgoščeno vrednost. Vsaka vrednost v drevesu je povezana s svojim staršem. Drevesna struktura temelji na razmerju starš – otrok. Vozlišča, višja od določenega vozlišča v isti liniji, se imenujejo starši, tisti pod njim pa so otroci (Antonopoulos, 2017, str. 202–206).

Slika 5: Korenina Merklovega drevesa



Vir: Bashir (2017, str. 203).

Na sliki 5 je primer delovanja Merklovega drevesa. Videti je, da se po zasnovi združijo vse transakcije v pare. Če je število vhodov liho, se prepiše zadnji vhod in se nato poveže sam s sabo, v konkretnem primeru je to transakcija C. Merklovo drevo sprva s pomočjo zgoščene funkcije pretvori transakcije v zgoščene vrednosti. Nato se vrednosti združijo v pare – transakcijo A, B in dvakrat C. Rezultat tega je prepolovitev števila vozlišč. Proces se ponovi, dokler se ne pride samo do ene vrednosti, ta vrednost se imenuje korenina Merklovega drevesa (Antonopoulos, 2017, str. 202–206).

2.4 Zgoščevalna funkcija in asimetrični ključi

Največji potencial tehnologije veriženja blokov je ravno varnost sistema. Za varno delovanje sistema in zaščito podatkov pred namernimi in nenamernimi spremembami se uporablja koncept asimetričnih ključev in enosmerne zgoščene funkcije.

Izraz zgoščevalna funkcija izvira iz zgodovine računalništva in označuje funkcijo, ki stisne niz poljubnega vhoda podatkov v niz fiksne dolžine podatkov. Imenuje se enosmerna zgoščena funkcija, saj je ni mogoče dešifrirati. Vrednosti je mogoče enostavno izračunati na podlagi vhodnih vrednosti, vendar ni mogoče iz podatka izhodne vrednosti ugotoviti izvirne vhodne vrednosti.

Enosmerna zgoščevalna funkcija mora izpolnjevati naslednje pogoje (Komodoplatform, 2018):

– Doseči mora računsko učinkovitost – zgoščene funkcije morajo biti učinkovite, tako da je mogoče izvesti matematično delo oziroma doseči vrednost zgoščene funkcije v zelo kratkem času.

- Deterističnost – za enako vhodno vrednost mora biti enaka izhodna vrednost. Če se vnese enak vhod desetkrat zaporedoma, mora zgoščevalna funkcija izračunati enako izhodno vrednost. Če bi kriptografska funkcija ustvarila različne izhode ob vnosu istega vhoda, bi bila funkcija naključna in zato neuporabna.
- Izhod kriptografske zgoščene funkcije ne sme razkriti nobenih podatkov o vhodnem podatku. Vhodne vrednosti so lahko kateri koli znaki, kot na primer ločila, besede, črke ali številke. Ne glede na vhodne vrednosti, bo izhodna vrednost vedno alfa numerična koda fiksne dolžine. To pomeni, da morebitni napadalec ne more sklepati na dolžino besede glede na dolžino izhodne vrednosti.
- Odpornost proti trku oziroma kolizija – pomeni, da mora biti zelo majhna verjetnost, da sta dva različna vhoda, ki ustvarita enak rezultat oziroma izhod. Glede na to, da je mogočih neskončno vhodov, izhodov pa obstaja fiksno število, je to mogoče.

Ena izmed zgoščevalnih funkcij je SHA256 (angl. Secure Hash Algorithm 256), omenjeno funkcijo uporablja omrežje bitcoin. V spodnji tabeli 1 je prikazan primer uporabe zgoščevalne funkcije SHA256 (Xorbin, 2019).

Tabela 1: Uporaba zgoščene funkcije SHA256

Vhoda vrednost	**Zgoščena vrednost izhodne vrednosti**
BC	768921a22b8e190c2cfafeb0688f0d58a5f76ee4c7fb369758a208c7ba5e9acb
Blockchain	625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
blockchain	ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

Vir: Xorbin (2019).

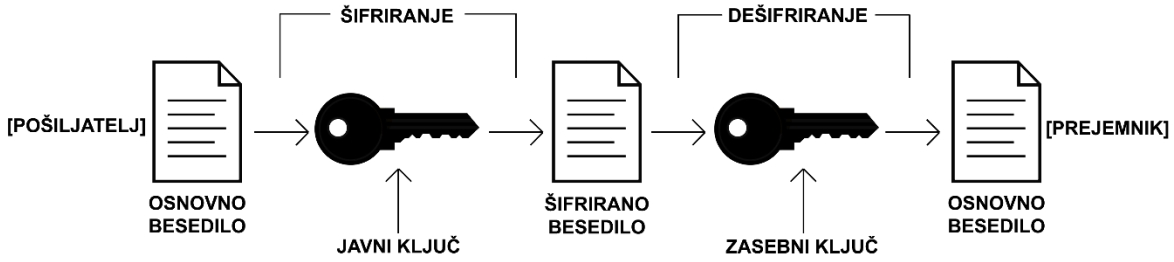
Zgoščena vrednost je, ne glede na dolžino besedila oziroma dolžino vhodnega niza, vedno enako dolga – točno 64 znakov. Vidno je, da je povzetek kombinacija črk in številk, kjer ni nobenih vzorcev ali namigov o tem, kaj je vhodna vrednost. Pri vhodni vrednosti »Blockchain« in »blockchain« se opazi, da se, tudi ko se naredi samo ena subtilna sprememba vhodne vrednosti, izhodna vrednost popolnoma spremeni (Komodoplatform, 2018).

Naslednji koncept, ki ga je treba opredeliti za razumevanje varnosti sistema, so asimetrični ključi oziroma kriptografija javnega ključa. Asimetrični ključ je vrsta kriptografije, ki se pri tehnologiji veriženja blokov uporablja za prepoznavanje uporabnikove identitete in za nadzor nad sredstvi.

S slike 6 je razviden osnovni koncept delovanja asimetričnih ključev. Zasebni ključ se uporablja za dešifriranje besedila, javni pa za šifriranje besedila. Pošiljatelj s prejemnikovim javnim ključem šifrira sporočilo. Nato prejemnik s svojim zasebnim ključem sporočilo dešifrira. Poleg asimetričnih obstajajo tudi simetrični ključi. Glavna razlika med njimi je, da se pri asimetričnih ključih ne uporablja enak ključ za šifriranje in dešifriranje besedila. Torej besedila ni mogoče dešifrirati s ključem, ki je bil uporabljen za šifriranje (Drescher, 2017).

Javni in zasebni ključ sta narejena v paru, in sicer tako, da je javni ključ izpeljan iz zasebnega.

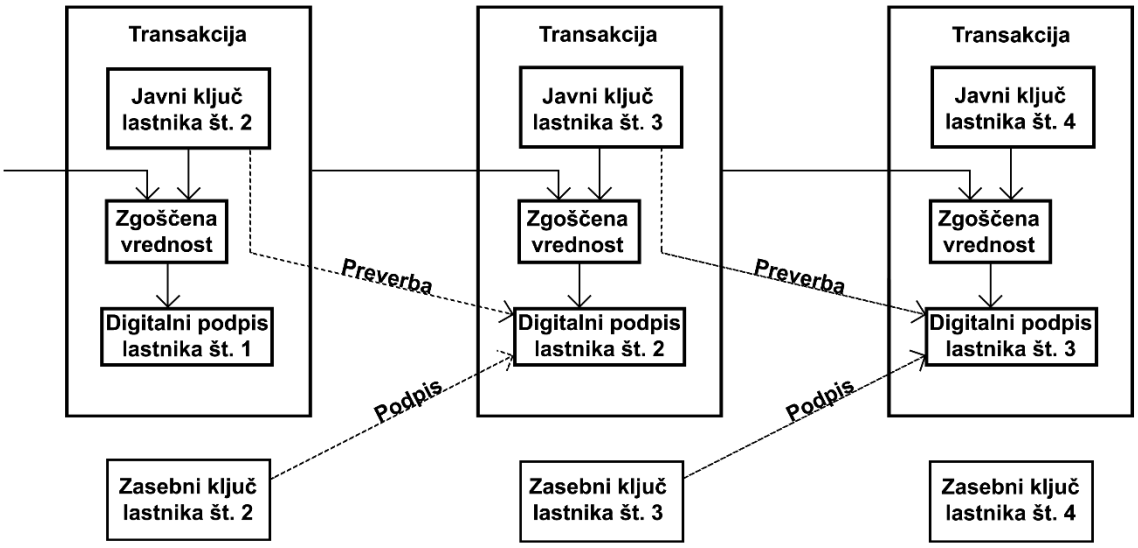
Slika 6: Shematski prikaz osnovnih konceptov in terminologija asimetričnih ključev



Vir: Drescher (2017).

Dostop do digitalnih sredstev in nadzor nad njimi se doseže z uporabo digitalnega podpisa. Veljavni digitalni podpis ima podobno funkcijo kot lastnoročni podpis, in sicer zagotavlja, da je podpisnik ustvaril sporočilo in ga ne more zatajiti, hkrati pa mora ostati sporočilo med pošiljanjem nespremenjeno. Pri tehnologiji veriženja blokov se transakcija podpiše z zasebnim ključem, preostala vozlišča pa preverijo in potrdijo transakcijo s pošiljateljevim javnim ključem. Preveri se, ali je podpisnik lastnik sredstev, ki jih pošilja.

Slika 7: Postopek potrjevanja transakcij



Vir: Satoshi (2008).

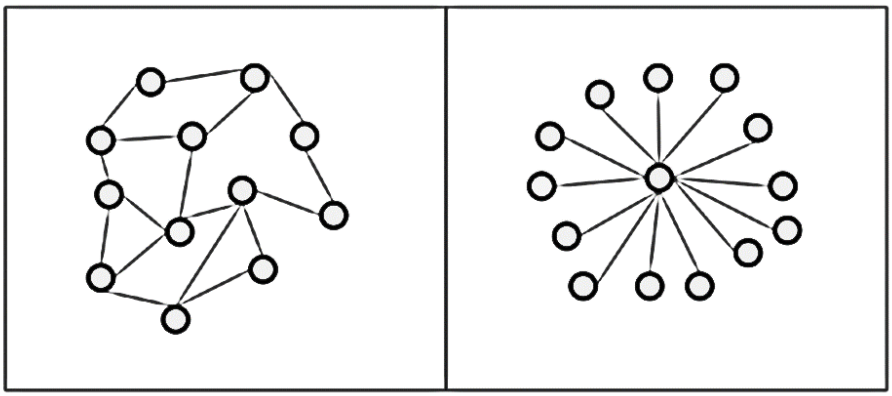
Digitalno sredstvo, ki se premika na verigi blokov, se razume kot veriga digitalnih podpisov. Vsak lastnik digitalnega sredstva lahko prenese lastništvo na naslednjega lastnika tako, da digitalno podpiše zgoščeno vrednost prejšnje transakcije, kar je prikazano na sliki 7. Ključi niso shranjeni v omrežju ali v verigi blokov, temveč jih ustvarijo in shranijo uporabniki v datoteki (Antonopoulos, 2017).

2.5 Distribuiran sistem

Razumevanje koncepta porazdeljenega sistema je bistveno za interpretacijo tehnologije veriženja blokov. V grobem se programska arhitektura razdeli na centralizirano in distribuirano oziroma porazdeljeno. Pri centraliziranih programskih sistemih so komponente povezane z eno osrednjo komponento. Na drugi strani so porazdeljeni sistemi, ki tvorijo mrežo povezanih komponent, ne da bi imeli osrednji element, ki usklajuje in nadzoruje omrežje.

Iz spodnje slike 8 se lahko razbereta dve različni arhitekturi. Krogi na sliki predstavljajo sistemske komponente, imenovane tudi vozlišča, medtem ko črte predstavljajo povezave med njimi. Na levi strani je prikazano distribuirano omrežje, kjer so komponente med seboj povezane brez osrednjega elementa. Opazno je, da nobene komponenta ni neposredno povezana z vsemi drugimi komponentami, hkrati pa so vse komponente med seboj povezane, vsaj posredno. Na desni strani je prikazana centralizirana arhitektura, kjer je vsaka komponenta povezana z eno osrednjo komponento. Komponente niso neposredno povezane in imajo samo eno neposredno povezavo z osrednjo komponento (Drescher, 2017).

Slika 8: Distribuirano in centralizirano omrežje



Vir: Drescher (2017).

Decentraliziran porazdeljen sistem je računalniška paradigma, pri kateri dve ali več vozlišč usklajeno sodelujejo med seboj, da bi dosegli skupen izid. Vozlišče se lahko povzame kot posamezni subjekt v porazdeljenem sistemu. Vsa vozlišča, ki imajo svoj spomin in procesor, lahko sprejemajo in pošiljajo sporočilo drug od drugega. Vozlišča so lahko poštena, napačna ali zlonamerna. Vozlišča, ki delujejo v nasprotju s pričakovanim ravnanjem, so zlonamerna in napačna vozlišča, tako imenovana bizantinska vozlišča. Glavni izziv pri načrtovanju porazdeljenega sistema je koordinacija med vozlišči in toleranca napak. Sistem mora delovati in doseči želen rezultat kljub bizantinskim vozliščem (Bashir, 2017).

Tehnologija veriženja blokov omogoča izmenjavo podatkov na konceptu »peer-to-peer« oziroma na omrežju vrstnikov. Podatki se pošiljajo distribuirano od enega vozlišča k

drugemu. Vsako vozlišče v omrežju lahko preveri pravilnost transakcije. Stanje verige blokov predstavljajo transakcije, ki jih vozlišča neprekinjeno generirajo in nato združijo v bloke. Vsa vozlišča imajo informacije trenutnega stanja verige blokov in vzdržujejo kopijo obstoječe verige blokov, ki vsebuje zgodovino prejšnjih transakcij (Antonopoulos, 2017).

Prednosti distribuiranega sistema so (Drescher, 2017):

- Višja zmogljivost – računalniška moč porazdeljenega sistema je rezultat združevanja računalniške moči vseh povezanih računalnikov.
- Znižanje stroškov – ker so porazdeljeni sistemi sestavljeni iz več računalnikov, so začetni stroški porazdeljenih sistemov večji od začetnih stroškov posameznega računalnika. Vendar so stroški vzdrževanja in delovanja precej manjši, še posebno, ker je mogoče zamenjati posamezne računalnike, ki nimajo pomembnega vpliva na delovanje celote.
- Večja zanesljivost – porazdeljeni sistemi lahko delujejo, tudi če se posamezni elementi odklopijo iz sistema. Porazdeljeni sistemi nimajo samo ene točke okvare.
- Sposobnost naravne rasti – računalniška moč porazdeljenega sistema je rezultat skupne računalniške moči in njenih komponent. Z dodajanjem komponent narašča tudi računalniška moč celotnega sistema.

Pomanjkljivosti porazdeljenih sistemov (Drescher, 2017):

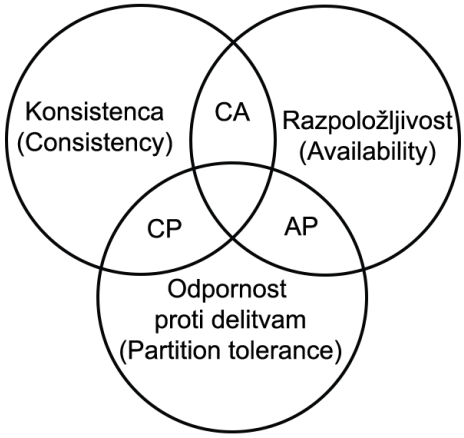
- Povečanje koordinacije in komunikacije – porazdeljeni sistemi nimajo osrednjih subjektov, ki usklajujejo komponente. Koordinacijo in komunikacijo sistema opravijo komponente same med seboj.
- Odvisnost od omrežij – kakršno koli komuniciranje zahteva medij, ki je odgovoren za prenos informacij med subjekti. Komponente v distribuiranih sistemih komunicirajo prek sporočil, ki se prenašajo po omrežju. Brez omrežja sistem ne more delovati, zato je za komuniciranje nujno potrebno omrežje.
- Večja kompleksnost – zaradi zgoraj omenjenih pomanjkljivosti mora vsaka komponenta reševati dodatne težave, kot so koordinacija, komunikacija in uporaba omrežja, kar povečuje zapletenost.

Da bi dobro razumeli distribuiran sistem, je treba na tej točki razložiti teorem CAP (ponazoritev sistema CAP je prikazana na sliki 9), ki ponazarja kompromis distribuiranih sistemom med tremi specifičnimi sistemskimi lastnostmi:

- Konsistenca (angl. Consistency) – lastnost, ki zagotavlja, da ima vsako vozlišče zadnjo kopijo podatkov. Torej dve vozlišči morata imeti vsak trenutek enak zapis podatkov. Če ni te lastnosti, se lahko pri poizvedovanju naleti na napačne podatke.
- Razpoložljivost (angl. Availabilty) – pomeni, da je sistem dostopen za branje in urejanje podatkov kadar koli, brez zamud. Torej, brez omenjene lastnosti pri poizvedovanju ne bi dobili podatka. Sistem ugotovi, da podatek ni osvežen, zato ga ne posreduje.

– Odpornost proti delitvam (angl. Partition tolerance) – zagotavlja, da sistem deluje, tudi če se med nekaterimi vozlišči omrežje prekine.

Slika 9: CAP-teorem



Vir: Drescher (2017).

Cilj vsakega distribuiranega sistema je, da bi imel vse tri lastnosti, vendar je to v temeljih nemogoče. Konkretno pri tehnologiji veriženja blokov ni konsistence, sta pa razpoložljivost in odpornost proti delitvi. Torej, odpornost proti delitvam je povezana z vsakim porazdeljenim sistemom, zato ima omenjeno lastnost tudi tehnologija veriženja blokov. Ker se ne da imeti vseh treh lastnosti, je treba sprejeti kompromis med razpoložljivostjo in konsistenco. To pomeni, da se konsistenca zagotovi šele po določenem časom (angl. eventual consistency), zato ima sistem zagotovljeno razpoložljivost podatkov. Zaradi konsistence obstaja koncept, ki se imenuje algoritem soglasja. Algoritem soglasja je postopek dogovora o enotnem rezultatu med skupino udeležencev, s tem se zagotovi skladnost podatkov. Transakcija se potrdi po določenem času, in sicer po določenem številu potrjenih blokov (Antonopoulos, 2017).

2.6 Pametne pogodbe

Zgodovina pametnih pogodb (angl. smart contracts) sega že v leto 1996. Prvi, ki je opisal koncept pametnih pogodb, je kriptograf in računalničar Nick Szabo. Predvidel je, da bo digitalna revolucija korenito spremenila poslovne odnose, saj bodo pametne pogodbe omogočale nov način formalizacije odnosov. Predvidel je, da se bodo pametne pogodbe razvijale iz predhodnih papirnatih oblik pogodb in jih počasi izpodrinile (Szabo, 1996).

Pametna pogodba je samoizvršljiva pogodba, avtonomni agent, zapisan v računalniški kodi, ki jo upravlja tehnologija veriženja blokov. V kodi so napisana pravila, po katerih se stranke pametne pogodbe dogovorijo za medsebojno sodelovanje. Pametne pogodbe omogočajo izmenjavo sredstev med strankami, ki si ne zaupajo. Popolna preglednost v postopku omogoča, da v postopku ni posrednikov, ki so po navadi nujni zaradi nezaupanja med

strankami. Pogodba deluje avtonomno in neodvisno. Ko so izpolnjeni vsi določeni pogoji, ki so zapisani v pogodbi, se pogodba samodejno izpelje (Blockchain Hub, 2019a).

Vsaka pametna pogodba vključuje tri sestavne dele (Cointelegraph, 2019):

- najmanj dva ali več udeležencev, ki uporabljajo pametno pogodbo. Z uporabo digitalnega podpisa udeleženci izrazijo strinjanje s pogoji sporazuma;
- predmet sporazuma, ki lahko obstaja v okolju pametnih pogodb ali pa v neposrednem dostopu;
- pogoje, ki morajo biti matematično zapisani s programskim jezikom.

Pametne pogodbe delujejo v decentraliziranem okolju, ki podpira uporabo kriptografije javnega ključa in zajema podatke iz odprte in decentralizirane podatkovne baze. Kriptografija javnega ključa omogoča uporabnikom, da se podpišejo oziroma potrdijo transakcijo. Pomembno je, da vsi udeleženci v pogodbi zaupajo v verigo blokov, ki se razume kot vir resnice (Cointelegraph, 2019).

Pametne pogodbe omogočajo avtonomijo in s tem izkoreninijo potrebo po posrednikih. Ker ni potrebe po notarjih, nepremičninskih agentih, klirinških hišah in drugih posrednikih, nastanejo prihranki. Poveča se tudi zaupanje, saj nihče ne more izgubiti podatkov, ti so varno šifrirani in hranjeni v sistemu. Nepristranski sistem pametnih pogodb nadomesti zaupanje med udeleženci.

3 TEHNOLOGIJA ZASEBNEGA IN JAVNEGA VERIŽENJA BLOKOV

V bistvu se lahko tehnologija veriženja blokov deli na zasebno in javno verigo. Glavne razlike med njima so razkritje identitete uporabnikov, hitrost potrjevanja transakcij in to, koliko je sistem decentraliziran.

V splošnem velja, da se tehnologija javnega veriženja blokov uporablja za kriptovalute, ki imajo implementiran algoritem soglasja dokaza o delu. Kot primer uporabe javne verige podatkovnih blokov se lahko vzame najbolj znana kriptovaluta bitcoin. Glavna lastnost javne verige podatkovnih blokov je, da so vse transakcije popolnoma transparentne in javno objavljene. Za prisostvovanje v sistemu ni treba posebne validacije, zato lahko vsak, kdor želi, prispeva k rasti verige blokov. Glavna pomanjkljivost tehnologije javnega veriženja blokov je, da se izredno počasi potrjujejo transakcije v primerjavi s tehnologijo zasebnega veriženja blokov. Ker se lahko vsak pridruži omrežju, to pomeni, da je vedno več vozlišč oziroma subjektov, s katerimi se mora omrežje sinhronizirati, to pa upočasni postopek potrjevanja transakcij. Tehnologija javnega veriženja blokov je primerna za aplikacije, kjer je potrebna transparentnost in se podatki lahko objavijo javno, hkrati pa si deležniki ne zaupajo med seboj (Raj, 2019). Tehnologija javnega veriženja blokov je popolnoma

decentralizirana, zato tudi nihče nima nadzora nad omrežjem, saj ga poganjajo vsi subjekti v omrežju.

Tehnologija zasebnega veriženja blokov se je razvila kot alternativna oblika tehnologije javnega veriženja blokov. Že kot samo ime pove, se pri tehnologiji zasebnega veriženja blokov podatki ne objavijo javno. Pri tovrstni tehnologiji se reši potreba po izvajanju tehnologije veriženja blokov med znanimi deležniki v sistemu. Tehnologija zasebnega veriženja blokov se uporablja predvsem v poslovnih aplikacijah v različnih panogah. V večini primerov se uporablja v dobavnih verigah, programih zvestobe, trgovalnih platformah ... S tehnologijo veriženja blokov se zmanjšajo stroški vzdrževanja tako zapletene podatkovne baze, saj se uporabljajo drugačni algoritmi soglasja. Tehnologija zasebnega veriženja blokov ne uporablja algoritma soglasja, dokaza o delu, zato je tudi energetsko učinkovitejša in hitrejša pri potrjevanju transakcij (Raj, 2019). Ker je hitrejša, je njena narava bolj centralizirana. To pomeni, da je mogoča hitrejša manipulacija zlonamernih akterjev in s tem manjša varnost celotnega sistema. Tehnologija zasebnega veriženja blokov omogoča uporabnikom različne stopnje dovoljenj, zato uporabniki nimajo enakega dostopa do aplikacije. Lahko rečemo, da ima tehnologija zasebnega veriženja blokov izboljšan nadzor nad subjekti omrežja, hkrati pa so tudi jasnejša pravila upravljanja platforme. Pomanjkljivost tehnologije zasebnega veriženja blokov je, da ni popolnoma decentralizirana, torej so vstopne ovire, da se lahko subjekti pridružijo.

Najbolj znani in uporabljeni rešitvi tehnologije zasebnega veriženja blokov sta projekta Hyperledger in zasebno omrežje Ethereum. Ethereum je odprtokodna programska platforma, ki je v bistvu tehnologija javnega veriženja blokov, vendar je odprtokodna rešitev, zato se lahko s pomočjo razcepitve verige omrežje oblikuje kot zasebno.

4 PORAZDELJENI ALGORITMI SOGLASJA

Ena izmed ključnih lastnosti tehnologije veriženja blokov so porazdeljeni algoritmi soglasja. Glede na to, da ideja tehnologije veriženja blokov temelji na decentralizaciji, torej ni centralne entitete, ki bi določala pravila igre, se sistem sam uravnava. Zaradi tega je nujen algoritem soglasja, ki določa pogoje za delovanje omrežja v distribuiranem omrežju. Glavni nalogi algoritmov soglasja sta potrjevanje transakcij in dodajanje novih blokov. V algoritmu soglasja je določeno, kako se bodo transakcije dodajale v blok in s tem zagotovile, da se ista transakcija ne zapiše dvakrat. Ključnega pomen je to, da se vsa vozlišča v sistemu strinjajo z zapisom transakcij. Na delovanje sistema ne bi smelo vplivati niti, če je skupina vozlišč poškodovanih oziroma se vedejo v nasprotju s pričakovanji. Omrežje se mora v celoti dogovoriti o vsaki transakciji, ki se prenaša. Pomembno je tudi, da so vozlišča omrežja razporejena tako, da ni člana ali kartela, ki bi preglasil večino, čeprav bi imeli za to sredstva in motivacijo.

4.1 Dokaz o delu

Dokaz o delu uporablja večino kriptovalut, tudi bitcoin. Rešitev je bila razvita že leta 1992, in sicer za zmanjšanje nezaželene (angl. spam) elektronske pošte. Metoda zahteva, da pri poslanem sporočilu pošiljatelj priloži zraven še dokaz o delu. Prejemnik je torej lahko videl, da je pošiljatelj porabil dodatno energijo za pošiljanje sporočila. S tem je lažje prepoznal nezaželena sporočila. Ideja dokaza o delu je, da se povečajo stroški pošiljanja za nezaželena sporočila in zlonamerno programsko opremo (Dwork & Naor, 1992).

Tudi algoritem soglasja dokaza o delu (angl. proof of work) temelji na ideji, da je treba veliko procesorske moči za gradnjo novega veljavnega bloka, v katerem so potrjene transakcije. V omenjenem algoritmu soglasja vozlišča tekmujejo med seboj, katero bo prvo izračunalo veljavno zgoščeno vrednosti in s tem pridobilo nagrado, ki je v sistemu Bitcoin določeno število kovancev. Če je zgoščena vrednost napačna, je treba prilagoditi vhodne podatke in zgoščeno vrednost spet izračunati. Vsak poskus ima popolnoma drugačno zgoščeno vrednost, zato se poskusi večkrat, dokler se ne najde prava rešitev. Vozlišča računajo matematično uganko, katere rešitev je enostavno dokazati oziroma preveriti. Prvo, ki reši uganko, pošlje rešitev drugim vozliščem v potrditev. Ko se preveri veljavnost rešitve, se doda nov blok v verigi blokov (Bashir, 2017). Če več vozlišč hkrati ugotovi uganko, se potrdi blok, ki se priključi najdaljši verigi. Zaradi tega je treba počakati na več blokov, ki jih omrežje potrdi, da je transakcija dokončno zapisana v verigo blokov. Obstaja verjetnost, da je transakcija vključena v tako imenovani osiroteli ali ločeni blok (Blockchain, 2019).

Spodnja enačba (1) določa nujni pogoj za potrjevanje transakcij in dodajanje novih blokov v verigo. Postopek, v katerem se potrjuje transakcije (Tx) oziroma se išče naključno arbitrarno število (N), ki je rešitev matematične uganke, se imenuje rudarjenje. Za rešitev uganke mora biti izpolnjen pogoj, ki ga določa spodnja enačba. Enačba je sestavljena iz dveh delov. Levi del enačbe predstavlja dvojno zgoščevalno funkcijo (H), ki se ji dodajo naključno arbitrarno število, vrednost zgoščevalne funkcije preteklega bloka in vse transakcije, ki bodo vključene v novem bloku. Med vhodnimi spremenljivkami se v zgoščevalni funkciji najprej izvede bitna operacija ALI, rezultat bitne operacije se poda v dvojno zgoščevalno funkcijo. Desni del enačbe predstavlja težavnost bloka, ki določa, kako velika je še lahko zgoščena vrednost bloka, da je blok potrjen. Težavnost bloka je predstavljena kot 256-bitno število in se skozi čas spreminja, s čimer se zagotovi, da se nov blok naredi približno vsakih 10 minut. Generiranje blokov je Poissonov proces, kar pomeni, da včasih traja eno minuto, včasih pa eno uro, v povprečju pa deset minut, da se najde iskana rešitev. Pri težavnosti obstaja pozitivna korelacija, višja je vrednost težavnosti bloka (angl. target), težje je najti pravo zgoščeno vrednost bloka. Ko rudar najde zgoščeno vrednost bloka, ki je manjša od težavnosti bloka, se blok potrdi in doda v verigo blokov. V sistemu Bitcoin se težavnost posodobi na vsake 2.016 blokov oziroma približno na dva tedna glede na to, koliko blokov se je generiralo v prejšnjem obdobju. Ugotovi se lahko, da je težavnost pomembna komponenta pri motivaciji, saj uganka ne sme biti pretežka zaradi časovne

potratnosti, po drugi strani pa ne sme biti prelahka zaradi varnostnih razlogov napada na omrežje (Bashir, 2017).

H (H (N || Zgoščena vrednost prejšnjega bloka || Tx || Tx … Tx)) < Težavnost bloka (1)

V sistemu Bitcoin je zaradi povečanja težavnosti treba za učinkovito rudarjenje imeti namensko strojno opremo oziroma zelo dobre grafične kartice. Glavni problem pri tem je, da je po eni strani onemogočeno sodelovanje vseh udeležencev, ki si ne morejo privoščiti strojne opreme, po drugi strani pa je še večji problem energetska potratnost. Na primer, omrežje Bitcoin porabi toliko električne energije kot Avstrija na dan 9. 8. 2019 (Digiconomist, 2019).

Ugotovi se lahko, da se za dokaz o delu potrebuje draga strojna oprema, hkrati pa se porabi tudi veliko elektrike za delovanje. Dokaz o delu se zato uvršča med najdražje algoritme soglasja. Na ceno vplivajo dejavniki, kot so velikost omrežja, cena električne energije in cena strojne opreme (Aste, 2016).

Za uspešno delovanje dokaza o delu je potrebna vsaj polovica vozlišč, ki delujejo v korist sistema. V nasprotnem primeru dobijo napadalci dovolj moči za nadzor nad omrežjem. Pri Bitcoinu je to skoraj nemogoč dogodek, saj bi bilo potrebno zelo veliko procesorske moči. Sistem je zasnovan tako, da ni motivacije za odklonsko obnašanje. Napadalcu se bolj izplača, da procesorsko moč usmeri v rudarjenje in za to prejme nagrado v obliki bitcoinov.

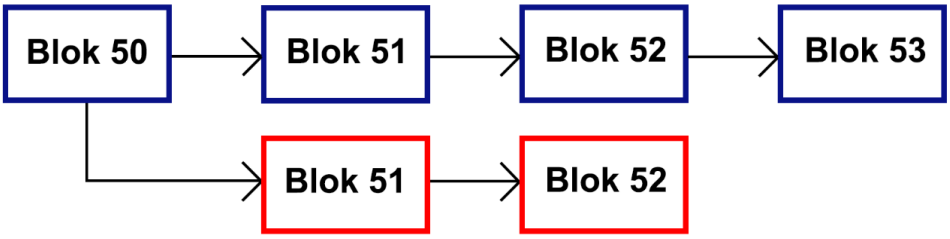
Dokaz o delu se uporablja predvsem pri tehnologiji javnega veriženja blokov, na primer za kriptovaluti bitcoin, ether. Transakcija je varno in dokončno zapisana po določenem številu dodanih blokov. Več kot ima transakcija potrditev, bolj je zapis dokončen. V splošnem velja, da so transakcije Bitcoina dokončne po šestih potrditvah. Glede na to, da se blok generira na deset minut, je treba počakati eno uro, da je transakcija dokončna. Pri omrežju Ethereum se šteje dokončnost pri 20–25 potrditvah. Povprečno se blok doda v verigo vsake 15 sekund, kar pomeni, da je transakcija varno zapisana po šestih minutah.

4.2 Dokaz o deležu

Prva kriptovaluta, v kateri je uporabljen algoritem soglasja dokaz o deležu (angl. proof of stake) se imenuje Peercoin. Leta 2011 je bil pod projektom Ppcoin predstavljen koncept starosti kovanca (angl. coin age), skupaj z dokazom o delu. Za starost kovanca se upošteva, koliko časa uporabnik hrani svoje kovance. Torej kdor ima v lasti večje število kovancev dlje časa, ima največjo možnost, da ga izberejo za potrjevalca bloka (King & Nadal, 2012). Dokaz deleža je alternativna oblika algoritmu soglasju dokaza dela. Rešuje problem čezmerne porabe energije, in sicer tako, da potrjevalec ustvari nov blok glede na status vložka.

Razvijalci, ki programirajo na platformi Ethereum, delajo na protokolu, imenovanem Casper. Pri tem se srečujejo z nekaterimi težavami. Ena izmed njih je napad brez tveganja (angl. nothing at stake problem), ki je prikazan na sliki 10. Torej, obstajata dve verigi – glavna (modra) in odcepljena veriga (rdeča). Daljša veriga je tudi varnejša veriga in jo je težje manipulirati, zato je pomembno, da se transakcije dodajajo samo na glavno verigo. Pri algoritmu soglasja dokaza o delu rudarji nimajo motivacije, da potrjujejo transakcije na obeh blokih, saj za obe verigi porabijo procesorsko moč. Rudar ne bo zapravljal resursov na rdeči verigi, ker ve, da ne bo potrjena. Medtem ko pri dokazu o deležu ni ekonomskih razlogov, zakaj ne bi potrjevali transakcije na obeh verigah, v vsakem primeru je določen delež. Potrjevalec lahko svoj delež preprosto vloži tako v rdečo kot v modro verigo brez kakršnega koli strahu pred posledicami. Ne glede na to, kaj se zgodi, bo vedno pridobil in ničesar ne bo izgubil.

Slika 10: Napad brez tveganja



Vir: Drescher (2017).

Zato se je pri protokolu Casper uvedel postopek, s katerim se kaznujejo vsi zlonamerni potrjevalci. Koncept upošteva idejo, da mora vsak, ki poskuša potrditi transakcijo, pred tem zastaviti določen delež kovancev (angl. staking), ki je večji od transakcijskih provizij. Zastavljeni delež se zaklene za določeno časovno obdobje. S tem se zavaruje, da bo transakcija pravilno zapisana. Če potrjevalec poskuša ponarediti transakcije, izgubi zastavljeni delež. Transakcije se sprva preverijo in po vnovični potrditvi se denarna sredstva podelijo potrjevalcu. Poleg naključnega faktorja je glavna utež, kdo potrjuje transakcijo, delež oziroma število kovancev, ki jih ima vozlišče. Več kot ima vozlišče v lasti kovancev, večja je verjetnost, da bo potrjevalo transakcije (Jain, Arora, Shukla, Patil & Sawant-Patil, 2018). Težava, ki lahko nastane pri tem, je, da ima lahko potrjevalec večinski delež in s tem nadzoruje celotno omrežje, kar pomeni, da lahko potrjuje transakcije, ki niso veljavne. Zaradi tega je pomembno, da ni edino merilo samo delež kovancev. Ena od nevarnosti je tudi ta, da potrjevalec ne potrdi transakcije. Rešitev je lahko, da ima vsak potrjevalec tudi rezervnega potrjevalca.

Medtem ko je platforma Ethereum še na stopnji implementacije, dokaza o deležu imajo nekatere druge kriptovalute, kot sta Cardano in EOS, že uspešno uveljavljen algoritem soglasja o deležu (Yaffe, 2020).

4.3 Praktično bizantinsko soglasje

Vzporednice algoritma soglasja v distribuiranih sistemih so lahko jasne iz zgodovinskih dogodkov, ki so pripomogli k temu, da je prišlo do uspešne uveljavitve v sedanjosti. Zgodovina bizantinskega soglasja (skrajšano BFT) sega v leto 1982, ko je bil izdan članek z naslovom The Byzantine Generals Problem. Vzporednice stanja, v katerem mora sistem obravnavati nasprotujoče si informacije, se lahko abstraktno izrazijo v bizantinski vojski. Generali se morajo med seboj dogovoriti o skupnem načrtu boja, vendar se morajo zavedati, da so med njimi izdajalci. Problem je najti ustrezen algoritem, ki bo zagotovil, da se zvesti generali dogovorijo med seboj o istem ukazu in s tem uspešno izvedejo napad (Lamport, Shostak & Pease, 1982).

Kako bi bilo, če bi se zgodba o bizantinskem imperiju preslikala v tehnologijo veriženja blokov, na primer v sistem Bitcoin. Novi bloki bi se generirali na deset minut, kar pomeni, da bi vsak general potreboval deset minut, da ustvari transakcijo s sporočilom in zraven priloži celotno zgodovino predhodnih transakcij. Če je nekdo izmed generalov izdajalec, bi bilo treba spremeniti vse transakcije za nazaj, saj so povezane. To bi pomenilo dodatni čas, ker se sporočila generirajo na deset minut, zato bi lahko posumili, da je vozlišče zlonamerno.

Leta 1999 se je iz bizantinskega soglasja razvil še bolj praktičen algoritem soglasja, imenovan praktično bizantinsko soglasje (angl. practical byzantine fault tolerance). Praktičen je, ker deluje v asinhronih okoljih, kot na primer na medmrežju. V primerjavi z bizantinskim algoritmom soglasja je imel nekaj optimizacij, zaradi katerih je bil hitrejši kot prejšnji BFT. Algoritem dokazuje, da je mogoče imeti varen sistem, če je več kot dve tretjini generalov zvestih. En izdajalec lahko vpliva in zavede dva zvesta generala.

$$F <= \frac{No-1}{3}. \quad (2)$$

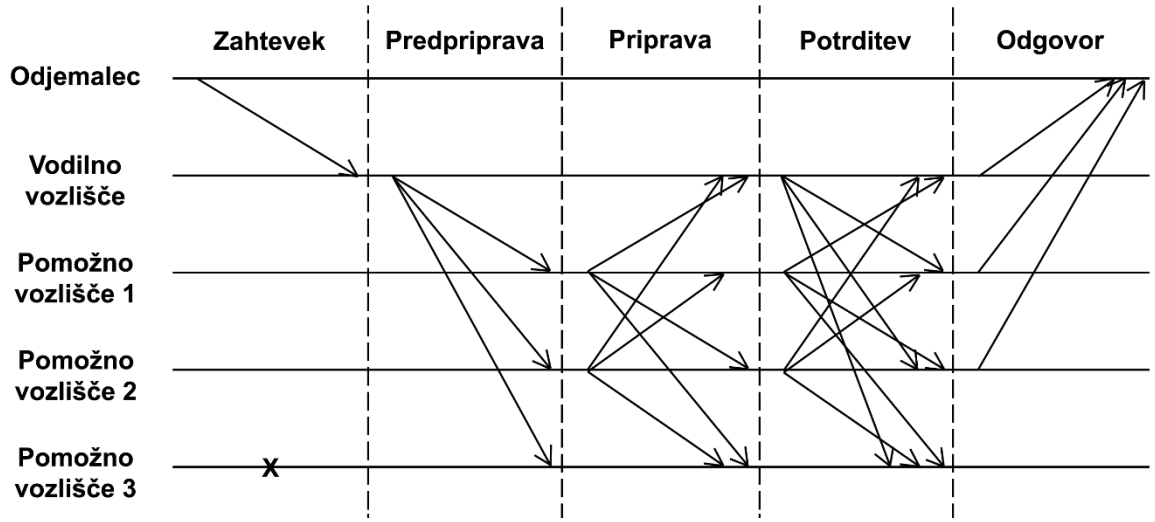
V enačbi (2) je zapis algoritma soglasja, kjer je F konstanta, ki ne sme biti presežena oziroma večja od desne strani enačbe, ki je izračunana. Drugače povedano: F določa maksimum števila slabih vozlišč. Ob tem pogoju bo kljub zlonamernim vozliščem omrežje delovalo pravilno. Oznaka No se določi kot število vozlišč v omrežju (Castro & Liskov, 1999).

Vozlišča v distribuiranem sistemu, ki podpira praktično bizantinsko soglasje, so zaporedno urejena, pri čemer je v vsaki iteraciji eno vozlišče glavno oziroma vodilno vozlišče, druga pa sekundarna oziroma rezervna vozlišča. Cilj je, da vsa poštena vozlišča pomagajo pri doseganju konsenza o stanju sistema z uporabo večinskega pravila.

Spodnja slika 11 prikazuje delovanje algoritma praktičnega bizantinskega soglasja. Na sliki so štiri vozliča. Vodilno vozlišče in tri pomožna vozlišča. Pomožno vozlišče 3 je bizantinsko vozlišče. Ne glede na to, da je eno izmed vozlišč nedelujoče, bo sistem še vedno deloval, ker je izpolnjen pogoj, da mora biti dve tretjini vozlišč pravilnih. Celotni sistem delovanja algoritma soglasja se lahko povzame v naslednjih korakih (Castro & Liskov, 1999):

1. V prvem koraku odjemalec pošlje zahtevo vodilnemu vozlišču.
2. Vodilno vozlišče pošlje zahtevo v druga pomožna vozlišča. To je razvidno na sliki pod korakom, imenovanim predpriprava.
3. Vsa vozlišča (vodilna in pomožna), ki so prejela zahtevo, jo izvedejo in pošljejo odgovor preostalim vozliščem. Na sliki so to koraki predpriprava, priprava in potrditev.
4. V zadnjem koraku odgovor vozlišča posredujejo odgovor odjemalcu.
5. Zahteva je uspešno potrjena, ko odjemalec prejme odgovor F+1 iz različnih vozlišč z enakim rezultatom. Za varno delovanje sistema mora odjemalec počakati F+1 vozlišč na enak odgovor, preden pošlje novo zahtevo. Na sliki je to zadnji korak, imenovan odgovor.

Slika 11: Delovanje algoritma praktičnega bizantinskega soglasja



Vir: Castro & Liskov (1999).

Vozlišča se v sistemu premikajo čez vrsto tako imenovanih pogledov (angl. views). Pogled se določi kot časovno obdobje, ko je eno izmed vozlišč vodilno vozlišče. Vsako vozlišče v tem neskončnem ciklu postane enkrat vodilno. Po potrebi lahko večina poštenih vozlišč glasuje o upravičenosti trenutnega vodilnega vozlišča in ga nadomesti z naslednjim vodilnim vozliščem v vrsti (Castro & Liskov, 1999).

Glavna pomanjkljivost praktičnega bizantinskega soglasja je predvsem v tem, da sistem ne omogoča popolne decentralizacije. Praktično bizantinsko soglasje zahteva, da si udeleženci med seboj vsaj deloma zaupajo. Torej ne more vsak sodelovati, saj se morajo vsi udeleženci strinjati o seznamu deležnikov. Praktično bizantinsko soglasje ni primerno za aplikacije, narejene na tehnologiji javnega veriženja blokov, ker se morajo deležniki med seboj vsaj deloma poznati. Algoritem deluje v nesinhronih sistemih in je optimiziran za visoko zmogljivost pošiljanja transakcij. To tudi pomeni, da ni primeren za sisteme z velikim številom vozlišč.

V primerjavi z algoritmom soglasja dokaza o delu je praktično bizantinsko soglasje hitrejše. Razlog tega je dokončnost bloka, potem ko je potrjen od omrežij. Ni potrebe po čakanju na dodatne potrditve novonastalih blokov tako kot pri dokazu o delu. Pri dokazu o delu vozlišča posebej preverijo vse transakcije, preden se doda nov blok v verigo blokov. Druga prednost, ki jo ima praktično bizantinsko soglasje, je energetska učinkovitost, saj se lahko doseže porazdeljeno soglasje tudi brez izvajanja zapletenih matematičnih računov tako kot pri dokazu o delu.

4.4 Dokaz oblasti

Dokaz oblasti (angl. proof of authority) je prvotno predlagal soustanovitelj Ethereuma Gavin Wood leta 2017, in sicer kot del ekosistema Ethereum za tehnologijo zasebnega veriženja blokov. Dokaz oblasti se lahko razume kot optimiziran in izboljšan algoritem soglasja dokaza deleža. Cilj dokaza oblasti je, da se poudari uporabnikova identiteta in ne, kakšen delež kovancev ima uporabnik. Algoritem temelji na naboru zaupanja vrednih vozlišč, ki se jih pozna kot potrjevalce ali avtoritete. Zavedati se mora, da so potrjevalci tisti, ki zagotavljajo celovitost in zanesljivost sistema, zato obstaja kar nekaj pogojev, kdo lahko postane potrjevalec. Pomembno je, da se identiteta potrjevalca preveri. Vsak, ki želi prisostvovati kot potrjevalec, mora skozi postopek preverjanja, ki je za vse enak in določen vnaprej. Algoritem soglasja dokaza oblasti temelji na ideji, da mora imeti potrjevalec visok ugled, zato je treba narediti selekcijo in dati možnost potrjevanja samo kredibilnim potrjevalcev. Selekcijski postopek zmanjšuje tveganje izbora vprašljivega potrjevalca (Zhang, Schmidt, White & Dubey, 2019).

V spodnji enačbi (3) je razložena formula za logiko delovanja algoritma soglasja, kjer oznaka F pomeni konstanto in oznaka No število vozlišč v omrežju. Sistem deluje optimalno, če je več kot polovica omrežja poštenega. S formulo se lahko to napiše kot:

$$F = \frac{No}{2} + 1. \quad (3)$$

Če je v omrežju samo en bizantinski potrjevalec, pomeni, da ta ne more narediti veliko škode, saj lahko potrjevalec podpiše blok samo enkrat. Na podlagi suma nepoštenega vozlišča ga drugi deležniki v sistemu lahko izključijo.

Glavna kritika algoritma soglasja je v tem, da potrjevalci niso anonimni, saj morajo izdati svojo identiteto. Ker se dela selekcija pri izbiri potrjevalca, pomeni, da sistem tudi ni popolnoma decentraliziran, torej ne morejo prisostvovati vsi. Glavna prednost, ki jo prinaša dokaz oblasti, je predvsem v tem, da ni potrebe po veliki količini elektrike, saj se ne računajo matematične uganke. Pozitivna posledica tega je, da ni treba imeti namenske strojne opreme za izvajanje algoritma soglasja. V primerjavi z dokazom o delu so transakcije mnogo hitreje potrjene in dodane v verigo blokov (Binance, 2019a).

4.5 Dokaz o pretečenem času

Leta 2016 je podjetje Intel, ki se ukvarja predvsem s proizvajanjem čipov, razvilo edinstven algoritem soglasja, imenovan dokaz o pretečenem času (angl. proof of elapsed time). Podjetje je razmeroma zgodaj začelo proučevati distribuiran sistem algoritmov soglasja. Algoritem soglasja o pretečenem času je bil predstavljen kot del projekta, imenovanega Sawtooth. Projekt Sawtooth uporablja dokaz o pretečenem času za sledenje lastništvu morske hrane skozi celotno dobavno verigo: od ribiča do velike samopostrežne trgovine (Rosic, 2017).

Principu delovanja algoritma soglasja dokaza o pretečenem času je zelo podoben algoritem soglasja dokaza o delu. Glavna razlika je v tem, da se pri delovanju ne porabi toliko procesorske moči. Razlog je, da so vozlišča delujoča samo takrat, kadar potrjujejo nov blok. Zato se porabi manj procesorske moči oziroma se porabi samo takrat, kadar je treba, preostali čas pa vozlišča čakajo oziroma so v mirovanju. Model je zasnovan tako, da ima vsako vozlišče enako možnost, da potrdi naslednji blok. Vsakemu udeležencu v omrežju je dodeljen naključni čas za čakanje in prvi udeleženec, ki konča čakanje, potrjuje naslednji blok. Drugače povedano, model je podoben vlečenju slamic. Tisto vozlišče, ki potegne najkrajšo slamico, lahko potrdi blok. Če bi nekdo zagnal več vozlišč, bi imel večjo verjetnost, da postane potrjevalec. Zato se v bistvu algoritem soglasja uporablja za tehnologijo zasebnega veriženja blokov. Potencialni potrjevalci bloka so torej znani, izbrani pa so naključno (Frankenfield, 2018).

Algoritem soglasja dokaza o pretečenem času mora zagotoviti dva pomembna pogoja. Prvi je ta, da si sodelujoča vozlišča naključno izberejo čakalni čas. Drugače bi vsak izbral najkrajši čas in si s tem zagotovil pravico do potrjevanja. Pogoj, ki sledi temu, je, da se preveri potrjevalca bloka tako, ali je zares končal zadano čakalno dobo. Na koncu morajo drugi udeleženci v sistemu preveriti, ali je bil potrjevalec izbran na zakonit način. Če kdo izigra pravilo, se udeleženca doda na črni seznam (Frankenfield, 2018).

Glavna slabost dokaza o pretečenem času je to, da deluje le na specializirani strojni opremi, imenovani Software Guard Extensions oziroma SGX. Težava je, da je edini proizvajalec opreme podjetje Intel. Lahko bi se reklo, da je v nasprotju s tehnologijo veriženja blokov, ki odpravlja zaupanje do posrednikov (Chen in drugi, 2017).

4.6 Primerjava porazdeljenih algoritmov soglasja

Vsi algoritmi soglasja imajo isti cilj, in sicer doseči soglasje v decentraliziranem omrežju. Čeprav imajo mehanizmi skupni cilj, se v pristopu doseganja močno razlikujejo. Čeprav popoln mehanizem za doseganje soglasja še ne obstaja, je zanimivo proučiti in analizirati različne algoritme soglasja po različnih specifikacijah.

V spodnji tabeli 2 so združeni vsi obravnavani algoritmi soglasja in njihove glavne razlike po različnih specifikacijah. Tabela je rezultat lastnega dela in je narejena s pomočjo agregacije predhodno opisanih porazdeljenih algoritmov soglasja. V prvem stolpcu je ime algoritma soglasja, v naslednjem stolpcu je kratek opis tega, na kakšen način se izbere potrjevalec novega bloka. V preostalih stolpcih so ocenjene določene lastnosti algoritma soglasja, in sicer binarno z 0 in 1. Če neka lastnost pripada določenemu algoritmu soglasja, je to označeno z 1. V nasprotnem primeru te lastnosti nima in se to označi s številom 0. Lastnosti oziroma specifikacije, ki jih bom opazovala, so:

- Energetska učinkovitost pove, koliko električne energije je potrebne za potrditev novega bloka. S številom 1 se označi algoritem soglasja, ki je energetsko učinkovit, v nasprotnem primeru je dodeljeno število 0.
- Specifičnost strojne opreme je določena kot potrebna namenska oprema za sodelovanje v sistemu potrjevanja blokov. Če je treba kupiti strojno opremo, ki se uporablja samo za to, da lahko uporabnik sodeluje v sistemu potrjevanja blokov, se to razume kot visoka specifičnost in se označi s številom 1.
- Hitrost potrjevanja transakcij je izredno pomembna lastnost, saj pove, koliko časa potrebuje omrežje, da se sinhronizira med vozlišči in dokončno potrdi predlagani blok. S številom 0 bom označila počasna omrežja in s številom 1 hitra omrežja, kjer se transakcija relativno hitro zapiše v verigo blokov.
- Decentralizacija in anonimnost povesta, kdo vse je lahko v sistemu potrjevanja blokov. Torej, kako anonimen lahko ostane uporabnik, da vseeno postane del omrežja. Čim manjše so vstopne ovire, tem bolj je omrežje decentralizirano. Če lahko vsak sodeluje in mu v zameno za to ni treba izdajati identitete, se to označi s številom 1.

Tabela 2: Primerjava algoritmov soglasja po različnih specifikacijah

Soglasje	**Mehanizem izbire potrjevalca**	**Energetska učinkovitost**	**Specifičnost strojne opreme**	**Hitrost potrjevanja transakcij**	**Decentralizacija in anonimnost**
Dokaz dela	Reševanje matematičnega problema	0	1	0	1
Dokaz deleža	Odstotek deleža	1	0	1	0
Praktično bizantinsko soglasje-PBFT	Glasovalna moč	1	0	1	0
Dokaz oblasti	Reputacija in identiteta	1	0	1	0
Dokaz o pretečenem času	Glede na čas čakanja	1	1	1	0

Vir: lastno delo.

Primerjava algoritmov soglasij prikaže, da je dokaz dela daleč najbolj energetsko potratna oblika potrjevanja blokov. Vzrok za to je, da potrjevalci pri dokazu o delu rešujejo zapletene matematične uganke. Drugi mehanizmi odpravljajo ravno to pomanjkljivost energetske potratnosti, zato so označeni kot energetsko najučinkovitejši.

Naslednja lastnost je specifičnost strojne opreme, pri kateri se opazi, da če je želja biti pri algoritmu soglasja dokaza o delu in dokaza o pretečenem času, je za to nujna namenska strojna oprema. Oba algoritma soglasja se zato označi s številom 1. Pri preostalih mehanizmih ni posebne naložbe v opremo, če bi radi sodelovali v omrežju.

Najpočasnejši algoritem soglasja z vidika hitrosti potrjevanja transakcij je algoritem soglasja dokaza o delu. Pri tem obstaja kompromis med številom vozlišč in hitrostjo potrjevanja transakcij. Več vozlišč kot ima omrežja, dlje časa traja, da se omrežje v celoti sinhronizira in s tem potrdi transakcijo, ki je zapisana v bloku. Zato je tudi tehnologija javnega veriženja blokov počasnejša od tehnologije zasebnega veriženja blokov. Drugi algoritmi soglasja, ki se uporabljajo pri tehnologiji zasebnega veriženja blokov, so zato hitrejši, označijo se kot zelo hitra s številom 1.

Decentralizacija in anonimnost sta lastnosti, ki delujeta v korist dokaza dela, zato se jih označi s številom 1. Uporabnikom omrežja je omogočena popolna anonimnost in zato ni nobenih vstopnih ovir. Deležniki v omrežju so ne poznajo med seboj in nobene potrebe ni po tem, da bi se identificirali. Za preostala soglasja se morajo deležniki v sistemu vsaj deloma poznati in zato tudi identificirati.

5 OMEJITVE IN IZZIVI TEHNOLOGIJE VERIŽENJA BLOKOV

Ker je uporaba tehnologije veriženja blokov še v zgodnjem obdobju množične prilagoditve, je treba proučiti, na kakšne omejitve in izzive naleti. Uporaba tehnologije veriženja blokov trči kar ob nekaj omejitev, ki so tehnične, zakonodajne in varnostne narave.

5.1 Tehnologija veriženja blokov in konvencionalna podatkovna baza

Obstaja veliko primerov uporabe tehnologije veriženja blokov, pri katerih bi bilo bolje, hitreje in ceneje uporabiti konvencionalno podatkovno bazo. Zato je treba dobro razumeti, kdaj je ta tehnologija uporabna. Vedeti je treba, da je v primerjavi s centralizirano konvencionalno podatkovno bazo dražja in počasnejša. Tehnologija veriženja blokov je smiselna, če je več subjektov, ki si med seboj ne zaupajo, vendar želijo sodelovati in skupaj posodabljati podatkovno strukturo.

Smiselno je uporabiti tehnologijo veriženja blokov, kadar obstaja potreba po dolgoročnem shranjevanju podatkov, saj se podatki ohranjajo in reproducirajo. Podatkov na verigi blokov ni mogoče brisati in spreminjati. Nepremičnost se doseže z decentraliziranim algoritmom soglasja. Vsako vozlišče sodeluje v algoritmu soglasja, s katerim preveri, ali je določena

transakcija veljavna. Vsako vozlišče v sistemu ima enako raven dostopa in zmogljivosti, kar daje trden temelj za gradnjo zaupanja, saj demokratizira celoten sistem. V tradicionalni bazi podatkov se je treba zanašati na en sam osrednji organ, ki nadzoruje pravice v sistemu. Centraliziran sistem je dober, če se subjektu, ki sistem nadzoruje, zaupa (Chowdhury, Colman, Kabir, Han & Sarda, 2018).

Pri tehnologiji veriženja blokov so transakcije javno potrjene v sistemu, kar pomeni, da ima vsak deležnik pravico preveriti stanje trenutnega sistema. Vsako transakcijo morajo potrditi potrjevalci. Opazovalci lahko preverijo, ali je bilo stanje spremenjeno v skladu s protokolom, in hkrati tudi vidijo vse transakcije. Medtem v centraliziranem sistemu opazovalci v večini primerov nimajo te pravice, torej ni mogoče pregledati vseh transakcij in predhodnih stanj, ali je bila sprememba pravilna oziroma v skladu s protokolom. Opazovalci morajo zaupati osrednjemu subjektu, ki jim prikazuje ustrezne transakcije in stanja. Podatki so pri tehnologiji veriženja blokov pregledno zapisani, proces posodabljanja podatkovne strukture pa je javno preverljiv (Wüst & Gervais, 2017).

Pomembno je, da med preglednostjo in zasebnostjo obstaja protislovnost. V centraliziranem sistemu je lažje zagotoviti zasebnost, pri tehnologiji veriženja blokov je mogoče doseči zasebnost s kriptografskimi tehnikami. Pri zapisovanju podatkov morajo biti informacije zaščitene pred nepooblaščenimi spremembami oziroma morajo biti podatki pravilni in celoviti. Redundanca podatkov je pri tehnologiji veriženja blokov sama po sebi zagotovljeno z ustvarjanjem kopij med vozlišči. V centraliziranem sistemu se to doseže z ustvarjanjem kopij fizičnih strežnikov z varnostnimi kopijami. Glavna prednost, ki jo prinaša tehnologija veriženja blokov, je predvsem varnost sistema. Ker napadalci nimajo možnosti napasti centralne entitete tako kot pri konvencionalni podatkovni bazi, je kibernetski napad pri decentraliziranih sistemih mnogo težje izvesti. Torej, več kot je vozlišč pri tehnologiji veriženja blokov, varnejši je sistem (Chowdhury, Colman, Kabir, Han & Sarda, 2018).

Razlika med tehnologijo veriženja blokov in centralizirano podatkovno bazo je v hitrosti potrjevanja transakcij. V centralizirani podatkovni bazi je latenca shranjevanja in posredovanja podatkov precej krajša. Tehnologija veriženja blokov je mnogo bolj zapletena, zato ker deluje na principu porazdeljenega algoritma soglasja. Torej je treba več časa za potrditev transakcije, saj se morajo udeleženci strinjati s spremembami. Obstaja pozitivna korelacija med številom udeležencev in hitrostjo potrditev transakcije. Več kot je udeležencev, daljši je čas potrjevanja transakcije.

5.2 Uporaba tehnologije veriženja blokov

Spodnji diagram na sliki 12 povzema bistvenih sedem vprašanja (označena z belim ozadjem), ki se postavljajo pred izvedbo tehnologije veriženja blokov.

Prvo vprašanje je, ali je več strank, s katerimi je treba posodabljati skupno podatkovno bazo. Sistemi, ki imajo samo eno entiteto, lahko uporabljajo druge razmeroma cenejše mehanizme

za doseganje enakih lastnosti, ki jih ima tehnologija veriženja blokov. Potencialno dober primer uporabe tehnologije veriženja blokov je v oskrbovalni verigi, kjer je veliko deležnikov, ki si med sabo ne zaupajo in imajo motivacijo po prekrivanju podatkov. Deležniki se srečujejo z regulativnimi in logističnimi omejitvami, ki segajo čez različne pristojnosti. Tehnologija veriženja blokov je primerna, kadar sta deležnika dva ali več (Lo, Xu, Chiam & Lu, 2017).

Drugo vprašanje se nanaša na to, ali je potreben zaupanja vreden subjekt, torej nekdo, ki je pooblaščen za izvajanje določene dejavnosti. Primer zaupanja vrednega subjekta je lahko banka ali vlada. Tehnologija veriženja blokov je primerna tam, kjer ni potrebe po pooblaščenih avtoritetah ali pa je ta decentralizirana na več deležnikov. Tehnologija veriženja blokov ima porazdeljeno zaupanje, torej ni neke osrednje avtoritete, ki bi odločala.

Tretje vprašanje se nanaša na centralizirano delovanje. Pri tehnologiji veriženja blokov nobeden subjekt v omrežju nima nadzora nad delovanjem in upravljanjem. Zato trenutna konfiguracije tehnologije veriženja blokov ni primerna za sistem, ki zahteva centralizirano delovanje.

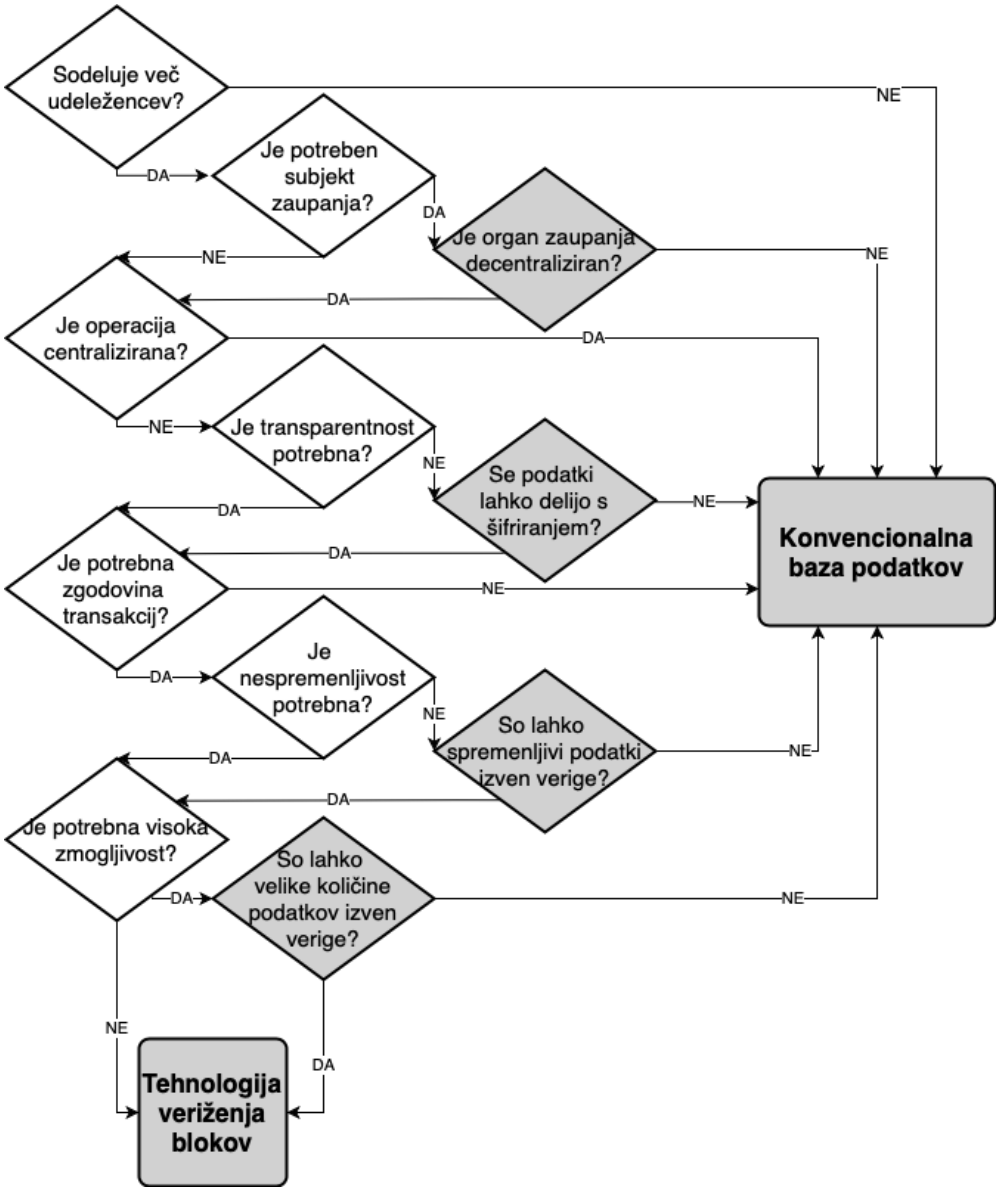
Četrto vprašanje se nanaša na potrebo po preglednosti in zaupnosti. Tehnologija veriženja blokov ponuja platformo, na kateri lahko vsi udeleženci vidijo objavljene podatke. V splošnem velja, da so podatki javno objavljeni, vendar je mogoče, da so podatki šifrirani, preden so dodani na verigo blokov in s tem se poveča zaupnost. Bistveno je proučiti, kateri podatki se zapišejo v verigo blokov na glavno verigo (angl. on-chain) in katere na stransko verigo (angl. off-chain).

Peto vprašanje se dotika celovitosti zgodovine transakcij, ki so zapisane v sistem. Integriteta podatkov v preteklih transakcijah je ključnega pomena za ustvarjanje sledljivosti izvora. Uporaba tehnologije veriženja blokov je smiselna ravno v primerih, kjer je želja zagotoviti sledljivost.

Šesto vprašanje zajema spremenljivost podatkov oziroma to, ali je mogoče, da se bo zapis podatkov spreminjal. Če si stranke med seboj ne zaupajo, morajo vedno imeti na razpolago en vir resnice. Podatkov pri tehnologiji veriženja blokov ni enostavno spreminjati, saj se nenehno kopirajo med vsa vozlišča. Ne glede na vse je treba med zasnovo sistema upoštevati pomisleke v zvezi z zgodovinskimi transakcijami.

Zadnje vprašanje se nanaša na potrebo po velikih zmogljivostih sistema. Trenutno je tehnologija veriženja blokov primerna samo za shranjevanje manjše količine podatkov. Pomembno je, da se samo bistveni podatki zapišejo v verigo. Ne glede na to, se lahko v prihodnosti pričakuje rešitev, ki bo poskušala rešiti težavo shranjevanja velike količine podatkov.

Slika 12: Diagram poteka, ki določa, ali je tehnologija veriženja blokov ustrezna tehnična rešitev



Vir: Lo, Xu, Chiam & Lu (2017).

5.3 Varnost

Od nastanka sistema Bitcoin oziroma od trenutno najvarnejše verige blokov, ki obstaja, je minilo že več kot deset let. Sistem deluje od leta 2009 brez prestanka in brez uspešnih kibernetskih napadov. Na drugi strani je veliko projektov, ki so še v začetni oziroma v testni fazi, kjer se še proučuje uporabna vrednost tehnologije veriženja blokov. Pomembno je, da se pred množično adaptacijo rešitev dobro testira in s tem predvidijo vsi scenariji, ki lahko ogrozijo varnost sistema. Pri implementaciji tehnologije veriženja blokov mora biti koda pravilno zapisana, brez kakršnih koli napak. Hkrati je treba biti pozoren, saj zaradi

decentralizirane narave tehnologije veriženja blokov lahko pride do izvajanja dveh različnih verig oziroma do razcepitve. Treba je tudi razmisliti, kdo bo upravljal zasebne ključe, ker predstavljajo nadzor nad sredstvi.

5.3.1 Zaupanje v kodo

Najbolj znan primer slabe varnosti pri izvedbi tehnologije veriženja blokov sega v leto 2016. Dogodek, ob katerem se lahko veliko nauči, se imenuje s kratico DAO oziroma decentralizirana avtonomna organizacija (angl. Decentralized Autonomous Organization). DAO se lahko opredeli kot sklad tveganega kapitala, ki deluje na pametnih pogodbah. Njihov namen je zagotoviti nov decentraliziran poslovni model za organizacije. Celotni sklad, na katerem se izvajajo pametne pogodbe, je zasnovan na platformi Ethereum. (Blockchain Hub, 2019b).

DAO deluje tako, da skupina razvijalcev napiše pametne pogodbe, ki bodo vodile organizacijo. Nato se izpostavi začetno obdobje financiranja s kratico, poimenovano ICO (angl. initial coin offering), pri katerem ljudje kupujejo žetone (angl. tokens), ki predstavljajo volilno pravico. Žetone se kupuje prek kriptovalute ether, ki deluje na omrežju Ethereum. Ko se obdobje financiranja konča, lahko začne delovati decentralizirana avtonomna organizacija. O porabi denarja, investicijah in vseh drugih odločitvah se demokratično glasuje glede na volilno pravico, ki se pridobi z investiranjem. Eden izmed projektov pod okriljem decentralizirane avtonomne organizacije se je imenoval »the DAO«. Po 28-dnevnem financiranju so skupaj zbrali 150 milijonov dolarjev, in to od več kot 11.000 članov. Pomembno je, da takoj ko je v pametni pogodbi večja količina finančnih sredstev, to pritegne pozornost napadalcev (Siegel, 2016).

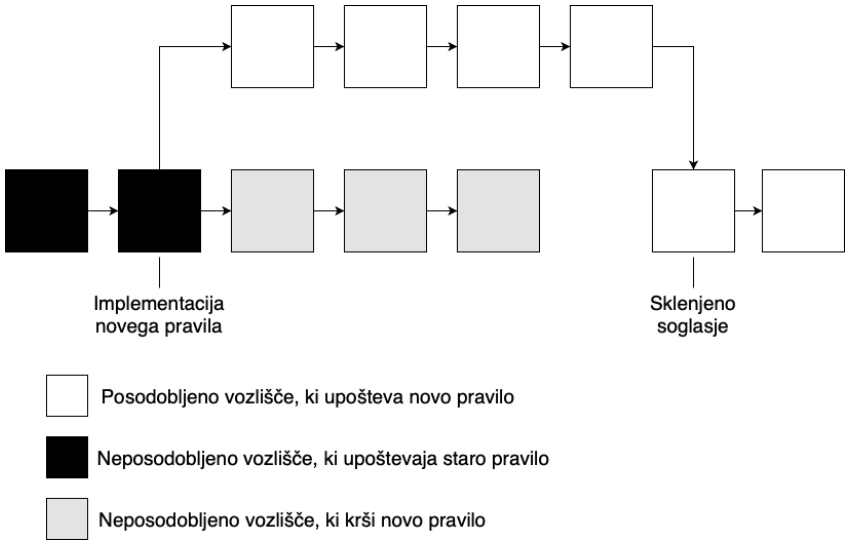
Mehanizem upravljanja, na katerem temelji projekt, je podoben upravljanju delniških družb, s katerimi se trguje na borzi. Ker so želeli zaščititi manjšino od večine, so omogočili, da ob sprejetju predloga, ki ga posameznik ne podpira, vlagatelj dobi vložena sredstva nazaj. Funkcija, ki omogoča uporabnikom povrnitev sredstev, se imenuje cepitev. Napadalci so ugotovili, da ima ravno funkcija cepitve varnostno luknjo (Siegel, 2016). V programski kodi je bila napaka, imenovana rekurzivna napaka klica (angl. recursive call exploit), kar je pomenilo, da so se določeni deli kode začeli rekurzivno ponavljati v neskončnost. Ker razvijalci niso upoštevali možnosti rekurzivnega klica, je napadalec večkrat pridobil sredstva, ki so bila na pametni pogodbi pred posodobitvijo stanja (Martin, 2018). Napadalci so s to napako pridobili dostop do 3,6 milijona ethrov, kar je približno 50 milijonov dolarjev (Reiff, 2019). Poudariti je treba, da platforma Ethereum deluje neodvisno od aplikacije, ki temelji na njej. To pomeni, da omrežje Ethereum deluje brezhibno in nima takšnih napak, kot se lahko najdejo v pametnih pogodbah.

5.3.2 Razcepitev

Ravno tako kot vsaka programska oprema tudi tehnologija veriženja blokov potrebuje stalne posodobitve v programski kodi. Glavni namen tega je, da se odpravijo težave v sistemu ali pa se optimizira zmogljivosti delovanja sistema. Pri tehnologiji veriženja blokov so znani primeri takšne posodobitve, kot recimo dodajanje funkcionalnosti ali pa spreminjanje velikosti bloka. Ker je tehnologija veriženja blokov decentralizirane narave, se morajo udeleženci soglasno dogovoriti o posodobitvah oziroma o novih pravilih delovanja protokola, ta proces se imenuje razcepitev (angl. fork). Sistem lahko deluje samo tako, da udeleženci upoštevajo ista pravila oziroma enak protokol. Zato je nujno, da so vsi seznanjeni s spremembo in imajo pravico odločanja o novi spremembi. Ker je mogoče, da se vsi udeleženci ne strinjajo s predlogom posodobitve, lahko to pripelje do različnih razcepitev verige. V osnovi se razcepitve ločijo na mehko ločitev (angl. soft fork) in grobo ločitev (angl. hard fork).

Mehka ločitev pomeni, da so predlagana nova pravila oziroma spremembe v programski kodi združljive s preteklostjo. Vozlišča, ki ne posodobijo svojega protokola, so zmožna potrditi transakcije in dodajati nove bloke v omrežje. Bloke lahko neposodobljena vozlišča dodajajo v omrežje, dokler ne kršijo novega protokola. Spodnja slika 13 prikazuje mehko ločitev. Vsak kvadrat predstavlja posamezni blok, ki ga vozlišča potrdijo. Kvadrati, ki so obarvani s črno, predstavljajo neposodobljena vozlišča, ki upoštevajo stara pravila. Beli kvadrati predstavljajo posodobljena vozlišča, ki upoštevajo nova pravila. Opazno je, da ob uvedbi novega pravila nastane poleg obstoječe verige še ena začasna veriga. Začasna veriga, ki krši nova pravila, je označena s sivimi kvadrati. Končen rezultat mehke ločitve je ena veriga, potem ko se vsa vozlišča posodobijo na nova pravila (Binance, 2019b).

Slika 13: Prikaz mehke ločitve

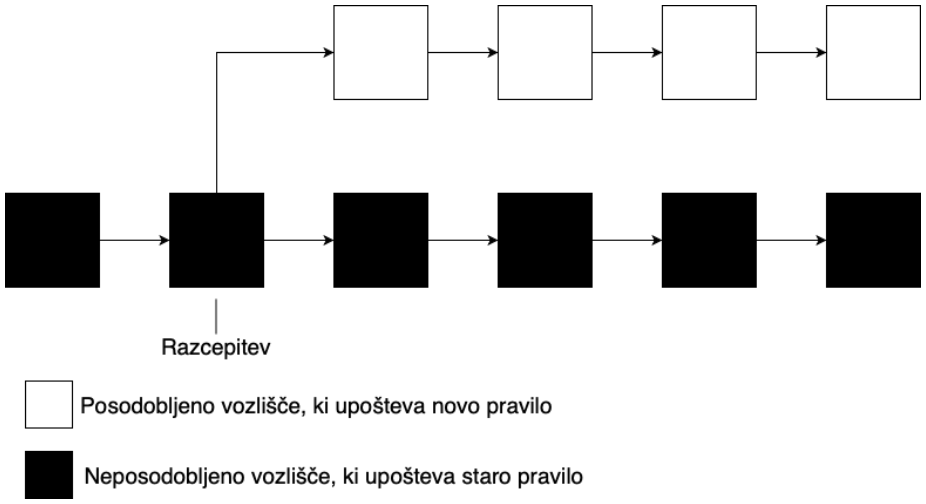


Vir: Frankenfield (2019a).

Primer mehke ločitve je zmanjšanje velikosti posameznega bloka s 4 megabitov na 2 megabita. Vozlišča, ki niso posodobila protokola, lahko še vedno potrjujejo bloke, ki so veliki 2 megabita ali manj. Če neposodobljena vozlišča potrdijo blok velikosti 3 megabitov, bodo blok zavrnili bloki, ki so posodobili svoj protokol. Zato se morajo vsa vozlišča čim hitreje posodobiti na zadnjo različico protokola (Binance, 2019b).

Groba ločitev se lahko vidi na sliki 14, ki se zgodi, kadar sistem preide na novo različico protokola oziroma nova pravila, ki niso združljiva s prejšnjimi. Ker pride do tako korenite spremembe protokola, so prej potrjeni bloki neveljavni za novo verigo. Glede na spodnjo sliko je razvidno, da ob morebitnem spreminjanju pravila v protokolu pride do razcepitve verige. Tako nastaneta dve ločeni verigi, ki se trajno razcepita. Veriga blokov, ki je sestavljena iz črnih kvadratov, predstavlja bloke, ki so jih potrdila neposodobljena vozlišča in upoštevajo stara pravila. Beli kvadrati predstavljajo bloke, ki so jih potrdila posodobljena vozlišča, ki upoštevajo nova pravila (Frankenfield, 2019b).

Slika 14: Prikaz grobe ločitve



Vir: Frankenfield (2019b).

Primer grobe ločitve je povečanje velikosti posameznega bloka z 2 megabitov na 4 megabite. Če bodo posodobljena vozlišča potrdila blok z velikostjo 3 megabitov, ga bodo neposodobljena vozlišča zavrnila. Tako bosta nastali dve nezdružljivi verigi blokov – veriga, ki bo potrjevala bloke, velike do 2 megabitov, in druga veriga, ki bo imela dovoljeno velikost bloka do 4 megabitov. Vsaka veriga bo upoštevala svoja pravila (Binance, 2019b).

5.3.3 Upravljanje zasebnih ključev

Tehnologija veriženja blokov temelji na zagotavljanju identitete prek digitalnih podpisov, ki temeljijo na kriptografiji zasebnih in javnih ključev. Ker lahko vsak, ki ima dostop do zasebnega ključa, premika sredstva, je treba zasebne ključe ustrezno shraniti in zaščititi. Največja varnostna ranljivost tehnologije veriženja blokov so torej lastniki zasebnih ključev,

saj se velikokrat ne zavedajo posledic, ki lahko nastanejo zaradi neupoštevanja varnostnih pravil. Glavni problem nastane pri izgubi ali kraji zasebnih ključev, saj s tem napadalec pridobi dostop do sredstev.

Ena izmed potencialnih rešitev se imenuje »multi-signatures«. Pri tej rešitvi je za odobritev transakcije nujen več kot en digitalni podpis. Pri implementaciji »multi-signatures« je treba opredeliti, kdo ima pravico odobriti transakcije in pogoje, pri katerih pride do odobritve transakcije. Torej pravico do odobritve si lahko lasti pet subjektov, pogoj za odobritev transakcije pa je potrditev vsaj dveh subjektov (Binance, 2019c).

5.3.4 Kibernetski napadi

Tehnologija veriženja blokov omogoča, da se distribuirana mreža vozlišč s pomočjo algoritmov soglasja odloča o vsaki transakciji in s tem omogoči varno zapisane transakcije. Največji dodani vrednosti tehnologije veriženja blokov sta varnost in zanesljivost sistema, ki nima veliko varnostnih lukenj. Vendar so v zelo skrajnih razmerah mogoče tudi varnostne težave, kot recimo napad Sybill (angl. Sybill attack) in 51-odstotni napad (angl. 51 % attack).

Napad Sybill izkorišča pomanjkljivost tehnologije veriženja blokov, ki sloni na popolnoma enakovrednih vrstnikih v omrežju. Napadalec poskuša nadzirati delovanje celotnega sistema in vplivati nanj z več lažnimi vozlišči. To pomeni, da je napadalec sposoben nadzorovati odločitve omrežja, in sicer tako, da vpliva na algoritem soglasja. Napad Sybill je predvsem težaven pri tehnologiji javnega veriženja blokov, saj uporabnikom ni treba razkriti identitete. Obstajajo nekatere omejitve v sistemu za povečanje varnosti in zmanjšanje potencialnega napada Sybill. Ena od rešitev je, da je nemogoče ustvariti veliko vozlišč v kratkem času. Takšne omejitve so znane pri algoritmu soglasja dokaza o delu. Če se želi ustvariti novo vozlišče, je treba imeti računalnik z določeno procesorsko močjo. Ker so s tem povezani finančni stroški, je napadalcu težje izvesti napad. Način boja proti napadom Sybill se lahko reši tako, da se vzpostavi zaupanje, preden se novo vozlišče pridruži sistemu. Eden izmed načinov je, da imajo lahko vozlišča, ki so že dlje časa prisotna in dejavnejša v sistemu, možnost povabiti nova vozlišča. S tem se omeji nenadzorovano povečevanje vozlišč. Ne glede na vse mogoče ukrepe je napad Sybill zelo težko preprečiti, saj včasih lahko pride do prekrivanja in lažnih vozlišč (Garner, 2018).

Naslednji napad, ki lahko ogrozi varnost sistema, je tako imenovani 51-odstotni napad. Primer takšnega napada so aplikacije, ki temeljijo na algoritmu soglasja dokaza o delu. Sistem je lahko ogrožen, kadar ima napadalec več kot polovico procesorske moči, ki bi jo lahko izkoriščal sebi v prid. Ta bi pomenila, da bi napadalec lahko spremenil vrstni red transakcij ali pa bi transakcijo izbrisal in spreminjal. Ker je napad odvisen od velikosti omrežja, je za nekatere sisteme, na primer za kriptovaluti bitcoin ali ethereum, skoraj nemogoč, saj je v sistemu preveč vozlišč in s tem povezane procesorske moči. Dejstvo je, da z dodajanjem novih blokov v verigo postanejo spremembe v začetnih blokih vedno težje. Več kot je nadaljnjih blokov, dražja bo sprememba v bloku, saj je treba spremeniti celo

verigo blokov, ki so med seboj povezane. Poleg vsega naštetega napadalec ne bi imel finančnih motivov za takšno početje, saj bi bila finančna naložba za dosego 51-odstotne celotne procesorske moči omrežja velika (Binance, 2019d).

5.4 Zakonodajne ovire

Kot pri vseh novih tehnologijah predstavljata regulativa in zakonska opredelitev vedno velik izziv, po eni strani regulatorjem in po drugi strani upravljalcem sistema ter končnim uporabnikom. Najprej je treba ugotoviti, kje točno bi se nova tehnologija lahko uporabljala in na katera področja zakonodaje posega.

5.4.1 Zakonodaja in pametne pogodbe

Ena izmed največjih zmogljivosti tehnologije veriženja blokov je uporaba pametnih pogodb. Poleg avtomatiziranega izvajanja je bistvo pametnih pogodb, da se same izvedejo. Primer pametne pogodbe je, da je v njej med najemnikom in najemodajalcem opredeljeno, da mora najemnik najemnino poravnati 1. v mesecu. Obveznost plačevanja najemnine bo izvedena samodejno, izvedbi pa se ni mogoče izogniti. (Fulmer, 2019).

Na področju zasebnega prava obstaja veliko odprtih vprašanj, ki jih bodo regulatorji in zakonodajalci proučevali. Glavno vprašanje se nanaša predvsem na to, kdo bo prevzel odgovornost, če je pogodba napačno sprogramirana. Naslednje vprašanje se nanaša na gotovost določitve identitete pogodbenih strank, saj s tem lahko stranka odgovarja za svoja dejanja. Na koncu sledi tudi vprašanje, kdo je odgovoren v primeru sporov v pogodbi. Z vidika javnega prava obstaja skrb, če stranki želita prekiniti pogodbo in nočeta, da se transakcija izvede, čeprav je pogoj izpolnjen. Pri pametnih pogodbah je nemogoče doseči, da bi pogodbo prekinili, torej ni mogoče manipulirati z njo in vplivati nanjo (Deloitte Touche Tohmatsu Limited, 2019).

V prihodnosti se lahko pričakuje, da bodo pametne pogodbe verjetno spoštovale enaka pravila kot tradicionalne pogodbe. Največji izziv pri tem bo prevesti besedni jezik v programsko kodo, tako da bo lahko delovala na tehnologiji veriženja blokov. Za zagotovitev, da se dogovor strank natančno odraža v programski kodi, bosta potrebni jasnost in natančnost pri interpretaciji strankinih želja. Ne glede na vse zakonske in regulatorne omejitve pametnih pogodb bi si lahko stranki z njihovo pomočjo znatno zmanjšali stroške in pridobili učinkovitost z avtomatizacijo pogodb (Fulmer, 2019).

5.4.2 Uredba o varstvu osebnih podatkov

Evropska unija si prizadeva zaščititi temeljne pravice o varstvu osebnih podatkov fizičnih oseb, zato je od maja 2018 naprej začela veljati uredba o varstvu osebnih podatkov (angl.

General Data Protection Regulation – GDPR) oziroma krajše GDPR. Uredba se v določenih segmentih razhaja s splošnimi koncepti tehnologije veriženja blokov.

Ker osebne podatke dobro varuje zakonodaja, je treba najprej razložiti, kaj so osebni podatki. Skladno z uredbo je osebni podatek vsak podatek, s katerim se lahko določi posameznika. To so, na primer, ime, priimek, naslov, e-poštni naslov, telefonska številka, IP-naslov … Razvidno je lahko, da so tudi javni ključi osebni podatek, saj se lahko neposredno ali posredno nanašajo na identifikacijo fizične osebe (European Parliament, 2019).

V uredbi o varstvu osebnih podatkov je opredeljeno, da ima posameznik pravico do vpogleda vseh podatkov, ki se zbirajo o njem. V 16. in 17. členu uredbe je opredeljeno, da se lahko podatki na zahtevo posameznika tudi zbrišejo ali spremenijo. Poudariti je treba, da je spreminjanje in brisanje podatkov pri aplikacijah, ki uporabljajo tehnologije veriženja blokov, zelo oteženo in praktično skoraj nemogoče. Prepovedano je tudi, da so osebni podatki šifrirani s pomočjo šifrirnih funkcij in zapisani na verigo blokov, kjer jih ni mogoče brisati in spreminjati. Razlog za to je, da so šifrirani podatki še vedno osebni podatki (European Parliament, 2019).

Uredbo o varstvu osebnih podatkov morajo spoštovati upravljavci podatkovnih baz, ki so lahko fizične ali pravne osebe. Upravljavci podatkovnih baz, ki obdelujejo in hranijo osebne podatke, morajo izpolnjevati obveznosti, ki so zapisane v uredbi. Ker tehnologija veriženja blokov temelji na decentraliziranosti, torej ni fizične ali pravne osebe, na katero se lahko posameznik obrne v zvezi z uveljavitvijo pravic, je to v nasprotju z uredbo. Težko bi tolmačili, kdo je odgovoren za kršenje uredbe, glede na to, da sta skupna lastništvo in nadzor nad podatkovno bazo (European Parliament, 2019).

6 UPORABA TEHNOLOGIJE VERIŽENJA BLOKOV V ENERGETIKI

Ne glede na to, da je tehnologija veriženja blokov sprva zaživela v finančnem svetu, jo danes proučujejo na veliko različnih področjih, kot na primer na področju zdravstva, dobavne verige, zavarovalništva in tudi v energetiki. Smernice v energetiki kažejo na to, da se tehnologija veriženja blokov ponuja kot ena izmed mogočih tehnologij, ki bi lahko pomagala pri energetski tranziciji. V članku z naslovom »Blockchain technology in the energy sector« je narejena raziskava, na katerih področjih v energetiki se tehnologija veriženja blokov najbolj razvija. V spodnji tabeli so zapisani rezultati analize, v kateri so analizirali več kot 140 projektov. V prvem stolpcu so napisana področja, na katerih delujejo aplikacije, zraven pa je napisan delež, ki izhaja iz študije o 140 pobudah v energetskem sektorju (Andoni in drugi, 2018).

Tabela 3: Razvrščanje primerov uporabe tehnologije veriženja blokov glede na njihovo področje dejavnosti

Klasifikacija projektov, ki delujejo na tehnologiji veriženja blokov glede na namen in področje dejavnosti	**Delež projektov**
Decentralizirano trgovanje z energijo	33
Kriptovalute in žetoni	19
Avtomatizacija in pametne naprave	11
Merjenje in odčitavanje	9
Upravljanje omrežja	8
Zeleni certifikati in trgovanje z ogljikovimi kuponi	7
Električna e-mobilnost	7
Pobude in konzorciji za splošne namene	6

Vir: Andoni in drugi (2018).

Na podlagi zgornje tabele 3 je razvidno, da je skoraj vsak tretji projekt povezan z decentraliziranim trgovanjem. Večina aplikacij je usmerjenih predvsem na omogočanje dostopnosti trgovanja med proizvajalci in kupci oziroma na neposredno trgovanje. Obstajajo tudi ideje, povezane s področjem trgovanja na veleprodajnih energetskih trgih (Andoni in drugi, 2018).

Na drugem mestu z 19 odstotki so projekti, povezani s kriptovalutami in žetoni. Kriptovalute in žetoni so lahko instrument za nagrajevanje želenega vedenja, predvsem za vlaganje v zeleno energijo. Eno izmed idej ima podjetje SolarCoin, ki uporablja kriptovaluto za nagrajevanje proizvodnje energije z nizko vsebnostjo ogljika in s tem spodbuja zeleno energijo. Podjetje podeljuje vsakemu uporabniku kriptovaluto, imenovano SolarCoin, ki proizvaja elektriko iz sončne energije. Kriptovaluto uradno priznava Mednarodna agencija za obnovljivo energijo in jo je mogoče zamenjati za druge kriptovalute ali fiatvalute (Andoni in drugi, 2018).

Na tretjem mestu z 11 odstotki so projekti, ki delujejo na področju avtomatizacije in pametnih naprav. Eno izmed podjetij, ki deluje na tem področju, je finsko energetsko podjetje Fortum, ki ponuja potrošnikom nadzor nad napravami. Rešitev omogoča optimiziranje naprav za porabo energije, pri tem se upoštevajo vremenska napoved, napoved porabe energije in cene električne energije v realnem času (Andoni in drugi, 2018).

Od vseh izbranih projektov ima 9 odstotkov projektov možnost, da se bo njihova tehnologija uporabljala za postopke merjenja in odčitavanja. Večina podjetij je razvijala svoje ideje predvsem v smeri avtomatiziranega obračunavanja energetskih storitev za porabnike, saj bi s tem zmanjšali stroške upravljanja. Ker tehnologija veriženja blokov omogoča sledljivost proizvedene in porabljene energije, bi lahko porabnike obveščali o izvoru in stroških njihove oskrbe z energijo. Poleg tega bi bili izboljšani zaščita podatkov in odpornost proti kibernetskim grožnjam. Na področju kibernetske varnosti in odčitavanja pametnih števcev deluje britansko podjetje Electron. Podjetje razvija platformo za registracijo pametnih

števcev za plin in elektriko ter s tem naprednih tehnik šifriranja, ki jih omogoča tehnologija veriženja blokov (Andoni in drugi, 2018).

Projekti, povezani z upravljanjem omrežja, predstavljajo 8 odstotkov vseh projektov, ki delujejo na tehnologiji veriženja blokov. Projekti temeljijo na avtomatizaciji in decentraliziranem upravljanju omrežja. Glavna izboljšava, ki bi jo lahko prinesla tehnologija veriženja blokov, je lažje uravnoteženje in usklajevanja ponudbe in povpraševanja na omrežju. Če se bo vse razvijalo v smeri tehnologije veriženja blokov, bi bilo treba prilagoditi merilne naprave in celotno omrežno infrastrukturo. Na področju upravljanja omrežja deluje tudi pilotni projekt Gridchain, ki simulira procese v prihodnosti in s tem omogoča lažje upravljanje omrežja v realnem času. (Andoni in drugi, 2018).

Od vseh 140 projektov jih deset predstavlja projekte, povezane z zelenimi certifikati in trgovanjem z ogljikovimi kuponi. Enega izmed projektov je razvila svetovna borza Nasdaq, ki je že leta 2016 preizkušala trgovanje z zelenimi certifikati. Proizvajalci, ki so proizvajali sončno energijo, so dobili certifikate, s katerimi so lahko trgovali prek Nasdaqove platforme. Z uporabo pametnih pogodb so tudi omogočili samodejno izdajanje in sledenje potrdil o obnovljivi energiji (Andoni in drugi, 2018).

Tehnologija veriženja blokov je zaradi svoje decentralizirane narave in omogočanja usklajevanja med več deležniki uvedena tudi na področju električne e-mobilnosti, skupaj to področje predstavlja 7 odstotkov projektov. Koordiniranje vozila, voznika, polnilne postaje in potnikov je eden izmed izzivov trenutne električne e-mobilnosti. Eden izmed projektov, imenovan Car eWallet, je razvil platformo, ki zapiše transakcije storitev, med njimi tudi polnjenje avtomobila in dajanja avtomobila v najem (Andoni in drugi, 2018).

Preostali projekti, 6 odstotkov, spadajo pod področje pobud in konzorcijev za splošne namene in delujejo v smeri raziskovanja aplikacij, ki uporabljajo tehnologije veriženja blokov. Raziskovalna pobuda Blockchain Futures Lab proučuje tehnologijo veriženja blokov in njen vpliv na družbo, ekonomijo in politiko. Tudi Evropska komisija je ustanovila EU Blockchain Observatory and Forum, ki spremlja in podpira adaptacijo tehnologije veriženja blokov v Evropi (Andoni in drugi, 2018).

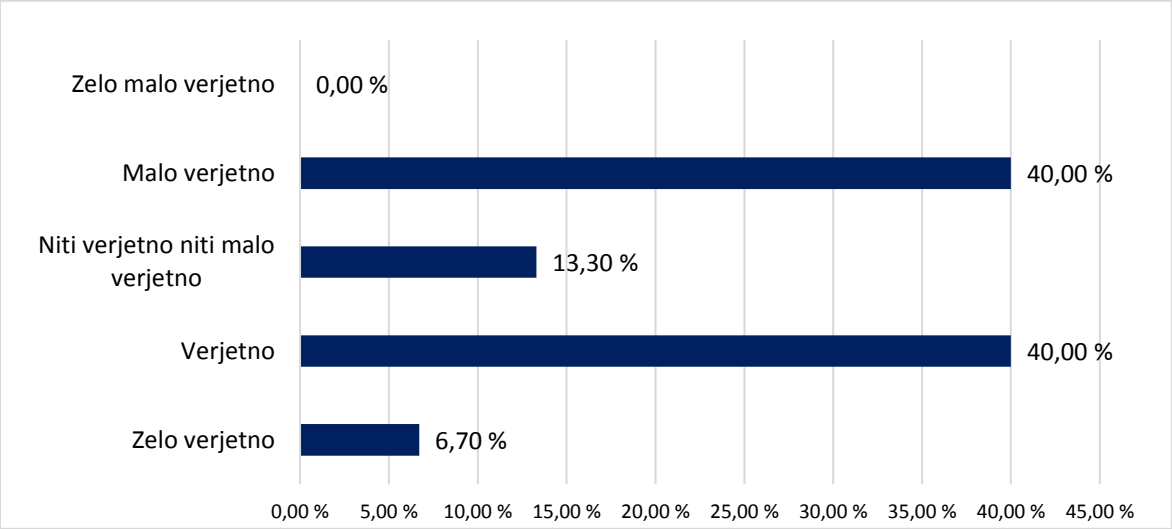
Članek ugotavlja, da večina projektov opazi največ poslovnih priložnosti v konceptu neposrednega trgovanja. Da je večina idej na temo trgovanja, je lahko razvidno iz tega, da je omenjeno področje najbližje finančni industriji, iz katerega se je tehnologija veriženja blokov razvila.

Ker je energetika izredno regulirana in strateška dejavnost, je treba ugotoviti, kakšno mnenje imajo strokovnjaki energetike o novi tehnologiji veriženja blokov. V članku z naslovom »Blockchain Technology and Electricity Wholesale Markets« je bila narejena raziskava o uporabi tehnologije veriženja blokov na področju trgovanja z električno energijo na veleprodajnem trgu. Na anketo so odgovarjali zaposleni, večinoma iz Nemčije, ki delujejo v energetskih podjetjih, javnih agencijah, raziskovalnih inštitutih in drugih podjetjih, ki

delujejo na področju energetike. Več kot večinsko, s 62,5 odstotka, so odgovorili, da bo neposredno trgovanje prvi primer uporabe, ki se bo komercialno uvedel v Evropski uniji s pomočjo tehnologije veriženja blokov (Dick & Praktiknjo, 2019).

Na spodnji sliki 15 so odgovorili na vprašanje: »Kako verjeten je scenarij, v katerem bodo platforme peer-to-peer nadomestile vse trge ali njihovo veliko večino?« Odgovori na to vprašanje so dokaj uravnoteženi med možnostmi: malo verjetno in verjetno (Dick & Praktiknjo, 2019).

Slika 15: Odgovor na anketno vprašanja: »Kako verjeten je scenarij, v katerem bi platforme peer-to-peer nadomestile vse trge ali njihovo veliko večino?«



Vir: Dick & Praktiknjo (2019).

Na podlagi raziskave lahko ugotovimo, da zaposleni v energetiki niso usklajeni v razumevanju vloge tehnologije veriženja blokov v prihodnosti. Ne glede na vse je spodbuden podatek, da jih več kot polovica meni, da bi lahko neposredno trgovanje nadomestilo vse trge oziroma njihovo veliko večino.

6.1 Opis problema

V magistrski nalogi sem proučila možnost uporabe tehnologije veriženja blokov kot rešitev za izzive, ki bodo nastali v energetskem sektorju v prihodnosti. Sprva je bila narejena raziskava za ustrezno rešitev, nato je sledila dejanska izvedba rešitve. Aplikacija je bila prvotno narejena za ameriški trg, vendar sem jo za potrebe magistrske naloge prevedla v slovenščino in prilagodila za trgovanja z elektriko v Sloveniji. Na koncu sledi kritična analiza rešitev s predlogi za izboljšavo in opisom nadaljnjega razvoja aplikacije.

Današnja oblika trgovanja z električno energijo ne omogoča neposrednega decentraliziranega trgovanja med kupci in prodajalci. Zdaj pomeni trgovanje z elektriko

kupovanje in prodajanje elektrike od drugih bilančnih shem pod določenimi pravili in pogoji. Vsak, ki želi sodelovati, potrebuje poleg finančnega vložka tudi časovni vložek. Da bi aktivni uporabnik dobičkonosno prodal ali poceni kupil svojo elektriko, mora imeti veliko znanja o trgovanju. Po koncu trgovanja je treba napovedati sistemskemu operaterju proizvodnjo in odjem elektrike. O vsaki transakciji morajo biti obveščeni tudi regulatorji. Tako trgovanje z energijo, kot tudi preostale dejavnosti, ki sledijo, vzamejo veliko časa in znanja, zato zdaj to odgovornost prevzemajo dobavitelji elektrike. S pomočjo ustreznih tehnologij in prilagoditvijo procesov se bodo v prihodnosti procesi spremenili.

Najtežji izziv je ugotoviti, na katerem področju tehnologija veriženja blokov ponuja nove priložnosti. Vedno bolj liberaliziran energetski trg omogoča vedno večjo decentralizacijo celotnega sistema. Z vidika produkcije vse več uporabnikov posredno podpira trajnostno uvajanje distribuirane proizvodnje energije, ki temelji na lokalno razpoložljivih obnovljivih virih energije. Obnovljivi viri energije so postali najhitreje rastoči vir električne energije in s tem prispevajo k večji razpršenosti virov energije. Ker bo proizvodnja električne energije dosegljiva vsakemu, lahko v prihodnosti pričakujemo, da bo vedno več uporabnikov v sistemu. Malim proizvajalcem električne energije, ki so trenutno izolirani od sistema, bi lahko s pomočjo tehnologije veriženja blokov omogočili lažje sodelovanje v sistemu. To bi pomenilo, da bi tehnologija veriženja blokov omogočala dvosmerno interakcijo med uporabniki v omrežju. Uporabniki bi lahko trgovali v decentraliziranem sistemu trgovanja. Neposredno decentralizirano trgovanje z elektriko med uporabniki upošteva koncept »peer to peer«. Za uporabo koncepta »peer to peer« je treba imeti decentralizirano platformo, na kateri se dva posameznika med seboj neposredno sporazumevata, brez posredovanja tretje osebe.

Koncept »peer to peer« je bil opisan leta 2007 v članku z naslovom »Peer-to-Peer Networks Applied to Power Grid«, vendar takrat še ni bilo ustreznih tehnologij, da bi idejo uresničili. V članku je ugotovljeno, da so omrežja, ki temeljijo na konceptu »peer to peer«, primerna izbira za električna omrežja zaradi dinamičnosti, možnosti samoorganiziranja in decentralizirane narave sistema (Beitollahi & Deconinck, 2007).

Energetska tranzicija daje vedno več poudarka na lokalnost. S tem so mišljena lokalna energetska omrežja, ki lahko delujejo samostojno ali pa so povezana v večja omrežja. Poleg neodvisnosti lokalnega energetskega omrežja takšne mikromreže znižujejo izgube v omrežju, ki nastanejo s prenosom elektrike.

Ne glede na to, da je tehnologija veriženja blokov še v povojih, so nekatere njene ključne značilnosti skladne s specifikacijami, ki bodo uporabne v prihodnosti, tudi na področju trgovanja z elektriko. Tehnologija veriženja blokov omogoča trgovanje brez centralnih institucij, ki so v trgovalnem sistemu borze. Tradicionalni model trgovanja z električno energijo postavlja trgovalni sistem kot center vseh transakcij. To pomeni, da mora vsak, ki želi trgovati, zaupati borzi. Tehnologija veriženja blokov pa omogoča, da se transakcije pošiljajo med uporabniki brez posrednikov, zaupanje pa se porazdeli med uporabnike. Vsak

udeleženec v sistemu ima popolnoma enako kopijo vseh transakcij, ki jih ni mogoče brisati in spreminjati. Za centralizirano trgovanje z električno energijo je potrebna akreditacija centralnega subjekta, ki nam omogoči pravico do trgovanja. Pri tehnologiji veriženja blokov pa ne poznamo centralnega subjekta, ker je ta pristojnost razporejena bolj demokratično med vse subjekte oziroma vsa vozlišča v sistemu.

Na podlagi opisanega diagrama poteka iz slike 12, ki določa, ali je tehnologija veriženja blokov ustrezna tehnična rešitev, si je treba odgovoriti na zastavljena vprašanja. Ugotovljeno je bilo, da je uporaba tehnologije veriženja blokov namenjena za več udeležencev, ki posodabljajo skupno podatkovno bazo in si med seboj ne zaupajo. Pri trgovanju z elektriko imamo veliko udeležencev, ki si med seboj pošiljajo podatke, na primer kupce, prodajalce, banko in sistemskega operaterja. Med njimi obstajajo navzkrižni interesi, zato si med seboj ne zaupajo. To govori v korist uporabe tehnologije veriženja blokov. Zdajšnje trgovanje z električno energijo poteka na podlagi zaupanja v subjekt zaupanja, kar je po navadi določena borza ali drugi posredniki. Tehnologija veriženja blokov je smiselna, kadar ni zahteve po centraliziranem delovanju. Glede na to, da se trgovanje z energenti vedno bolj spreminja in postaja vedno bolj decentralizirano, predvsem z vidika produkcije. Vedno več virov energije bo treba prodati na trgu, kar pomeni, da je v tem pogledu tehnologija veriženja blokov primerna rešitev. Sledijo vprašanja, ki se nanašajo na transparentnost, zgodovino in nespremenljivost podatkov. To, da se pri tehnologiji veriženja blokov zapišejo podatki tako, da jih vidijo vsi udeleženci v sistemu, je dobro zaradi transparentnosti. Podatkov tudi ni mogoče spreminjati, zato ostanejo zapisi za vedno. Javni in celovit zapis zgodovine transakcij je pomembna funkcija, saj s tem lahko dokažemo, kdaj in med katerimi uporabniki so se transakcije zgodile. S tem lahko pohitrimo določene procese, na primer to, da je treba vsako transakcijo, ki se zgodi med prodajalcem in kupcem, prijaviti pristojnemu regulatorju. Če bi regulator imel dostop do transparentno zapisanih transakcij, bi jih lahko pregledal kar sam. Na koncu se vprašamo, ali je potrebna visoka zmogljivost prenašanja podatkov v omrežju. Glede na problem hitrosti in velikosti prenašanja podatkov v omrežju, je nujno, da se omeji število uporabnikov omrežja. Manjše kot je število uporabnikov, hitrejši bo prenos podatkov. Zato bi bila smiselna uporaba tehnologije veriženja blokov pri trgovanju z elektriko na drobnoprodajnem trgu.

6.2 Izbira orodja

Ideja je simulirati uporabo tehnologije veriženja blokov, ki temelji na konceptu trgovanja »peer to peer« na mikroomrežju z obnovljivo električno energijo med uporabniki. Namen aplikacije je ponazoriti neposredno in decentralizirano trgovanje z električno energijo prek tehnologije veriženja blokov. Aplikacija temelji na ideji, da se bo v prihodnosti vzpostavil liberaliziran mikrotrg v takšni obliki, kot je trenutno veleprodajni trg. To pomeni, da bi mali proizvajalci elektrike lahko svojo energijo prodajali po dogovorjeni ceni na distribucijskem omrežju.

Pri izbiri orodja sem se osredotočila predvsem na rešitve, ki omogočajo hitro potrjevanje transakcij. Ker je ideja simulacija trgovalne platforme, ki deluje na mikroomrežju z razmeroma malo udeleženci, ki živijo v isti soseski, se lahko predvideva, da se uporabniki med seboj vsaj deloma poznajo. Hitro potrjevanje transakcij in deležnikov v sistemu, ki si deloma zaupajo, nakazuje na uporabo tehnologije zasebnega veriženja blokov. Glavna prednost tehnologije zasebnega veriženja blokov je to, da se aplikacijo lažje razvija, saj so transakcije bolj zasebne, kar pomeni prednost, da ničesar ne objavimo javno.

Sprva sem proučila dve rešitvi tehnologij zasebnega veriženja blokov, to sta Hyperledger Farbric in zasebno omrežje Ethereum. Analiza dveh rešitev je opisana v članku z naslovom »Performance Analysis of Private Blockchain Platforms in Varying Workloads«. Članek osvetli težavo zmogljivosti, ki je največja težava tehnologije veriženja blokov. V članku je opredeljena latenca, kot razlika med časom, ko transakcijo pošljemo v omrežje, in časom, ko je transakcija potrjena. Ugotovljeno je bilo, da je povprečna latenca pri majhnem številu transakcij približno dvakrat hitrejša pri Hyperledger Fabric. Pretočnost je v članku opredeljena kot število transakcij na sekundo, ki jih potrdi sistem. Testiranje pokaže, da ima Hyperledger večjo pretočnost v primerjavi s platformo Ethereum. Na koncu je bila testirana tudi zmogljivost sistema, test je potekal tako, da se je sočasno poslalo 10.000 transakcij, in postopek se je ponovili večkrat, dokler sistem ni sporočil napake. Izkaže se, da ima Hyperledger Farbic večjo omejitev, saj je sistem zmožen obdelati 20.000 transakcij, medtem ko je omrežje Ethereum zmožno procesirati 50.000 sočasnih transakcij. V članku je bilo torej ugotovljeno, da je latenca in pretočnost podatkov mnogo večja na razvojnem okolju Hyperlegerj Fabric, medtem ko omrežje Ethereum lahko obravnava več transakcij sočasno (Pongnumkul, Siripanpornchana & Thajchayapong, 2017). Pri vsaki rešitvi so določene prednosti, ki imajo veliko težo pri razvoju aplikacij. Za razvoj decentralizirane trgovalne platformo sem na koncu kot najboljšo rešitev izbrala Hyperledger Farbic.

V magistrski nalogi sem za simuliranje trgovalne platforma uporabila rešitev Hyperledger Fabric, ki izhaja s projekta Hyperledger. Tega je leta 2015 ustanovil Linux Foundation in je eden izmed najbolj znanih projektov, ki uporabljajo tehnologijo veriženja blokov (Rosic, 2018). Glavni cilj projekta je olajšati sodelovanje med različnimi podjetji in razvijalci. Danes ima projekt več kot 250 članov, med njimi so tudi velika podjetja, kot so IBM, SAP, Huawei, Samsung, Intel … (Hyperledger, 2018).

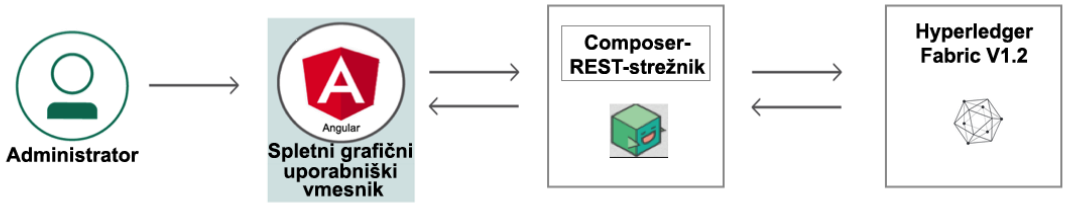
Krovna strategija Hyperledger je spodbujati veliko vrst različnih poslovnih aplikacij tehnologije veriženja blokov. Zaradi različnosti so Hyperledeger razdelili na naslednje projekte (Rosic, 2017):

- Projekt Hyperledger Sawtooth je zasnovalo podjetja Intel. Glavna značilnost platforme je uporaba algoritma soglasja dokaza o pretečenem času.
- Projekt Hyperledger Iroha je ustvarilo nekaj japonskih podjetji, da bi ustvarila ogrodje za projekte.

- Projekt Hyperledger Burrow razvija pametne pogodbe za projekte, ki uporabljajo tehnologijo zasebnega veriženja blokov.
- Projekt Hyperledger Explorer je zasnovala organizacija Linux Foundation zato, da ustvari do uporabnika prijazno spletno aplikacijo, kjer bi lahko preveril podatke, povezane s transakcijami, bloki in drugimi podatki.
- Projekt Hyperledger Indy je zbirka orodij, knjižnic za ustvarjanje decentralizirane digitalne identitete.
- Projekt Hyperledger Cello želi biti operacijska nadzorna plošča, ki je potrebna za upravljanje in uporabo tehnologije veriženja blokov.
- Projekt Hyperledger Composer je ogrodje za razvoj in lažje razvijanje aplikacij, ki uporabljajo tehnologijo veriženja blokov. S pomočjo Hyperledger Composer lahko hitro in enostavno razvijamo aplikacije tehnologije veriženja blokov, saj omogoča lažjo komunikacijo med uporabniškim vmesnikom in Hyperledger Fabricom.
- Projekt Hyperledger Fabric je modularna, varna in odprtokodna rešitev za razvijanje aplikacij, zasnovalo jo je podjetje IBM. Modularna struktura omogoča prilagajanje funkcionalnosti, kot sta na primer izvedba različnih algoritmov za šifriranje podatkov ali izvedba različnih algoritmov soglasji. Ker je Hyperledger Fabric odprtokodno razvojno okolje, lahko vsi prosto dostopajo do nje in jo uporabljajo ter po želji spreminjajo.

Za trgovalno aplikacijo sem uporabila orodje Hyperledger Composer 0.20 in razvojno okolje Hyperledger Fabric različice 1.2. Ker orodje Hyperledger Composer podpira obstoječo infrastrukturo Hyperledger Fabric, to omogoča poenostavljen razvoj aplikacije. Uporabniški vmesnik je implementiran s pomočjo ogrodja Angular verzije 7.0.0. Ogrodje Angular omogoča aplikaciji dinamično spreminjanje strani in prikazovanje statičnih komponent. Komunikacija med uporabniškim vmesnikom Angular in razvojnim okoljem Fabric je izvedena v zalednem sistemu uporabniškega vmesnika, napisanega v programskem jeziku Typescript, in orodju Composer, ki ga izvajamo s pomočjo ogrodja Node.js 8.15.1. Node.js ustvarja virtualno okolje, v katerem se izvajajo zaledne aplikacije, in dinamično pošilja vsebino na uporabniški vmesnik. Podatkovna baza za shranjevanje transakcij, ki jo uporablja Fabric, je couchDB. Trgovalna platforma se izvaja na operacijskem sistemu Linux, distribucija Ubuntu 18.04 LTS in orodju Docker 18.09.5. Docker omogoča hitro in lažjo namestitev okolja za zaganjanje aplikacije. Izvorna programska koda uporabniškega vmesnika in aplikacije je bila pridobljena na spletni gostiteljski rešitvi Github, in sicer na IBM-ovem repozitoriju, imenovanem Decentralized-Energy-Composer (Github, 2019). Celotni sistem je bil testiran v lokalnem okolju.

Slika 16: Delovanje aplikacije



Vir: Github (2019).

Slika 16 prikazuje delovanje aplikacije, ki poteka prek spletnega grafičnega uporabniškega vmesnika, ki je oblikovan na platformi Angular. Aplikacija obdela uporabniške zahteve in jih posreduje prek REST API (angl. Representiational State Transfer Application Program Interface) klicev, implementiranih s Hyperledger Composer. REST API je aplikacijski vmesnik, ki sprejema podatke, jih obdela in vrne odgovor glede na zahtevo. Primer takega klica REST API je preverjanje lastništva sredstev uporabnika, ki želi izvesti transakcijo. Prek Composer-REST-strežnika poteka komunikacija med zalednim sistemom uporabniškega vmesnika in Hyperledger Fabric-om. Hyperledger Fabric je sestavljen iz več delov, kot so vozlišča, veriga blokov, razvrščevalna vozlišča, potrjevalna vozlišča, veriga kod. Za pridobivanje stanja verige blokov se uporablja REST API. Uporabniški vmesnik trgovalne platforme pridobi podatke prek REST API klicev (Github, 2019).

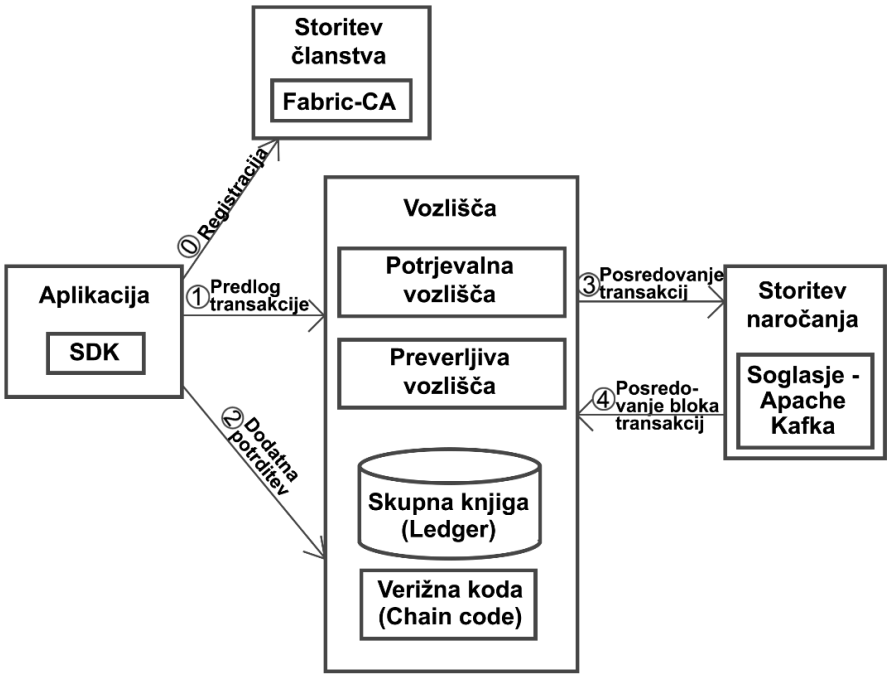
Vloge v razvojnem okolju Hyperledger Fabric:

- Odjemalec aplikacije (angl. client) je v tem primeru uporabniški vmesnik trgovalne platforme, prek katerega uporabnik vnaša podatke in izvaja akcije. Uporabniški vmesnik z zalednim sistemom izvaja klice v imenu osebe, ki predlaga transakcijo v omrežje.
- Vozlišča (angl. peers) so odgovorna za ohranitev stanja omrežja. V osnovi jih delimo na dve vrsti vozlišč, in sicer na potrjevalna vozlišča (angl. endorsment peer) in preverljiva vozlišča (angl. commiter peers). Potrjevalna vozlišča so tista, ki simulirajo in potrdijo predlog transakcije, medtem ko preverljiva vozlišča preverijo transakcijo, ki je že bila simulirana.
- Storitev naročanja (angl. ordering service) sprejme potrjene transakcije in jih razporedi v bloke.

Spodnja slika 17 prikazuje proces potrjevanja transakcij v razvojnem okolju Hyperledger Fabric. Še pred začetkom se uporabnik registrira v storitev članstva (angl. membership service), kar je na sliki označeno s številko 0. Identiteta uporabnika se preveri s storitvijo Fabric-CA. Fabric-CA zagotavlja prikazovanje podatkov glede na pooblastila uporabnika. V ustvarjeni aplikaciji je narejen administratorski profil, ki daje vpogled v vse zapisane podatke. Ko uporabnik dobi pravico do uporabe aplikacije, lahko začne pošiljati transakcije. Transakcija se začne z uporabniškim vnosom podatkov po uporabniškem vmesniku trgovalne platforme. Nato aplikacija SDK (angl. Software Development Kit), ki deluje v

zaledju uporabniškega vmesnika trgovalne platforme, prebere vnesene podatke, generira predlog transakcije in jo posreduje potrjevalnim vozliščem. To lahko vidimo na shemi pod številko 1. Vsako potrjevalno vozlišče simulira predlagano transakcijo tako, da preveri pravilnost izvedbe pametne pogodbe. Logika, na podlagi katere delujejo pametne pogodbe za potrjevanje transakcije, je zapisana v verižni kodi (angl. chain code). Verižna koda definira poslovno logiko aplikacije in s tem zagotavlja, da se vse transakcije, ki prenašajo lastništvo, potrjujejo pod enakimi pravili in pogoji. Povedano drugače, v verižni kodi se določijo parametri za spremembo lastništva digitalnega sredstva. Konkretno v tem primeru se preveri, ali ima kupec dovolj kovancev na računu, prodajalec pa dovolj elektrike. Nato vozlišča še ne zapišejo transakcije v verigo blokov, ampak sporočijo aplikaciji SDK zahtevo o zavrnitvi oziroma odobritvi transakcije. Aplikacija SDK preveri potrditve predloga transakcij in primerja odgovore predlogov. Če je treba, SDK pošlje predlog transakcije še preostalim udeležencem v procesu, kar je določeno s poslovnimi pravili. Ta korak je na spodnji sliki označen s številko 2. Pri tehnologiji veriženja blokov morajo biti transakcije zapisane v skupno knjigo (angl. ledger), in to v doslednem zaporedju, za kar je potrebno soglasje. V tretji točki se transakcija pošlje v aplikacijo, t. i. storitev naročanja (angl. orderer service). Aplikacija skrbi za soglasje, kar pomeni, da sprejme in preveri transakcije iz omrežja in jih kronološko razvrsti v bloke. Urejene bloke storitev naročanja v točki 4 posreduje preverljivim vozliščem. Preverljiva vozlišča bloke s transakcijam še enkrat pregledajo in dokončno zapišejo blok v verigo blokov. Če je transakcija zavrnjena, bo še vedno zapisana v blok, vendar označena kot neveljavna (Merz, 2019).

Slika 17: Proces potrjevanja transakcij v razvojnem okolju Hyperledger Fabric

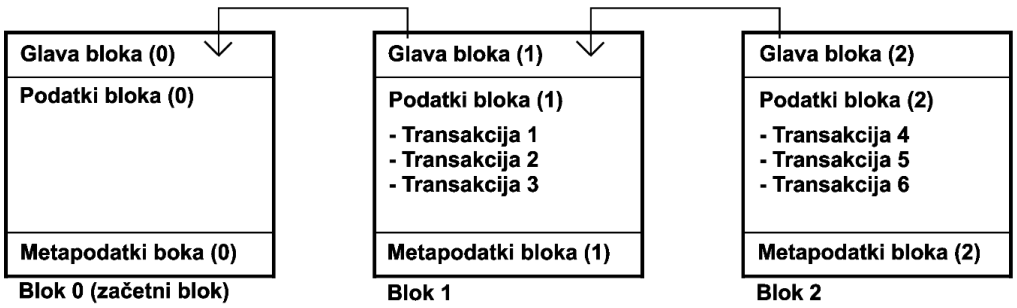


Vir: Merz (2019).

Doseganje dogovora in soglasja o enotnem zapisu transakcij je ključnega pomena pri vsakem trgovalnem sistemu. Pri izvedbi tehnologije veriženja blokov je treba določiti, kateri algoritem soglasja za potrjevanje transakcij bo aplikacija uporabljala. Na podlagi članka, ki proučuje 140 projektov v energetiki, je bilo ugotovljeno, da večinski delež s 55 odstotki predstavlja dokaz o delu. Na drugem mestu sledi praktično bizantinsko soglasje s 15 odstotki. Sledi dokaz oblasti s 13 odstotki in dokaz o pretečenem času s 3 odstotki. Drugi algoritmi soglasja, ki so uporabljeni pri projektih, predstavljajo 14 odstotkov (Andoni in drugi, 2018). Konkretno, arhitektura Fabric 1.2 je zasnovana tako, da za algoritem soglasja poskrbi storitev naročanja. Storitev naročanja je komponenta, ki jo je mogoče vključiti in izključiti iz aplikacije. Hyperledger Fabric omogoča uporabo različnih algoritmov soglasja, med njimi tudi praktično bizantinsko soglasje. V tem primeru sem izbrala privzeto storitev za naročanje, imenovano Apache Kafka, ki deluje s pomočjo storitve Zookeeper. Apache Kafka uporablja strukturo voditelja in sledilcev, zato je zelo odporna proti napakam, dokončnost transakcije pa se zgodi v nekaj sekundah. Vodilno vozlišče je tisto vozlišče, ki razporeja transakcije in ustvarja nove bloke. Storitev Zookeeper skrbi, da je samo eno vozlišče vodilno vozlišče. Če je vodilno vozlišče nedejavno oziroma ne deluje, Zookeeper poskrbi in določi novo vodilno vozlišče. Omenjeno soglasje ima nekatere dobre lastnosti, recimo to, da je energetsko učinkovito in hitro pri potrjevanju transakcij (Hyperledger-fabric, 2019).

Spodnja slika 18 prikazuje delovanje razvojnega okolja Hyperledger Fabric. Kot je razvidno, je vsak blok sestavljen iz treh delov, in sicer glave (angl. block header), podatkov (angl. block data) in metapodatkov bloka (angl. block metadata). Bloki so med seboj povezani prek glave bloka. Glava bloka je oštevilčena in vsebuje trenutno zgoščeno vrednost bloka in zgoščeno vrednost prejšnjega bloka. V strukturi podatkov bloka so razporejene vse transakcije po časovnem vrstnem redu. Metapodatki bloka so šifrirani in vsebujejo podatke o digitalnih podpisih, javnih ključih in o veljavnosti transakcije (Bchainledger, 2019).

Slika 18: Arhitektura in povezava med bloki v razvojnem okolju Hyperledger Fabric



Vir: Bchainledger (2019).

Za šifriranje, ki predstavlja zaščito in varnost podatkov, se uporablja zgoščevalna funkcija SHA256. Vsaka transakcija vsebuje tudi digitalni podpis, ki omogoča lažje preverjanje podatkov o transakciji.

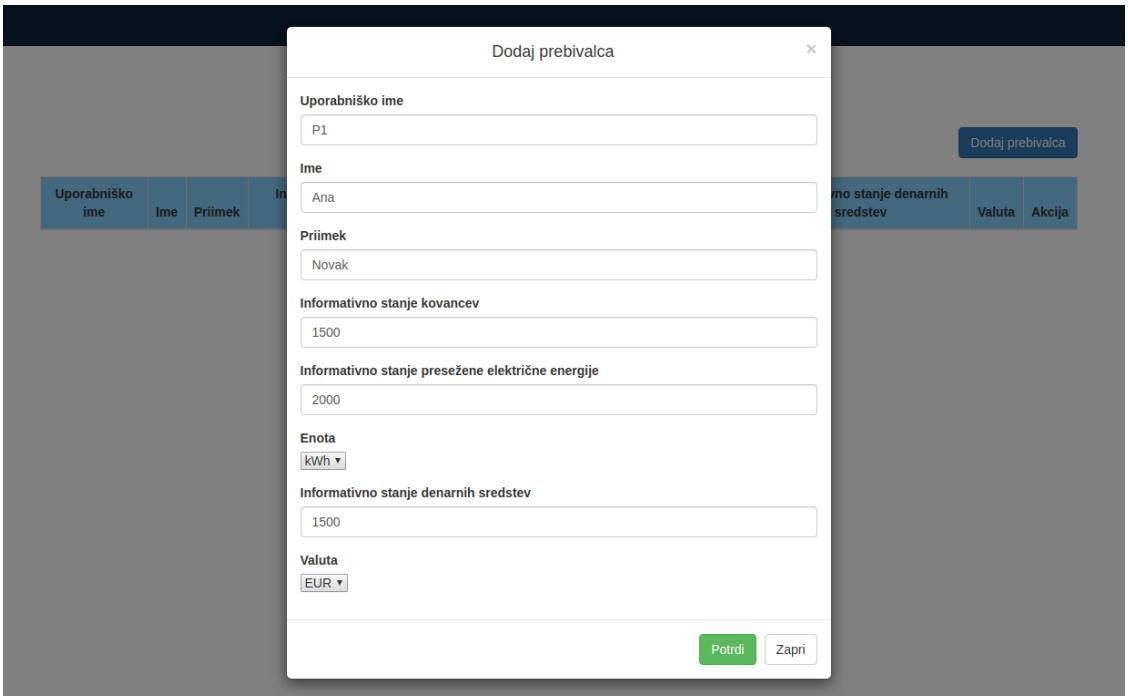
6.3 Delovanje aplikacije

Aplikacija je namenjena uporabnikom, ki si bodo med seboj izmenjevali elektriko in kovance. Za prisostvovanje se uporabljajo certifikati, ki so izpeljani iz zasebnih in javnih ključev, kar se uporablja za identifikacijo uporabnikov. Vsak uporabnik ima dostop le do svojih sredstev, ki jih lahko upravlja. Pri transakcijah se preveri veljavnost certifikata in s tem zasebnih ključev, ki omogočajo uporabnikom upravljati lastništvo s svojimi sredstvi. S certifikati se določajo tudi omejitve dostopa, to pomeni, do katerih podatkov lahko uporabnik dostopa. Aplikacija je namenjena prebivalcem, ki so povezani v isto mikroomrežje, operaterju distribucijskega omrežja in banki. Prebivalce delimo na kupce, ki samo kupujejo elektriko iz omrežja, in dejavne uporabnike, ki so hkrati porabniki in proizvajalci električne energije. Dejavni uporabniki oskrbujejo svoja gospodinjstva z električno energijo, proizvedeno iz obnovljivih virov energije, hkrati pa odvečno elektriko oddajajo v omrežje. Če dejavni uporabnik nima dovolj lastnih zmogljivosti, tudi sami sodelujejo kot odjemalci elektrike. Zaradi tehničnih razlogov je treba omejiti, da se elektriko prodaja samo med tistimi kupci in prodajalci, ki so v omrežje povezani prek iste transformatorske postaje. Zato lahko dejavni uporabniki ponudijo elektriko samo odjemalcem, ki so priključeni v isto lokalno omrežje. Veliko vlogo ima tudi operater distribucijskega omrežja, ki skrbi za stabilnost sistema, kar pomeni, da skrbi za deviacije, ki nastanejo pred fizično dobavo. Eden izmed subjektov v aplikaciji je tudi banka, ki je odgovorna predvsem za pretvarjanje kovancev v valuto in obratno. Ker elektrike ne moremo neposredno kupovati in prodajati z evri, so kovanci za povezovalni člen.

Aplikacija omogoča transakcije med prebivalci, med prebivalcem in sistemskim operaterjem ter med prebivalcem in banko. V aplikaciji je prikazano, da se digitalna sredstva izmenjajo, kar se zapiše na verigi blokov in na koncu lahko vse transakcije vidijo vsi udeleženci. Digitalno sredstvo, ki se premika med vozlišči, je denar v valuti evro, elektrika v enoti kilovatne ure in kovanci. S tem lahko kupec sledi, od kod je kupil energijo in za koliko, prodajalec pa lahko vidi, komu jo je prodal.

Spodnje slike prikazujejo transakcijo med prebivalcema, ki trgujeta po fiksnem menjalnem tečaju. Za lažji pregled funkcionalnosti trgovalne aplikacije dostopamo do aplikacije iz administratorskega profila. Spodnja slika 19 prikazuje potrebne podatke, ki jih ima vsak prebivalec, ki bi želel prodati ali kupiti elektriko. Poleg osebnih podatkov profil vsebuje tudi informativno stanje presežne električne energij v kilovatnih urah oziroma kWh, stanje kovancev in finančno informativno stanje v evrih.

Slika 19: Prikaz dodajanja novega prebivalca v aplikaciji



Vir: lastno delo.

Naslednja slika 20 prikazuje transakcijo med dvema uporabnikoma, torej kupcem na eni strani in prodajalcem na drugi. Ker je aplikacija poenostavljena, je fiksen menjalni tečaj, in sicer 1 kovanec predstavlja 1 kWh. V tem konkretnem primeru prodajalec pod šifro P1 proda 100 kWh elektrike kupcu pod šifro P2. S klikom na gumb »potrdi transakcijo«, prodajalcu P1 se prišteje 100 kovancev in odšteje 100 kWh elektrike, kupcu P2 pa se odšteje 100 kovancev in prišteje 100 kWh elektrike. Ker je menjalni tečaj vnaprej določen, se morata kupec in prodajalec dogovoriti o količini, ki jo bosta izmenjala.

Slika 20: Transakcija med dvema prebivalcema

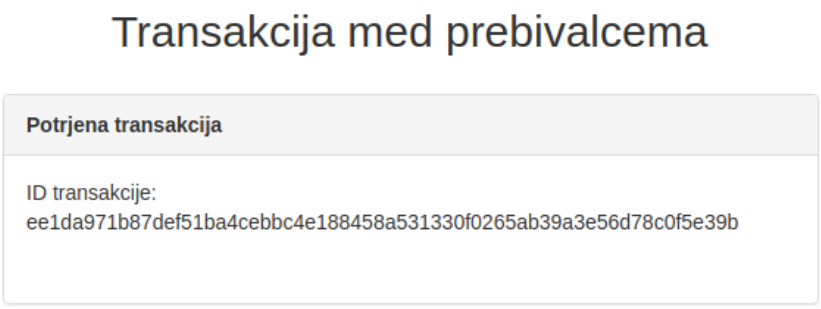
Vir: lastno delo.

Vsaka transakcija dobi svojo zgoščeno vrednost, ki je šifrirana z algoritmom SHA 265, z njo lahko preverimo zapisane informacije. Vsaka zgoščena vrednost vsebuje tudi časovni žig, ki nam pove, kdaj se je transakcija zgodila. To pomeni, da je v transakciji zapisano, katero vozlišče je premaknilo digitalno sredstvo do drugega vozlišča.

Spodnja slika 21 prikazuje zgoščeno vrednost zgornje transakcije, ki je v aplikaciji poimenovana kot ID transakcije. V konkretnem primeru je zgoščena vrednost transakcije med P1 in P2 naslednja:

ee1da971b87def51ba4cebbc4e188458a531330f0265ab39a3e56d78c0f5e39b.

Slika 21: ID transakcije oziroma zgoščena vrednost transakcije



Vir: lastno delo.

Zaradi uporabe tehnologije veriženja blokov se transakcije ne morejo spreminjati. Aplikacija omogoča, da transakcije v sistemu lahko pregledujejo vsi uporabniki.

6.4 Analiza in ocena delovanja aplikacije

Glavni prednosti, ki ju aplikacija ponuja, sta lažji dostop in odprava ovir do trga z električno energijo, saj uporabnik potrebuje samo certifikat, ki ga podpira aplikacija. Aplikacija približa trg končnemu uporabniku, saj jo lahko uporabljajo vsi prebivalci v soseski. Ker s tem opolnomočimo ljudi, lahko pričakujemo več dejavnih uporabnikov na trgu. Aplikacija upošteva smernico, ki poudarja večjo demokratičnost, saj omogoča večjo vključenost in udeležbo pri trgovanju z elektriko. Ker so vsi udeleženci v sistemu enakovredni, je smiselna uporaba tehnologije veriženja blokov, ki zagotovi decentralizirano in neposredno delovanje, ki deluje na konceptu »peer to peer«. Decentralizacija je tudi ena izmed smernic, ki se bo dotikala ljudi v prihodnosti. Iz tega se lahko sklepa, da z decentralizirano trgovalno platformo tako kupci kot prodajalci v tem modelu zmagajo. Po eni strani aplikacija omogoča, da lahko porabniki izbirajo prodajalca, torej lahko kupujejo elektriko od znanega vira elektrike. Če porabnik raje kupuje od specifičnega vira oziroma soseda, mu je to omogočeno. Ker prebivalci soseske proizvajajo elektriko iz obnovljivih virov, se s tem podpira

brezogljična družba in s tem povezana smer dekarbonizacije. S pomočjo tehnologije veriženja blokov se izpostavi sledljivost, kar pomeni, da kupci točno vedo, iz kod izvira elektrika. Po drugi strani prodajalci lahko prodajajo odvečno električno energijo sosedom v soseski. S tem se izognemo izgubi v omrežju, ki nastane zaradi pretoka. Transakcije so izvajajo neposredno med prebivalci, kar pomeni, da nimamo v tem modelu nobenih posrednikov in velikih trgovcev z električno energijo. Aplikacija spodbuja, da prebivalci v soseski dejavno sodelujejo v sistemu, torej ni velikih centralnih objektov, ki zagotavljajo elektriko. Ker kupci in prodajalci zaupajo v tehnologijo veriženja blokov, ni potrebe po centralni instituciji. Tehnologija veriženja blokov zagotovi, da so vse transakcije transparentno zapisane, zato velja med kupci in prodajalci popolna preglednost.

Aplikacija sloni na vseh smernicah, ki se bodo postavile v prihodnosti. S tem je mišljeno, da delovanje decentralizirane aplikacije podpira brezogljično družbo, ki omogoča dejavnim uporabnikom, da sodelujejo demokratično in brez večjih vstopnih ovir v sistem trgovanja z energijo.

Glavni prednosti uporabe tehnologije veriženja blokov sta dodatna varnost in s tem nezmožnosti spreminjanja zapisanih podatkov. Pomembno je, da se podatki, ki so zapisani na trgovalni platformi, ne spreminjajo in s tem ostanejo celotni. Ohranjanje zgodovine podatkov je predvsem pomembno pri morebitnih sporih in tožbah. Če nekoga ali neko podjetje tožijo, se lahko vzame podatke kot vir resnice, saj vemo, da jih ni mogoče spreminjati. Z uporabo tehnologije veriženja blokov odstranimo posrednike, kar pomeni, da potekajo transakcije neposredno med uporabniki.

Ne glede na to, da aplikacija ponuja kar veliko rešitev, so po drugi strani stvari, ki jo omejujejo in ovirajo. Največji problem, ki nastane pri uporabi aplikacije v resničnem okolju, je vzpostavitev cene in likvidnosti trga. Glede na to, da se aplikacija uporablja za omejeno število uporabnikov oziroma samo za tiste, ki so priključeni na isto transformatorsko postajo, bo malo ponudb in povpraševanja. Na veleprodajnem trgu je veliko več ponudnikov in prodajalcev elektrike, kar pomeni, da se cena najbolj približa optimumu. Tehnologija veriženja blokov odstrani vlogo posrednikov, ki pomagajo, da se prodajalec in kupec lažje dogovorita za ceno. V ustvarjeni aplikaciji ni vloge posredništva, zato je mogoče, da cena ne bo optimalna oziroma bodo posli težje sklenjeni. Ker aplikacija omogoča, da odgovornost prevzamejo deležniki platforme, se moramo vprašati, ali lahko sami uporabniki tako dobro skrbijo za trgovanje z elektriko.

Tehnologija veriženja blokov ponuja velik odmik od tradicionalno centralno vodenega modela trgovanja. Aplikacija se spopada z veliko zakonodajnimi ovirami energetske zakonodaje kot tudi z ovirami splošnih uredb. Ker je trgovanje z električno energijo zelo regulirana dejavnost, se je treba spoprijeti z veliko zakonodaje in izpolniti še več zahtev. Trenutno še niti ni mogoče neposredno trgovanje, kar pomeni, da model ne deluje v skladu z zakonodajo. Če se v teoriji upošteva zakonodaja na veleprodajnih trgih, so vstopne ovire za malega proizvajalca električne energije in kupce prevelike. Glede na to, da bi moral vsak,

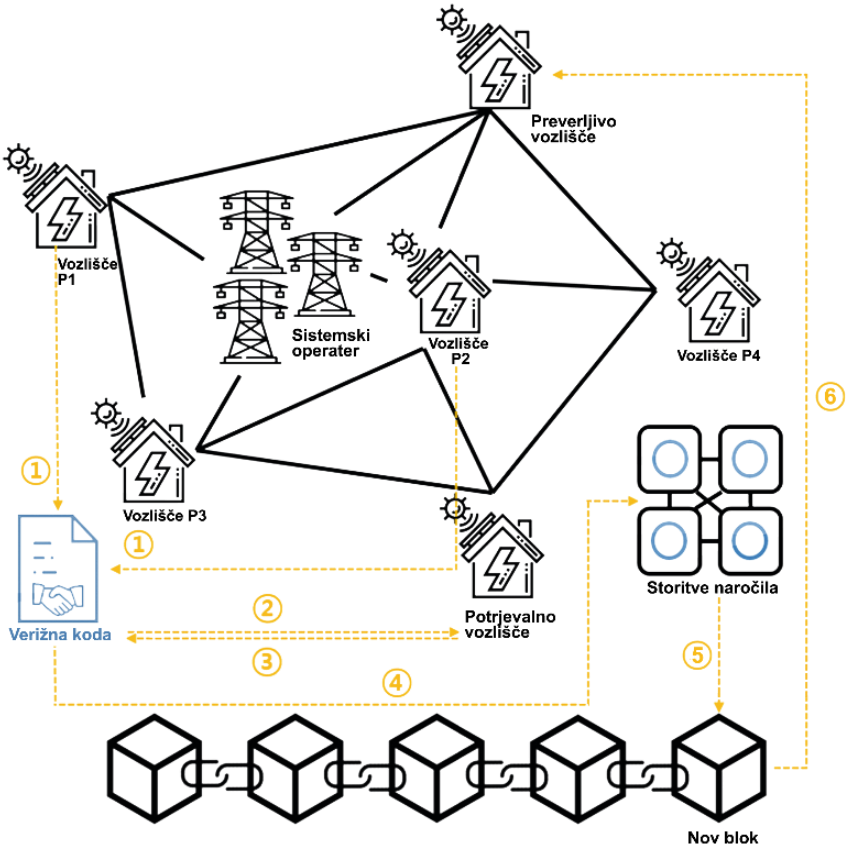
ki bi želel kupovati ali prodajati elektriko, biti del bilančne sheme, to pomeni visoke stroške. Poleg vsega naštetega ta ideja tudi ne spoštuje Splošne uredbe o varstvu osebnih podatkov. Ker vsaka transakcija vsebuje podatek, kdo je komu prodal elektriko, pomeni javno objavljanje osebnih podatkov, ki jih ni mogoče brisati. Čeprav so podatki šifrirani pod zgoščeno vrednostjo, je to prepovedano.

Drugi problemi se nanašajo na tehnične ovire, ki jih prinaša tehnologija veriženja blokov. Pri uporabi aplikacije trgovalne platforme sem ugotovila, da tehnologija še ni dovolj zrela, da bi jo lahko že funkcionalno uporabljali. Tukaj imam v mislih predvsem hitrost potrjevanja transakcije, ki je zelo pomembna pri trgovanju. Dodatno težavo predstavljajo uporabniki, ki prevzamejo odgovornost nadzora nad zasebnimi ključi. Ker ima vsak uporabnik sam nadzor nad sredstvi, mu v primeru izgub in zlorab zasebnih ključev niso zagotovljena povratna sredstva. Zato je treba uporabnike dobro tehnično naučiti upravljanja zasebnih ključev in jih posvariti pred potencialnimi nevarnostmi v zvezi z zlorabami in izgubo zasebnih ključev. Težava tehnologije veriženja blokov je tudi ta, da potrebujemo veliko prostora za shranjevanje podatkov. Ta tehnologija deluje tako, da morajo vsa vozlišča vsebovati celotno kopijo vseh transakcij, ki so se kdaj koli zgodile v omrežju. Zavedati se je treba, da so tradicionalno porazdeljene arhitekture, pri katerih vozlišča sodelujejo in ne podvajajo podatkov, hitrejše pri potrjevanju transakcij in učinkovitejše pri izrabi prostora. To pomeni, da so tudi cenejše, vendar pa ne zagotavljajo toliko varnost, kot jo tehnologija veriženja blokov.

6.5 Nadaljnje izboljšave in razvoj aplikacije

Aplikacija omogoča temeljne funkcionalnosti decentraliziranega trgovanja z električno energijo, vendar je še vedno veliko prostora za izboljšavo. Spodnja slika 22 prikazuje nadgrajeno aplikacijo, ki bi bila lahko vključena v energetski sistem. S pomočjo razvojnega okolja Hyperledger Fabric bi transakcija med prodajalcem P1 in kupcem P2 potekala na naslednji način. Sprva se kupec in prodajalec dogovorita o ceni in količini, ki se zapiše v transakcijo pametne pogodbe na verižno kodo (1). Verižna koda nato pošlje predlog transakcije vsem potrjevalnim vozliščem (2). Potrjevalno vozlišče preveri predlog transakcije in pošlje odgovor o odobritvi oziroma zavrnitvi predloga transakcije spet na verižno kodo (3). Verižna koda nato pošlje transakcijo v storitev naročanja, kjer se transakcija zapiše v blok (4). Nato storitev naročanja posreduje blok preverljivemu vozlišču (6), ki ga potrdi in zapiše v verigo blokov (5). Transakcija je končana in posel je sklenjen ter dostopen sistemskemu operaterju, ki s pridobljenimi podatki poskrbi za stabilnost sistema.

Slika 22: Delovanje aplikacije trgovanja z električno energijo



Vir: Park, Moon, Lee & Jang (2020).

Prvi korak, ki bi bil potreben pri nadgradnji aplikacije, je razširitev, kar pomeni, da bi dodali več vozlišč v omrežje. Trenutno imamo samo administratorsko vozlišče, v nadaljevanju pa bi bilo treba narediti to, da ima vsak kupec, prodajalec, sistemski operater in banka svoje vozlišče. S tem bi lahko aplikacijo v celoti simulirali in uporabljali.

Ker v trenutni aplikaciji uporabniki ročno vnašajo vrednosti v trgovalno platformo, lahko to pripelje do napak, hkrati se porabi veliko časa. Zato bi bila smiselna nadgradnja to, da zapisi podatkov temeljijo na avtomatskem zapisovanju pametnih števcev.

Naslednja funkcionalnost, ki bi jo bilo treba dodati, je razširitev komunikacije med pametnimi števci, ki odčitavajo električno energijo, in trgovalno platformo v resničnem času. S tem bi v prihodnosti lahko omogočili samodejno trgovanje med napravami glede na uporabnikove želje. Uporabnik bi lahko izbiral med različnimi algoritmi trgovanja, na primer glede na ceno elektrike, izvor elektrike itd ... Olajšali bi tudi delo sistemskemu operaterju, saj bi lahko s pomočjo strojnega učenja in analitike sprejemala podatke o ceni in količini električne energije v preteklosti in s tem napovedovala in optimizirala delovanje omrežja v prihodnosti. Tehnologija veriženja blokov bi lahko potem pomagala, da bi bil sistem vedno stabilen, nikomur ne bi bilo treba skrbeti za ceno in dobavo električno energije.

SKLEP

Raziskava magistrske naloge je korak k boljšemu razumevanju energetskih smernic in tehnologije veriženja blokov. Trenutne smernice v energetiki dajejo vedno večji poudarek na lokalnost in lastno proizvodnjo električne energije in s pomočjo tehnologije veriženja blokov bi podprli in sledili tem velikim spremembam, ki jih kažejo smernice. Tehnologija veriženja blokov lahko prinese večjo opolnomočenost posameznikov, saj bi jim omogočili večjo vključenost in lažjo dostopnost pri trgovanju z električno energijo. To pomeni, da bi lahko tehnologija veriženja blokov poskrbela za sklenitve poslov prek borze brez posrednikov, ki bi jih izvajale naprave neposredno med seboj, in hkrati omogočila sistemskemu operaterju in regulatorjem dostop do vseh podatkov. S pomočjo testiranja aplikacije sem dokazala, da je mogoče izvesti transakcije brez posrednikov, neposredno med kupcem in prodajalcem. Na koncu se je transakcija zapisala v verigo blokov, ki so jo lahko preverili vsi v sistemu.

Integriteta, transparentnost in varstvo podatkov so lastnosti tehnologije veriženja blokov, ki so pomembne in nadvse zaželene tudi pri trgovanju z energenti. Omenjene lastnosti dajejo zaupanje v trgovalno platformo in s tem omogočajo, da se lahko posamezniki dogovorijo med seboj brez potrebe po tretji osebi, ki bi omogočala dogovarjanje ali spreminjanje dogovora. Ko so podatki zapisani v verigo blokov, je to dokončno in se ne morejo spreminjati.

S pomočjo teoretičnega dela sem v empiričnem delu ugotovila, da je uporaba tehnologije veriženja blokov pri trgovanju z električno energijo smiselna. Da ima tehnologija veriženja blokov veliko možnosti v energetiki, je opazilo že veliko podjetij in zato tudi večina podjetij ter projektov deluje ravno pri rešitvi trgovanja z energenti.

V magistrski nalogi sem preverila, katere stvari je treba dobro raziskati pred samo implementacijo. Na začetku je treba proučiti razliko med tehnologijo zasebnega in javnega veriženja blokov in se odločiti za tisto, ki je primernejša za rešitev. V tem konkretnem primeru sem se odločila za uporabo tehnologijo zasebnega veriženja blokov predvsem za to, ker omogoča hitrejšo potrjevanje transakcij. Nato se je treba odločiti, kdo bo deležnik v sistemu, kaj bo digitalno sredstvo, ki se bo prenašalo med deležniki, in med katerimi deležniki so transakcije mogoče. V aplikaciji je določeno, da si prebivalci med seboj izmenjujejo digitalno sredstvo kovance, in električno energijo.

Glavni namen magistrske naloge je bil osvetliti področje uporabe tehnologije veriženja blokov na praktičnem primeru trgovanja z električno energijo. Proučila sem delovanje aplikacije, ki deluje v razvojnem okolju Hyperledger Fabric, in ugotovila, da so na poti do rešitve tako tehnične ovire tehnologije veriženja blokov kot tudi težka izvedba v resničnem okolju. Z vidika tehničnih ovir so glavne težave predvsem v nezrelosti tehnologije veriženja blokov. Tehnologija je trenutno še prepočasna za vpeljevanje v resnično okolje, hkrati pa ni dovolj usmerjena za preproste uporabnike. Tukaj imam v mislih, da še ni preproste rešitve, ki bi dala uporabniku dostop do digitalnih sredstev, hkrati pa mu ponudila zaščito v primeru

izgube zasebnega ključa. Poleg tehničnih je tudi veliko zakonskih in regulativnih omejitev. To pomeni, da težko interpretiramo zakone, saj še vedno ni regulacije na področju tehnologije veriženja blokov in pametnih pogodb. Zato si lahko nekatere uredbe, na primer uredbo o varstvu osebnih podatkov, vsak interpretira na drugačen način.

Naj zaključim s tem, da je v tehnologiji veriženja blokov velik potencial, saj bi lahko popolnoma spremenila delovanje energetskega sistema. Uspešno sem prikazala delovanje aplikacije in njene učinke na trenutni energetski sektor. Ne glede na to, da je pred tehnologijo veriženja blokov še vedno veliko izzivov, preden se bo uveljavila v splošni rabi, menim, da ima tehnologija velik potencial, ki ga bomo kmalu lahko izkoristili.

LITERATURA IN VIRI

1. Agencija za energijo. (2017). *Obračun odstopanj.* Pridobljeno 10. januarja 2020 iz https://www.agen-rs.si/izvajalci/elektrika/veleprodajni-trg/obracun-odstopanj
2. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P. & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews, 100,* 143–174.
3. Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain* (2. izd.). Sebastopol: O'Reilly Media, Inc.
4. Augstsprieguma tikls AS. (2019). *Organisation of the electricity market.* Pridobljeno 10. oktobra 2019 iz http://www.ast.lv/en/content/organisation-electricity-market
5. Aste, T. (2016). *The fair cost of Bitcoin proof of work.* London. University College London.
6. Bashir, I. (2017). *Mastering blockchain* (1.izd.). Livery Place: Packt Publishing Ltd.
7. Bchainledger. (2019). *Hyperledger Fabric V1.0: Block Structure (Part 1*) [objava na blogu]. Pridobljeno 10. decembra 2019 iz http://www.bchainledger.com/2017/04/hyperledger-fabric-v10-block-structure.html
8. Beitollahi, H. & Deconinck, G. (2007). Peer-to-peer networks applied to power grid. *In Proceedings of the International conference on Risks and Security of Internet and Systems (CRiSIS)* (str. 1-8). Belgium: Katholieke Universiteit Leuven
9. Besnainou, J. (2017). Cleantech Group. *Diving into blockchain use cases: Wholesale energy trading.* Pridobljeno 10. decembra 2019 iz https://www.cleantech.com/diving-into-blockchain-use-cases-wholesale-energy-trading/
10. Binance. (2019a). *Proof of Authority Explained.* Pridobljeno 10. avgusta 2019 iz https://www.binance.vision/blockchain/proof-of-authority-explained
11. Binance. (2019b). *Hard forks and soft forks.* Pridobljeno 10. avgusta 2019 iz https://www.binance.vision/blockchain/hard-forks-and-soft-forks
12. Binance. (2019c). *What is a multisig wallet.* Pridobljeno 10. avgusta 2019 iz https://www.binance.vision/security/what-is-a-multisig-wallet
13. Binance. (2019d). *What is a 51 percent attack.* Pridobljeno 10. avgusta 2019 iz https://www.binance.vision/security/what-is-a-51-percent-attack

14. Blockchain. (2019). *Osiroteli bloki.* Pridobljeno 17. julija 2019 iz https://www.blockchain.com/btc/orphaned-blocks
15. Blockchain Hub. (2019a). *Smart Contracts.* Pridobljeno 17. septembra 2019 iz https://blockchainhub.net/smart-contracts/
16. Blockchain Hub. (2019b). *Tokenized Networks: What is a DAO?.* Pridobljeno 17. septembra 2019 iz https://blockchainhub.net/dao-decentralized-autonomous-organization/
17. Buck, M., Graf, A., Graichen, P. & Energiewende, A. (2019). *European Energy Transition 2030: The Big Picture: Ten Priorities for the next European Commission to meet the EU's 2030 targets and accelerate towards 2050.* Berlin. Agora Energiewende.
18. Castro, M. & Liskov, B. (1999). Practical Byzantine fault tolerance. *OSDI*, 173-186
19. Cointelegraph. (2019). *What Are Smart Contracts? Guide For Beginners*. Pridobljeno 15. septembra 2019 iz https://cointelegraph.com/ethereum-for-beginners/what-are-smart-contracts-guide-for-beginners/
20. Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y. & Shi, W. (2017). *On security analysis of proof-of-elapsed-time (poet).* Cham: Springer International Publishing.
21. Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J. & Sarda, P. (2018). Blockchain versus database: a critical analysis. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (str. 1348-1353). New York: IEEE.
22. Deloitte Touche Tohmatsu Limited. (2019). *Blockchain Legal implications, questions, opportunities and risks.* Pridobljeno 10. oktobra 2019 https://www2.deloitte.com/content/dam/Deloitte/za/Documents/legal/za_legal_implications_of_blockchain_14052019.pdf
23. Dick, C. I. & Praktiknjo, A. (2019). Blockchain Technology and Electricity Wholesale Markets: Expert Insights on Potentials and Challenges for OTC Trading in Europe. *Energies*, *12*(5), *832*.
24. Digiconomist. (2019). *Bitcoin Energy Consumption Index.* Pridobljeno 9. avgusta 2019 iz https://digiconomist.net/bitcoin-energy-consumption
25. Drescher, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps. Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Frankfurt am Main: Apress.
26. Dwork, C. & Naor, M. (1992). Pricing via processing or combatting junk mail. *In Annual International Cryptology Conference* (str. 139-147). Berlin: Springer.
27. European Parliament. (2019). *Blockchain and the General Data Protection Regulation.* Pridobljeno iz 10. oktobra 2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf
28. Frankenfield, J. (2018). *Proof of Elapsed Time (Cryptocurrency)*. Pridobljeno 19. avgusta 2019 iz https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp
29. Frankenfield, J. (2019a). *Soft fork.* Pridobljeno 10. decembra 2019 iz https://www.investopedia.com/terms/s/soft-fork.asp
30. Frankenfield, J. (2019). *Hard fork (Blockchain).* Pridobljeno 10. decembra 2019 iz https://www.investopedia.com/terms/h/hard-fork.asp

31. Fulmer, N. (2019). Exploring the Legal Issues of Blockchain Applications. *Akron Law Review, 52*(1), 5.
32. Garner, B. (2018). *What's a Sybil Attack & How Do Blockchains Mitigate Them?* Pridobljeno 10. oktobra 2019 iz https://coincentral.com/sybil-attack-blockchain/
33. Gitbuh. (2019). *IBM/Decentralized-Energy-Composer.* Pridobljeno 10. decembra 2019 iz https://blockgeeks.com/guides/hyperledger/
34. Hyperledger-Fabric. (2019). *The Ordering Service*. Pridobljeno 10. decembra 2019 iz https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer/ordering_service.html
35. Hyperledger. (2018). *Hyperledger Passes 250 Members with Addition of 9 Organizations*. Pridobljeno 10. decembra 2019 iz https://www.hyperledger.org/announcements/2018/07/31/hyperledger-passes-250-members-with-addition-of-9-organizations
36. Jain, A., Arora, S., Shukla, Y., Patil, T. & Sawant-Patil, S. (2018). Proof of stake with casper the friendly finality gadget protocol for fair validation consensus in ethereum. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(3), 291–298.
37. Jakovac, B. (2010). Določitev tržne cene električe energije v sloveniji po deregulaciji trga. *Zbornik. 7*, 139–146.
38. Kandaswamy, R & Furlonger, D. (2018). *Blockchain-Based Transformation: A Gartner Trend Insight Report.* Pridobljeno 27. marca 2018 iz https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/3869696-blockchain-based-transformation-a-gartner-trend-insight-report.pdf
39. King, S. & Nadal, S. (2012). *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake.* Pridobljeno 20. maja 2019 iz https://decred.org/research/king2012.pdf
40. Komodoplatform. (2018). *Cryptographic Hash Functions Explained: A Beginner's Guide.* Pridobljeno 14. avgusta 2019 iz https://komodoplatform.com/cryptographic-hash-function/
41. Lamport, L., Shostak, R. & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS), 4*(3), 382–401.
42. Levy H.P. (2018). *Understand how blockchain will evolve until 2030 and today's hype versus reality*. Pridobljeno 20. maja 2019 iz https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/
43. Lo, S. K., Xu, X., Chiam, Y. K. & Lu, Q. (2017). Evaluating suitability of applying blockchain. *In 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)* (str. 158-161). Japan: IEEE
44. Martin, R. (2018). *5 Blockchain Security Risks and How to Reduce Them.* Pridobljeno 3. oktobra 2019 iz https://igniteoutsourcing.com/blockchain/blockchain-security-vulnerabilities-risks/
45. Merz, M. (2019). *Blockchain for B2B integration*. Hamburg. MM Publishing Michael Merz.
46. Murray, M. (2018). *Blockchain explained.* Pridobljeno 10. decembra 2019 iz http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html
47. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Pridobljeno 15. decembra 2019 iz https://bitcoin.org/bitcoin.pdf

48. Park, I. H., Moon, S. J., Lee, B. S. & Jang, J. W. (2020). A P2P Surplus Energy Trade Among Neighbors Based on Hyperledger Fabric Blockchain. *In Information Science and Applications* (str. 65–72). Singapore: Springer.
49. Park, I. H., Moon, S. J., Lee, B. S. & Jang, J. W. (2020). A P2P Surplus Energy Trade Among Neighbors Based on Hyperledger Fabric Blockchain. *In Information Science and Applications* (str. 65–72). Singapore: Springer.
50. Raj, K. (2019). *Foundations of Blockchain: The Pathway to Cryptocurrencies and Decentralized Blockchain Applications*. Livery Place. Packt Publishing Ltd.
51. Reiff, N. (2019). *What Is the DAO?* Pridobljeno 3. oktobra 2019 iz https://www.investopedia.com/tech/what-dao/
52. Rosic, A. (2017). *What Is Hashing? [Step-by-Step Guide-Under Hood Of Blockchain]*. Pridobljeno 4. avgusta 2019 iz https://blockgeeks.com/guides/what-is-hashing/
53. Rosic, A. (2018). *What Is Hyperledger? [The Most Comprehensive Step-by-Step Guide!*. Pridobljeno 10. decembra 2019 iz https://blockgeeks.com/guides/hyperledger/
54. Siegel, D. (2016). *Understanding The DAO Attack*. Pridobljeno 3. oktobra 2019 iz https://www.coindesk.com/understanding-dao-hack-journalists
55. Szabo, N. (1996). Smart contracts: building blocks for digital markets. *The Journal of Transhumanist Thought*, *18*(16), 2.
56. Tapscott, D. & Tapscott, A. (2018). *Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world.* New York. Portfolio.
57. Thomson Reuters. (2019). *Are you ready for blockchain?* Pridobljeno 15. avgusta 2019 iz https://www.thomsonreuters.com/en/reports/blockchain.html
58. Wüst, K. & Gervais, A. (2018). Do you need a blockchain?. *In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (str. 45–54). Switzerland: IEEE.
59. Xorbin. (2019). *SHA-256 hash calculator.* Pridobljeno 15. avgusta 2019 iz https://www.xorbin.com/tools/sha256-hash-calculator
60. Yaffe, L. (2020). *Proof-Of-Stake Isn't Broken. Why Are So Many People Trying To Fix It?* Pridobljeno 15. marca 2020 iz https://cryptodaily.co.uk/2020/02/proof-stake-broken-fix-it
61. Zhang, P., Schmidt, D. C., White, J. & Dubey, A. (2019). Consensus mechanisms and information security technologies. *Role of Blockchain Technology in IoT Applications*, 181–217.
62. Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *In 2017 IEEE international congress on big data (BigData congress)* (str. 557–564). USA: IEEE.