Aktualne dejavnosti, primerne za uporabo veriženja podatkovnih blokov

Bor Krizmanič[1], Aleš Groznik[1]
[1]Univerza v Ljubljani, Ekonomska fakulteta, Kardeljeva ploščad 17, 1000 Ljubljana, Slovenija
bor.krizmanic@ef.uni-lj.si, ales.groznik@ef.uni-lj.si

Izvleček

Tehnologija veriženja podatkovnih blokov (angl. Blockchain) se v zadnjih letih omenja v povezavi z uporabo v najrazličnejših panogah in za zelo raznolike načine uporabe. Težko je presoditi, katera področja so resnično najbolj primerna za uporabo te tehnologije. V članku smo obdelali osnovne lastnosti, prednosti in slabosti tehnologije veriženja podatkovnih blokov in predstavili štiri, po naši oceni najprimernejša področja dejavnosti za uporabo te tehnologije. Potencial za uporabo te tehnologije smo po posameznih področjih ocenjevali na podlagi pregleda pravnega, tehnološkega in sociološkega vidika morebitne implementacije ter idej in primerov uporabe. Po našem mnenju so za uporabo najperspektivnejša področja: finančne in zavarovalniške dejavnosti, dejavnost prometa in skladiščenja, trgovina, vzdrževanje in popravila motornih vozil ter kot zadnje, informacijske in komunikacijske dejavnosti.

Ključne besede: dokaz o deležu, dokaz o delu, kriptovalute, tehnologija razpršene evidence, tehnologija veriženja podatkovnih blokov

Abstract

In recent years, the use of a blockchain technology has been discussed in connection with a variety of industries and different applications. It is difficult to judge which areas are best suited for the use of this technology. In this article we have described the basic characteristics, advantages and disadvantages of blockchain technology and presented four economic sectors which we believe are most suitable for the use of this technology. For each sector, we evaluated the potential for the use of this technology based on a review of the legal, technological and sociological aspects of possible implementation, ideas and applications. In our view, the most promising areas of application are financial and insurance activities; transporting and storage; wholesale and retail; repair of motor vehicles and motorcycles; information and communication services.

Keywords: proof of work, proof of stake, cryptocurrency, distributed ledger technology, blockchain.

1 UVOD

Tehnologija veriženja podatkovnih blokov je vse od njenega pojava v letu 2008, s prvo zasnovo platforme Bitcoin za namen delovanja istoimenske kriptovalute, deležna velike pozornosti tako laične, kot tudi strokovne javnosti. Čeprav je pozornost v zadnjem letu, po občutnem padcu vrednoti večine kriptovalut generalno upadla, pa se še vedno namenja veliko pozornosti uporabi tehnologije veriženja podatkovnih blokov v namene, ki niso povezani s kriptovalutami. Cilj tega članka je definirati tiste dejavnosti, ki so najperspektivnejše za uporabo te tehnologije. Ker je iz objavljene strokovne literature razvidno, da se predvideva uporaba te tehnologije v skoraj vseh dejavnostih, je zato namen tega članka trezno in preudarno preučiti, katere dejavnosti so primerne za uporabo in katere ne. V luči tega je v tem članku podan krajši pregled najprimernejših dejavnosti za uporabo te tehnologije, opredeli pa se tudi tistih, ki morda niso najbolj primerne, a so vendarle deležne velikega zanimanja javnosti.

S tehnologijo veriženja podatkovnih blokov so se do sedaj ukvarjali in jo tudi sooblikovali številni pomembni avtorji s tega področja. Tako je to tehnologijo prvi zasnoval in opisal skrivnostni snovalec Bitcoina pod psevdonimom Satoshi Nakamoto. Pred njim se je s podobnimi koncepti ukvarjal in o njih pisal ameriški pravnik in računalniški znanstvenik Nick

Szabo, ki je tudi zasnoval, v več pogledih predhodnika Bitcoina, digitalno valuto Bit Gold[1]. Po uveljavitvi Bitcoina in z začetki širšega zanimanja za tehnologijo, ki ga omogoča, sta postala vplivna avtorja še Alex in Don Tapscott.

2 RAZLAGA POJMOV

Tehnologija veriženja podatkovnih blokov (angl. Blockchain) lahko opišemo kot tehnični protokol, ki omogoča izmenjavo podatkov in vzpostavitev zaupanja brez potrebe po centralnih posrednikih (Seffinga, Lyons & Bachmann, 2017, str. 7). Informacije se shranjujejo v verigo podatkovnih blokov, ki vsebujejo niz transakcij oz. podatkov, ki so nastali v času od nastanka predhodnega bloka. V osnovni zasnovi tehnologije veriženja podatkovnih blokov se za izdelavo blokov uporablja t. i. protokol dokaza o delu (angl. proof-of-work), pri katerem vozlišča (tj. udeleženci omrežja), imenovana rudarji, uporabljajo t. i. zgoščevalno funkcijo (angl. hash function) z namenom iskanja pravilne zgoščene vernosti (angl. hash). Zgoščevalna funkcija šifrira vhodne podatke poljubne dolžine v standardno število znakov (številk in črk). Ko rudarji najdejo zgoščeno vrednost, ki ustreza zahtevam, izdelajo nov blok. Vsak blok vsebuje to zgoščeno vrednost vseh transakciji oz. podatkov, ki so nastali v določenem obdobju, spremenljivko imenovano nonce in zgoščeno vrednost predhodnega bloka. Vsak nov blok se javno objavi, nato pa ostala vozlišča pregledajo ali je bil blok izdelan pravilno in ga potrdijo s konsenzom večine vozlišč. Vsak novi blok se sklicuje na zgoščeno vrednost predhodnega bloka in tako tvori verigo. Vsak zapis je preko podatkovnih blokov dodan nespremenljivi verigi in deljen vsem vozliščem omrežja (Nakamoto, 2008, str. 1–3). Če bi želel nekdo spremeniti katerikoli zapis, ki je bil že zgoščen v blok v verigi, bi moral na novo izračunati zgoščeno vrednost tega in vseh drugih blokov v verigi. To bi bilo računsko izjemno zahtevno in v večjem omrežju z velikim številom zapisov domala nemogoče. Protokol omogoča dostop in preverjanje vseh zapisov, vse od prvega zapisa na verigi dalje. Ta tehnologija tako omogoča nespremenljiv, deljen, pregleden in preverljiv zapis vseh zapisov (Reyna, Martín, Chen, Soler & Díaz, 2018, str. 174).

[1] http://unenumerated.blogspot.com/2005/12/bit-gold.html (zadnji obisk 25.8.2020)

Kot alternativo dosedanjemu protokolu dokaza o delu poizkušajo številni projekti razviti praktično uporaben in delujoč protokol dokaza o deležu (angl. proof-of-stake), pri katerem ne izdelujejo novih blokov vsa vozlišča v omrežju naenkrat, temveč se iz nabora potrjevalcev po izbranem ključu izmenjujejo vozlišča, ki izdelajo in potrdijo nov blok. S tem se zmanjša računska in energetska zahtevnost izdelave novega bloka (Ethereum Foundation, 2020). Pogosteje omenjena alternativa dokaza o delu je tudi protokol dokaza o avtoriteti (angl. proof-of-authority), pri katerem nove bloke potrjujejo le v naprej preverjeni in potrjeni uporabniki (imenovani tudi potrjevalci). Ker se sistem zanaša na ugled uporabnika, se mu lahko ob neprimernem delovanju tudi odvzame pravice za potrjevanje. Dokazu o deležu, z nekaj podobnostmi dokaza o avtoriteti, je precej podoben tudi delegiranemu dokazu o deležu (angl. delegated proof-of-stake), kjer se glede na lastništvo kovancev razporedijo glasovalne pravice potrjenih uporabniku o tem kdo bo izdelal nov blok (Ramuta, 2018). Dokaz o kapaciteti (angl. proof-of-capacity) ali tudi dokaz o prostoru (angl. proof-of-space) je zelo podoben konceptu dokaza o delu, le da mora v tem primeru vozlišče namesto računske moči vložiti veliko prostora na trdem disku. Ta koncept naj bi bil predvsem manj energetsko potrošen in zato bolj prijazen okolju kot dokaz o delu (Hayes, 2020). Sledi še protokol, ki bi ga lahko prevedli kot dokaz o izgorevanju ali kurjenju (angl. proof-of-burn) kjer morajo vozlišča za potrjevanje žrtvovati kovance, proporcionalno s količino porabljenih kovancev pa pridobijo pravice za izdelavo novega bloka. Kurjenje se tehnično izvede tako, da se kovance nakaže na poseben naslov, ki kovance le sprejema, ne pa tudi vrača. Tako postanejo pokurjeni kovanci za vedno nedostopni (Karantias, Kiayias & Zindros, 2020, str. 523-524).

Omrežja veriženja podatkovnih blokov se delijo tudi po tem, kakšne so omejitve za dostop do omrežja. Najbolj pogost in sprva tudi edini tip omrežja je javna veriga podatkovnih blokov (angl. public blockchain), ki dopušča, da se omrežju lahko pridruži kdorkoli iz svetovnega spleta, brez potrebne predhodne prošnje in odobritve za pristop k omrežju, ter brez kakršnega koli preverjanja pristnosti identitete. Najpomembnejši primer takšnega tipa omrežja je seveda Bitcoin. Ker se lahko omrežju pridruži kdorkoli in ga lahko tudi kadarkoli zapusti, so tovrstna omrežja načeloma zasnovana tako, da ne računajo na

samovoljno pripravljenost udeležencev za vzdrževanje omrežja, temveč udeležbo pri tem nagrajuje s spodbudami za ohranjanje omrežja. Tako na primer v primeru protokola dokaza o delu, sistem nagrajuje rudarje za njihov doprinos k delovanju omrežja (Lai & Lee Kuo Chuen, 2018, str. 153).

Obstaja pa tudi tip zasebne verige podatkovnih blokov (angl. private blockchain), ki za priključitev omrežju zahteva predhodno preverjanje pristnosti identitete in odobritev dostopa (Lai & Lee Kuo Chuen, 2018, str. 153–154). Tovrstna omrežja predpostavljajo, da so vsi udeleženci znani ter imajo pravico in motivacijo za udeležbo, zato ni nujno potrebno ustvarjati notranje spodbude kot pri javni blokovni verigi (Lai & Lee Kuo Chu en, 2018, str. 154). Mehanizmi nadzora dostopa se razlikujejo. Tako lahko o novih udeležencih odločajo obstoječi udeleženci ali pa nekakšen regulatorni organ, neke vrste administrator omrežja, ki izdaja dovoljenja za sodelovanje (Jayachandran, 2017). Poleg osnovne delitve na javne in zasebne verige podatkovnih blokov obstajajo tako še druge, vmesne delitve. Med njimi se največkrat omenja t. i. konzorcij, kjer je protokol konsenza nadzorovan s strani vnaprej izbranih, preverjenih vozlišč, ki potrjujejo nove bloke. Kdo lahko bere te bloke, se lahko omejuje, ali pa tudi ne. Ena od vmesnih rešitev je tudi delno zasebna veriga podatkovnih blokov, kjer eno podjetje ali organizacija dodeljuje dostop uporabnikom, ki izpolnjujejo pogoje zanj. Vse te različne oblike omejenega dostopa se načeloma uporabljajo pri uporabi tehnologije veriženja podatkovnih blokov med podjetji (Dobson, 2018).

Pomemben koncept v tehnologiji veriženja podatkovnih blokov so tudi t. i. pametne pogodbe (angl. smart contract). V pravnem smislu ne gre nujno za pravo pogodbo temveč gre za računalniško kodo, ki je vgrajena v verigo podatkovnih blokov in je posledično na enak način, kot to velja za samo verigo, tudi sama nespremenljiva (Reed, Sathyanarayan, Ruan & Collins, 2018, str. 161). S tem se lahko brez udeležbe zaupanja vredne tretje stranke omogoča izvrševanje sporazumov med strankami, ki si med seboj ne zaupajo (Alharby & Moorsel, 2017). Za integracijo pametnih pogodb v tehnologijo veriženja podatkovnih blokov so se oblikovale številne nove platforme, med katerimi je najpomembnejša platforma Ethereum[2], ki za pisanje pametnih pogodb uporablja za to razvit programski jezik Solidity (Lai & Lee Kuo Chuen, 2018, str. 172-173). Za samo izvedbo pogodbenih klavzul je potreben nek sprožilec oz. signal, zato pametne pogodbe potrebujejo verodostojen dostop do podatkov o stanjih in dogodkih v realnem svetu. Te vire podatkov imenujejo t. i. preroki (angl. oracles), ki so ključni za uspešno integracijo pametnih pogodb v realnem svetu. Tako ima na primer, platforma Ethereum že nekaj varnih virov, ki črpajo podatke iz zaupanja vrednih spletnih mest, vendar ti viri jamčijo točnost podatkov zgolj na podlagi ugleda upravljavcev teh spletnih mest (Zhang, Cecchetti, Croman, Juels & Shi, 2016, str. 270).

Decentralizirane aplikacije (angl. decentralized application) ali pogosto imenovane DApps so na aplikacije, ki tečejo na decentraliziranem omrežju tipa »vsak z vsakim«. Omrežja tehnologija veriženja podatkovnih blokov, kot je na primer Ethereum, predstavljajo zelo primeren porazdeljen sistem za njihovo delovanje. To pomeni, da takšne aplikacije nimajo kakšnega centralnega strežnika, kar bi lahko ob nedelovanju povzročilo nedelovanje celotne aplikacije (Bambara, Allen, 2018, str. 233-234).

3 PREDNOSTI IN SLABOSTI TEHNOLOGIJE VERIŽENJA PODATKOVNIH BLOKOV

Glavna prednost tehnologije veriženja podatkovnih blokov je zmožnost vzpostavitve zaupanja v decentraliziranem okolju, brez centralnih posrednikov. Njen protokol rešuje t. i. problem dvojne porabe znotraj decentraliziranega omrežja tipa »vsak z vsakim« (angl. peer-to-peer). Tako ta tehnologija omogoča vzpostavitev konsenza o eni zgodovini dogodkov in sicer v omrežju z udeleženci, ki se med seboj ne poznajo in si ne zaupajo, in to brez pomoči tretje, zaupanja vredne stranke (Nakamoto, 2008, str. 1–2).

Med prednosti te tehnologije lahko štejemo tudi sledljivost in preverljivost. Vse transakcije ali podatki se namreč javno objavijo in za vedno zapišejo v vseh glavnih knjigah udeležencev oz. tistih udeležencev, ki se odločijo hraniti celotno knjigo. Vse to omogoča, da so vsi zapisi oz. celotna zgodovina v verigi podatkovnih blokov kadarkoli vidni vsem članom omrežja. To poleg sledljivosti in preverljivosti pomeni tudi, da tehnologija veriženja podatkovnih blokov ne omogoča brisanja transakciji ali podatkov – to zadnje pa predstavlja istočasno tudi oviro za določene primere uporabe (Hooper, 2018). To ima v prvi vrsti vpliv na uporabo povsod, kjer so vklju-

[2] https://ethereum.org/ (zadnji obisk 20.8.2020)

čeni osebni podatki- več o tem v odstavku glede zakonskih omejitev. Podobno pa velja tudi za lastnost transparentnosti, ki se prav tako pogosto omenja kot prednost. Tako je na primer v omrežju Bitcoin moč videti vse transakcije in ključne podatke o njih (npr. količina prenesenih kovancev, naslove spletnih denarnic) za celotno zgodovino omrežja. To ima tako pozitivne učinke na preglednost omrežja kot tudi ovira, za na primer ohranjanja poslovnih skrivnosti (Reyna, Martín, Chen, Soler & Díaz, 2018, str. 176).

Na drugi strani pa se tehnologija veriženja podatkovnih blokov sooča s številnimi ovirami oz. slabostmi. Kot prvo gre izpostaviti problem omejene razširljivosti oz. omejene kapacitete omrežja. Veriga podatkovnih blokov z novimi zapisi le raste in se nikoli ne krajša, saj so, kot že omenjeno, vsi zapisi za vedno vdelani v verigo podatkovnih blokov. Zaradi tega morajo vozlišča v omrežju shranjevati vedno večjo glavno knjigo, kar zahteva vedno več strojnih in mrežnih virov (Reyna, Martín, Chen, Soler & Díaz, 2018, str. 177). V času največjega zanimanja za kriptovalute tekom leta 2018 je Bitcoinova veriga podatkovnih blokov rastla s hitrostjo okoli 50 GB na leto (Bank for International Settlements, 2018, str. 99). Novembra 2019 pa je veriga blokov Bitcoin presegla velikost kar 230 GB (Bitcoin.com, 2019). Za primerjavo - uveljavljena plačilna sistema Mastercard in Visa opravita oba skupaj med 3500 in 2000 transakciji na sekundo (angl. transactions per second- TPS), v enakem času pa omrežje Bitcoin izvede skoraj tisočkrat manj transakcij (Bank for International Settlements, 2018, str. 99). Praktično vsa omrežja verige podatkovnih blokov na tem področju iščejo izboljšave, v skladu s tem pa se je pojavilo nekaj potencialnih rešitev. Že samo omrežje Bitcoin je zasnovano tako, da celotno glavno knjigo hranijo le t. i. polna vozlišča (angl. full nodes), ki lahko v celoti potrdijo transakcijo. Kapaciteto omrežja se lahko prilagaja tudi s spreminjanjem zahtevnosti izdelave novega bloka in velikostjo nagrade za rudarje, ki vpliva na interes le-teh za izdelavo novih blokov (ConsenSys, 2019). Kot rešitev se predlaga tudi protokol konsenza na principu dokaza o deležu. Prav slednji protokol bo uporabljala tudi nova verzija omrežja Ethereum (Ethereum 2.0) in s tem po napovedih zelo močno povečala kapaciteto omrežja (Ethereum, 2020). Omenjajo se še t. i. rešitve izvajale transakcije izven verige (angl. off-chain transactions), kar bi povečalo kapaciteto na račun večje verjetnosti izgube podatkov. Ena izmed predlaganih rešitev je tudi zmanjšanje časovnega zamika pri potrjevanju novih blokov, kar bi skrajšalo čas potovanja transakcij na račun zmanjšane varnosti (Reyna, Martín, Chen, Soler & Díaz, 2018, str. 174–175).

Drugo veliko oviro pri širši uporabi tehnologije veriženja podatkovnih blokov v različnih dejavnostih pa predstavljajo zakonske omejitve in negotovosti, pri katerih prevladujejo omejitve v povezavi z varstvom osebnih podatkov. Zaradi leta 2016 sprejete Uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Ur. l. EU št. 2016/679) je možnost uporabe te tehnologije za hranjenje osebnih podatkov močno vprašljiva. Ker je omrežje tehnologije veriženja podatkovnih blokov decentralizirano, ni mogoče določiti pooblaščene osebe za varstvo osebnih podatkov in obdelovalca podatkov, kot to zahteva omenjena uredba v primeru hranjenja osebnih podatkov. Težko bo tudi doseči omejitev prenašanja osebnih podatkov izven Evropske unije, ki z izjemo nekaj določenih držav ni dovoljena. Prav tako velik problem predstavlja načelo, da je vsak posameznik lastnik svojih osebnih podatkov in lahko kadarkoli zahteva izbris le-teh. Glede na to, da tehnologija veriženja podatkovnih blokov vse podatke deli med vsa vozlišča v omrežju, ki lahko te podatke shranijo, hkrati pa ne omogoča brisanja česarkoli že shranjenega v verigi podatkovnih blokov, se zdi, da osebnih podatkov ne bo moč shranjevati na verigi podatkovnih blokov (Millard, 2018, str. 845).

Z zakonodajo pa je omenjena tudi uporaba tehnologije veriženja podatkovnih blokov za beleženje lastninskih in drugih pravic na sredstvih, ki niso del verige podatkovnih blokov (kot so kriptovalute) in se nahajajo izven le-te. V osnovni zasnovi te tehnologije namreč ni možnosti identifikacije strank v transakcijah (v osnovni zasnovi so anonimizirane) in ni mogoče spreminjati zapisov o pravicah na sredstvih s strani tretje, zaupanja vredne stranke, kot bi bilo to potrebno na primer ob sodni odločbi o zaplembi premoženja. Sedanja zasnova za vsako transakcijo namreč zahteva soglasje takratnega lastnika (Reed, Sathyanarayan, Ruan & Collins, 2018, str. 170–181). Ker je ta tehnologija dokaj nova in precej drugačna od katerekoli druge, se sodna praksa v povezavi z njo šele oblikuje. To povzroča negotovost glede možnosti njene uporabe (Bacon, Michels, Millard, & Singh, 2018, str. 78 & 106).

4 PREGLED NAJPERSPEKTIVNEJŠIH GOSPODARSKIH PANOG ZA UPORABO TEHNOLOGIJE VERIŽENJA PODATKOVNIH BLOKOV

Pri pripravi tega članka smo ubrali podobno pot kot Andoni in drugi v njihovem članku z naslovom Tehnologija veriženja podatkovnih blokov v energetskem sektorju: Sistematičen pregled izzivov in priložnosti (angl. Blockchain technology in the energy sector: A systematic review of challenges and opportunities.) (Andoni in drugi, 2019, str. 143–156). Z metodo pregleda literature smo poizkusili združiti znanje iz znanstvenih člankov in drugih virov, kjer se združuje znanje s področja te tehnologije (poročila svetovalnih podjetij, blogi, bele knjige projektov itd.). Uvodnemu delu s predstavitvijo osnovnih principov delovanja tehnologije, ključnih prednosti in slabosti sledi pregled in ocena najperspektivnejših dejavnosti za uporabo te tehnologije. Do izbranih dejavnosti smo prišli po preučitvi vseh 21. področji dejavnosti, definiranih s Standardno klasifikacijo dejavnosti. Za posamezna področja smo pregledali osnovne možnosti in doslej predlagane načine uporabe te tehnologije, morebitno uporabo pa smo preučil tudi s pravnega, tehnološkega in sociološkega vidika. Glede na doslej znane primere uporabe, številčnost poizkusov ter ob upoštevanju prej navedenih prednosti in slabosti, smo nato ocenili najbolj obetavna področja uporabe. V nadaljevanju povzemamo ugotovitve za štiri področja, pri vsakem od področji pa je predstavljen tudi konkreten primer uporabe oz. poizkusa uporabe te tehnologije.

5 FINANČNE IN ZAVAROVALNIŠKE DEJAVNOSTI

Kot prvo lahko izpostavimo finančne in zavarovalniške dejavnosti, kamor spadajo med drugim bančne dejavnosti, dejavnosti finančnih skladov in holdingov (Statistični urad Republike Slovenije, 2010, str. 237). V literaturi se področje finančnih dejavnosti omenja kot eno od najperspektivnejših za uporabo tehnologije veriženja podatkovnih blokov (The Economist, 2015). Prav tako se tu tudi največ vlaga v razvoj projektov uporabe te tehnologije. Subjekti iz ZDA, ki so povezani z finančnimi dejavnostmi, imajo največ vloženih zahtevkov za pridobitev patenta iz področja tehnologije veriženja podatkovnih blokov (Lee, 2018). Zelo veliko zanimanje izkazujejo banke, zagonska podjetja in strokovna javnost za uporabo te tehnologije v procesu mednarodnih denarnih transferjev med bankami. Proces prenosa denarja iz banke v eni državi v tujo banko namreč večinoma še vedno traja več dni. Čeprav so nekateri nacionalni in regionalni sistemi za poravnavo, kot je na primer Evropski sistem SEPA, precej učinkoviti, pa mednarodni sistem poravnav temelji na zapleteni mreži klirinških organov in korespondenčnih bank. V literaturi so prisotna pričakovanja, da bi lahko s tehnologijo veriženja podatkovnih blokov odpravili te probleme (Seffinga, Lyons & Bachmann, 2017, str. 3).

Ker je za finančne dejavnosti je značilna visoka stopnja reguliranosti, je pravni vidik eden ključnih pri ocenjevanju možnosti uporabe te tehnologije in tako ni presenečenje, da ti predpisi postavljajo kar nekaj ovir. Zakon o bančništvu (Ur. l. RS št. 25/15, 44/16 – ZRPPB, 77/16 – ZCKR, 41/17 in 77/18 – ZTFI-1) v 125. in 126. členu definira kot zaupne podatke vse podatke, dejstva in okoliščine o posamezni stranki, s katerimi razpolaga banka, in določa, da jih je banka dožna varovati. To pomeni, da teh podatkov ni moč objaviti in uporabljati na javni verigi podatkovnih blokov. Pomembna je tudi Direktiva Evropske unije št. 2015/849 o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranje terorizma. Ena od ključnih zahtev, ki jih bankam nalaga ta direktiva, je izvajanje ukrepov za poznavanje svojih strank (angl. know your customer – KYC), kar vključuje preverjanje istovetnosti strank in oceno tveganja za zlorabo bančnih računov za nezakonite namene. Zaradi varstva osebnih podatkov bo to na verigi podatkovnih blokov težko izvajati.

Pri informacijskih sistemih na področju finančnih storitev, še posebej bančništva in zavarovalništva, sta v ospredju zanesljivost in varnost sistemov. Ker se sistemi med seboj povezujejo, jih je zelo težko zamenjati z novejšimi. Tako je na primer zasnova najpomembnejšega medbančnega mednarodnega sistem Swift[3], ki se uporablja pri okoli polovici vseh mednarodnih plačilih na svetu, stara že 45 let (Arnold, 2018). Ker tehnologija veriženja podatkovnih blokov predstavlja veliko spremembo in drugačno arhitekturo glede na sedanje medbančne sisteme, bo klub interesu bank to tehnologijo zelo težko uveljaviti (Larios-Hernández, 2017, str. 870). Zaradi pravnih in tehničnih ovir bo potrebno razviti rešitve, ki bodo uporabljale drugačno arhitekturo in način delova-

[3] https://www.swift.com/our-solutions/global-financial-messaging (zadnji obisk 10.9.2020)

nja, kot je postavljena v osnovni zasnovi delovanja omrežja in tehnologije veriženja podatkovnih blokov.

Eden od projektov uporabe te tehnologije na področju medbančnih transakciji je rešitev RippleNet[4], razvita s strani ameriškega podjetja Ripple Labs Inc, ki želi vzpostaviti sistem, ki bi omogočal mednarodne transakcije med bankami s pomočjo kriptovalute XRP. Ta valuta bi opravljala vlogo nekakšne vmesne valute med dvema klasičnima valutama. Vendar pa je potrebno poudariti, da kljub prevladujočemu prepričanju, pri rešitvi RippleNet, strogo gledano ne gre za tehnologijo veriženja podatkovnih blokov temveč gre za tehnologijo razpršene evidence (angl. distributed ledger technology – DLT). Ta je sicer podobna in ima nekatere elemente in lastnosti tehnologije veriženja podatkovnih blokov, vendar predstavlja širši pojem oz. celoten sklop tehnologij. Pri tehnologiji razpršene evidence se zapisi shranjujejo en za drugim v rastočo evidenco in ne v verigo podatkovnih blokov. Vsak zapis pa mora biti potrjen s strani nabora potrjevalcev (Government Office for Science, 2016, str. 16-17). Omrežje RippleNet se tako kar precej razlikuje od klasičnega omrežja veriženja podatkovnih blokov, saj v omrežju ni rudarjev, transakcije pa se ne zapisujejo v podatkovne bloke, ki bi tvorili verigo. Transakcije preverja in potrjuje omejeno število izbranih in preverjenih vozlišč, gre za protokol imenovan Ripple Protocol Consensus Algorithm (RPCA). Transakcije pa se zapisujejo v razpršeno evidenco, kar pomeni, da vozlišča, vsako pri sebi, hranijo kopijo enega enotnega seznama transakciji- evidenco (Ripple, 2017, str. 4–16). Ta rešitev je tehnično manj zahtevna in ni povsem decentralizirana v primerjavi s tehnologijo veriženja podatkovnih blokov in je zaradi tega lažje izvedljiva in bolj verjetna. Podobne pristope uporabe tehnologije razpršenih evidenc sta ubrala tudi druga večja poizkusa uporabe tehnologije veriženja podatkovnih blokov v bančništvu. To sta konzorcija bank R3 z rešitvijo Corda in platforma Stellar (Newton, 2018). Najpomembnejša aplikacija podjetje Ripple Labs je xCurrent za izvajanje transakcij med bankami. Ta uporablja poseben sistem za pošiljanje sporočil med bankami, preko katerega se koordinira izmenjavo informacij in denarnih sredstev, imenovan *Interledger Protocol* ali *ILP*. xCurrent v primeru dveh bank iz različnih držav, ki uporabita korespondenčno banko za usmerjanje plačil, preko sistema *ILP* pridobi podatke o provizijah in izračuna celotne stroške transakcije. Sledi validacija podatkov pred izvedbo same transakcije. Vse tri banke poznajo vse podatke in lahko potrdijo transakcijo vnaprej in tako zagotovijo visoko stopnjo uspešnosti transakcij. Nato sledi koordinacija sredstev med zasebnimi ILP glavnimi knjigami bank (npr. nostro računi). V vseh treh knjigah aplikacija xCurrent pripravi in zaklene sredstva potrebna za transakcijo. Vse ILP knjige nato generirajo elektronske podpise, ki zagotavljajo, da so sredstva za transakcijo na voljo. Nato se sredstva v vseh treh knjigah sočasno sprostijo. Tako napaka pri izvedeni poravnavi ni mogoča, transakcija se izvede v celoti ali pa se v primeru napake v celoti ne izvede (Ripple, 2017, str. 4–16).

Na področju zavarovalništva bi lahko tehnologijo veriženja podatkovnih blokov s pomočjo pametnih pogodb uporabili tako, da bi te spremljale ali so vsi pogoji za veljavnost zavarovanja izpolnjeni (npr. vse zavarovalniške premije so plačane), nato pa bi v primeru spremembe stanja predmeta zavarovanja avtomatsko izplačale zavarovalnino. Tu bi bilo ključno, da so preroki, ki poročajo v stanjih preverjeni, potrjeni in verodostojni (Tsankov, 2018). Primer poizkusa uporabe tehnologije veriženja podatkovnih blokov in pametnih pogodb je projekt Insuwave[5] podjetij Ernst and Young in Guardtime, ki sta v sodelovanju z več logističnimi podjetji razvili platformo za poslovna zavarovanja s poudarkom na transportu. Obstajajo tudi ideje, da bi se tehnologijo veriženja podatkovnih blokov uporabljalo za hitrejše preverjanje novih strank (predvsem za izmenjavo podatkov med različnimi zavarovalnicami) ter za preprečevanje zavarovalniških goljufij. To pa naj bi dosegli s pomočjo varnega hranjenja in deljenja informacij na verigi podatkovnih blokov (Lorenz in drugi, 2016, str. 3–5).

6 PROMET IN SKLADIŠČENJE

Med bolj perspektivne za uporabo tehnologije veriženja podatkovnih blokov spada tudi področje prometa in skladiščenja, torej logistike. Na tem področju je bolj zanimiv del povezan z prevozom blaga in zajema poslovanje med podjetji. Procesi v prometu in skladiščenju vključujejo večje število poslovnih partnerjev, ki se med seboj morda ne poznajo, poleg tega mednarodni promet blaga vključuje veliko količino administracije. In prav večje zaupanje in manj-

[4] https://ripple.com/ripplenet (zadnji obisk 10.9.2020)

[5] https://insurwave.com/ (zadnji obisk 18.9.2020)

šo stopnjo administracije želijo na to področje uvesti projekti uporabe tehnologije veriženja podatkovnih blokov.

Mednarodni promet in skladiščenje blaga sta predmet urejanja številnih lokalnih zakonov, predpisov in dajatev. Čeprav bi rešitve na podlagi tehnologije veriženja podatkovnih blokov lahko povečale transparentnost in zmanjšale obseg administracije, pa ne bi bilo mogoče zaobiti vseh uvozno-izvoznih postopkov in dokumentov. Ne gre namreč pričakovati, da bi države povsem prilagodile zakonodajo tehnologiji veriženja podatkovnih blokov. Zaradi tega bodo morale biti rešitve na podlagi te tehnologije dovolj prilagodljive na vse posebnosti različnih trgov (Groenfeldt, 2017).

Kljub temu, da so pričakovanja o vplivu tehnologije veriženja podatkovnih blokov na področju prometa in skladiščenja dokaj velika, pa za sedaj na tem področju primanjkuje ekspertnega znanja (Dobrovnik, Herold, Fürst & Kummer, 2018, str. 1). Anketa iz leta 2017 med 152 strokovnjaki s področja logistike je pokazala, da velika večina pričakuje pozitiven vpliv te tehnologije na področje logistike, vendar večina ne ve natanko, kako bodo do teh sprememb prišli (Hackius & Petersen, 2017, str. 11–12).

Rešitve na podlagi te tehnologije za področje logistike obljubljajo zmanjšanje števila interakcij med strankami v postopkih, vendar pa bi še vedno vključevale vso sedaj predpisano dokumentacijo. Verjetno najbolj konkreten in najdlje razvit primer uporabe te tehnologije na področju logistike je platforma TradeLens[6], ki je nastala v sodelovanju podjetja Maersk, največjega kontejnerskega prevoznika na svetu, in podjetja IBM, ki je eno najbolj aktivnih tehnoloških podjetij na področju tehnologije veriženja podatkovnih blokov (Groenfeldt, 2017). TradeLens je rešitev za celostno digitalizacijo procesa dobave blaga, podprta s tehnologijo Hyperledger Fabric 1.0[7] in računalniškim oblakom IBM Cloud[8] (White, 2018). Platforma Hyperledger, krovni projekt fundacije Linux, je odprtokoden sistem v prvi vrsti namenjen poslovanju med podjetji. Zaradi velike prilagodljivosti in modularnosti omogoča dobro prilagajanje različnim primerom uporabe. Tako se lahko uporabijo različne stopnje zasebnosti verige podatkovnih blokov. Podobno kot pri Ripplu pa tudi tu ne gre strogo gledano za tehnologijo veriženja podatkovnih blokov temveč bolj za neko vrsto tehnologije razpršene evidence (DLT). Platforma TradeLens pri sledenju in upravljanju posamičnih pošiljk deluje s pomočjo pametnih pogodb, ki se v platformi Hyperledger Fabric imenujejo tudi chaincode. Maersk je v letu 2018, ko je testna rešitev zaživela, uspel k projektu privabiti več kot 100 organizacij, kot so pristanišča, špediterji, ladijski prevozniki pa tudi carinski organi (Scott, 2018). V prvem letu testiranja platforme se je na njej zabeležilo kar 154 milijonov dogodkov povezanih z blagovnim prometom (Maersk, 2018).

7 TRGOVINA, VZDRŽEVANJE IN POPRAVILA MOTORNIH VOZIL

Trgovina, vzdrževanje in popravila motornih vozil je zelo široko področje, ki zajema trgovino na drobno in debelo vseh vrst blaga, v to področje pa spadajo tudi vse storitve povezane s prodajo. Tako v to področje spadajo tudi dejavnosti popravila motornih vozil (Statistični urad Republike Slovenije, 2010, str. 197). Trgovina je zadnji člen v dobavni verigi blaga do končnega kupca in se tako močno povezuje s področjem prevoza in skladiščenja. Za uporabo tehnologije veriženja podatkovnih blokov je zanimivo sledenje porekla blaga in poti po dobavni verigi. V to področje spada tudi trgovanje s hrano in zdravili pri katerih je, zaradi vpliva na zdravje ljudi, še posebej pomembno spremljanje njihovega porekla in poti od proizvodnje do končnega potrošnika.

Kot je bilo na že začetku nakazano, zapisi na verigi podatkovnih blokov ne predstavljajo pravno veljavnega dokaza o lastništvu nekega sredstva izven verige podatkovnih blokov. Temu primerno se ta tehnologija ne more uporabljati za trgovino samo, temveč jo je možno uporabiti kot platformo za sledenje zgodovine in stanja nekega sredstva (Reed, Sathyanarayan, Ruan & Collins, 2018, str. 170–181). Zanimiva je uporaba te tehnologije pri prodaji rabljenih vozil in beleženju stanja vozil tekom njihove življenjske dobe. Na verigi podatkovnih blokov bi tako lahko shranjevali podatke o zgodovini stanja in vzdrževanja vozila (Berryhill, Bourgery & Hanson, 2018, str. 43). V povezavi s preprečevanjem zlorab na tem področju in s tem povezanim beleženjem zgodovine vozil velja poudariti, da Zakon o motornih vozilih (Ur. l. RS, št. 75/2017) manipulacijo s kilometrskim števcem prikaza prevožene razdalje vozila, opredeljuje kot kaznivo dejanje.

[6] https://www.tradelens.com/platform (zadnji obisk 19.9.2020)
[7] https://www.hyperledger.org/hyperledger-fabric-1-0 (zadnji obisk 19.9.2020)
[8] https://www.ibm.com/cloud (zadnji obisk 19.9.2020)

Leta 2016 je bila sprejeta uredba Evropske Komisije (2016/161), ki je določila podrobna pravila za zaščitne elemente na ovojnini zdravil za uporabo v humani medicini. Uredba od proizvajalcev zdravil zahteva t. i. serializacijo, kar pomeni, da je potrebno vsaki proizvedeni seriji zdravil dodeliti unikatno šifro in ustrezno označiti pakiranje izdelkov (šifra in črtna koda) (Ur. l. EU št. 2016/161). Že pred tem, leta 2013 je bil podoben zakon sprejet tudi v ZDA in sicer Zakon o varnosti oskrbe z zdravili, ki za implementacijo določa časovni okvir desetih let. Ta pravila naj bi zagotovila, da bi bilo mogoče zelo natančno slediti posameznim farmacevtskim izdelkom po celotni dobavni poti od proizvodnje do končnega kupca. To je področje, kjer se lahko v prihodnosti uporabi tehnologija veriženja podatkovnih blokov (Kherrat & Hernandez, 2018). Kar zadeva tehnični vidik serializacije zdravil omenjena Evropska direktiva nalaga, da je potrebno podatke o serijah zdravil pošiljati v centralni sistem regulatornih organov. Med tem ko, se je za tak pristop odločila tudi Kitajska, pa Ameriška zakonodaja ne predvideva centraliziranega pristopa, temveč naj bi proizvajalci podatke hranili sami. Slednje bi povzročilo veliko število podatkovnih baz in različnih rešitev, kar pomeni, da je potencial za uporabo tehnologije veriženja podatkovnih blokov na tem področju v ZDA večji kot v Evropi ali na Kitajskem (Whyte, 2016, str. 10–11).

Kot primer poizkusa uporabe tehnologije veriženja podatkovnih blokov za preprečevanje goljufij z manipulacijo števca prevoženih kilometrov v vozilih lahko navedemo skupni projekt enega največjih proizvajalcev avtomobilskih sestavnih delov, nemškega podjetja Bosch in univerze ETH Zürich. Rešitev vključuje namestitev majhne naprave v vozilo, ki zajema različne podatke o stanju vozila in jih najprej pošlje v računalnik ali pametni telefon lastnika avtomobila, kjer se neobdelani podatki šifrirani. Za identifikacijo bi uporabili identifikacijsko številko vozila (angl. vehicle identification number – VIN), vtisnjeno na šasiji vozila. Transakcija se lokalno podpiše z zasebnim ključem uporabnika in šele nato se zgoščena vrednost podatkov pošlje preko interneta v verigo podatkovnih blokov, ki temeljijo na platformi Ethereum. Vsi podatki bi bili tako pred prenosom na verigo podatkovnih blokov lokalo šifrirani. Lastnik vozila bi lahko prostovoljno delil zapise o zgodovini prevoženih kilometrov s komurkoli bi želel, sistem pa bi zagotavljal, da se podatki ne morejo spreminjati za nazaj (Chanson, Fleisch, Wortmann & Bogner, 2017, str. 2–4).

Tudi na področju sledenja zdravil se že pojavljajo določeni projekti, enega izmed njih razvija nemško tehnološko podjetje SAP. Rešitev bi podatke o serijalizaciji in sledenju poti zdravil po dobavni verigi shranjevala na verigo podatkovnih blokov zasnovano na platformi MultiChain[9]. Ta veriga bi bila zasebnega tipa, vozlišča pa bi poleg SAP-a predstavljali tudi proizvajalci zdravil. Z zapisovanjem podatkov na verigo podatkovnih blokov bi se izognili številnim razdrobljenim podatkovnim bazam različnih proizvajalcev, trgovci in kupci pa bi lahko na verigi preverili pristnost zdravila. Rešitev je za sedaj še v fazi razvoja (Morris, 2018a).

8 INFORMACIJSKE IN KOMUNIKACIJSKE DEJAVNOSTI

Področje informacijske in komunikacijskih dejavnosti je precej široko področje, ki vključuje založništvo (knjig, glasbe, filmov), telekomunikacije, obdelavo podatkov, izdajanje programja (Statistični urad Republike Slovenije, 2010, str. 230–236). Tehnologija veriženja podatkovnih blokov je na tem področju najbolj zanimiva za morebitno zapisovanje in nadziranje uporabe licenc programske opreme (Felin & Lakhani, 2018, str. 35).

Za nadzor in upravljanje z licencami programske opreme nekatera podjetja uporabljajo t. i. orodja za upravljanje s programsko opremo (angl. software asset management – SAM), ki pa so primarno namenjena za notranji nadzor in obvladovanje licenc s strani poslovnih uporabnikov. Med tem pa se morebitne rešitve na osnovi tehnologije veriženja podatkovnih blokov bolj osredotočajo na nadzor s strani ponudnikov programske opreme. Z uporabo te tehnologije bi lahko izboljšali ažurnost informacij o uporabi programov, ki zaradi posrednikov, kot so velike distribucijske platforme, ni najboljša (Morris, 2018b).

Zanimiva je rešitev na osnovi tehnologije veriženja podatkovnih blokov za upravljanje licenc računalniških igric, ki jo je v sodelovanju s svetovalnim podjetjem Ernst and Young razvilo podjetje Microsoft (Ernst & Young Global Limited, 2018). Rešitev temelji na verigi podatkovnih blokov Quorum[10] in Microsoftovi oblačni rešitvi Azure[11] (Varshney,

[9] https://www.multichain.com/ (zadnji obisk 20.9.2020)
[10] https://consensys.net/quorum/ (zadnji obisk 22.9.2020)
[11] https://azure.microsoft.com/ (zadnji obisk 22.9.2020)

2018), ter bi v verigi podatkovnih blokov implementirala pametne pogodbe. S pomočjo te rešitve bi razvijalci in založniki računalniških igric, ki svoje igrice ponujajo na Microsoftovi platformi Xbox Live, imeli v realnem času vpogled v prodajo njihovih izdelkov. Microsoftovi partnerji sicer dobivajo poročila o prodaji, a njihova priprava lahko traja dalj časa, tudi do 45 dni ali več (Ernst & Young Global Limited, 2018).

9 DRUGE POGOSTO OMENJENE DEJAVNOSTI

Možnost uporabe tehnologije veriženja podatkovnih blokov se sicer omenja v povezavi z domala vsemi področji dejavnosti. Eno izmed največkrat omenjenih področji je zdravstvo in socialno varstvo. Vendar pa bi bilo zaradi zelo visokih standardov pri varstvu osebnih podatkov na področju zdravstva moč tehnologijo veriženja podatkovnih blokov možno uporabiti le kot varnostno plast za dostop do zdravniških evidenc in ne za shranjevanje zdravstvenih podatkov samih (Zhu, Wu, Gai & Choo, 2019, str. 529). Podobno velja za prav tako pogosto omenjeno področje javne uprave, kjer je urejanje javnih evidenc najbolj perspektivno področje (npr. zemljiški register). Vendar pa tudi tu obstajajo podobne zakonske ovire kot pri zdravstvu, hkrati pa ne rešujejo problema netočnih osnovnih, že obstoječih, podatkov (Vos, 2017, str. 23). Uporaba tehnologije veriženja podatkovnih blokov bi bila možna tudi na področju iger na srečo, kjer bi lahko preko pametnih pogodb in decentraliziranih aplikacij, t. i. DApps, uporabili omrežje verige podatkovnih blokov za sklepanje stav neposredno med stavci ali igralniško aplikacijo, ki bi bila posledično povsem decentralizirana (Gainsbury & Blaszczynski, 2017, str. 483). Ena izmed slednjih je na primer porazdeljena aplikacija Dice[12] deluje na omrežju verige podatkovnih blokov ESO[13]. Med glavnimi izzivi tovrstne uporabe so ponovno zakonske omejitve, saj zakonodaja na področju iger na srečo v večini držav zahteva implementacijo že omenjenega koncepta poznavanja svoje stranke in ukrepov proti preprečevanju pranja denarja (Gainsbury & Blaszczynski, 2017, str. 485).

10 SKLEP

Tehnologija veriženja podatkovnih blokov se precej razlikuje od vseh zdaj uveljavljenih tehnologij in je unikatna v tem, da omogoča vzpostavitev zaupanja v decentraliziranem okolju med strankami, ki se ne poznajo in si med seboj ne zaupajo. V članku smo na podlagi raziskovalne metode pregleda literature, izmed vseh 21 področij dejavnosti, definiranih v Standardni klasifikaciji dejavnosti, določili najbolj obetavne dejavnosti za uporabo te tehnologije. Perspektivnost panoge za uporabo te tehnologije smo ocenili na podlagi predlogov uporabe v posamezni dejavnosti ter pregledu pravnega, tehnološkega in sociološkega vidika morebitne implementacije te tehnologije na posameznem področju. Pri ocenjevanju smo upoštevali tudi glavne prednosti in slabosti ter njihovo težo v posamičnih primerih uporabe.

V članku smo podrobneje predstavili le najbolj obetavna področja dejavnosti za uporabo tehnologije veriženja podatkovnih blokov. Tako smo izpostavili finančne in zavarovalniške dejavnosti, kjer je najbolj perspektiven proces mednarodnih denarnih transferjev. V tem primeru je sicer bolj verjetna uporaba tehnologije razpršenih evidenc kakor strogo definirane tehnologije veriženja podatkovnih blokov. Med bolj obetavne smo uvrstili tudi področje prometa in skladiščenje, kjer bi se lahko uporabljalo to tehnologijo za boljšo izmenjavo podatkov pri logističnih procesih, za zmanjšanje števila stikov med vpletenimi poslovnimi partnerji in povečanje zaupanja v pravilnost podatkov. Podobno smo ugotovili, da ima potencial tudi področje trgovine, vzdrževanja in popravila motornih vozil, ki se v delu, ki se nanaša na trgovanje s hrano povezuje tudi s področjem kmetijstva, lova, gozdarstva in ribištva. Na tem področju bi ta tehnologija lahko omogočila boljše spremljanje in zanesljivejše hranjenje podatkov o zgodovini blaga. Kot panogo, kjer je verjetna uporaba tehnologije veriženja podatkovnih blokov, smo identificirali tudi področje informacijskih in komunikacijskih dejavnosti, kjer bi se lahko ta tehnologija uporabljala za hranjenje in nadzor licenc programja.

Druge dejavnosti izkazujejo manjšo verjetnost za uporabo te tehnologije. Za večino dejavnosti predvsem ne obstaja izkazana dovolj velika potreba po decentraliziranem zaupanju ali pa so ostale omejitve, kjer prednjačijo omejitve pri razširljivosti ter zakonske omejitve, prevelike. Ocenjujemo, da je tehnologijo veriženja podatkovnih blokov bolj smiselno povezovati s specifičnimi primeri uporabe in ne toliko s celotnimi področji dejavnosti. Za uporabo so najbolj primerne rešitve, kjer ni obdelave osebnih podatkov ali lastniških in drugih pravic na sredstvih, temveč se

[12] https://dice.one/portfolio (zadnji obisk 3.10.2020)
[13] https://eos.io/eos-public-blockchain/ (zadnji obisk 3.10.2020)

tehnologija veriženja podatkovnih blokov uporablja bolj kot dokaz o stanju in zgodovini nekega sredstva.

Ker se veliko projektov ukvarja z razvojem tehnologij razpršenih evidenc, in ne le strogo tehnologije veriženja podatkovnih blokov, menimo, da bi se bilo smiselno posvetiti tudi raziskovanju ostalih različic te tehnologije.

LITERATURA

[1] Alharby, M & Moorsel, A. (2017, avgust). *Blockchain-Based Smart Contracts: A Systematic Mapping Study*. Pridobljeno 20. decembra 2018 iz https://www.researchgate.net/publication/319603816_Blockchain_Based_Smart_Contracts_A_Systematic_Mapping_Study

[2] Allen, M. (2018, 14. december). *Switzerland sets legal foundations for blockchain industry*. Pridobljeno 10. februarja 2019 iz https://www.swissinfo.ch/eng/business/dlt-report_switzerland-sets-legal-foundations-for-blockchain-industry/44617654

[3] Arnold, M. (2018, 6. junij). *Ripple and Swift slug it out over cross-border payments.* Pridobljeno 16. decembra 2018 iz https://www.ft.com/content/631af8cc-47cc-11e8-8c77--ff51caedcde6

[4] Bacon, J., Michels, J. D., Millard, C. & Singh, J. (2018). Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers. *Richmond Journal of Law & Technology*, 25(1), 1-106.

[5] Bambara, J. J. & Allen, P. (2018). *Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions.* New York City: McGraw-Hill Education

[6] Bank for International Settlements. (2018, junij). *Annual Economic June 2018 Report.* Pridobljeno 28. decembra 2018 iz https://www.bis.org/publ/arpdf/ar2018e.pdf

[7] Berryhill, J., Bourgery, T. & Hanson, A. (2018), Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. *OECD Working Papers on Public Governance*, 28.

[8] Bitcoin.com. (2019). *Blockchain Size*. Pridobljeno 15. novembra 2019 iz https://charts.bitcoin.com/btc/chart/blockchain--size

[9] Chanson, M., Fleisch, M., Wortmann, F. & Bogner, A. (2017, avgust). *Blockchain as a Privacy Enabler: An Odometer Fraud Prevention System*. Pridobljeno 17. novembra 2018 iz http://cocoa.ethz.ch/media/documents/2017/08/None_UbiComp_2017-Privacy_Poster_final_1.pdf

[10] ConsenSys (2019, 10. januar). *The Thirdening: What You Need To Know*. Pridobljeno 10. avgusta 2020 iz https://media.consensys.net/the-thirdening-what-you-need-to-know--df96599ad857

[11] Dobrovnik, M., Herold, D. M., Fürst, E. & Kummer, S. (2018, 3. september). Blockchain for and in Logistics: What to Adopt and Where to Start. *Logistics 2018*, 2(3).

[12] Dobson, D. (2018, 13. februar). *The 4 Types of Blockchain Networks Explained*. Pridobljeno 10. septembra 2020 iz https://iltanet.org/blogs/deborah-dobson/2018/02/13/the-4--types-of-blockchain-networks-explained?ssopc=1

[13] Ernst & Young Limited. (2018, 21. junij). *EY and Microsoft launch blockchain solution for content rights and royalties management for media and entertainment industry*. Pridobljeno 15. decembra 2018 iz https://www.ey.com/en_gl/news/2018/06/ey-and-microsoft-launch-blockchain-solution-for-content-rights

[14] Ethereum Foundation (2020, 11. junij). *Proof of Stake FAQs*. Pridobljeno 25. september 2020 iz https://eth.wiki/en/concepts/proof-of-stake-faqs

[15] Ethereum Foundation (2020, 28. september). *Ethereum 2.0 (Eth2)*. Pridobljeno 1. oktobra 2020 iz https://ethereum.org/en/eth2/

[16] Felin, T. & Lakhani, K. (2018). What Problems Will You Solve With Blockchain? *MIT Sloan Management Review*, 60, 32–38.

[17] Gainsbury, M. & Blaszczynski, A. (2017, september). How Blockchain and Cryptocurrency Technology Could Revolutionize Online Gambling. *Gaming Law Review*, 21(7), 482–492.

[18] Government Office for Science. (2016). *Distributed Ledger Technology: Beyond Block Chain*. Pridobljeno 1. junija 2018 iz https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16--1-distributed-ledger-technology.pdf

[19] Groenfeldt, T. (2017, 5. marec). *IBM And Maersk Apply Blockchain To Container Shipping*. Pridobljeno 9. novembra 2018 iz https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#1329a0c03f05

[20] Hackius, N. & Petersen, M. (2017, oktober). *Blockchain in Logistics and Supply Chain*: *Trick or Treat?* Pridobljeno 11. novembra 2018 iz https://tubdok.tub.tuhh.de/bitstream/11420/1447/1/petersen_hackius_blockchain_in_scm_and_logistics_hicl_2017.pdf

[21] Hayes, A. (2020, 24. septembra). *Proof of Capacity (Cryptocurrency)*. Pridobljeno 7. septembra 2020 iz https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp#:~:text=Proof%20of%20capacity%20(PoC)%20is,mining%20rights%20and%20validate%20transactions

[22] Hooper, M. (2018, 22. februar). *Top five blockchain benefits transforming your industry*. Pridobljeno 26. november 2018 iz https://www.ibm.com/blogs/blockchain/2018/02/top-five--blockchain-benefits-transforming-your-industry

[23] Karantias, K., Kiayias, A., & Zindros, D. (2020, februar). Proof--of-burn. *International Conference on Financial Cryptography and Data Security, 24*, 523-540.

[24] Kherrat, R. & Hernandez, A. (2018, 24. oktober). *Understanding the complexities of global serialisation & traceability regulations.* Pridobljeno 22. decembra 2018 iz https://www.europeanpharmaceuticalreview.com/webinar/79102/understanding-the-complexities-of-global-serialisation-traceability-regulations

[25] Lai, R. & Lee Kuo Chuen, D. (2018). Blockchain- From Public to Private. *Handbook of Blockchain, Digital Finance, and Inclusion, 2*, 145–177.

[26] Larios-Hernández, G. J. (2017, november-december). Blockchain entrepreneurship opportunity in the practices of the unbanked. *Business Horizons*. 60(6), 865–874.

[27] Lee, A. (2018, 12. januar). *Blockchain patent filings dominated by financial services industry*. Pridobljeno 14. novembra 2019 iz http://patentvue.com/2018/01/12/blockchain-patent-filings-dominated-by-financial-services-industry

[28] Lorenz, J., Münstermann, B., Higginson, M., Olesen, P. B., Bohlken, N. & Ricciardi, V. (2016, julij). *Blockchain in insurance –opportunity or threat?* Pridobljeno 18. decembra 2019 iz https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/blockchain%20in%20insurance%20opportunity%20or%20threat/blockchain-in--insurance-opportunity-or-threat.ashx

[29] Maersk. (2018, 9. avgust). *Maersk and IBM Introduce TradeLens Blockchain Shipping Solution*. Pridobljeno 9. decembra 2018 iz https://www.maersk.com/en/news/2018/06/29/maersk-and--ibm-introduce-tradelens-blockchain-shipping-solution

[30] Millard, C. (2018, avgust). Blockchain and law: Incompatible codes? *Computer Law & Security Review*. 34(4), 843–846.
[31] Morris, N. (2018a, junij). *SAP leads Pharma Supply Chain blockchain.* Pridobljeno 9. januarja 2019 iz https://www.ledgerinsights.com/sap-pharma-supply-chain/
[32] Morris, N. (2018b, junij). *EY and Microsoft announce royalties blockchain*. Pridobljeno 14. decembra 2018 iz https://www.ledgerinsights.com/ey-microsoft-royalties-blockchain/
[33] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Najdeno 9. junija 2018 na spletnem naslovu https://bitcoin.org/bitcoin.pdf
[34] Newton, D. (2018, 5. junij). *What is Corda?*. Pridobljeno 13. decembra 2018 iz https://medium.com/corda/what-is-corda-6417b14c8dc7
[35] Ramuta, M. (2018, 30. april). *Why DPoS is not really a PoS, but rather a PoA protocol*. Pridobljeno 6. septembra 2020 iz https://hackernoon.com/why-dpos-is-not-really-a-pos-but-rather-a-poa-protocol-5bb1aa305625
[36] Reed, C., Sathyanarayan U. M., Ruan, S. & Collins, J. (2018). Beyond BitCoin- legal impurities and off-chain assets. *International Journal of Law and Information Technology*, 26(2), 160–182.
[37] Reyna, A., Martín, C., Chen, J., Soler, E. & Díaz, M. (2018). On blockchain and its integration with IoT. *Challenges and opportunities. Future Generation Computer Systems, 88*, 173–190.
[38] Ripple. (2017, oktober). *Product Overview*. Pridobljeno 20. decembra 2018 iz https://ripple.com/files/ripple_product_overview.pdf
[39] Scott, T. (2018, 27. september). *TradeLens: How IBM and Maersk Are Sharing Blockchain to Build a Global Trade Platform.* Pridobljeno 9. decembra 2018 iz https://www.ibm.com/blogs/think/2018/11/tradelens-how-ibm-and-maersk-are-sharing-blockchain-to-build-a-global-trade-platform/
[40] Seffinga, J., Lyons, L. & Bachmann, A. (2017). *The Blockchain (R)evolution – The Swiss Perspective*. Pridobljeno 15. aprila 2018 iz https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-blockchain-revolution.pdf
[41] Statistični urad Republike Slovenije. (2010). *Standardna klasifikacija dejavnosti 2008*. Ljubljana: Statistični urad Republike Slovenije, 11.
[42] The Economist. (2015, 31. oktober). Blockchains: *The great chain of being sure about things*. Pridobljeno 15. septembra 2018 iz https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things
[43] Tsankov, A. (2018, 21. junij). *The "Oracle Problem« isn't a Problem, and why Smart Contracts makes Insurance better for everyone*. Pridobljeno 1. oktobra 2020 iz https://medium.com/@antsankov/the-oracle-problem-isnt-a-problem-and-why-smart-contracts-makes-insurance-better-for-everyone-8c979f09851c
[44] Varshney, N. (2018, 21. junij). *Microsoft launches ambitious blockchain project to help creators get paid.* Pridobljeno 15. decembra 2018 iz https://thenextweb.com/hardfork/2018/06/21/microsoft-and-ey-launch-blockchain-for-copyrights-and-royalties/
[45] Vos, J. (2017, 10. februar). Blockchain-Based Land Registry: Panacea, Illusion Or Something In Between? *European Land Registry Association Annual Publication, 7*. Pridobljeno 3. januarja 2019 iz https://www.elra.eu/wp-content/uploads/2017/02/10.-Jacques-Vos-Blockchain-based-Land-Registry.pdf
[46] White, M., (2018, 16. januar). *Digitizing Global Trade with Maersk and IB.* Pridobljeno 9. decembra 2018 iz https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/
[47] Whyte, J. (2016) *Serialization: An Implementation Guide*. Pridobljeno 9. januarja 2019 iz http://www.worldpharmatoday.com/whitepapers/rockwell_automation_11082016.pdf
[48] Zhang, F., Cecchetti, E., Croman, K., Juels, A. & Shi, E. (2016). Town Crier: An Authenticated Data Feed for Smart Contracts. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (str. 107–283). Dunaj. ACM.
[49] Zhu, L., Wu, Y., Gai, K. & Choo K. R. (2019, februar). Controllable and Trustworthy Blockchain-Based Cloud Data Management. *Future Generation Computer Systems*, 91, 527–5

▪

Bor Krizmanič je diplomiral in magistriral na Ekonomski fakulteti Univerze v Ljubljani, smer poslovna informatika. Ukvarjal se je z revizijo informacijskih sistemov in svetovanjem na področju informatizacije bank in zavarovalnic. Sedaj pa je asistent na Ekonomski fakulteti Univerze v Ljubljani, na katedri za poslovno informatiko in logistiko.

▪

Aleš Groznik je redni profesor na Ekonomski fakulteti Univerze v Ljubljani, katedra za poslovno informatiko in logistiko. Glavna področja njegovega raziskovalnega dela predstavljajo management oskrbovalne verige, elektronsko poslovanje in sodobna mobilnosti.