VARNOST TEHNOLOGIJE VERIŽENJA PODATKOVNIH BLOKOV

Avtorica: Janja Kotnik

Visoka šola za poslovne vede, Management in informatika (2. stopnja)

Povzetek

Kriptovaluta Bitcoin se je začela uporabljati pred nekaj več kot desetimi leti in zaradi potrebe po varnih transakcijah je bila hkrati zasnovana tehnologija veriženja podatkovnih blokov (blockchain). Za tehnologijo je značilna komunikacija v razpršenem omrežju tipa "vsak z vsakim" (peer-to-peer), v katerem vsak udeleženec omrežja sodeluje pri postopku potrjevanja podatkovnih blokov. Podatkovni bloki se nizajo v verige podatkovnih blokov in vsebujejo informacije o transakcijah, zgoščenih vrednostih, kriptografskih številkah, časovnih žigih ter druge podatke. Glavne prednosti tehnologije so v zaupanju med uporabniki, razpršenem in decentraliziranem okolju, sledljivosti transakcij, preverljivosti in transparentnosti. Slabosti tehnologije so velike količine podatkov, ki zahtevajo vedno več sredstev za vzdrževanje omrežja, zakonodajne omejitve in varstvo osebnih podatkov. Ranljivost tehnologije predstavljajo tudi zlonamerni napadi na omrežje, varnost zasebnega ključa in kriminalna dejavnost. Kljub temu da je tehnologija morda za na videz manj varna, gre za varno tehnologijo, saj vsak od udeležencev v omrežju teži k vzdrževanju varnosti omrežja in svojih podatkov.

Ključne besede: tehnologija veriženja podatkovnih blokov, blockchain, varnost

Uvod

Tehnologija veriženja podatkovnih blokov (*blockchain*) je tehnologija shranjevanja informacij na varen način, ki se je začela uporabljati hkrati s pojavom kriptovalut. Transakcije kriptovalut so zahtevale odprto komunikacijo med vsemi udeleženci ter zanesljive in predvsem varne povezave. Podatki o transakcijah se zapisujejo v obliki podatkovnih blokov, ki se ob vsaki transakciji oziroma spremembi dodajajo prejšnjim podatkovnim blokom in tvorijo verigo podatkovnih blokov. Prednost tehnologije je razpršena mreža uporabnikov, ki nima centraliziranega sistema shranjevanja podatkov, temveč vsak udeleženec v omrežju hrani svojo kopijo vseh preteklih transakcij in tako omogoča zaupanje v razpršenem okolju, kjer se udeleženci med seboj ne poznajo, vendar imajo enak interes, in sicer zaupanja vredno in varno omrežje (Krizmanič in Groznik, 2020). Tehnologija veriženja podatkovnih blokov je zelo primerna za področja, ki zahtevajo varnost in sledljivost podatkov (Krizmanič in Groznik, 2020).

Varnost tehnologije zagotavlja več mehanizmov, med katerimi se najpogosteje omenjajo razpršenost omrežja, algoritem soglasja oziroma soglasno mnenje vseh udeležencev, dokaz o delu oziroma dokaz o deležu, zgoščevalna funkcija ter drugi mehanizmi. Kljub vsem naštetim mehanizmom se tudi pri tej tehnologiji pojavljajo tveganja, ki grozijo predvsem s strani zlonamernih teženj posameznikov ali kriminalnih združb. Ker tehnologija zaradi razpršenega omrežja morda navidezno deluje manj varno, je v tem članku narejen pregled največkrat omenjenih varnostnih vidikov in tveganj te tehnologije.

Tehnologija veriženja podatkovnih blokov (*blockchain*)

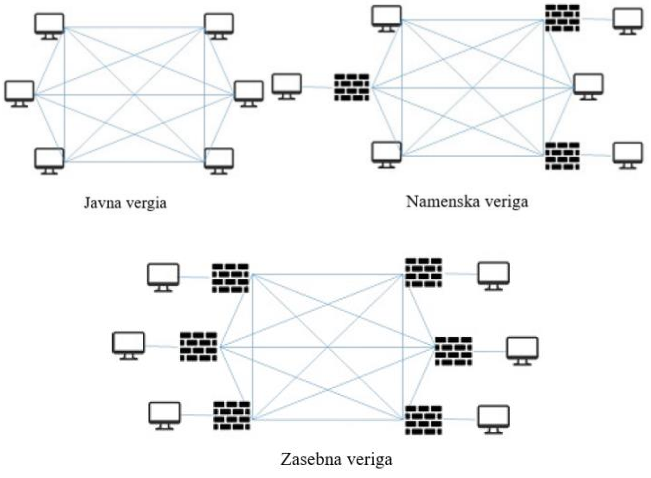
Tehnologija veriženja podatkovnih blokov (*blockchain*) je računalniški algoritem za komunikacijo v omrežju tipa "vsak z vsakim" (*peer-to-peer*) in zagotavljajo varne transakcije med udeleženci, ki se med seboj ne poznajo (Dasgupta in drugi, 2019). Poleg umetne inteligence in masovnih podatkov je ta tehnologija ena od treh temeljnih informacijskih tehnologij prihodnosti v finančnih panogah (Zhang in drugi, 2019). Uporabljati se je začela skupaj s kriptovalutami, natančneje z Bitcoinom, pred nekaj več kot desetimi leti (Zhang in drugi, 2019), ko je tehnologijo zasnoval neznani avtor, poznan pod psevdonimom Satoshi Nakamoto (Krizmanič in Groznik, 2020). Razvijala se je v dveh fazah. V prvi fazi, imenovani *blockchain 1.0* je bila usmerjena predvsem na uporabo pri kriptovalutah, v drugi fazi, *blockchain 2.0*, pa se je njena uporabnost razširila še na druga področja in vključevati so se začele tudi pametne pogodbe (Li in drugi, 2020).

Pri tehnologiji veriženja podatkovnih blokov gre za razpršeno bazo podatkov, pri kateri se vsaka transakcija zabeleži v blok, ti pa se povezujejo v verige (Zhang in drugi, 2019). Varnost in pravilnost beleženja blokov v verigi zagotavljajo kriptografija in uporabniki omrežja, ki so vključeni v omrežje "vsak z vsakim" (Zhang in drugi, 2019). Tehnologija je zasnovana tako, da ta lahko v javni verigi podatkovnih blokov sodeluje vsakdo, ki ima dostop do interneta, brez predhodne privolitve ali vloge za dostop do omrežja in brez preverjanja identitete (Krizmanič in Groznik, 2020).

Vsak podatkovni blok vsebuje informacije o dogajanju v verigi oziroma transakcijah, zgoščeno vrednost (*hash value*) istega in predhodnega bloka, enkratno kriptografsko število (*nonce*), časovni žig in ostale informacije, kot so podpis bloka in ostali podatki, ki jih določi uporabnik (Lin in Liao, 2017). Bloki se zaporedno dodajajo v verigo in zaradi podatkov, ki jih vsak blok vsebuje, verige ni mogoče spreminjati za nazaj. Ta tehnologija predstavlja varnost, saj je vsaka sprememba opazna s strani ostalih udeležencev v omrežju, imenovanih tudi rudarji, oziroma vozlišča (*node*), ki spremljajo in potrjujejo transakcije (Krizmanič in Groznik, 2020). Vsak udeleženec omrežja prejme kopijo verige podatkovnih blokov z vsemi transakcijami in vsako dodajanje novega bloka morajo potrditi ostali udeleženci, zato se uporablja kot varna, pregledna, decentralizirana oziroma razpršena podatkovna baza beleženja transakcij (Zhang in drugi, 2019), ki uporabnikom zagotavlja anonimnost, varnost in neodvisnost (Lin in Liao, 2017).

Po načinu delovanja verigo podatkovnih blokov razdelimo na tri tipe (slika 1), in sicer na javno verigo (*public blockchain*), v kateri lahko sodeluje vsak, ki ima dostop do internetne povezave, na namensko verigo (*consortium blockchain*), pri kateri imajo nekateri uporabniki prednostne in vnaprej določene vloge ter na zasebno verigo (*private blockchain*), v kateri lahko sodelujejo le izbrani uporabniki (Lin in Liao, 2017).

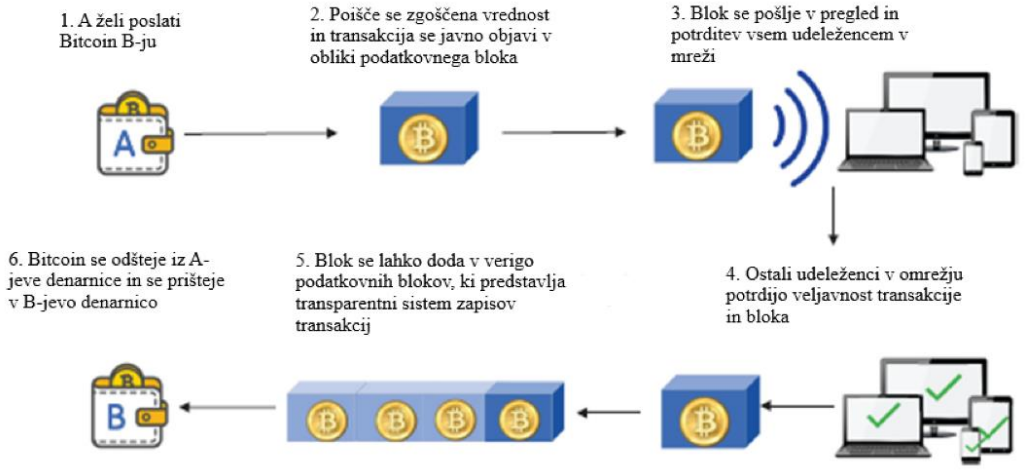
Slika 1: Prikaz treh tipov verig podatkovnih blokov (prirejeno po Lin & Liao, 2017).



Tehnologija veriženja podatkovnih blokov deluje tako, da udeleženci omrežja iščejo pravilno zgoščeno vrednost (*hash*) s pomočjo zgoščevalne funkcije (*hash function*). Ta postopek se imenuje protokol dokaza o delu (*proof-of-work, PoW*) (Krizmanič in Groznik, 2020). Ko udeleženec omrežja najde ustrezno zgoščeno vrednost, ustvari nov blok, ga javno objavi, ostali udeleženci blok pregledajo in potrdijo in blok se doda verigi predhodnih blokov (Krizmanič in Groznik, 2020).

Na sliki 2 je poenostavljen prikaz delovanja tehnologije veriženja podatkovnih blokov na primeru transakcije s kriptovaluto Bitcoin. Udeleženec A v omrežju želi opraviti transakcijo in predati Bitcoin udeležencu B v omrežju. Udeleženec A bo ustvaril transakcijo, za katero je potrebno poiskati zgoščeno vrednost, ki jo poiščejo udeleženci omrežja (podatkovni rudarji). Če so podatki o transakciji ustrezni in pravilni, se objavijo v obliki podatkovnega bloka (Lin in Liao, 2017), ki ga morajo pregledati in potrditi ostali udeleženci v mreži, postopek se imenuje dokaz o delu (*Proof-of-Work, PoW*), s čimer potrjujejo verodostojnost podatkov (Li in drugi, 2020). Dokaz o delu je zapleten postopek reševanja kriptografskih ugank, ki zahteva zmogljivejšo strojno opremo (Mohanty in drugi, 2020). Ko je podatkovni blok potrjen s strani ostalih udeležencev, se blok doda k verigi blokov, opravi se transakcija Bitcoina od uporabnika A k uporabniku B in transakcija postane dokončna in legitimna (Zhang in drugi, 2019).

Slika 2: Prikaz delovanja tehnologije veriženja podatkovnih blokov (prirejeno po Zhan, Xue & Liu, 2019).



Prednosti in slabosti tehnologije

Prednosti tehnologije veriženja podatkovnih blokov so zaupanje med uporabniki v razpršenem, decentraliziranem okolju, sledljivost, preverljivost in transparentnost podatkov (Krizmanič in Groznik, 2020). Podatki, ki so že zabeleženi in v obliki bloka dodani v verigo, ni mogoče več spreminjati, zato je tehnologija varna, uporabniki za pristop in uporabo ne potrebujemo odobritve, uporaba je anonimna, hitra, stabilna, avtonomna in globalna (Li in drugi, 2020).

Slabosti tehnologije so velike količine podatkov, saj je veriga vedno daljša, kar zahteva vedno več sredstev za vzdrževanje mreže in zaradi tega je težava tudi v razširljivosti omrežja. Slaba stran so tudi zakonske omejitve in negotovosti, med najbolj izpostavljenimi je varstvo osebnih podatkov, saj se v blokih shranjujejo tudi določeni podatki, ki jih ni mogoče brisati. Glede na to, da uporabnikov ni mogoče identificirati, je težko določiti lastninske in ostale pravice (Krizmanič in Groznik, 2020). Slabost tehnologije so tudi visoki stroški ter velika poraba časa in energije (Mohanty in drugi, 2020).

Najprimernejša področja za uporabo

Poleg uporabe pri poslovanju s kripotavluatmi, za kar je bila tehnologija tudi prvotno namenjena (Lin in Liao, 2017), so najprimernejša področja za uporabo tehnologije veriženja podatkovnih blokov še finančne in zavarovalniške dejavnosti, banke, zagonska podjetja, podjetja za skladiščenje in logistiko ter trgovine z avtomobili in avtomobilskimi deli, kjer je potrebno zagotoviti sledljivost (Krizmanič in Groznik, 2020). Zadnje čase se tehnologija vse bolj uporablja v industriji (Halpin in Piekarska, 2017). Tehnologija je zanimiva tudi za prehrambno industrijo in za področje medicine, slednja zaradi težav z varovanjem občutljivih osebnih podatkov bolj v smislu dostopnosti do podatkov in beleženja transakcij ter sledljivosti (Krizmanič in Groznik, 2020). Tehnologija je zanimiva tudi za področje informacije in komunikacijske dejavnosti predvsem za sledljivost in nadzor nad licencami programske opreme in varovanje intelektualne lastnine (Krizmanič in Groznik, 2020), certificiranje identitete, javno upravo, mednarodna

plačila ter za internet stvari (*IoT*) (Lin in Liao, 2017). Za uporabo te tehnologije je vse večji interes tudi na področju industrije, saj omogoča varne pogodbe in varne finančne transakcije, ki so hitrejše od teh, ki so trenutno v uporabi (Dasgupta in drugi, 2019).

Tveganja in varnost tehnologije

Kljub temu da velja tehnologija veriženja podatkovnih blokov za varno tehnologijo, ni mogoče zagotoviti njene popolne varnosti in v preteklosti je že bilo zabeleženih nekaj napadov (Li in drugi, 2020). Tehnologija se je in se še vedno razvija in trenutna tehnologija uporablja izboljšane mehanizme ter postopke, s katerimi se izogiba kibernetskim napadom (Dasgupta in drugi, 2019).

Tveganja

Li in drugi (2020) so v raziskavi o tveganjih te tehnologije navedli devet najbolj običajnih nevarnostni in tveganj, ki so predstavljeni v tabeli 1.

Tabela 1: Najpogostejše nevarnosti in tveganja (prirejeno po Li, Jiang, Chen, Luo & Wen, 2020).

TVEGANJE	PODROČJE
51% ranljivost	Mehanizem soglasja
Varnost zasebnega ključa	Enkripcijska shema javnega ključa
Kriminalna dejavnost	Uporaba kriptovalut
Podvojene transakcije	Mehanizem potrjevanja transakcij
Razkrivanje zasebnosti transakcij	Napaka pri oblikovanju transakcij
Pametne pogodbe za kriminalna dejanja	Uporaba pametnih pogodb
Ranljivost v pametnih pogodbah	Napaka pri oblikovanju programa
Nezadostno optimizirane pametne pogodbe	Napaka pri pisanju programa
Podcenjene operacije	Napaka pri oblikovanju EVM (*Ethereum Virtual Machine)*

Tveganje 51 % ranljivost pri tehnologiji veriženja podatkovnih blokov se nanaša na mehanizem potrjevanja in soglasja udeležencev omrežja (konsenz), ki ustvarja varnost in zaupanje med udeleženci. Tveganje nastane, kadar eden od udeležencev (ali skupina napadalcev) poseduje 51 % vozlišč, saj si s tem zagotovi večino, ki jo lahko izkoristi za manipulacije verige in prevzem celotne verige (Li in drugi, 2020). Tveganje predstavlja tudi zasebni ključ, katerega upravlja le uporabnik in ni centraliziranega sistema, ki bi imel nadzor nad zasebnimi ključi. Če uporabnik omrežja ključ izgubi ali mu je ukraden s strani kriminalnih združb, tega ključa ni mogoče več povrniti oziroma lahko kriminalne združbe upravljajo njegov račun (Li in drugi, 2020). Tveganja predstavljajo še načini uporabe tehnologije, saj lahko kriminalne združbe ali škodoželjni posamezniki uporabljajo to tehnologijo za slabe namene, kot so finančne transakcije in nakazila kriminalnim združbam, trgovinam z mamili, podpora terorističnim organizacijam, poleg nakazil se lahko za kriminalna dejanja uporabljajo tudi pametne pogodbe (Li in drugi, 2020). Ranljivost

tehnologije predstavljajo tudi napake v programu, morda zaradi oblikovanja in strukture samega programa, ali pa zaradi pojava napak in hroščev pri pisanju programskih kod (Li in drugi, 2020).

Varnost in zasebnost

Varnostnih mehanizmov pri tehnologiji veriženja podatkovnih blokov je precej, predvsem s pomočjo kriptografije, vendar se v literaturi najpogosteje omenjajo razpršenost omrežja, algoritem soglasja, dokaz o delu in deležu, anonimnost, enkripcija in zgoščevalna funkcija.

Razpršenost omrežja

Ena od pomembnejših lastnosti tehnologije veriženja podatkovnih blokov je razpršenost omrežja. Transakcije, ki se odvijajo znotraj omrežja, se zapisujejo v podatkovne verige, ob vsaki transakciji pa vsak udeleženec prejme kopijo verige. Enaki podatki so varno shranjeni na več lokacijah in niso centralizirani (Zhang in drugi, 2019), v nasprotju s centraliziranimi sistemi, kjer je nekdo odgovoren za centralno bazo podatkov, se za varnost in zanesljivost omrežja trudi vsak udeleženec omrežja posebej (Taylor in drugi, 2020). S tem se zagotavljata varnost in zanesljivost glavne knjige in se preprečuje izvajanje nepoštenih praks (Zhang in drugi, 2019).

Algoritem soglasja

Vsi udeleženci v omrežju (vozlišča) uporabljajo mehanizem soglasnega mnenja oziroma algoritma soglasja (*consensus algorithm*). Z njim potrjujejo ustreznost izdelanega bloka in pravilnost postopka (Lin in Liao, 2017), saj je vsak blok, preden se pripoji verigi, javno objavljen in ga morajo potrditi udeleženci omrežja. S tem vzdržujejo mrežo in nadzirajo pravilnost podatkov ter preprečujejo zlorabe in spremembe verige, potrditev oziroma soglasje pa mora podati večina udeležencev omrežja (Zhang in drugi, 2019).

Dokaz o delu in dokaz o deležu

Dokaz o delu (*Proof-of-Work, PoW*) je zahtevno delo, tako stroškovno kot časovno, in je prav tako eden od zanesljivih varnih mehanizmov. Izračunavanje dokaza o delu zahteva veliko električne energije in zmogljivosti računalnika za opravljanje zgoščevalne funkcije (*hash function*) in pridobivanje naključne vrednosti (*nonce*), ki so ključne vrednosti vsakega bloka in je mehanizem, ki otežuje dostop do bloka (Lin in Liao, 2017).

Pri metodi dokaz o deležu (*Proof-of-Stake, PoS*) v nasprotju z metodo dokaza o delu ni potrebno rudariti, ampak lahko udeleženci ustvarijo nov blok z deležem, ki ga prispevajo iz svojega digitalnega premoženja. Metoda je varna tudi zaradi tega, ker bi bila izvedba napada na to omrežje za napadalca veliko dražja od tega, kar bi z napadom pridobil (Lin in Liao, 2017).

Anonimnost

Udeležencem za pristop v omrežje ni potrebno razkrivati svoje identitete, dovolj je le uporaba zasebnega ključa in psevdonim za transakcijo (Halpin in Piekarska, 2017).

Enkripcija in zgoščevalna funkcija

V vsakem podatkovnem bloku se zapisi shranjujejo v enkriptirani obliki in v obliki zgoščenih vrednosti (Taylor in drugi, 2020), kar napadalcem otežuje napad in spreminjanje podatkov.

Zaključek

Vsaka tehnologija ima dobre in slabe strani, prednosti in pomanjkljivosti. Tehnologija veriženja podatkovnih blokov se je razvila pred približno desetimi leti z namenom varnega poslovanja s kriptovalutami, zato je bila glavna naloga tehnologije varnost. Zagotavljanje varnosti v digitalnem svetu je precej zahtevno in nikoli ne moremo trditi, da smo popolnoma varni pred zlonamernimi napadalci.

Tehnologija veriženja podatkovnih blokov je inovativna in namesto običajnega centraliziranega sistema shranjevanja podatkov temelji na decentraliziranem sistemu oziroma na razpršenih omrežjih. Centralizirani sistemi so enostavnejša tarča zlonamernih napadalcev, saj si morajo zagotoviti dostop le do ene točke, ki je običajno dobro zavarovana in zanjo skrbi ena ali nekaj oseb. Pri razpršenem sistemu shranjevanja, kot je to pri tehnologiji veriženja podatkovnih blokov, je shramba razpršena med vse udeležence in vsak izmed njih hrani kopijo vseh preteklih transakcij. Zlonamerni napadalci imajo zato veliko težje ali celo nemogoče delo, pridobiti vse kopije vseh preteklih transakcij, ki so poleg tega, da so shranjene na različnih lokacijah, zavarovane še z drugimi mehanizmi.

Kljub temu da gre pri tej tehnologiji morda za na videz dvomljivo varnost, saj se udeleženci omrežja med seboj ne poznajo, njihova prava identiteta je skrita, do omrežja pa lahko dostopa vsakdo, ki ima povezavo na internet, vsi udeleženci stremijo k istemu cilju – vsak si želi varno in zanesljivo omrežje. Zato s potrjevanjem novih blokov, ki morajo biti potrjeni z večino udeležencev ustvarjajo varnost, saj se zavedajo, da s tem skrbijo tudi za varnost svojih podatkov.

Viri in literatura

Dasgupta, D., Sherin, J., & Gupta, K. D. (2019). A survery of blockchain from security perspective. *Jurnal of Banking and Financial Technology*, 1-17.

Halpin, H., & Piekarska, M. (2017). Introductino to Security and Privacy on the Blockchain. *2nd IEEE European Syposium on Security and Privacy, France*, 1-3.

Krizmanič, B., & Groznik, A. (2020). Aktualne dejavnosti, primerne za uporabo veriženja podatkovnih blokov. *Uporabna informatika, 4*(XXVIII), 175-185.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, 1-25.

Lin, I.-C., & Liao, T.-C. (2017). A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security, 19*(5), 653-659.

Mohanty, S. N., Ramya, K., Sheeba Rani, S., Gupta, D., Shankar, K., Khanna, A., & Lakshmanaprabu, S. (2020). An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems, 102*, 1027-1037.

Taylor, P., Dargahi, T., Dehghantanha, A., Parizi, R., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*, 147-156.

Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. *ACM Comput. Surv., 52*(3), 34.