IZZIVI TEHNOLOGIJE VERIŽENJA BLOKOV

BORUT WERBER, UROŠ RAJKOVIČ
Univerza v Mariboru, Fakulteta za organizacijske vede, Kranj, Slovenija
borut.werber@um.si, uros.rajkovic@um.si

Sinopsis Tehnologije veriženja blokov so že več kot desetletje v uporabi in njihova vsestranska uporabnost jih širi na različna področja delovanja človeka. Namen tega poglavja je predstaviti kratko zgodovino nastanka in osnovne principe delovanja. Poleg primarne možnosti za trgovanje s kriptovalutami so prikazane še druge uporabe tehnologije veriženja blokov. Prikazane so tudi manj ugodne posledice delovanja tovrstnih sistemov v smislu velike porabe električne energije in toplotnih izgub pri obdelavi transakcij. Predstavljeni so nekateri rezultati raziskav, ki so merili porabo električne energije, in prikazane so nekatere izboljšave, kako lahko na to vplivamo. V zaključku so povzete možnosti izboljšav na področju programske opreme v obliki učinkovitejših algoritmov, ki ne zmanjšujejo varnosti obstoječega sistema, uporabe ustrezne strojne opreme in uvajanja ustrezne politike in zakonodaje.

Ključne besede:
tehnologija veriženja blokov,
zgodovina,
prednosti,
poraba energije,
ogljični odtis

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/um.fov.6.2022.7
ISBN 978-961-286-637-2

CHALLENGES OF BLOCKCHAIN TECHNOLOGIES

BORUT WERBER, UROŠ RAJKOVIČ
University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
borut.werber@um.si, uros.rajkovic@um.si

Abstract Blockchain technologies have been in use for more than a decade and their versatility can be extended to various areas of human activity. The purpose of this chapter is to acquaint the reader with a brief history of its origin and basic principles of operation. Some possibilities of using blockchain technology in addition to the primary one for cryptocurrency trading are shown. The less favourable consequences of the operation of such systems in terms of high electricity consumption and heat losses in transaction processing are also shown. Some research results that measured electricity consumption are presented and some improvements are shown on how we can influence this. In conclusion, the possibilities of improvements in the field of software are summarized in the form of more efficient algorithms that do not reduce the security of the existing system, the use of appropriate hardware and the introduction of appropriate policies and legislation.

Keywords: blockchain, history, advantages, energy consumption, carbon footprint

https://doi.org/10.18690/um.fov.6.2022.7 DOI
978-961-286-637-2 ISBN

University of Maribor Press

1 Uvod

Tehnologija veriženja blokov (angl. Blockchain technlogy) je danes že splošno znana in razširjena na več področij. Iz primarnega področja kriptovalut se je razširila na raznolika področja, kjer delovanje zahteva robusten in zanesljiv sistem, ki zagotavlja varnost in preprečuje vdore, poneverbe in poskuse prirejanja podatkov o preteklih transakcijah. Za delovanje tehnologije veriženja blokov je potrebno večje število strežnikov (rudarjev), ki so povezani v skupine in zaradi načina delovanja sistema rezultirajo v zahtevnejših operacijah, kar povzroča potrebo po več računalniških resursih, posledično pa to pomeni večjo porabo električne energije in večji toplotni vpliv na okolico. V tem poglavju bomo predstavili osnovne pojme in zgodovino razvoja tehnologije veriženja blokov, predstavili, kje se danes omenjena tehnologija uporablja in kakšen vpliv ima na povečanje potreb po električni energiji in njeni porabi. Predstavljeni bodo rezultati raziskav, ki so proučevale različne možnosti porabe električne energije in ogljičnega odtisa kot posledico uporabe tehnologije veriženja blokov, ter predlogi, kako se s temi problemi soočamo in kakšne možnosti imamo, da porabo električne energije in ogljični odtis zmanjšamo.

2 Zgodovina tehnologije veriženja blokov

Že v pradavnini so si ljudje izmenjevali dobrine. Najprej so glede na povpraševanje in dostopnost določili razmerje in na tej osnovi zamenjali žito za vino ali koruzo za sol. Tisti, ki so imeli več kot za lastne potrebe, so lahko posojali svoje dobrine in zaračunavali obresti, sprva v obliki iste dobrine. Sledilo je obdobje, ko je dobrine nadomestil denar, najprej v obliki kovancev, kasneje v papirni obliki in v obliki delnic. Nekoč je denar predstavljal dejansko vrednost, na primer srebrnik določene teže je dejansko predstavljal vrednost na trgu. Danes bankovci nimajo več dejanske vrednosti, saj banke nimajo zlata, ki bi zagotovilo vrednost papirnatih bankovcev in kovancev v obtoku, in če banka propade, s tem tudi papirni denar te banke izgubi vrednost (Beattie, 2020). Danes sistem bančništva deluje na centraliziranem sistemu – neka banka izvaja finančne transakcije med klienti, posoja denar in pri vsaki transakciji zaračunava provizijo, za čas izposoje denarja pa obresti. Ti zneski so lahko visoki. Na primer: dvig gotovine na bankomatih s kreditne kartice zaračunajo ne glede na količino dviga v določenem minimalnem znesku oz. za večje dvige kot delež zneska dviga. Nakazilo gotovine v tujino ima lahko zelo velik razpon (NovaKBM, 2022). Zaradi teh in podobnih razlogov so iskali decentraliziran varen sistem, ki bi

omogočal spletna plačila elektronske gotovine neposredno med uporabniki, ne da bi šla skozi finančne institucije (Satoshi, 2009).

Teoretična osnova za razvoj tehnologije veriženja blokov je bila postavljena konec osemdesetih in v začetku devetdesetih, ko je leta 1989 Leslie Lamport razvil protokol Paxos in ga leta 1998 objavil pod naslovom The Part-Time Parliment. Po vzoru parlamenta z otoka Paxox, ki je deloval na osnovi porazdeljenega sistema, kjer so predstavniki zakonodajalcev dosledno ohranjali kopije dokumentov, sprejetih v parlamentu, so razvijalci zasnovali porazdeljen sistem, kjer več računalnikov v skupini doseže konsenz za nek rezultat, tudi če nekateri med njimi niso delujoči. Leta 1991 je bila kot elektronska knjiga za digitalno podpisovanje dokumentov uporabljena podpisana informacijska veriga. Uporabljena je bila na način, ki je zlahka prikazal, da ni bil noben podpisan dokument v zbirki spremenjen (Yaga et al., 2018). Oba koncepta so združili leta 2008 v objavi, ki jo je pod psevdonimom objavil Nakamoto Satoshi, z naslovom Bitcoin: A Peer-to-Peer Electronic Cash System. Na osnovi tega je bila leta 2009 s pomočjo tehnologije veriženja blokov ustanovljena kriptovaluta bitcoin (Amy Whitaker, 2019; Yaga et al., 2018). Nakamoto Satoshi je prvi predlagal koncept tehnologije veriženja blokov, ki temelji na principu Proof-of-Work in kriptografiji »hash« (Zou et al., 2020). Omrežje veriženja blokov kriptovalute bitcoin je bilo osnova za razvoj drugih omrežij veriženja blokov.

Uporaba tehnologije veriženja blokov je omogočila implementacijo bitcoina na porazdeljen način, tako da noben od uporabnikov ni imel nadzora nad elektronsko gotovino in zato ni obstajala možnost napake. Glavna prednost je bila omogočiti neposredne transakcije med uporabniki brez potrebe po zaupanja vrednem posredniku, kot so npr. banke. Sistem je omogočil novo obliko posrednikov, ki jih imenujemo rudarji. To so osebe ali podjetja, ki z razpoložljivo računalniško opremo, vključeno v omrežje veriženja blokov, zagotavljajo možnost dodajanja in potrjevanja novih blokov ter hranjenje njihovih kopij. Avtomatizirano plačevanje rudarjev je omogočilo porazdeljeno administracijo sistema brez potrebe po organizaciji (Yaga et al., 2018). Z uporabo veriženja blokov in vzdrževanja, ki temelji na soglasju, je bil ustvarjen mehanizem samokontrole, ki je zagotavljal, da so bile v verigo blokov dodane samo veljavne transakcije in bloki. Da bi zagotovil doslednost omrežja v tehnologiji veriženja blokov, je Nakamoto predlagal soglasni mehanizem Proof-of-Work (PoW), kar pomeni, da je z večjim obsegom dela, ki ga opravi rudar, večja verjetnost, da bo ustvaril ustrezen blok, in večja je možnost, da pridobi plačilo. Kljub temu ima mehanizem Proof-of-Work (PoW) še vedno težave, kot sta zapravljanje

računalniških virov in nizka učinkovitost, zato so naknadno predlagali še mehanizem soglasja Proof-of-Stake (PoS) in Delegated Proof-of-Stake (DPoS) (Zou et al., 2020).

Leta 2014 je Vitalik Buterin predstavil protokol Ethereum – strukturo pametne pogodbe, ki je omogočala tokenizacijo. Medtem ko Bitcoin, izvirni protokol veriženja blokov, od uporabnika zahteva več funkcionalnega obvladovanja mehanike, Ethereum predstavlja enostavnejši vmesnik in prispeva k strukturi žetonov, ki finančno delujejo v mnogih pogledih tako kot naložbe v umetnost. Ethereum je posplošil nekaj skriptnega jezika za Bitcoin, da bi lahko zagnal številne vrste programov. Sčasoma so nekateri od teh programov – pametne pogodbe – postali standardni (Amy Whitaker, 2019; Wood, 2018).

Tehnologije veriženja blokov so priznane kot revolucionarni izumi, od katerih velja izpostaviti petih inovacij (Golosova & Romanovs, 2018). Kot prva inovacija tehnologije veriženja blokov, Bitcoin predstavlja eksperiment digitalne valute. Druga inovacija je bila sama tehnologija veriženja blokov, ko so razvijalci spoznali, da se temelji tehnologije Bitcoin lahko uporabijo za druge namene. Tretja inovacija je bila pametna pogodba (angl. Smart contract), ki je izvedena v drugi generaciji tehnologije veriženja blokov in poimenovana Ethereum (Wood, 2018). Četrta pomembna inovacija je Proof of Stake (POS), kjer so bili podatkovni centri zamenjani s kompleksnimi finančnimi instrumenti, ki zagotavljajo podobno oziroma višjo stopnjo varnosti. POS je mehanizem soglasja kriptovalute za obdelavo transakcij in ustvarjanje novih blokov znotraj omrežja veriženja blokov. Naslednja inovacija, ki ji raziskovalci posvečajo največjo pozornost, je skaliranje procesov tehnologije veriženja blokov. V bistvu raziskovalci iščejo rešitve, kako pospešiti proces transakcije brez oslabitve varnosti.

2.1 Karakteristike in klasifikacije tehnologij veriženja blokov

Tehnologije veriženja blokov so na splošno sestavljene iz šestih ključnih elementov oz. lastnosti: decentraliziranost, transparentnost, odprtokodna rešitev, avtonomija, nespremenljivost in anonimnost (Niranjanamurthy et al., 2019).

Decentralizacija je osnovna značilnost tehnologije veriženja blokov, kar pomeni, da se ni več treba zanašati na centralizirano vozlišče. Podatki se lahko beležijo, shranjujejo in posodabljajo v več sistemih sočasno.

Transparentnost pomeni, da je vsak zapis podatkov v sistemu viden za vsako vozlišče. Vsako od teh vozlišč lahko nadalje posodobi te podatke, doda nov blok, ki je viden vsem in ga potrdijo ali zavrnejo, zaradi česar so pregledni in zaupanja vredni.

Večina odprtokodnih sistemov tehnologije veriženja blokov je odprta za vsakogar, zapis je mogoče javno preveriti in razvijalci lahko uporabljajo tehnologije veriženja blokov za ustvarjanje poljubnih aplikacij.

Avtonomija zaradi osnove konsenza omogoča, da lahko vsako vozlišče v sistemu tehnologije veriženja blokov varno prenaša ali posodablja podatke. Zamišljeno je, da sistem zaupa tako posamezniku kot celotnemu sistemu in nihče ne more neopaženo spremeniti vsebine verige. Nespremenljivost se nanaša na stalno hrambo podatkov, v kateri podatkov ni možno spreminjati. Izjema je možna, kadar se s spremembo strinja več kot polovica vozlišč.

Tehnologije veriženja blokov omogočajo anonimnost, kar je rešilo problem zaupanja med vozlišči, tako da sta prenos podatkov ali celo transakcija lahko anonimen postopek. Ni treba vedeti, kdo je pošiljatelj ali prejemnik. Dovolj je poznati njegov naslov v omrežju tehnologije veriženja blokov (Niranjanamurthy et al., 2019).

Ločimo štiri najpomembnejše značilnosti tehnologije veriženja blokov (Zou et al., 2020):

- *Anonimnost* tehnologije veriženja blokov pomeni, da ima vsakdo v verigi blokov virtualno identiteto (je anonimen). Na primer: uporabniki Bitcoin imajo javne ključe za transakcije, javni ključi pa niso edinstveni.
- *Decentralizacija* tehnologije veriženja blokov pomeni, da ni potrebna nobena centralna institucija in je vsako vozlišče enakovredno. Tehnologija veriženja blokov je osnovna tehnologija digitalnih kriptovalut, kot sta bitcoin in ethereum.
- *Odpornost* veriženja blokov *proti nedovoljenim posegom* pomeni, da nobenih informacij o transakcijah, shranjenih v verigi blokov, ni mogoče spreminjati med in po postopku generiranja blokov. Podatkovno strukturo verige blokov tvorijo urejeni povezovalni bloki, ki vsebujejo informacije o transakcijah.
- *Sledljivost* verige blokov pomeni, da je virom transakcij mogoče slediti preko strukture shranjevanja podatkov in strukture verige.

Tehnologija veriženja blokov ima štiri različice, ki so razvrščene na podlagi dostopa do podatkov. Tabela 1 prikazuje klasifikacijo in definicije razredov (Golosova & Romanovs, 2018).

Tabela 1: Delitev tehnologij veriženja blokov po dostopu do podatkov

Razred	Opis
Javna	Brez omejitev pri branju blokov in ob oddaji transakcij za vključitev v veriženje blokov.
Privatna	Ima seznam vnaprej določenih uporabnikov, ki lahko neposredno dostopajo do blokov in oddajajo transakcije.
Neomejena	Brez omejitev za uporabnike – vsi so primerni za ustvarjanje blokov transakcij.
Omejena	Ima seznam vnaprej določenih uporabnikov, ki so upravičeni za obdelavo transakcij.

Druga klasifikacija temelji na obdelavi transakcij in dostopu do podatkov. Tehnologije veriženja podatkov delimo na tri vrste, ki imajo omejen ali neomejen dostop, in sicer javne, regulirane in privatne.

Sistem omrežja Bitcoin je omogočal psevdo-anonimnost, saj so bili lastniki računov neznani, po drugi strani pa njihove transakcije javne. Bitcoin sistem namreč ne zahteva vpisa osebnih podatkov in računi niso vezani na neko osebo.

Ker je bil Bitcoin psevdo-anonimen, je bilo nujno ustvariti mehanizme za ustvarjanje zaupanja v okolju, kjer uporabnikov ni bilo mogoče zlahka prepoznati. Pred uporabo tehnologije veriženja blokov je bilo to zaupanje običajno posredovano preko posrednikov, ki sta jim zaupali obe strani. Brez zaupanja vrednih posrednikov omogočajo potrebno zaupanje v omrežju veriženja blokov štiri ključne značilnosti, ki so (Yaga et al., 2018):

- Razpršena evidenca (glavna knjiga) – tehnologija uporablja samo evidenco s funkcijo dodajanja, da s tem zagotovi celotno zgodovino transakcij. Za razliko od tradicionalnih baz podatkov pa pri tej tehnologiji ni mogoče popravljati transakcij in vrednosti v verigi blokov.
- Varnost – verige blokov so kriptografsko varne, kar zagotavlja, da podatki v razpršeni evidenci niso bili spremenjeni in da so podatki v evidenci potrjeni.

- Deljenost – evidenca je v skupni rabi med več udeleženci. To zagotavlja preglednost med udeleženci vozlišča v omrežju veriženja blokov.
- Porazdeljeno – tehnologija veriženja blokov omogoča razširjanje. To pomeni povečanje števila vozlišč v omrežju, da omrežje postane bolj odporno na napade. S povečanjem števila vozlišč se zmanjša možnost napadov znotraj omrežja tako, da se vpliva na protokol soglasja, ki ga omrežje uporablja. Mejna vrednost števila vozlišč za uspešno potrjevanje dodanega bloka je 51 %.

Za omrežja veriženja blokov, ki vsakomur omogočajo anonimno ustvarjanje računov in sodelovanje (imenovana omrežja veriženja blokov brez dovoljenja), te zmogljivosti zagotavljajo raven zaupanja med strankami, ki se med seboj ne poznajo. To zaupanje lahko posameznikom in organizacijam omogoči neposredne transakcije, kar omogoči hitrejše delovanje in nižje stroške. Za omrežje veriženja blokov, ki strožje nadzoruje dostop (imenovano omrežje veriženja blokov z dovoljenjem), kjer je med uporabniki lahko prisotno nekaj zaupanja, te zmogljivosti pomagajo okrepiti zaupanje med sodelujočimi (Yaga et al., 2018).

2.2 Struktura blokov

Tehnologija veriženja blokov je globalna digitalna knjiga, kjer se vse transakcije sestavljajo v mrežo veriženja blokov. Bloki tvorijo linearno zaporedje in se v verigo dodajo v rednih intervalih. Po drugi strani ima vsak blok nekaj polj z informacijami, ki so v veliki meri odvisne od vrste omrežja veriženja blokov. Ena od variant je prikazana v tabeli 2 (Golosova & Romanovs, 2018).

Tabela 2: Struktura blokov

Ime polja	Definicija	Velikost
ID_bloka	Enolična številka bloka	4 bajte
Čas	Čas, ko je bil blok ustvarjen	4 bajte
ID_uporabnika	Enolična številka uporabnika, ki je ustvaril blok	5 bajtov
Nivo	Nivo, na katerem je bil rudar v času nastanka bloka	2 bajta
Podpis	Podpis iz (TYPE, BLOCK_ID, PREV_BLOCK_HASH, TIME, USER_ID, LEVEL, MRKL_ROOT) – ustvarjen z uporabo ključa vozlišča	128-512 bajtov
Transakcije	Transakcije	Do 3 MB

Vsak blok vsebuje kriptografski »hash« prejšnjega bloka, to je eden od razlogov, zakaj ni možen vdor s spreminjanjem zapisov v blokih. Hash ne vsebuje nobenih informacij, ki bi jih kdorkoli lahko spremenil, to pomeni, da so vse »hash« informacije ustvarjene samodejno. Tako "MRKL_ROOT" (tabela 2) vključuje vse prejšnje transakcije in njene zgoščene vrednosti (Golosova & Romanovs, 2018).

3 Primeri uporabe tehnologije veriženja blokov v praksi

Glede na prednosti, ki jih predstavlja tehnologija veriženja blokov, bi pričakovali, da bodo to tehnologijo uporabili vsi, ki imajo opravka bodisi z denarnimi sredstvi bodisi s produkti visokih vrednosti, a ni tako. Na srečanju predstavnikov za informacijsko varnost leta 2021 v Novi Gorici so se zbrali predstavniki najuspešnejših podjetij iz Slovenije. Moderator je postavil vprašanje, ali nameravajo v prihodnje vključiti tehnologijo veriženja blokov v svoje procese prodaje. Predstavnik podjetja, ki ima mednarodni sloves in prodaja izdelke z visoko dodano vrednostjo po celem svetu ter se dnevno srečuje s poskusi plagiatorstva svojih izdelkov, je dejal, da pri njih pristnost prodanih izdelkov zagotavljajo na drugačne načine in se jim zato tehnologija veriženja blokov zdi nesmiselna. Poglejmo, kje vse se je tehnologija veriženja blokov izkazala kot uspešna.

3.1 Tehnologija veriženja blokov v umetnosti

Najznačilnejši primeri uporabe tehnologije veriženja v umetnosti so registri izvora in pristnosti za nove medije in generativno umetnost, delni lastniški kapital, nove oblike registra avtorskih pravic ter »Digital scarcity«. Pametne pogodbe in žetoni, ki temeljijo na Ethereumu, omogočajo tudi specifične strukture naložb in intelektualne lastnine (Amy Whitaker, 2019).

Jeseni 2018 je podjetje Artory postalo prvo, ki je objavilo večjo prodajo umetnin na dražbi, ki je bila osnovana na tehnologiji veriženja blokov. Ko so postavili register zbirke Ebsworth Collection, je bila ta 13. novembra 2018 prodana v Christie's New York za 318 milijonov dolarjev. Prodaja je vključevala dvainštirideset umetniških del in postavila številne rekorde (Macdonald-Korth et al., 2018). Artory, zgrajen na tehnologiji veriženja blokov Ethereum, je zbiralcem ponudil kodirano potrdilo o pristnosti.

3.2 Tehnologija veriženja blokov v transportu in logistiki

Mednarodno trgovino vodi množica vpletenih strani, med drugim pri prodaji, nakupu, preprodaji, shranjevanju ali prevozu blaga. Interakcije med temi deležniki ustvarjajo zapleteno matriko pravnih in dejanskih razmerij, ki je občutljiva na človeške napake in izgubljene komunikacije. Kot primer: globalna kontejnerska linija danskega logističnega podjetja Maersk je sledila eni sami pošiljki avokada in vrtnic iz Kenije v Evropo in odkrila, da je prišlo do več kot 200 komunikacij med skoraj tridesetimi zaposlenimi in organizacijami (Albrecht, 2019).

Veliko dejavnosti uporabe tehnologije veriženja blokov poteka v sektorju logistike in dobavnih verig. Bilo je izvedenih veliko pilotnih projektov in demonstracij v sodelovanju med IBM-om in danskim logističnim podjetjem Maersk in tudi s pristaniščem Rotterdam. Vsi iščejo načine, kako lahko povečajo preglednost in sledljivost v dobavni verigi. Kdor dela na tem področju, mora biti pozoren na razvoj tehnologij veriženja blokov. Prenos sredstev med več organizacijami v dobavni verigi je skoraj popolno okolje za uvedbo te tehnologije in verjetno bo kmalu uvedena po vsem svetu.

Drug vodilni primer prihaja iz Velike Britanije. Letališče Heathrow je uvedlo pilotno različico za izmenjavo podatkov in doseglo soglasje o operativnih informacijah o zamudah letov in premikih potnikov med letališči in letalskimi družbami na svetovni ravni. To pomeni, da se lahko vsa letališča dogovorijo, kdaj je predviden let ali kje je potnik na določenem potovanju, kar omogoča ustrezno optimizacijo sistemov za boljšo uporabniško izkušnjo in učinkovitejšo razporeditev virov (Carter, 2020).

Sama digitalizacija ni tehnični, ampak pravni problem, saj manjka zakonodaja, ki bi podprla digitalne transportne liste in digitalne podpise izenačila s parafami in žigi. Dokler bo obstajala ta zakonodajna neskladnost, bo tehnologija veriženja blokov počasi prehajala v mednarodna logistična področja delovanja (Albrecht, 2019).

3.3 Tehnologija veriženja blokov v zdravstvu

V zdravstvu ima tehnologija veriženja blokov široko paleto uporabnosti na različnih področjih. Tehnologija razpršene evidence pomaga raziskovalcem v zdravstvenem varstvu odkriti načine, kako omogočiti varen prenos zdravstvenih kartotek bolnikov, omogočiti interoperabilno uporabo zdravstvenih kartotek bolnikov in upravljati

dobavne verige z zdravili. Zaščita zdravstvenih podatkov, različno upravljanje genomike, elektronsko upravljanje podatkov, zdravstvenih kartotek, interoperabilnost, digitalizirano sledenje boleznim in izbruhom itd. so nekatere izmed tehnično odlično izpeljanih impresivnih funkcij, ki uporabljajo tehnologijo veriženja blokov. Povsem digitalizirani vidiki tehnologije veriženja blokov in njena uporaba v aplikacijah, povezanih z zdravstvom, so pomembni razlogi za njeno sprejetje (Haleem et al., 2021).

Tanwar s sodelavci (Tanwar et al., 2020) navaja primer uporabe tehnologije veriženja blokov za podporo v zdravstvu, ki prikazuje primere več rešitev za izboljšanje trenutnih omejitev v zdravstvenih sistemih, vključno z okvirji in orodji za merjenje učinkovitosti takšnih sistemov.

Tehnologije veriženja blokov se lahko uspešno uporabljajo v zdravstvu. Omogočajo nam, da naredimo prave izbire ob pravem času. Porazdeljena platforma tehnologije veriženja blokov ponuja zdravstvenemu sektorju priložnosti za sledenje goljufijam, zmanjšanje režijskih stroškov, zanesljivo ustvarjanje novih delovnih mest, odpravo podvajanja dela ter uveljavljanje odprtosti v zdravstvenem okolju. Poleg tega se tehnologije veriženja blokov uporabljajo za popisovanje osnovnih sredstev, saj omogočajo nespremenljivost in zaupanje ter decentralizacijo podatkov. Tehnologija veriženja blokov je uporabna tudi za izvajanje kliničnih študij in izbiro organizacij, saj poveča zanesljivost, revizijo in odgovornost zdravstvenih delavcev in raziskovalcev. Prednost uporabe tehnologije veriženja blokov za paciente je v tem, da je njihova anamneza bolj zaščitena in varovana in da njihova diagnostična natančnost izboljša možnosti za nadaljnjo oskrbo (Pandey & Litoriya, 2020).

3.4 Tehnologija veriženja blokov na drugih področjih

Obstaja veliko področij, na katerih se lahko uporabi tehnologija veriženja blokov. Na primer: samo finančno področje ni omejeno zgolj na kriptovalute, kot sta bitcoin in ether. Tehnologija je uporabna tudi za knjiženje premoženja. Finančne institucije izmenjujejo sredstva različnih vrst, kot npr. delnice, obveznice itd.

Druga možnost je odkrivanje goljufij. Stranke finančnih operaterjev bi lahko poskušale goljufati in izkoristiti dejstvo, da v nekaterih primerih operaterji ne izmenjujejo informacij. Primer je storitev, ki jo banke ponujajo imetnikom računov: če lastnik računa predloži račun, ki ga mora stranka pozneje plačati, banka rezervira

denar. Problem nastane v primeru, ko stranka isti račun dostavi več kot eni banki, da bi denar prejela večkrat. Platforma, kot je HyperLedger Fabric, bi lahko bila prava rešitev: ko banka prejme račun od lastnika računa, se račun registrira, drugim bankam pa se sporoči, da je denar že rezerviran.

Ena izmed možnosti je pametna pogodba med finančnimi operaterji. Ko dva ali več finančnih operaterjev podpiše pogodbo, bi to lahko opravljali v obliki pametne pogodbe. Cilj je zagotoviti preglednost in preprečiti napačno razlago, ker se mora pogodbo obravnavati v več informacijskih sistemih (Bringas et al., 2020).

Tudi področje zavarovalništva je primerno za uporabo te tehnologije. Zavarovanje za primere nevarnosti in naravnih nesreč je primer, kjer bi lahko s tehnologijo mreženja blokov preprečili goljufije in skrajšali čas izplačila odškodnin po nastali škodi (Pagano et al., 2019).

Tukaj je še področje javne uprave, kjer je veliko funkcij: od identifikacije, izdaje dokumentov, volitev do certifikatov. Ne smemo pozabiti na pametne hiše, pametna mesta in internet stvari. Vsa ta področja ponujajo veliko možnosti uporabe tehnologije veriženja blokov, ki niso vezana na kriptovalute.

4 Izboljšave s ciljem zmanjšati porabo energije in ogljični odtis

Ena izmed največjih prednosti uporabe tehnologije veriženja blokov je njena varnost, ki jo zagotavljajo algoritmi konsenza. Rezultati raziskav so pokazali, da je rudarjenje algoritma POW potratno z vidika rabe energije, procesorske moči in nekaterih varnostnih aspektov(Amy Whitaker, 2019). Ugotovili so, da velika procesorska moč ne vpliva na družbo, razen da zagotavlja višjo varnost omrežja Bitcoin. Ugotovili so tudi, da algoritem POW ni ustrezen za izvajanje plačil v realnem času. Predlagana je bila strategija GHOST za skrajšanje časa generiranja blokov, ki se hkrati lahko spopada s problemom vilic in prepreči napade dvojne porabe. Predlagan je nov protokol za zaščito veriženja blokov, imenovan Prism, ki se lahko upre večini napadov in s tem izboljša varnost sistema. Protokol ProofofStake (PoS) je bil predlagan zaradi nepoštenega razmerja rudarjenja po algoritmu PoW. Nxt je prva elektronska valuta, ki v celoti podpira protokol PoS.

Več ko imajo rudarji kovancev, večja je možnost, da izkopljejo naslednji blok. Da bi prešli omejitve obstoječega protokola PoS v smislu pravičnosti in varnosti, so predlagali nov protokol, imenovan Proof of Sharing (PoS), ki temelji na pravičnosti in dinamičnem upravljanju skupne rabe (Lee et al., 2019). Larimerjeva ideja je bila uporabiti pravice in interese kot dokaz glasovanja (Rhodes, 2020), ne pa kot priložnost za rudarjenje novega bloka. Ta soglasni algoritem se imenuje Delegated Proof of Stake (DPoS). Nekateri mislijo, da je konsenz algoritem, ki ga uporablja PPCoin, prva različica PoS (Zou et al., 2020).

Mechkaroska s sodelavci (Mechkaroska et al., 2018) navaja, da obstaja več rešitev za razširljivost tehnologije veriženja blokov, ki so bili ali se še bodo izvajali. Nekateri izmed glavnih so:

- proces Segwit,
- povečanje velikosti bloka,
- tehnika Sharding in
- protokol Proof of Stake.

Segwit ali ločena priča (angl. segregated witness) je alternativna rešitev za razširljivost tehnologije veriženja blokov, ki temelji na povečanju števila transakcij v bloku, ne da bi se povečala velikost bloka. Princip »ločena priča« pomaga povečati prostor za nove transakcije, tako da odstrani podatke o podpisu iz transakcij z bitcoini. Rešitev temelji na osnovi odstranitve digitalnih podpisov in njihovega shranjevanja zunaj osnovnega transakcijskega bloka. Na ta način je bil "potrditveni" del ločen od "učinkovitega" dela transakcije. Zato se lahko v blok vstavi več transakcij, pri čemer se ohrani velikost bloka.

Povečanje velikosti bloka: V verigi Bitcoin je velikost bloka omejena na največ 1 MB. Obstaja več argumentov za in proti povečanju velikosti blokov. Glavni argument proti povečanju velikosti blokov je, da bo povzročilo večjo centralizacijo. Rudarji bi imeli koristi od povečanja velikosti bloka, saj povečana velikost bloka pomeni več transakcij na blok. To bi povečalo znesek transakcijskih provizij, ki jih lahko rudar zasluži z rudarjenjem bloka.

Eden največjih problemov za kriptovalute je hitrost preverjanja transakcij. Vsako polno vozlišče v omrežju mora shraniti celotno verigo blokov. S tehniko **Sharding** lahko razdelimo transakcijo na več manjših delov, ki jih razširimo po omrežju. Vozlišča delujejo na posameznih delih transakcije vzporedno. Na ta način se skrajša skupni porabljen čas.

Večina kriptovalut sledi protokolu »proof of work«, kar pomeni, da rudarji rudarijo kriptovalute z reševanjem kripto-ugank z uporabo namenske strojne opreme. Prednost uporabe protokola »**proof of stake**« (dokazilo o vložku) v primerjavi s protokolom »proof of work« je v bistveno manjši porabi energije. Posledično je bolj stroškovno učinkovit (Mechkaroska et al., 2018).

Vse navedene dopolnitve in spremembe so poskušale izboljšati delovanje in pravično delitev plačil med rudarji. Vendar to niso edini načini, kako lahko vplivamo na porabo energije, ki je potrebna za veliko zahtevnih operacij na oddaljenih vozliščih. Računalniška strojna oprema, ki omogoča rudarjenje, je lahko zelo različna. Predpogoj je, da lahko sledi potrebam transakcij znotraj omrežja. Poglejmo nekaj možnosti strojne opreme, ki se uporablja za rudarjenje. Najprej omenimo specializirano strojno opremo ASIC (Application-Specific Integrated Circuit). Druga možnost so FPGA (Field Programmable Gate Array), ki jih lahko poljubno dograjujemo, in omogočajo pri isti porabi energije od 6- do 20-krat višje hitrosti v primerjavi z grafičnimi procesnimi enotami (GPU) (FPGA Guide, 2019). Kot tretja opcija so močne grafične kartice GPU. Kot četrta, nekoč primarna možnost, je uporaba močnih centralnih procesnih enot (CPU). Uporaba različne strojne opreme poleg hitrosti operacij in razpoložljivosti pogojuje tudi potrebno količino električne energije.

Po nekaterih ocenah je računalniška moč, ki jo potrebuje samo omrežje Bitcoin, enaka vsej moči, ki jo porabi Irska (The Economist, 2018). Številni zagovorniki tehnologije veriženja blokov si prizadevajo za zmanjšanje tega vpliva na okolje in prvotni izumitelji te tehnologije opozarjajo na potrebo po obravnavi teh stroškov (Amy Whitaker, 2019). Velika poraba energije s strani rudarjev omrežja Bitcoin, je posledica dejstva, da poskušajo rudarji v prizadevanjih za potrditev transakcij z uporabo velikih količin računalniške moči izvesti do 450 tisoč bilijonov rešitev na sekundo (Niranjanamurthy et al., 2019).

O'Dwyer in Malone sta leta 2014 uporabila strojno opremo različne učinkovitosti: povprečno strojno opremo in visoko učinkovito ASIC opremo. Izračunali so, da je skupna poraba energije med 0,1 in 10 GW, odvisno od tega, katera strojna oprema je bila uporabljena pri rudarjenju (Küfeoğlu & Özkuran, 2019; Vranken, 2017).

Hayes je domneval, da če bi mejni stroški rudarjenja Bitcoin presegli ceno Bitcoin, bi se rudarjenje Bitcoin ustavilo (Hayes, 2017). Hipotetične zgornje meje za rudarjenje je izračunal tako, da je vzel ceno energije kot 13,952 centov/kWh in učinkovitost strojne opreme kot 1,15 J/GH.

Vranken je izračunal, da je povpraševanje po energiji za rudarjenje med 400 MW (cena električne energije 2 c/kWh) in 2,3 GW (cena električne energije 3,5 centov/kWh) (Vranken, 2017). Ocenjuje, da bi bila poraba energije za rudarjenje najverjetneje v območju 100–500 MW (kar ustreza 3–16 PJ na leto).

Rezultati raziskave (Küfeoğlu & Özkuran, 2019) so pokazali, da je zelo pomembno, kakšno računalniško strojno opremo izberemo za rudarjenje. Če bi za rudarjenje še naprej uporabljali samo CPE, bi bila do leta 2018 minimalna poraba energije višja od skupne porabe energije Združenih držav in Kitajske skupaj.

V raziskavi (Li et al., 2019) so testirali porabo energije po algoritmu POW in dokazali, da ima algoritem vpliv na porabo. Na osnovi rezultatov testiranja zaključujejo, da je pri razvoju kriptovalut potrebno razviti energetsko učinkovitejše in okolju prijaznejše algoritme.

Kot drugo pomembno dejavnost navajajo iskanje rešitev, kako uporabiti ali pretvoriti toplotno energijo, ki nastaja zaradi segrevanja strojne procesne opreme med rudarjenjem.

Ogljični odtis kot posledica rudarjenja je drugi vidik, ki skrbi raziskovalce. V raziskavi (Jiang et al., 2021) ugotavljajo, da bi naraščajoča poraba energije in s tem povezana emisija ogljika pri rudarjenju Bitcoin lahko potencialno spodkopala globalna trajnostna prizadevanja. Z raziskovanjem tokov emisij ogljika pri delovanju veriženja blokov Bitcoin na Kitajskem s simulacijskim modelom emisij ogljika v verigi Bitcoin, ki temelji na simulaciji, ugotavljajo, da naj bi brez kakršnih koli političnih posegov letna poraba energije tehnologije veriženja blokov Bitcoin na Kitajskem dosegla najvišjo vrednost leta 2024 pri 296,59 Twh in ustvarila 130,50 milijona metričnih ton

emisij ogljika. Na mednarodni ravni bi ta emisija presegla skupne letne emisije toplogrednih plinov Češke republike in Katarja. Gledano s stališča Kitajske, bo emisija enaka 10 največjim med 182 mesti in 42 industrijskimi sektorji. Ugotavljajo, da se je z leti spremenila strojna programska oprema, ki je od CPU prešla na GPU, zatem na ASIC, ki so specializirane za izvajanje tovrstnih kalkulacij. Na osnovi različnih matematičnih modelov sklepajo, da bo rast omrežij veriženja blokov povečala porabo električne energije in posledično njeno proizvodnjo, ki se izvaja še vedno pretežno na osnovi premoga. Ker je to v nasprotju s podpisom okoljevarstvenega dogovora, bo Kitajska povečala ceno električne energije, ki izhaja iz premoga, in obdavčila podjetja, ki se ukvarjajo z rudarjenjem (Jiang et al., 2021). Stopnja »Bitcoina hash« predstavlja vrednost, ki kaže, koliko energije rudarji porabijo za en Bitcoin, in se je od avgusta 2018 zmanjšala za več kot 40 %. To pomeni, da je bilo od septembra leta 2018 zaprtih približno 1,5 milijona centrov za rudarjenje Bitcoinov (Denisova et al., 2019). Da Kitajska misli resno, se vidi tudi iz zadnjih ukrepov v letu 2021, ko so zaprli 26 območij rudarjenja kriptovalut v jugozahodni provinci Sečuan (STA, 2021).

In še primer uporabe tehnologije veriženja blokov v podporo zmanjšanja ogljičnega odtisa. Sprejetje definicije toplogrednih plinov s strani podjetij je bil odgovor na pritiske zainteresiranih strani in predpisov v smeri trajnostnega upravljanja dobavne verige (SSCM). Z uporabo te tehnologije bi aplikacija lahko odpravila težave s sledenjem zapisom zgodovine proizvedenih izdelkov in povezanim ogljičnim odtisom (Diniz et al., 2021).

5 Zaključek

Pregled strokovne literature s področja tehnologij veriženja blokov potrjuje, da se je nova tehnologija precej razširila na različna področja delovanja: od primarno finančnega področja do proizvodnje, pametnih storitev, zdravstva in kulture. Poleg prednosti, ki jih prinaša, smo opozorili na nekaj slabosti, med katerimi so najpomembnejše: velika poraba električne energije, velika izguba toplote in posledično povečanje ogljičnega odtisa. Raziskovalci iščejo rešitve, kako zmanjšati negativen vpliv delovanja tehnologij rudarjenja blokov z uvajanjem bolj učinkovitih algoritmov, ki bi ob enaki varnosti potrebovali manj resursov in porabili manj energije. Iz osnovnega algoritma POW smo prešli na POS, nato na DPOS, a videti je, da optimizacija še vedno ni zadovoljiva.

Kar ne bo mogoče optimizirati s prilagoditvijo programske opreme, je možno optimizirati z uporabo specializirane strojne opreme. Izvajalci rudarjenja so prešli iz primarnih strojnih rešitev na osnovo uporabe CPU na GPU, nato na ASIC, ki je namenska oprema, prilagojena posebej za podporo omrežjem kriptovalut. Posledično ima slabost, saj se ob spremembi kriptovalute njena uporabnost konča. Na voljo je tudi FPGA, ki je precej hitrejša od GPU in cenejša od ASIC, a se lahko uporablja tudi v druge namene.

Naslednja možnost omejevanja porabe energije in ogljičnega odtisa je z ustrezno narodno in mednarodno politiko (Truby, 2018). Podobno kot se počasi pravno ureja davčne obveznosti mednarodnih korporacij, bodo slej kot prej sprejeta pravna določila, ki bodo zahtevala delež dobička, s katerim se bo zmanjševal ogljični odtis, ali pa se bo investiralo v trajnostno proizvodnjo električne energije.

Zahvala

Raziskava je bila podprta s strani Javne agencije za raziskovalno dejavnost Republike Slovenije v okviru programa P5-0018 – Sistemi za podporo odločanju v digitalnem poslovanju.

Literatura

Albrecht, C. (2019). Blockchain Bills of Lading: The End of History? Overcoming Paper-Based Transport Documents in Sea Carriage Through New Technologies. *Tulane Maritime Law Journal*, *43*(2), 251–288.

Amy Whitaker. (2019). Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts. *ARTIVATE: A JOURNAL OF ENTREPRENEURSHIP IN THE ARTS*, *8*(2), 21–46.

Beattie, A. (2020). The History of Money: From Barter to Bitcoin. *Investopedia*, 20. https://www.investopedia.com/articles/07/roots_of_money.asp

Bringas, P. G., Pastor-López, I., & Psaila, G. (2020). BlockChain Platforms in Financial Services: Current Perspective. *Business Systems Research*, *11*(3), 110–126. https://doi.org/10.2478/bsrj-2020-0030

Carter, C. (2020). Blockchain: do we have your attention yet? *Logistics & Transport Focus*, *22*(6), 42–43. https://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=145998324&site=ehost-live

Denisova, V., Mikhaylov, A., & Lopatin, E. (2019). Block chain infrastructure and growth of global power consumption. *International Journal of Energy Economics and Policy*, *9*(4), 22–29. https://doi.org/10.32479/ijeep.7685

Diniz, E. H., Yamaguchi, J. A., Rachael dos Santos, T., Pereira de Carvalho, A., Alégo, A. S., & Carvalho, M. (2021). Greening inventories: Blockchain to improve the GHG Protocol Program in scope 2. *Journal of Cleaner Production*, *291*. https://doi.org/10.1016/j.jclepro.2021.125900

FPGA Guide. (2019). *Cryptocurrency Mining: Why Use FPGA for Mining? FPGA vs GPU vs ASIC Explained | by FPGA Guide | FPGA Mining | Medium*. https://medium.com/fpga-guide/cryptocurrency-mining-why-use-fpga-for-mining-fpga-vs-gpu-vs-asic-explained-5aaa400082b9

Golosova, J., & Romanovs, A. (2018). Overview of the Blockchain Technology Cases. *59th International*

Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2018 - Proceedings. https://doi.org/10.1109/ITMS.2018.8552978

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*(September), 130–139. https://doi.org/10.1016/j.ijin.2021.09.005

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, *34*(7), 1308–1321. https://doi.org/10.1016/j.tele.2016.05.005

Jiang, S., Li, Y., Lu, Q., Hong, Y., Guan, D., Xiong, Y., & Wang, S. (2021). Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China. *Nature Communications*, *12*(1), 1–10. https://doi.org/10.1038/s41467-021-22256-3

Küfeoğlu, S., & Özkuran, M. (2019). Bitcoin mining: A global review of energy and power demand. *Energy Research and Social Science*, *58*(July), 101273. https://doi.org/10.1016/j.erss.2019.101273

Lee, D. R., Jang, Y., & Kim, H. (2019). Poster: A Proof-of-Stake (PoS) blockchain protocol using fair and dynamic sharding management. *Proceedings of the ACM Conference on Computer and Communications Security*, 2553–2555. https://doi.org/10.1145/3319535.3363254

Li, J., Li, N., Peng, J., Cui, H., & Wu, Z. (2019). Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies. *Energy*, *168*, 160–168. https://doi.org/10.1016/j.energy.2018.11.046

Macdonald-Korth, D., Lehdonvirta, V., & Meyer, E. T. (2018). *The Art Market 2.0 Blockchain and Financialisation in Visual Arts Executive summary Key findings*.

Mechkaroska, D., Dimitrova, V., & Popovska-Mitrovikj, A. (2018). Analysis of the Possibilities for Improvement of BlockChain Technology. *2018 26th Telecommunications Forum, TELFOR 2018 - Proceedings*, 20–23. https://doi.org/10.1109/TELFOR.2018.8612034

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, *22*(s6), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5

NovaKBM. (2022). *Cenik nadomestil za posle s potrošniki - NKBM*. CENIK NADOMESTIL ZA POSLE S POTROŠNIKI - NKBM. https://www.nkbm.si/downloadfile.ashx?fileid=2085

Pagano, A. J., Romagnoli, F., & Vannucci, E. (2019). Implementation of Blockchain Technology in Insurance Contracts against Natural Hazards: A Methodological Multi-Disciplinary Approach. *Environmental and Climate Technologies*, *23*(3), 211–229. https://doi.org/10.2478/rtuect-2019-0091

Pandey, P., & Litoriya, R. (2020). Securing and authenticating healthcare records through blockchain technology. *Cryptologia*, *44*(4), 341–356. https://doi.org/10.1080/01611194.2019.1706060

Rhodes, D. (2020). *What is Delegated Proof of Stake? An Overview of DPoS Blockchains*. Komodo. https://komodoplatform.com/en/academy/delegated-proof-of-stake/

Satoshi, N. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

STA. (2021). *Bitcoin: Kitajska nadaljuje z udarci po rudarjih kriptovalut - Svet kapitala*. Svet Kapitala. https://svetkapitala.delo.si/aktualno/kitajska-nadaljuje-z-udarci-po-rudarjih-kriptovalut/

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*. https://doi.org/10.1016/j.jisa.2019.102407

The Economist. (2018). *Why bitcoin uses so much energy*. The Economist. https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy

Truby, J. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Research and Social Science*, *44*(February), 399–410. https://doi.org/10.1016/j.erss.2018.06.009

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, *28*, 1–9. https://doi.org/10.1016/j.cosust.2017.04.011

Wood, D. (2018). A Future History of International Blockchain Standards. *The Journal of the British Blockchain Association*, *1*(1), 1–10. https://doi.org/10.31585/jbba-1-1-(11)2018

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview - National

Institute of Standards and Technology Internal Report 8202. *NIST Interagency/Internal Report*, 1–57. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

Zou, Y., Meng, T., Zhang, P., Zhang, W., & Li, H. (2020). Focus on blockchain: A comprehensive survey on academic and application. *IEEE Access*, *8*, 187182–187201. https://doi.org/10.1109/ACCESS.2020.3030491