

TERMINOLOGIJA ULANČANIH BLOKOVA NA HRVATSKOME JEZIKU

Andro Babić

Sažetak

Blockchain ili ulančani blokovi recentna su tehnologija za koju se pokazao izniman interes na svjetskim tržištima. Korištenje takve disruptivne tehnologije unutar jezične zajednice zahtijeva razumijevanje problematike na jeziku te zajednice. U ovom slučaju riječ je o hrvatskom jeziku, koji se u terminološkome smislu nedovoljno brzo prilagođava tehnološkim inovacijama. Činjenica da tehnologija ulančanih blokova ima niz potencijalnih primjena u raznim aspektima poslovanja i ljudskog života ukazuje na potrebu za popisivanjem, opisivanjem i ujednačavanjem terminologije koja se odnosi na tu tehnologiju. U ovome se radu razmatraju engleski termini povezani s tehnologijom ulančanih blokova i njihovi potencijalni terminološki ekvivalenti na hrvatskome jeziku te nudi pojmovnik ključnih termina i njihovih definicija. Istraživanjem provedenim u sklopu rada ispituju se stavovi stručnjaka i entuzijasta o predloženim terminima na hrvatskom jeziku. Nastoji se ponuditi polazište za obradu terminologije disruptivnih tehnologija, uključivanjem mišljenja stručnjaka u terminološki rad.

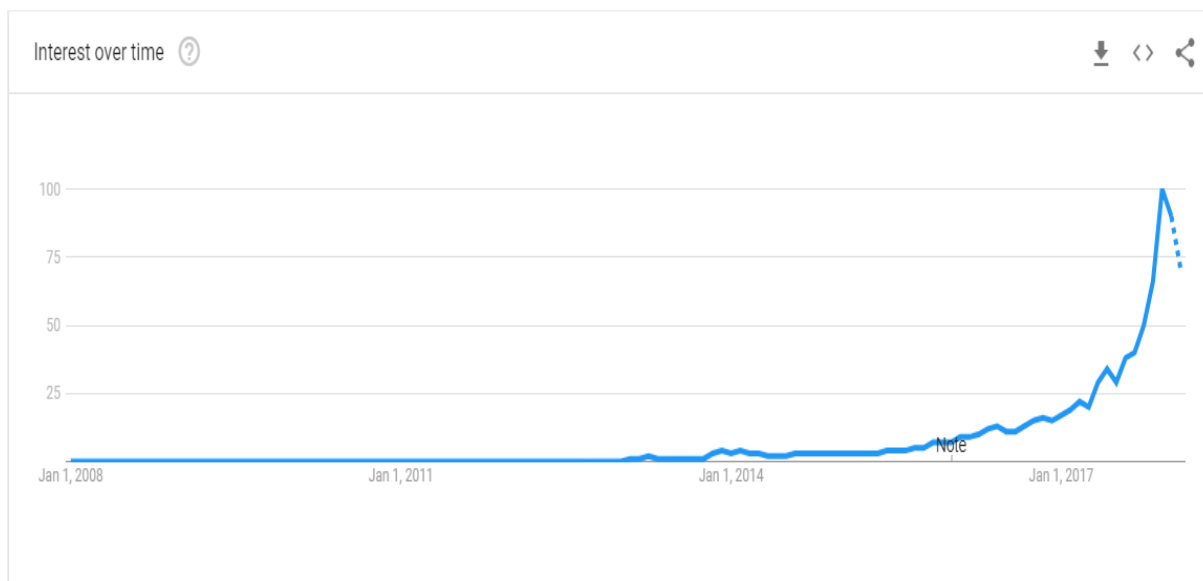
1. Uvod

Blockchain ili tehnologija ulančanih blokova recentna je ometajuća ili disruptivna tehnologija čiji je hitri razvoj i rast popularnosti nadmašio mogućnosti znanstvene zajednice da opiše i definira tu računalnu tehnologiju i sve njezine funkcije. Trend institucionalne nezainteresiranosti naglo se promijenio proteklih godina kad su razni oblici odgovorne i ekonomski isplative uporabe tehnologije ulančanih blokova razbili stigmatu sive ekonomije i nelegalnog trgovanja novcem. Literatura koja se bavi ovom tematikom obiluje proturječnim definicijama i shvaćanjima ključnih pojmova te će se u ovom radu pokušati ponuditi različite interpretacije kako bi se stvorila što cjelovitija slika tehnologije ulančanih

blokova, njene povijesti, potencijalne primjene i tehničkih funkcija u svrhu popisivanja i ujednačavanja s njome povezane terminologije.

Prva i do danas najuspješnija primjena tehnologije ulančanih blokova zasigurno je digitalna valuta *bitcoin*. U bijeloj knjizi *bitcoina* iz 2008. godine naslovljenoj „*Bitcoin: A Peer-to-Peer Electronic Cash System*“ prvi je put predloženo korištenje ulančanih blokova kao temelja za sustav digitalnog plaćanja (Nakamoto 2008). Članak potpisuje Satoshi Nakamoto, što je pseudonim za autora ili autore zadužene za osmišljavanje i implementaciju prvog sustava ulančanih blokova, a do danas nije otkriveno tko stoji iza tog pseudonima. *Bitcoin* se još naziva i kriptovalutom (engl. *cryptocurrency*) jer je tehnologija utemeljena na kriptografiji. Od 2008. *bitcoin* bilježi nagli rast u vrijednosti, a platforma doživljava stostruki porast korisnika. Po uzoru na *bitcoin* nastaju alternativne kriptovalute (engl. *altcoin*), od kojih se kao najuspješnija pokazala kriptovaluta *ethereum*. Uspjeh primjene tehnologije ulančanih blokova na projekt *bitcoin* otvorio je vrata novim interpretacijama i primjenama te tehnologije. Alternativne kriptovalute najbolji su pokazatelj svestranosti tehnologije i njenih šarolikih primjena. Osim kriptovaluta, tržišni uspjeh doživjele su i platforme za razvoj *blockchaina* u poslovanju. Hyperledger, projekt Zaklade Linux (2018), nudi alate otvorenog koda za razvoj sustava ulančanih blokova i aplikacija koje se njima služe, dok IBM-ova platforma za *blockchain* nudi komercijalna rješenja te usluge razvoja i implementacije ulančanih blokova u poslovanju i komunikaciji između institucija (IBM 2018).

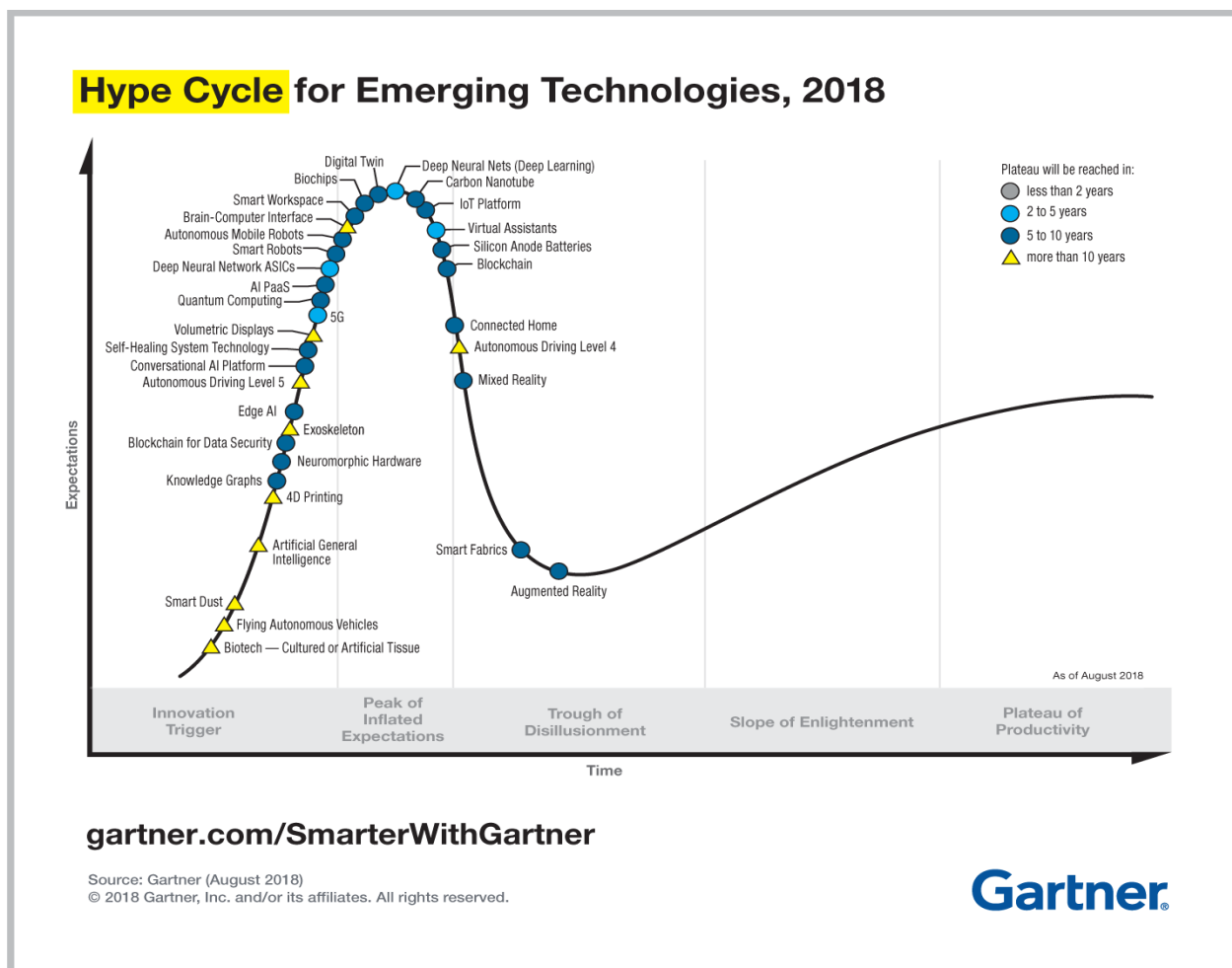
Popularnost ove tehnologije najbolje se može vidjeti upravo iz mrežnih izvora. Usluga Google trendovi dobar je pokazatelj interesa javnosti za određenu temu jer bilježi broj pretraživanja nekog pojma tijekom vremena. Tehnologija ulančanih blokova svijetu je predstavljena 2008., a od sredine 2013. interes za nju blago raste te je od početka 2016. zabilježen drastičan porast javnog interesa (Slika 1).



Slika 1 – Google trendovi, popularnost pretraživanja pojma „blockchain“

U svrhu mjerenja ciklusa trendova u informacijskim tehnologijama tvrtka Gartner (2019) osmislila je *hype cycle*, vizualni prikaz razvoja tehnoloških trendova. Takvi trendovi počinju inovacijom te zatim prolaze kroz vrhunac preuveličanih očekivanja, nakon kojeg slijedi pad uzrokovan razočaranjem u tehnologiju te se tek uslijed razočaranja postiže razumijevanje ili prosvjetljenje, nakon kojeg slijedi razina stabilne produktivnosti (plato) tijekom koje tehnologija zaista doživljava svoj potpuni potencijal. Prema metodologiji tvrtke Gartner, ulančani blokovi vrhunac će doživjeti tek za pet do deset godina, a trenutno se nalaze na prijelazu iz faze preuveličanih očekivanja u fazu razočaranja (Slika 2).

Ulančani blokovi u ciklusu trendova prate sličnu putanju kao i sljedeće napredne tehnologije: autonomna vozila, pametne kuće i stanovi te strojno učenje. Razumijevanje ciklusa trendova važno je kako bi se izbjeglo preuveličavanje važnosti neke tehnologije. Senzacionalizam, tehnološki entuzijazam i optimizam utječu na pogrešno tumačenje i razumijevanje ometajućih tehnologija. Naime, prepoznavanje potencijala neke tehnologije da promijeni svijet i realizacija te promjene dva su događaja često udaljena desecima godina. *Hype cycle* tvrtke Gartner ukazuje na dvije ključne činjenice o tehnologiji ulančanih blokova: ona je trenutno izrazito popularna i atraktivna ulagačima, znanstvenicima i javnosti, no i dalje je tehnologija u povojima čiji rastući trend nipošto ne jamči potpunu realizaciju svih pretpostavljenih promjena. Istraživanju i interpretaciji te tehnologije stoga treba pristupiti s dozom skepse.



Slika 2 – Gartnerov ciklus trendova

Jedan od načina kojima se može potaknuti i olakšati istraživanje novih tehnoloških trendova unutar neke jezične zajednice zasigurno je uspostava terminologije. Terminologija je „leksička komponenta specijaliziranog jezika [koja se] javlja zbog teorijskih i tehnoloških inovacija, novih znanstvenih uvida i novih alata koji obogaćuju konceptualna i praktična okruženja stručnjaka i u tom procesu proširuju njihov vokabular“ (Geeraerts 2015: xvii). Iz prethodnih dijelova teksta jasno je da su ulančani blokovi upravo takva, nova tehnologija, koja se razvija na engleskom govornom području, zbog čega se terminologija spontano razvija na engleskom jeziku. Na drugim jezicima, uključujući i hrvatski, spontani bi razvoj terminologije trajao predugo. Naime, disruptivne tehnologije odlikuju se naglim i snažnim utjecajem na tržište. Uslijed takvih naglih tehnoloških promjena vrijeme prilagodbe igra ključnu ulogu. Prilagodba se u ovom slučaju može smatrati prilagodbom tradicionalnih tržišnih aktera na tržišne

promjene, ali i prilagodbom nekog društva ili jezične zajednice na disruptivnu tehnologiju. Ovladavanje terminologijom disruptivnih tehnologija unutar jezične zajednice omogućuje bržu prilagodbu i povećava potencijal iskorištavanja tehnologije u korist iste zajednice. Teresa M. Cabré (1999: 26) na tu temu piše:

Terminološki rad povezan s jezičnim planiranjem za cilj ima ojačati i proširiti korištenje jezika, čineći ga tako iskoristivim u svim kontekstima. Iako mogućnost svakog jezika da opiše svaku specifičnu situaciju nije osporiva, društvene i gospodarske nejednakosti među državama omogućile su nekim jezicima da se razvijaju prirodno u toku s tehnološkim i komercijalnim razvojem, dok su drugi jezici u tome zaostajali. Jezik koji se ne može koristiti u svim kontekstima osuđen je na nestanak, a jezik nije moguće koristiti ukoliko nema potrebnu terminologiju.

Neosporivo je da se hrvatski nalazi među jezicima koji se spontano ne razvijaju dovoljno brzo u toku s globalnim tehnološkim i komercijalnim razvojem pa je ovakvo sistematsko razjašnjavanje i popisivanje termina jedan od načina koji mogu oplemeniti jezik i omogućiti njegovo korištenje u novim tehnološkim kontekstima te obogatiti informatičku pismenost unutar jezične zajednice. Potreba za razvojem i standardizacijom terminologije na hrvatskom jeziku jasno je vidljiva jer je tema ulančanih blokova u svijetu sve više prisutna u sferi javnog života, medija, poslovanja i znanstvenog istraživanja pa se takav trend može očekivati i u Hrvatskoj.¹ Tu potrebu prepoznale su i druge skupine, poput Međunarodnog ureda za standarde, čiji se rad na terminologiji ulančanih blokova odvija usporedno s ovim prikupljanjem i istraživanjem terminologije ulančanih blokova (HZN/TO 307, 2019.; ISO/TC 307, 2019.). Budući da Međunarodni ured za standarde posjeduje veće resurse i širi tim stručnjaka, njihov rad, kada postane dostupan, svakako treba konzultirati u slučaju manjkavosti i nedostataka ovog rada.

Motivacija za ovu temu proizlazi, dakle, iz prepoznavanja jezične potrebe za obradom terminologije ulančanih blokova na hrvatskome jeziku. Cilj je rada potaknuti oblikovanje terminologije u tome području, kao i u području drugih disruptivnih tehnologija.

¹ vidi: The Increased Popularity of Blockchain Technology in Various Sectors, <https://www.prnewswire.com/news-releases/the-increased-popularity-of-blockchain-technology-in-various-sectors-885208900.html>

2. Definicije tehnologije ulančanih blokova

Izgradnja i razvoj terminologije zahtjevan je proces koji iziskuje prepoznavanje novih pojmova (konceptata), definiranje tih pojmova te iznalaženje odgovarajućih naziva (termina) za te pojmove. Promotrimo stoga najprije nekoliko definicija samoga termina „ulančani blokovi“ iz nedavno objavljene literature. William (2016: 1) ulančane blokove definira kao „skupinu transakcija, koje čine zajedničku glavnu knjigu, koje su upisane u bazu podataka i provjerene od strane više izvora“. Tapscott i Tapscott (2016: 45) iz financijske perspektive ulančane blokove smatraju „globalnom distribuiranom glavnom knjigom [...] koja omogućuje izravno slanje novca među korisnicima, zaobilazeći banke, tvrtke koje izdaju kreditne kartice ili Paypal“. Narayanan i sur. (2016: 45) ulančane blokove opisuju kao „ključnu komponentu *bitcoina*; glavnu knjigu u koju su na siguran način zapisane sve *bitcoin* transakcije“. Bashir (2017: 16) ulančane blokove interpretira slijedećim riječima:

Ulančani blokovi u srži su distribuirana glavna knjiga na *peer-to-peer* mreži, koja je kriptografski osigurana, na koju se mogu isključivo dodavati podaci, koja je nepromjenjiva i koja se može ažurirati isključivo pomoću konsenzusa ili slaganja između ravnopravnih računala na mreži.

Iz tih se definicija jasno može zaključiti da ulančani blokovi čuvaju zapise. U kontekstu kriptovalute (*bitcoina*) čuvaju se zapisi o novčanim transakcijama, no ulančani blokovi kao tehnologija imaju daleko širu primjenu od bilježenja isključivo novčanih transakcija. Nijedna od navedenih definicija nije potpuna, no svaka sadrži relevantan element u definiranju termina ulančani blokovi. Ti su elementi redom: poistovjećivanje ulančanih blokova s glavnom knjigom, organizacija mreže *peer-to-peer*, odnosno distribuiranost sustava, aspekt digitalne baze podataka, sigurno zapisivanje podataka te potreba za konsenzusom. Potpunu definiciju nije moguće ponuditi bez detaljnijeg pregleda teme kojim će se popisati svi tehnički i tehnološki elementi sustava.

2.1 Tehnički aspekti ulančanih blokova

Tehnologija ulančanih blokova zasniva se na konceptu distribuirane glavne knjige. Distribuirana glavna knjiga (engl. *distributed ledger*) mrežna je baza podataka s otvorenim pristupom kojoj mogu pristupiti i koju mogu ažurirati svi

umreženi sudionici (Mills i sur. 2016: 10). Prijenos podataka i informacija je trenutno, a točnost se podataka kontrolira kriptografski (Economist 2015). U svrhu preciznijeg opisivanja osnovnog pojma, uz definicije navedene u prethodnom odlomku, potrebno je razmotriti još neke koje nude stručnjaci. Jedna od četiriju najvećih konzultantskih tvrtki KPMG ulančane blokove definira kao „bazu podataka u obliku distribuirane glavne knjige koja čuva stalno rastuću količinu zapisa o transakcijama poredanih u blokove zaštićene od falsifikacije i naknadnog mijenjanja“ (Samman i Seibold 2018). Deloitte (2016: 9) pak ulančane blokove smatra „generičkim imenom za obitelj tehnologija koje nude istu funkcionalnost kao *bitcoin*, no koje koriste različiti pristup u realizaciji tih funkcija, koristeći različite algoritme“. PWC (2018) za ulančane blokove kaže da su „distribuirana glavna knjiga svih transakcija unutar mreže, koja decentralizira povjerenje i omogućuje protok vrijednosti bez posrednika“. Prema Crespigny (2016: 63) Ernst & Young ulančane blokove pak definira kao vrstu „baze podataka koja bilježi rastući popis nepromjenjivih zapisa, tzv. blokova“.

Ulančani blokovi u svakom su slučaju distribuirana glavna knjiga, koja se ponekad opisuje i kao baza podataka. U svakoj definiciji opisan je način zapisivanja podataka u tu glavnu knjigu; naime, važno je da su podaci logički organizirani u blokove te da su kriptografski osigurani. Neke definicije spominju transakcije, dok druge govore isključivo o čuvanju zapisa u širem smislu. U tom slučaju, za definiciju je prikladniji pojam šireg značenja kako sama definicija ne bi ograničila poimanje primjene tehnologije. Velik je naglasak na nekrivotvorivosti i nepromjenjivosti zapisa unutar ulančanih blokova, što je jedna od ključnih funkcija sustava. Za potrebe ovoga rada, ulančani blokovi definirani su kao baza podataka u obliku distribuirane glavne knjige u kojoj se bilježe nepromjenjivi zapisi organizirani u kriptografski osigurane blokove.

Glavna knjiga kao pojam iz računovodstva označava dokument kojim se bilježe zapisi o poslovanju poduzeća. Distribuirana glavna knjiga decentralizirani je način čuvanja zapisa u kojem više entiteta podatke može upisivati u glavnu knjigu. U ovom slučaju atribut distribuiranosti proizlazi iz decentralizirane prirode sustava jer sva računala na mreži mogu upisivati podatke u glavnu knjigu. Lanac blokova ustvari je kriptografski zapisana glavna knjiga, organizirana u blokove koji povezani čine logički lanac. Takav lanac blokova omogućuje dugoročno čuvanje zapisa upisanih u distribuiranu glavnu knjigu bez mogućnosti mijenjanja

i ažuriranja postojećih zapisa. Potpuna otvorenost sustava postiže se kriptografskim konsenzusom. Opisujući *bitcoin* sustav, Narayanan i sur. (2016: 15) poistovjećuju ulančane blokove i distribuiranu glavnu knjigu: „još jedna ključna komponenta *bitcoina* su ulančani blokovi: glavna knjiga koja na siguran način bilježi transakcije“. Taj siguran način bilježenja ovaj sustav postiže kombinacijom kriptografije, logičkog slijeda podataka i vremenskih oznaka (Ibid.).

U distribuiranom otvorenom sustavu, kao što je lanac blokova, kriptografija osigurava integritet glavne knjige, autentičnost zapisa u njoj, povjerljivost pri upisivanju podataka u lanac te jedinstveni identitet sudionika u mreži. Svaki blok u lancu ustvari je skup zapisa kriptiranih funkcijom SHA-256. SHA-256, punim nazivom *Secure Hash Algorithm*, kriptografska je funkcija za sažimanje (engl. *cryptographic hash function*) koja određeni tekstualni unos pretvara u *hash* vrijednost. *Hash* vrijednost je niz brojeva i znamenki jedinstven za svaki unos. Iz *hash* vrijednosti nije moguće rekonstruirati originalni zapis, no vlasnik originalnog zapisa može provjeriti točnost jedinstvene *hash* vrijednost u bloku. Na taj se način osigurava transparentnost, povjerljivost i pristup podacima. *Hash* vrijednost je jedinstvena jer čak i najmanja promjena informacije pri unosu potpuno mijenja zapis. Narayanan i sur. (2016) definiraju kriptografsku funkciju za sažimanje adekvatnu za sustav ulančanih blokova kao matematičku funkciju koja zadovoljava nekoliko kriterija. Na primjer, kriptografska funkcija za sažimanje mora podržavati ulaznu vrijednost neograničene veličine, što omogućuje da se u ulančane blokove spremaju sve vrste digitalnih zapisa, neovisno o njihovoj veličini. Nadalje, ulazna vrijednost proizvodi izlaznu vrijednost predodređene veličine; u slučaju enkripcije funkcijom SHA-256 riječ je o zapisu veličine 256 bita. Kriptografska funkcija u sustavu ulančanih blokova mora ulaznu vrijednost brzo preračunati u izlaznu, odnosno kriptografska funkcija za sažimanje u kontekstu ulančanih blokova mora se moći lako izračunati. Osim što mora imati gore navedene funkcije, kriptografska funkcija za sažimanje mora biti otporna na koliziju, tj. dva različita ulaza ne smiju proizvesti jednaku izlaznu vrijednost. Kriptografska funkcija za sažimanje k tome mora biti i skrivajuća; ako je $y = hash(x)$, onda nije moguće izračunati vrijednost x iz vrijednosti y . Zadnje svojstvo koje kriptografska funkcija za sažimanje mora podržavati jest mogućnost postavljanja kriptografske zagonetke (engl. *puzzle*

friendliness)(Ibid.). To svojstvo izrazito je važno za konsenzusne protokole opisane u nastavku teksta.

Lanac blokova grade računala spojena u *peer-to-peer* mrežu. Računala koja sudjeluju u izgradnji lanca u mreži mogu služiti kao čvor (engl. *node*) ili rudar (engl. *miner*). Čvor je svako računalo na mreži koje čuva kopiju cijelog lanca blokova i provjerava točnost novih zapisa te ih odobrava ili odbija. Konsenzus se postiže prihvaćanjem novog bloka od strane kvalificirane većine (50 % plus 1) čvorova na mreži. Kod nekih konsenzusnih mehanizama, uobičajeno kad je riječ o kriptovalutama, novi blokovi nastaju rudarenjem. U mreži ulančanih blokova rudari su računala koja koriste procesorsku snagu za izračun novog bloka i stjecanje kriptovrijednosti. Samo čvor koji je prvi izračunao traženu vrijednost drugim čvorovima predlaže novi blok. To je moguće postići uz korištenje velike količine procesorske snage, najčešće međusobno povezanog velikog broja grafičkih kartica. Takav pristup, utemeljen na konceptu dokaza o radu (engl. *proof-of-work*) omogućava stjecanje virtualne vrijednosti, kao što je to *bitcoin*, jer se u zamjenu za dokaz o radu dobiva kriptovaluta. Postoje i konsenzusni mehanizmi distribuirane glavne knjige koji ne zahtijevaju dokaz o radu jer nije cilj stjecanje virtualne vrijednosti.

Računala u funkciji čvorova nadalje mogu biti djelomični čvorovi (engl. *partial node*) i potpuni čvorovi (engl. *full node*). Bashir (2017: 21) čvorove unutar ulančanih blokova opisuje na sljedeći način:

Čvor u mreži ulančanih blokova obavlja razne funkcije ovisno o ulozi koju preuzima. Čvor može predlagati i potvrđivati transakcije, rudariti kako bi se ojačao konsenzus i osigurali ulančani blokovi. To se postiže konsenzusnim protokolom (najčešće protokolom PoW). Čvorovi također mogu obavljati druge funkcije, na primjer jednostavno potvrđivanje uplata, provjeravanje i mnoge druge funkcije ovisno o vrsti ulančanih blokova i ulozi koja je pridana čvoru.

Korisnik koji želi sudjelovati u izgradnji ulančanih blokova na svoje će računalo instalirati željeni softver, čijim će pokretanjem spojiti svoje računalo na mrežu i započeti obavljanje određene funkcije unutar mreže.

Povjerenje u sustav ulančanih blokova postiže se distribuiranim konsenzusom računala spojenih na mrežu. Pojam „konsenzus“ u ovom kontekstu prelazi svoje općejezično značenje. Budući da svaki entitet spojen na mrežu može pohranjivati podatke u lanac blokova, neophodno je da najmanje kvalificirana većina

distribuiranih sudionika provjeri podatke i složi se s njihovim upisivanjem u lanac. U umreženim sustavima to se postiže konsenzusnim algoritmima, čiji je cilj onemogućiti neovlašteno upisivanje podataka ili dvostruke transakcije (engl. *double spending*). Povjerenje u distribuirani konsenzus proizlazi iz tzv. bizantske tolerancije na pogreške (engl. *Byzantine fault tolerance*). Naime, svaki sustav koji koristi distribuirani konsenzus mora riješiti tzv. problem bizantskih generala (engl. *Byzantine generals problem*).² U otvorenom (engl. *permissionless*) sustavu ulančanih blokova konsenzus se može postići pomoću raznih algoritama. Najuspješniji konsenzusni algoritmi trenutno su: dokaz o radu (engl. *proof of work, PoW*)³ i dokaz o ulogu (engl. *proof of stake, PoS*). U zatvorenom (engl. *permissioned*) sustavu konsenzus se ne mora utvrđivati pomoću konsenzusnih algoritama, već administrator kontrolira broj računala u mreži koja će konsenzusom donositi odluke, dok se u otvorenom bilo koje računalo može priključiti i sudjelovati u donošenju konsenzusa. Također se razlikuju i javni (engl. *public*) i privatni (engl. *private*) sustavi ulančanih blokova. Razlika je u tome da u otvorenim sustavima nije potrebno dobiti autorizaciju za upisivanje

² Problem bizantskih generala klasična je logička zagonetka u kojoj skupina bizantskih generala opsjeda neki grad. Svaki general zapovijeda dijelom vojske, a generali komuniciraju putem poruka kako bi razvili zajednički plan napada. Među njima je određen broj izdajnika, koji namjerno mogu sabotirati dogovore. Cilj je da se korištenjem matematike postigne da svi lojalni generali napadnu u isto vrijeme, a da ih izdajnički generali ne nagovore na loš plan. Matematički je dokazano da konsenzus u ovakvom slučaju nije moguć ako je više od jedne trećine izdajničkih generala (Narayanan i sur. 2016.). Svaki sustav ulančanih blokova koji se zasniva na distribuiranom konsenzusu mora ponuditi rješenje za ovaj problem te pokazati da sustav ima bizantsku toleranciju na pogreške. U sustavu ulančanih blokova računala zauzimaju mjesto generala, dok je dogovor o planu napada u stvari konsenzus o upisivanju podataka u ulančane blokove. Maliciozna računala ne smiju moći omesti rad benevolentnih računala kako bi se postigao distribuirani konsenzus.

³ Algoritam *dokaza o radu* kriptografska je zagonetka koja služi kao dokaz da je neko računalo utrošilo procesorski kapacitet kako bi došlo do rješenja. Algoritam su predložili Jakobson i Juels (1999) kao mjeru sprječavanja nepoželjnih (*spam*) poruka. U sustavu ulančanih blokova algoritam dokaza o radu od rudarskih računala iziskuje izračun jednokratnog kriptografskog izraza (engl. *nonce*) prema pravilima mreže. Za rješavanje jedne kriptografske zagonetke potrebna je golema količina procesorske snage nekog računala. Vrijednost jednokratnog kriptografskog izraza definirana je pravilima koja tu vrijednost čine izrazito vremenski zahtjevnom za izračun. Ovaj mehanizam zahtjeva da rudar koji upisuje novi blok u lanac utroši pozamašnu količinu procesorske snage, no i sprječava naknadno mijenjanje zapisa upisanih u lanac. Kako bi se već upisani zapis promijenio, maliciozni akter mora ponuditi novi izračun jednokratnog kriptografskog izraza za blok koji mijenja, kao i za svaki prijašnji blok u lancu. Budući da je za svaki postojeći blok već ponuđen dokaz o radu u obliku jednokratnog kriptografskog izraza i činjenice da lanac stalno raste, procesorska snaga utrošena za mijenjanje zapisa u lancu mora biti veća od one utrošene u izračunavanje svih blokova nastalih nakon promijenjenog bloka. U otvorenom sustavu to znači da maliciozni akter mora posjedovati više od 50 % procesorske snage u cijeloj mreži, a u zatvorenom sustavu kontrolirati više od 50 % računala kako bi izgradio najdulji lanac blokova. Time bi mogao preuzeti kontrolu nad daljnjim razvojem lanca blokova, ali i dalje ne bi mogao mijenjati ono što je do tog trenutka zapisano i što su svi ostali čvorovi potvrdili kao istinu.

podataka u ulančane blokove, dok u zatvorenim sustavima korisnici moraju imati autorizaciju; u javnom sustavu ulančanih blokova pak mogu sudjelovati svi, dok u privatnim mogu sudjelovati samo računala pozvana u mrežu.

Svi navedeni elementi zajedno čine sustav ulančanih blokova u kontekstu kriptovaluta, čija se logička struktura zasniva na povezanosti između kriptografskih jedinica – blokova. Blok je niz zapisa kriptiranih u jednu cjelinu s nekim dodanim informacijama. Bashir (2017: 19) blok opisuje ovako: „Blok se sastoji od više transakcija i drugih elemenata kao što su *hash* vrijednost prijašnjeg bloka, *hash* pokazivač, vremenska oznaka i jednokratni kriptografski niz“. Svaki blok u sebi ima zapisanu *hash* vrijednost prijašnjeg bloka. Ta vrijednost ustvari ima funkciju povezivanja uzastopnih blokova u slijed. *Hash* vrijednost prijašnjeg bloka ima funkciju pokazivača jer pokazuje koji blok dolazi prije trenutnog bloka, čime se osigurava točan raspored blokova te onemogućava naknadno mijenjanje zapisa u ulančanim blokovima. Narayanan i sur. (2016: 10-11) pišu:

Hash pokazivač jednostavno je pokazivač koji pokazuje gdje se nalazi informacija, uz kriptografsku *hash* vrijednost te informacije. Dok obični pokazivač nudi mogućnost pronalaska informacije, *hash* pokazivač također omogućuje da provjerite je li informacija promijenjena.

Sve informacije pridodane bloku bilježe se u zaglavlje bloka (engl. *block header*). Osim *hash* pokazivača u bloku se nalaze kriptirane informacije u obliku Merkleovog stabla. Na primjer, sustav ulančanih blokova koje koristi *bitcoin* u blokove bilježi *hash* vrijednosti novčanih transakcija. Svaka transakcija se u lancu prikazuje kao jedinstvena *hash* vrijednost. Iz te *hash* vrijednosti ne može se zaključiti identitet sudionika ni vrijednost transakcije, ali sudionici posjeduju dokaz da je transakcija obavljena. No neopreznim korištenjem kriptovaluta moguće je doznati identitet korisnika.^{4, 5} Kad se u jednom bloku zabilježi dovoljan broj transakcija ili kad prođe određeno vrijeme između formiranja dvaju blokova zadano sustavom, sve novozaprimljene *hash* vrijednosti zajedno s *hash* vrijednošću prethodnog bloka koja u sebi sadrži *hash* vrijednosti prijašnjih

⁴ Vidi: How can I trace a Bitcoin wallet owner using their wallet address?, <https://www.quora.com/How-can-I-trace-a-Bitcoin-wallet-owner-using-their-wallet-address>

⁵ Vidi: Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address, <https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/>

blokova kriptiraju se istom funkcijom, čime se dobiva jedinstvena *hash* vrijednost cijelog bloka. Logičkim slijedom blokova u kojem svaki novi blok sadrži *hash* vrijednost svih prijašnjih blokova omogućava se dugoročno, sigurno čuvanje zapisa o transakcijama. Takav logički slijed *hash* vrijednosti naziva se Merkleovim stablom. Merkleovo stablo kriptografski je alat koji omogućuje sigurnu i brzu provjeru sadržaja velike količine podataka (Becker 2008: 12). Blok se, dakle, sastoji od *hash* vrijednosti zapisa i zaglavlja u kojem se nalazi *hash* vrijednost prijašnjeg bloka, *hash* pokazivač i vremenska oznaka.

U sustavu ulančanih blokova razlikujemo više vrsta blokova. Prvi blok u ulančanim blokovima naziva se inicijalnim blokom (engl. *genesis block*). Budući da prvom bloku ne možemo pridodati *hash* pokazivač na prijašnji, u njega umjesto *hash* pokazivača bilježimo neku arbitrarnu informaciju koja će služiti kako bismo dali vremenski kontekst pokretanju sustava. Pri izradi inicijalnog bloka provenijencija je neupitna jer inicijalni blok rudari računalo koje kontrolira autor sustava.

3. Terminologija i terminografija

Cabré (1999: 10) terminologiju shvaća kao proces prikupljanja, opisivanja, obrađivanja i prezentiranja termina iz specijaliziranih polja znanja na jednom ili više jezika. Specijalna polja znanja nužno stvaraju jezik struke, koji je skup termina nekog specijalnog polja znanja. Sager i sur. (1980: 40) ovako opisuju razliku između općeg jezika i jezika struke:

Priroda jezika je takva da opći jezik i jezik struke mogu postojati unutar jednog prirodnog jezika; osnovne karakteristike jezika manifestiraju se i u engleskom jeziku i u jeziku kemijskog inženjerstva, kako u francuskom tako i u jeziku fizike. Razlika između općeg jezika i jezika struke je razlika u količini, a ne vrsti, osnovnih karakteristika koje jezik maksimalno ili minimalno koristi. Jezik struke koristi se s više svijesti o jeziku od općeg jezika, a situacije u kojima se koristi osnažuju korisnikovu brigu za jezik.

Svrha svakog, pa tako i jezika struke jest komunikacija, a uspješna komunikacija na jeziku struke unutar jezične zajednice zahtijeva upravljanje terminologijom. Steurs i sur. (2015: 224) o važnosti upravljanja terminologijom pišu:

Prikladno upravljanje terminologijom ključno je za svakog stručnjaka koji radi sa specijaliziranim znanjem. Adekvatno upravljanje terminologijom povećava

konzistentnost tekstova koji se proizvode, što ne samo da povećava njihovu iskoristivost i čitljivost, već i njihovu prevodivost na druge jezike.

Jezična politika igra važnu ulogu u stvaranju terminologije u jeziku struke i u razvoju struke unutar jezične zajednice. Terminološke smjernice UNESCO-a (2005: iv) to potvrđuju sljedećim riječima:

Ljudi čiji materinski jezik nije (ili nije dostatno) razvijen s gledišta terminologije i jezika struke (SPL) ili kojima je uskraćena uporaba njihova materinskog jezika u obrazovanju i usavršavanju, za pristup informacijama ili u međudjelovanjima na njihovim radnim mjestima, često su u nepovoljnome položaju.

Nadalje, u Smjernicama upozoravaju da manjak razvoja terminologije i jezičnog planiranja može dovesti do niza negativnih posljedica:

Posljedica jetogadaterminološkoplaniranjetrebadanasrazumjetiumnogoširojperspektivii novacijaiinformacija, znanja, pa čak strategija e-sadržaja. Jezična zajednica čiji jezik nije razvio znanstvena i tehnička nazivlja prisiljen je upotrebljavati drugi, strani jezik za komunikaciju u određenom području (UNESCO 2005: 1).

Upotreba drugog, stranog jezika u znanstvenom i tehničkom nazivlju, prema Smjernicama, dovodi do slabije proizvodnje u istraživanju i razvoju, rjeđe upotrebe, težeg zapisivanja i obrade tehnologije, slabijeg prijenosa znanja i na kraju manje primjene znanja unutar jezične zajednice.

U ovom se radu terminologiji pristupa iz prijevodne perspektive (usp. Cabré 1999: 13), kao sredstvu koje pomaže premostiti jaz između tehnološki dominantnog jezika i tehnološki subordiniranog jezika. Inicijalno se takav pristup pojavio u višejezičnim društvima poput Quebeca ili Belgije, no globalizacijom je svako društvo postalo djelomično višejezičnim. Razvoj jezika, kao što je već naglašeno u ovome radu, usko je povezan s tehnološkim napretkom te se razvoj jezika smatra prvom fazom prijenosa tehnologije i industrijskog napretka (Sager 2001: 253). S ciljem daljnjeg što bržeg razvoja terminologije hrvatskoga jezika, u sklopu ovog rada, koji je izvorno bio autorov diplomski rad na Filozofskom fakultetu Sveučilišta u Zagrebu⁶, izrađena je dvojezična terminološka baza tehnologije ulančanih blokova, koja je upotpunjena istraživanjem stavova stručnjaka o toj terminologiji, kao što će biti opisano u idućem poglavlju.

⁶ Izvorni rad dostupan je ovdje: <https://zir.nsk.hr/islandora/object/ffzg%3A523>

4. Cilj i metodologija istraživanja

4.1 Cilj

Cilj je ovoga istraživanja bio izraditi bazu terminologije tehnologije ulančanih blokova te ispitati stavove i mišljenja dijela relevantnih ispitanika o pristupu razvoju i popisivanju terminologije te o samim ponuđenim terminima.

4.2 Metodologija

Nkwenti-Azeh (2001: 249) terminološku bazu definira kao svaki sustav u kojemu se čuva specijalizirani vokabular – termini – u elektroničkom obliku. Termin ili naziv, osnovna jedinica jezika struke, nastaje u procesu zvanom primarna tvorba termina, dok je prijevod tako dobivenog termina i njegova prilagodba za korištenje na nekom drugom jeziku dio procesa koji se naziva sekundarna tvorba termina (Sager 2001: 252-3). Sager (2001: 253) detaljnije opisuje primarnu i sekundarnu tvorbu termina te navodi da u slučaju primarne tvorbe termina termin nema jezični presedan, dok se u slučaju sekundarne tvorbe uvijek koristi postojeći model. Primarna tvorba termina uglavnom je spontana, dok se sekundarnom može upravljati (Ibid.). Primarnom tvorbom nastaju novi termini, a sekundarnom se postojeći termini preuzimaju iz drugih jezika u obliku prevedenica, posuđenica, novotvorenica i parafraza (Ibid.). Sagerova podjela i njegovo shvaćanje tvorbe termina bilo je ključno u formiranju hrvatskih termina u terminološkoj bazi koja je izrađena u sklopu ovoga istraživanja.

Prema Cabré (1999:48), kvalitetna terminologija na više jezika mora sadržavati sljedeće elemente:

uz ekvivalente na drugim jezicima, terminologija pripremljena za prevoditelje mora sadržavati kontekste koji pružaju informacije o korištenju termina i idealno informacije o konceptu, kako bi omogućila prevoditeljima da koriste precizne oblike koji se odnose na specifični sadržaj.

Iz tog razloga terminološka baza sastavljena u sklopu ovog istraživanja sadrži termine na engleskom i hrvatskom jeziku, njihovu definiciju na jednom i drugom jeziku te citate iz literature kojima se pruža kontekst u kojem se termin koristi. Primjer unosa u terminološku bazu naveden je u Tablici 1.

Tablica 1. - Primjer unosa u terminološku bazu

Term (EN)	Definition	Citation	Syndetic relationship
block	set of cryptographically recorded data with a header containing the hash of the previous block, a timestamp, a hash pointer and a nonce	A block is composed of multiple transactions and some other elements such as the previous block hash (hash pointer), timestamp and nonce. - Bashir, Mastering blockchain	NT: Genesis block RT: block header, timestamp, nonce
Termin (HR)	Definicija	Citat	Sindetska veza
blok	niz kriptografski zapisanih podataka sa zaglavljem koje sadrži <i>hash</i> vrijednost prijašnjeg bloka, vremensku oznaku, <i>hash</i> pokazivač i jednokratni niz	Blok se sastoji od više transakcija i nekih drugih elemenata poput <i>hash</i> vrijednosti prijašnjeg bloka (<i>hash</i> pokazivača), vremenske oznake i jednokratnog niza. - Bashir, Mastering blockchain	Podređeni termin: inicijalni blok Povezani termini: zaglavlje bloka, vremenska oznaka, jednokratni niz

Posebno je važno da terminološka baza podataka bude čitljiva i razumljiva čovjeku, ali i lako prilagodljiva za korištenje u računalnim softverima čija je funkcija pisanje, korektura ili prevođenje. Baza terminologije izrađena u sklopu ovoga istraživanja dostupna je u Dodatku. Budući da se terminologija neprestano razvija, terminološka baza predstavlja sliku tehnologije u određenom trenutku. Termini su u svojim izvornim, engleskim oblicima prikupljeni iz recentne literature sredinom 2018. godine, a ponuđeni prijevodi ispitani su anketnim istraživanjem provedenim u ožujku 2019.

Upitnik je izrađen sustavom LimeSurvey⁷, a sastojao se od triju dijelova. U prvome dijelu prikupljeni su demografski podaci o dobi i spolu ispitanika te njihovom završenom formalnom obrazovanju, poznavanju engleskog jezika, kao i procjena vlastite upoznatosti sa sljedećim područjima: *blockchain*, DLT i kriptovalute. Drugim su se dijelom upitnika ispitali stavovi ispitanika o razvoju terminologije ulančanih blokova. U trećem su dijelu navedeni konkretni primjeri termina te su ispitanici zamoljeni da odaberu najbolja rješenja među ponuđenima ili da sami ponude rješenja za određene termine.

Upitnik je poslan skupini stručnjaka, entuzijasta i istraživača koji se bave tehnologijom ulančanih blokova ili njenom primjenom u kriptovalutama,

⁷ <http://limesurvey.srce.hr/>

kontaktiranih putem e-maila ili grupa na društvenim medijima. Ispitanici su sami procijenili svoju upoznatost s tehnologijom ulančanih blokova, a zajedničko im je da su direktno ili indirektno iskazali interes za tehnologiju, njen razvoj ili primjenu. Od 49 ispitanika koji su pristupili upitniku, 34 unosa odbačeno je zbog nepotpunih odgovora. Ukupni broj ispitanika čiji su rezultati obrađeni bio je 15. Rezultati istraživanja prikazani su u sljedećem poglavlju.

5. Rezultati istraživanja

5.1 Demografski podaci

Uzorak ispitanika (N=15), starosne dobi između 24 i 46 godina, sastojao se od dviju osoba ženskog i 13 osoba muškog spola. Od 15 ispitanika, njih četvero završilo je srednjoškolsko obrazovanje, jedan ispitanik završio je veleučilišni stručni studij, jedan preddiplomski, sedmero diplomski studij i dvoje poslijediplomski. Trinaest ispitanika procjenjuje svoje poznavanje engleskog jezika odličnim, između CEFR razina C1 i C2, dok dvoje ispitanika smatra da je njihovo poznavanje jezika dobro, između razina B1 i B2. Na skali od 1-5 (1 = slabo upoznat; 5 = stručan) ispitanici su procijenili svoju upoznatost s područjima *blockchain*, DLT i kriptovalute. Srednja vrijednost odgovora za područje *blockchain* iznosila je 4,27, što ukazuje na vrlo dobru informiranost ispitanika kad je riječ o ovoj temi. Nešto slabija bila je upoznatost s tehnologijom distribuirane glavne knjige, odnosno DLT. Srednja vrijednost upoznatosti s tim područjem iznosila je 3,8. Uzimajući u obzir mišljenja i opservacije iznesene u ovom radu, ne začuđuje da su ispitanici procijenili da najbolje poznaju područje kriptovaluta, s rezultatom srednje vrijednosti 4,33.

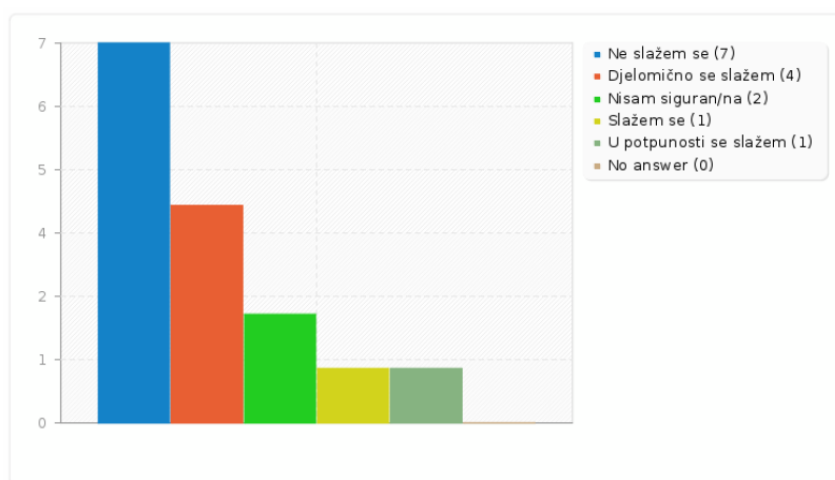
5.2 Stavovi o terminologiji

U drugom dijelu upitnika ispitanici su odgovarali na pitanja o svojim stavovima u vezi s ulogom prevođenja u razvoju *blockchain* terminologije te u vezi sa svojim korištenjem engleskih odnosno hrvatskih termina povezanih s ovom tehnologijom.

U prvim dvama pitanjima ispitivalo se slaganje s tvrdnjama koristeći sljedeće vrijednosti: (1) Ne slažem se, (2) Djelomično se slažem, (3) Nisam siguran/na,

(4) Slažem se i (5) U potpunosti se slažem. Prva tvrdnja glasila je: *Prevođenje terminologije ulančanih blokova olakšat će stručnu komunikaciju u području ove tehnologije*. Većina ispitanika izrazila je neslaganje s tvrdnjom (Slika 3). Točnije, njih sedmero „ne slaže“ se s tvrdnjom, dok se četvero ispitanika samo „djelomično slaže“ s tvrdnjom. Neutralno mišljenje o tvrdnji ima dvoje ispitanika, koji su odabrali „nisam siguran/na“. Samo se dvoje ispitanika „slaže“ ili „u potpunosti slaže“ s tvrdnjom.

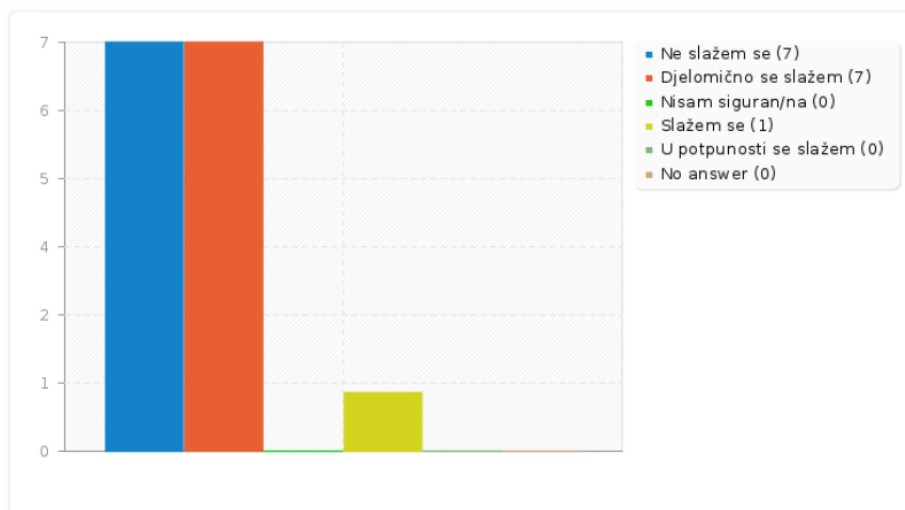
Prevođenje terminologije ulančanih blokova olakšat će stručnu komunikaciju u području ove tehnologije. []



Slika 3 – Prevođenje terminologije olakšava stručnu komunikaciju

Na drugu tvrdnju, *Smatram da terminologiju tehnologija blockchain i DLT treba prevoditi s engleskog na hrvatski jezik*, velika većina odgovora bila je negativna (Slika 4). Njih sedmero „ne slaže“ se s ovom tvrdnjom, sedmero ih se „djelomično slaže“, a samo se jedan ispitanik „slaže“. Rezultati ovog pitanja utjecali su na izradu terminološke baze i na pristup popisivanju terminologije pa je više anglizama uvršteno u stupac s hrvatskim terminima.

Smatram da terminologiju tehnologija blockchain i DLT treba prevoditi s engleskog na hrvatski jezik []



Slika 4 – Treba li prevoditi *blockchain* terminologiju

Treće pitanje pruža uvid u stručnu komunikaciju povezanu s *blockchain* terminologijom te su ispitanici morali odabrati jednu od ovih triju tvrdnji:

1. U profesionalnoj komunikaciji povezanoj s kriptovalutama ili tehnologijama *blockchain* i DLT najčešće koristim termine na engleskom jeziku.
2. U profesionalnoj komunikaciji povezanoj s kriptovalutama ili tehnologijama *blockchain* i DLT najčešće koristim termine na hrvatskom jeziku.
3. U profesionalnoj komunikaciji povezanoj s kriptovalutama ili tehnologijama *blockchain* i DLT najčešće koristim mješavinu termina na hrvatskom i engleskom.

Većina ispitanika, njih jedanaestero, odabrali su prvu tvrdnju, četvero ih je odabralo treću tvrdnju, a nitko nije odabrao drugu tvrdnju. Odgovori pokazuju da se ispitanici većinom koriste engleskim terminima u svojoj stručnoj komunikaciji, dok se neki koriste i hrvatskim i engleskim terminima.

Iako ispitanici većinom smatraju da prevođenje termina na hrvatski jezik nije potrebno (prva dva pitanja), čini se da postoji potreba za razradom terminologije na hrvatskom jeziku jer je unutar jezične zajednice pristup znanju i informacijama povezanim s ovom tehnologijom u ovom trenutku isključivo dostupan osobama koje izvrsno poznaju engleski jezik. U trenutku pisanja ne

postoji nijedan izvor u obliku rječnika ili glosara koji bi razjasnio i jezično približio ovu tematiku, a stručnjaci većinom koriste englesku terminologiju. Takav glosar ne bi nužno morao sve termine *prevesti* na hrvatski jezik, već ih može i kao posuđenice pokušati opisati na hrvatskom ako nemaju svoje uvriježene hrvatske ekvivalente, na što ukazuju i odgovori iz posljednje skupine pitanja koja se bave samim terminima.

5.3 Odabir termina

Cilj posljednje skupine pitanja bio je ispitati korištenje odgovarajućih termina u hrvatskom kontekstu. Ovim dijelom upitnika ispitivali su se sljedeći termini: *blockchain, DLT, cryptographic hash function, mining, timestamp, double spending, genesis block, P2P network* i *PoW – proof of work algorithm*. Navedeni termini neki su od ključnih termina za opisivanje ulančanih blokova, a nemaju ustaljene terminološke ekvivalente na hrvatskom jeziku. Ispitanici su morali odabrati rješenje koje smatraju najboljim među ponuđenima ili sami ponuditi rješenje. Svi termini bili su ponuđeni u sklopu rečenice na engleskom jeziku i njezinih različitih prijevoda na hrvatski jezik. Prvo pitanje odnosilo se na termin *blockchain*, a ispitanici su mogli birati između anglizma (posuđenice) i dvaju ponuđenih termina na hrvatskom (prevedenica).

Tablica 2. - Termin *blockchain*

Koje je od ponuđenih rješenja najbolji ekvivalent ovoj rečenici na engleskom jeziku:
One solution is the Blockchain, a growing list of records which are linked and secured cryptographically.

ODGOVOR	BROJ ISPITANIKA
Jedno rješenje je blockchain, rastući niz zapisa koji su povezani i osigurani kriptografski.	10
Jedno rješenje su ulančani blokovi, rastući niz zapisa koji su povezani i osigurani kriptografski.	4
Jedno rješenje je lanac blokova, rastući niz zapisa koji su povezani i osigurani kriptografski.	1

Kao što se vidi iz Tablice 2, desetero ispitanika odlučilo se za posuđenicu *blockchain*, dok se njih četvero odlučilo za hrvatski oblik ulančani blokovi, a tek jedan ispitanik odabrao je kalk, odnosno doslovan prijevod lanac blokova. Rezultati ukazuju da većina ispitanika ne bi prevodila termin već bi ga ostavila u izvornom engleskom obliku, što je uzeto u obzir pri izradi terminološke baze.

Sljedeći termin ispitan upitnikom bio je DLT, odnosno *distributed ledger technology*. U ovom pitanju ispitanici biraju između triju termina u hrvatskim rečenicama: tehnologija *distributed ledger*, tehnologija distribuirane glavne knjige i tehnologija zajednički vođene glavne knjige. Najpopularniji termin bio je tehnologija *distributed ledger*, koji je odabralo 7 ispitanika, dok je drugi termin, distribuirana glavna knjiga, odabralo 5 ispitanika. Najmanje ispitanika odlučilo se za termin zajednički vođena glavna knjiga, njih troje. I ovdje su ispitanici pokazali da preferiraju termin što bliži izvorniku, a ne onaj prilagođen hrvatskom jeziku. Unatoč tome, važno je napomenuti da engleska riječ *ledger*, inače računovodstveni termin, ima svoj ustaljeni i prihvaćeni oblik na hrvatskom, glavna knjiga. Uzimajući u obzir da je većina ispitanika odabrala anglizam u hrvatskoj rečenici, očito je važno da se sam termin previše ne udaljava od izvornog termina. Stoga je potrebno ponuditi rješenje koje zadovoljava pravila standardnog hrvatskog jezika, ali i ne ostavlja dvojbe u tumačenju termina. Prijedlog je autora da se zadrži hrvatski red riječi i hrvatska terminologija, s engleskom pokratom u zagradi: tehnologija distribuirane glavne knjige (DLT).

Sljedeće pitanje bilo je otvorenog tipa, a ispitalo je termin *cryptographic hash function*. Pitanje je postavljeno na sljedeći način: Kriptografija je jedan od osnovnih elemenata svakog sustava ulančanih blokova. Osnovna matematička funkcija koja osigurava integritet sustava na engleskom se naziva *cryptographic hash function*. Kako biste na hrvatskom izrazili taj termin? Za ovo pitanje posebno je zanimljivo da termin iz polja kriptografije već postoji u hrvatskom jeziku, no ispitanici, čini se, nisu upoznati s njim jer nitko nije ponudio rješenje kriptografska funkcija sažimanja.⁸ Čak sedmero ispitanika ponudilo je rješenje kriptografska *hash* funkcija. Unatoč tomu što u terminologiji kriptografije postoji ustaljeni prijevod ovog termina, u terminološku tablicu bit će uvrštena dva termina: kriptografska funkcija sažimanja na prvom mjestu i kriptografska *hash* funkcija na drugom zbog učestalosti ovog termina, kako u spontanoj jezičnoj produkciji kod ispitanika, tako i u tekstovima na temu kriptografije koji se mogu pronaći na internetu (npr. CARNet CERT 2009).

Četvrto pitanje u ovoj skupini odnosilo se na engleski termin *mining*, a glasilo je: Kako biste na hrvatskom nazvali aktivnost u kojem računalo koristi

⁸ Vidi Hrvatska enciklopedija – kriptografija,
URL: <http://www.enciklopedija.hr/natuknica.aspx?ID=33988>

procesorsku snagu kako bi gradilo sustav ulančanih blokova? Ispitanici su na pitanje nudili odgovore otvorenog tipa te su sami upisivali tekst. Većina rješenja sadržavala je ili hrvatsku prevedenicu rudarenje (5) ili anglizam *mining* (3). Zanimljivo je da termin *mining* u digitalnom kontekstu u hrvatskom već ima ustaljeni oblik zbog poslovne aktivnosti upravljanja podacima zvane *data mining* – rudarenje podataka. Unatoč tome što je riječ o posve različitim aktivnostima, termin rudarenje se u kontekstu ulančanih blokova javlja u spontanom izričaju ispitanika, što ukazuje na to da će termin biti bolje prihvaćen ako je njemu sličan termin već poznat u nekom drugom području. Nadalje, unatoč tome što su ispitanici većinom tvrdili da ne koriste hrvatske termine u komunikaciji povezanoj s ulančanim blokovima, odgovori na ovo pitanje pokazali su suprotno.

Sljedeći termin ispitan upitnikom bio je *timestamp*, koji u hrvatskom ima ustaljen oblik od početka korištenja digitalnih potpisa u poslovnoj komunikaciji. Ponudeni su bili odgovori vremenski žig, vremenska oznaka i vremenski pečat te su korisnici mogli dodati svoj odgovor. Njih šestero odabralo je najneutralniji pojam vremenska oznaka, dok je njih četvero odabralo već prihvaćeni pojam vremenski pečat. Troje se ispitanika odlučilo za rješenje vremenski žig unatoč tome što je ekvivalent engleskog pojma *stamp* pečat, a ne žig (*seal*). Preostalo dvoje ispitanika odabralo je upisati svoje rješenje te su upisali anglizam *timestamp*.

U sljedećem pitanju ispitan je termin koji se pokazao problematičnim prilikom izrade terminološke baze, *double spending*. Rezultati upitnika nažalost nisu ponudili jednoznačan odgovor, kao što se vidi iz Tablice 3.

Tablica 3 – Termin *double spending*

Odaberite ekvivalent engleskom terminu *double spending* na hrvatskom jeziku. Ako ne biste iskoristili nijedan od navedenih termina, upišite termin koji koristite.

ODGOVOR	BROJ ISPITANIKA
dvostruko trošenje	5
dvostruka transakcija	5
drugo:	
double spending ili dvostruko trošenje	1
double spending	1
dupli trošak	1
dupla transakcija	1
kopirana transakcija	1

Iz rezultata se vidi da se jednak broj ispitanika odlučio za rješenja dvostruko trošenje i dvostruka transakcija. Stoga će se u terminološku tablicu uvrstiti oba pojma, a vrijeme i jezična ekonomija pokazat će koji će od njih postati uvriježen prijevod za ovaj termin. Zbog deskriptivne prirode rada i uzimajući u obzir da oba termina funkcioniraju u kontekstu hrvatskog jezika, oba rješenja su prihvatljiva. S druge strane, moguća je i pojava termina duplo trošenje, koji je najprecizniji. Ovaj unos u terminološku tablicu stoga će imati tri termina na hrvatskom.

Sedmo pitanje odnosilo se na termin *genesis block*, koji je posebno zanimljiv zbog biblijskih konotacija. Taj se termin odnosi na prvi zapis nekog sustava ulančanih blokova; iako bi najjednostavnije bilo nazvati ga prvim blokom, takvo ime ne bi bilo dostatno jer njegova važnost seže daleko iznad činjenice da je prvi. *Genesis block* temelj je sustava ulančanih blokova na kojemu se gradi cijeli lanac, a sadrži pravila i informacije o sustavu, ali i potencijalnu poruku autora. Prijedlog je da se kao terminološki ekvivalent prihvati inicijalni blok, s čime su se i ispitanici složili u velikoj većini. Njih čak dvanaestero (od petnaestero) odlučilo se za rješenje inicijalni blok.

6. Zaključak

Blockchain, odnosno tehnologija ulančanih blokova, prema svim pokazateljima može se smatrati disruptivnom tehnologijom. Uzimajući u obzir definiciju potonjega pojma, disruptivne tehnologije imaju potencijal drastično promijeniti određeni aspekt ljudskog života. U kontekstu ulančanih blokova riječ je o čuvanju zapisa svih vrsta, poglavito imovine, bilo financijske ili fizičke, ali i neopipljivih zapisa poput glasova ili zdravstvenih podataka. Ulančani blokovi nude nov, revolucionaran pristup koristeći distribuirano povjerenje. Naime, povjerenje u sustav ne proizlazi iz treće strane već iz njegove matematičko-kriptografske sposobnosti da pohranjuje bilo koju vrstu digitalnog zapisa, bez mogućnosti izmjene i naknadne manipulacije.

Prepoznavanje potencijala ovakve digitalne revolucije bila je jedna od motivacija za pisanje ovog rada. Literatura iz područja terminologije naglašava važnost razvoja terminologije unutar jezične zajednice iz mnoštva razloga, od kojih je po mišljenju autora najvažniji razlog da razvoj terminologije omogućava

jezičnoj zajednici da ovlada, iskoristi, razvija i prenosi stručna znanja povezana s novim tehnologijama. Neupitno je da ovladavanje terminologijom nadolazećih tehnologija može dovesti do boljitka unutar jezične zajednice jer društvo koje ovladava, iskorištava, razvija i prenosi znanja omogućava pojedincima unutar te jezične zajednice ili društva lakši pristup informacijama, bolje razumijevanje i brže učenje.

Stoga je u sklopu ovog istraživanja izrađena terminološka baza u kojoj su na engleskom i hrvatskom jeziku razjašnjeni ključni pojmovi povezani s tehnologijom ulančanih blokova. U vezi s hrvatskim terminima provedeno je ispitivanje koje je uključivalo stručnjake i entuzijaste za ovu novonastalu suvremenu tehnologiju. Pokazalo se da je u procesu izrade terminologije povezane s novom tehnologijom osobito važno razjašnjavanje tih pojmova na hrvatskom jeziku. Time se omogućuje pristup znanju stručnog područja u nastajanju koje nije ograničeno poznavanjem jezika. Aktivnosti ovog rada provedene su u nadi da će poslužiti kao polazište za razvoj terminologije u kontekstu novih tehnologija. Jedno od ograničenja ove metodologije zasigurno je pronalaženje ispitanika jer kad je riječ o disruptivnim tehnologijama ne postoji formalizirana definicija stručnjaka. Uključivanje hrvatskih jezikoslovaca i jezičnih stručnjaka u daljnja istraživanja na ovu temu obogatilo bi rezultate istraživanja i proširilo sliku problematike.

Literatura

- Afrić, Petar. 2014. „Pregled kriptografskih algoritama“. URL: http://sigurnost.zemris.fer.hr/algoritmi/2014_afric/Pregled_kriptografskih_algoritama_3-0.html
- Bashir, Imran. 2017. *Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks*. Birmingham: Packt.
- Becker, Georg. 2008. Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Ruhr-Universität Bochum. URL: https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf
- Cabré, M. Teresa. 1999. *Terminology: Theory, Methods and Applications*. Amsterdam/Philadelphia: John Benjamins.

- CARNet CERT. 2009. „TLS protokol CCERT-PUBDOC-2009-03-257“. URL:
<https://www.cert.hr/wp-content/uploads/2009/03/CCERT-PUBDOC-2009-03-257.pdf>
- Crespigny, Angus Champion de. 2016. „Blockchain: the hype, the opportunity and what you should do“. *Banking Perspectives* 4(4): 62-70. URL:
<https://www.theclearinghouse.org/banking-perspectives/2016/2016-q4-banking-perspectives/articles/blockchain-hype-opportunity>
- Deloitte. 2016. *Bitcoin, Blockchain and distributed ledgers, caught between promise and reality*. URL:
<https://www2.deloitte.com/content/dam/Deloitte/au/Images/infographics/au-deloitte-technology-bitcoin-blockchain-distributed-ledgers-180416.pdf>
- Economist, The. 2015. „Blockchains: The great chain of being sure about things“. URL:
<https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>.
- Gartner Inc. 2019. „Gartner Hype Cycle“. URL:
<https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>
- Geeraerts, Dirk. 2015. „Foreword“. U: Kockaert, Hendrik J. i Steurs, Frieda (ur.), *Handbook of Terminology, Volume 1*. Amsterdam/Philadelphia: John Benjamins, xvii-xix.
- Linux Foundation, The. 2018. „About Hyperledger“. URL:
<https://www.hyperledger.org/about>
- HZN [Hrvatski zavod za norme], TO 307. 2019. „Ulančani blokovi i tehnologija elektroničke distribuirane glavne knjige“. URL: <https://www.hzn.hr/>
- IBM. 2018. „IBM Blockchain platform“. URL: <https://www.ibm.com/blockchain/platform/>
- ISO [International Standards Office], TC 307. 2019. „Blockchain and electronic distributed ledger technologies“. URL: <https://www.iso.org/committee/6266604.html>
- Jakobson, Markus i Juels, Ari. 1999. „Proofs of work and bread pudding protocols“. U: Preneel, Bart (ur.), *Secure Information Networks. IFIP – The International Federation for Information Processing, vol 23*. Boston: Springer.
- Mills, David, Wang, Kathy, Malone, Brendan, Ravi, Anjana, Marquardt, Jeff, Chen, Clinton Badev, Anton, Brezinski, Timothy, Fahy, Linda, Liao, Kimberley, Kargenian, Vanessa, Ellithorpe, Max, Ng, Wendy i Baird, Maria. 2016. *Distributed ledger technology in payments, clearing, and settlement. Finance and Economics Discussion Series 2016-095*. Washington: Board of Governors of the Federal Reserve System. URL:
<https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>

- Nakamoto, Satoshi. 2008. *Bitcoin: A peer-to-peer electronic cash system*. URL: <https://bitcoin.org/bitcoin.pdf>
- Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew i Goldfeder, Steven. 2016. *Bitcoin and cryptocurrency technologies*. Princeton: Princeton University Press.
- Nkwenti-Azeh, Blaise. 2001. „Term banks“. U: Baker, Mona i Saldanha, Gabriela (ur.), *Routledge Encyclopedia of Translation Studies*, 1. izd. London/New York: Routledge, 249-251.
- PWC. 2018. „Blockchain Overview“. URL: <https://mytaxpartner.pwc.com/media/1247992/blockchain-overview.pdf>
- Sager, Juan C. 2001. „Terminology; application“. U: Baker, Mona i Saldanha, Gabriela (ur.), *Routledge Encyclopedia of Translation Studies*, 1. izd. London/New York: Routledge, 251-255.
- Sager, Juan C., Dungworth, David i McDonald, Peter F. 1980. *English special languages: Principles and practice in science and technology*. Wiesbaden: Brandstetter.
- Samman George i Seibold, Sigrid. 2018. *Consensus: Immutable agreement for the Internet of Value*. URL: <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf>
- Steurs, Frieda, De Wachter, Ken i De Malsche, Evy. 2015. „Terminology tools“. U: Kockaert, Hendrik J. i Steurs, Frieda (ur.), *Handbook of Terminology Volume 1*. Amsterdam/Philadelphia: John Benjamins, 222-249.
- Tapscott, Alex i Tapscott, Don. 2016. *Blockchain Revolution*. New York: Portfolio/Penguin.
- UNESCO. 2005. *Smjernice za terminološke politike, Oblikovanje i provedba terminološke politike u jezičnim zajednicama*. Pariz: UNESCO. Hrvatski prijevod. URL: http://www.infoterm.info/pdf/activities/guidelines/SmjerniceZaTerminoloskePolitike_hr.pdf
- William, Jacob. 2016. *Blockchain: The simple guide to everything you need to know*. Seattle: Amazon Createspace Independent Publishing Platform.