Aktualne dejavnosti, primerne za uporabo veriženja podatkovnih blokov

Eva Bizilj

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana
E-mail: eb2044@student.uni-lj.si

Povzetek. V seminarju so predstavljene osnovne značilnosti hitro razvijajoče se tehnologije veriženja podatkovnih blokov ter njene glavne prednosti in slabosti. Predstavljena so štiri področja dejavnosti za uporabo te tehnologije, ki sta jih avtorja članka Krizmanič in Groznik leta 2020 prepoznala kot najperspektivnejša na podlagi pregleda pravnega, tehnološkega in sociološkega vidika morebitne implemetacije in primerov uporabe.

Ključne besede: tehnologija veriženja podatkovnih blokov, dokaz o delu, kriptovalute, pametne pogodbe, decentralizacija

1 Uvod

Tehnologija veriženja podatkovnih blokov je relativno nova, a hitro razvijajoča se tehnologija, ki jo je leta 2008 zasnoval skrivnostni izumitelj pod psevdonimom Satoshi Nakamoto kot temeljno tehnologijo platforme Bitcoin.
V zadnjih letih se strokovna javnost veliko ukvarja z njeno uporabo v različnih panogah in z različnimi nameni, ki pa niso povezani samo s kriptovalutami.

2 Osnove tehnologije veriženja podatkovnih blokov

Tehnologija veriženja podatkovnih blokov (ang. *blockchain*) je tehnični protokol, ki omogoča izmenjavo podatkov neposredno med strankami znotraj decentraliziranega omrežja brez potrebe po posrednikih, kot so na primer banke, državne agencije ipd.

Informacije se shranjuje v verigo podatkovnih blokov, ki vsebujejo niz transakcij oz. podatkov, ki so nastali v času od nastanka predhodnega bloka. Za izdelavo blokov se uporabljajo različni protokoli, od katerih je najbolj znan protokol dokaza o delu (ang. *proof-of-work*). Pri tem protokolu vozlišča (udeleženci omrežja), imenovana rudarji (ang. *miners*), uporabljajo zgoščevalno funkcijo (ang. *hash function*) z namenom iskanja pravilne zgoščene vrednosti (ang. *hash*). Rudarji ob izračunu zgoščene vrednosti izdelajo nov blok, ki ustreza zahtevam. Vsak blok vsebuje zgoščeno vrednost vseh transakcij, ki so nastale v določenem obdobju, spremenljivko nonce in zgoščeno vrednost predhodnega bloka. Vsaka transakcija oz. podatki so tako preko blokov dodani nespremenljivi verigi in distribuirani vsem vozliščem omrežja. Kdorkoli v sistemu lahko kadarkoli preveri veljavnost katerekoli transakcije oz. podatkov.

Omrežja veriženja podatkovnih blokov se delijo po omejitvi dostopa do omrežja na javne in zasebne verige podatkovnih blokov. Najpogostejši tip omrežja je javna veriga podatkovnih blokov (ang. *public blockchain*), ki dopušča, da se omrežju lahko pridruži kdorkoli in ga tudi lahko kadarkoli zapusti. Primer takšnega omrežja je Bitcoin. V primeru protokola dokaza o delu tovrstna omrežja nagrajujejo rudarje za njihov doprinos k delovanju omrežja v obliki nagrade, ki je večinoma elektronski kovanec npr. bitcoin. Le-ta naj bi imel v realnem svetu ob menjavi neko vrednost. Zasebne verige podatkovnih blokov (ang. *private blockchain*) pa za priključitev omrežju zahtevajo predhodno preverjanje pristnosti identitete in odobritev dostopa.

Pomemben koncept v tej tehnologiji so pametne pogodbe (ang. *smart contracts*). To je nespremenljiva računalniška koda, ki je vgrajena v verigo podatkovnih blokov in omogoča izvrševanje sporazumov med strankami, ki si ne zaupajo. Za integracijo slednjih so se oblikovale nove platforme, kot je Ethereum in Hyperledger.

Omrežje tehnologije veriženja podatkovnih blokov pa predstavlja tudi zelo primeren porazdeljen sistem za delovanje decentraliziranih aplikacij (ang. *decentralized application*).

3 Prednosti in slabosti tehnologije veriženja podatkovnih blokov

Glavna prednost tehnologije veriženja podatkovnih blokov je zmožnost vzpostavitve zaupanja v decentraliziranem okolju, kar omogoča poslovanje in vzpostavitev soglasja o eni zgodovini dogodkov med udeleženci, ki si med seboj ne zaupajo in ni prisotne tretje zaupanja vredne centralne inštitucije. Ostale prednosti so transparentnost, nespremenljivost, sledljivost in preverljivost.

Po drugi strani pa je tehnologija veriženja podatkovnih blokov še nezrela tehnologija in se zato spopada s številnimi izzivi. Med eno izmed glavnih slabosti te tehnologije spada problem omejene razširljivosti oz.

kapacitete omrežja. Veriga podatkovnih blokov namreč z novimi zapisi le raste in se nikoli ne zmanjšuje. Drugo veliko slabost pa predstavljajo zakonske omejitve in negotovosti, pri katerih prevladujejo omejitve v povezavi z varstvom osebnih podatkov (Ur. l. EU št. 2016/679) in uporabo zapisov na verigi podatkovnih blokov kot dokaz o pravicah na sredstvih (npr. evidentiranje lastništva), ki niso del verige podatkovnih blokov (kot so kriptovalute) in obstajajo izven le-te.

4 PREGLED NAJPERSPEKTIVNEJŠIH GOSPODARSKIH PANOG ZA UPORABO TEHNOLOGIJE VERIŽENJA PODATKOVNIH BLOKOV

Najperspektivnejše dejavnosti za uporabo tehnologije veriženja blokov lahko najdemo znotraj štirih gospodarskih panog:

1. finančne in zavarovalniške dejavnosti
2. promet in skladiščenje
3. trgovina, vzdrževanje in popravila motornih vozil
4. informacijske in komunikacijske dejavnosti

4.1 Finančne in zavarovalniške dejavnosti

Področje finančnih dejavnosti se v literaturi pojavlja kot eno izmed najperspektivnejših za uporabo te tehnologije. Proces mednarodnih denarnih transferjev je še vedno časovno zelo potraten, zato bi lahko tehnologija veriženja podatkovnih blokov predstavljala rešitev te težave. Eden od projektov uporabe te tehnologije na področju medbančnih transakcij je rešitev RippleNet, ki sicer spada na področje širše pojmovane tehnologije razpršene evidence (ang. *distributed ledger technology*). Na področju zavarovalniških dejavnosti bi lahko to tehnologijo uporabili s pomočjo pametnih pogodb. Primer take rešitve je projekt Insurwave, v okviru katerega so razvili platformo za poslovna zavarovanja s poudarkom na transportu.

4.2 Promet in skladiščenje

Procesi v prometu in skladiščenju so administrativno zelo zahtevni in vključujejo veliko število poslovnih partnerjev, ki se med seboj večinoma ne poznajo. Rešitve, ki temeljijo na tej tehnologiji, bi lahko prinesle zmanjšanje števila stikov med poslovnimi partnerji in večjo stopnjo zaupanja ter transparentnosti. Ena izmed rešitev na področju logistike je platforma TradeLens, ki celostno digitalizira proces dobave blaga in deluje z uporabo pametnih pogodb. Nastala je v sodelovanju med podjetjema Maersk in IBM.

4.3 Trgovina, vzdrževanje in popravila motornih vozil

Tehnologijo veriženja podatkovnih blokov bi lahko uporabili za sledenje porekla blaga in poti po dobavni verigi. Podobno kot blagu pa bi bilo možno slediti tudi zdravilom, ki zahtevajo še višjo stopnjo sledljivosti. Na področju prodaje rabljenih vozil bi lahko to tehnologijo uporabili za shranjevanje podatkov o zgodovini stanja in vzdrževanja vozila ter tako naslovili težave povezane z zlorabami na tem področju. Primer uporabe tehnologije veriženja podatkovnih blokov najdemo v skupnem projektu podjetja Bosch in univerze ETH Zürich, kjer sta to tehnologijo uporabila za preprečevanje goljufij z manipulacijo števca prevoženih kilometrov v vozilih.

4.4 Informacijske in komunikacijske dejavnosti

Tehnologija veriženja podatkovnih blokov je na tem področju najbolj zanimiva za zapisovanje in nadziranje uporabe licenc programske opreme. Z uporabo te tehnologije bi lahko izboljšali ažurnost informacij o uporabi programov, ki zaradi posrednikov ni na zadovoljivi ravni. Primer rešitve na tem področju je sistem za upravljanje licenc računalniških igric, ki sta ga razvili podjetji Microsoft in Ernst & Young. Pri tej rešitvi bi s pomočjo pametnih pogodb razvijalci in založniki računalniških igric, ki svoje igrice ponujajo na Microsoftovi platformi Xbox Live, lahko imeli vpogled v prodajo njihovih izdelkov v realnem času.

5 SKLEP

Tehnologijo veriženja podatkovnih blokov je na splošno možno smiselno uporabiti v veliko manj dejavnostih in primerih, kot je to sicer splošno prepričanje oz. to želijo prikazati nekateri strokovnjaki in podjetja z interesi na tem področju. Te tehnologije namreč ne moremo uporabiti povsod in za vse namene, kot se to poizkuša sedaj. Pri številnih idejah uporabe, je zelo vprašljivo ali so le-te dejansko izvedljive, ali so v skladu z zakonodajo in ali prinašajo dovolj dodane vrednosti v primerjavi s sedanjimi tehničnimi rešitvami. Za uporabo te tehnologije so najbolj primerna področja, kjer je zelo pomembna sledjivost izdelkov na njihovi celotni poti od nastanka do porabe ter področja, kjer ni obdelave osebnih podatkov ali različnih pravic na sredstvih.
Menim, da ima tehnologija veriženja podatkovnih blokov zaradi številne in aktivne zainteresirane javnosti, ki je že oblikovala nekatere alternative osnovni arhitekturi obravnavane tehnologije, velik potencial, da spremeni številne gospodarske panoge.

LITERATURA

[1] Krizmanič, B., & Groznik, A. (2020). Aktualne dejavnosti, primerne za uporabo veriženja podatkovnih blokov. Uporabna informatika, 28(4). Pridobljeno s https://uporabna-informatika.si/index.php/ui/article/view/86
[2] http://www.cek.ef.uni-lj.si/magister/krizmanic3444-B.pdf