

POTENCIJAL PRIMENE BLOCKCHAIN TEHNOLOGIJE

POSSIBILITIES IN BLOCKCHAIN TECHNOLOGY APPLICATION

Bačević Jelena | Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, Srbija | jelena.bacevic@vspep.edu.rs

JEL klasifikacija: O32

DOI: 10.5937/trendpos2301077B

UDK: 336.7:004.056.5

004.738.5.056

COBISS.SR-ID 119436553

Sažetak

Tehnologija lanca blokova (Blockchain tehnologija) sve više dobija na značaju jer počinje da se primenjuje u mnogim oblastima poslovanja. Blockchain služi kao nepromenljiva knjiga zapisa koja omogućava da se transakcije odvijaju u decentralizovanom okruženju. Iako je to relativno nova tehnologija (prvi teorijski rad 2008. godine), koja je prvenstveno razvijena i primenjena u sistemima plaćanja (Bitcoin) pokazalo se da su njene potencijalne mogućnosti daleko veće. U periodu od svog nastanka do danas, ova tehnologija je znatno usavršena, algoritmi koji se primenjuju su unapređeni i prilagođeni savremenom poslovnom okruženju. Istraživanje oblasti primene ove tehnologije rađeno je na osnovu dostupne literature i radova objavljenih u relevantnim časopisima.

Rad predstavlja sveobuhvatan pregled mogućnosti primene tehnologija lanca blokova u savremenom poslovnom okruženju, njene prednosti i mane kao i probleme sigurnosti koji se javljaju u teoriji i praksi. Takođe se u radu analiziraju mogući trendovi primene u ovoj oblasti.

Abstract

Block chain technology is becoming more and more important as it is being applied in many fields of business. Blockchain serves as a continuing book of records enabling transactions to develop in decentralized circumstances. Although it is a relatively new technology (first theoretical work dates from 2008), developed and applied primarily in payment systems (Bitcoin), it appeared that its potentials are far beyond it. Within the period from its beginning until the present day, this technology has been considerably improved, applied algorithms perfected and accommodated to contemporary business environment. Research in the field of application concerning this technology was made on the basis of available literature and papers published in relevant journals.

The paper represents a comprehensive review of possibilities in Blockchain technology application in contemporary business environment, its benefits and shortcomings as well as security problems appearing in theory and practice. This paper also deals with the analysis of possible trends in the mentioned field.

Ključne reči: Blockchain tehnologija, kripto valute, decentralizovane finansije, e-poslovanje

Keywords: Blockchain technology, crypto currency, decentralized finance, e-transactions.

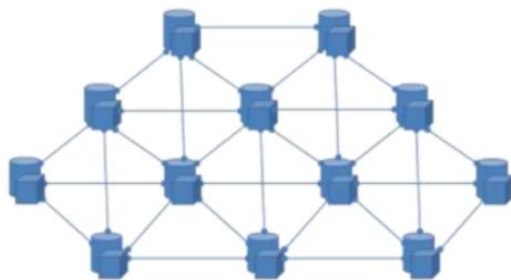
Uvod

Tehnologije lanca blokova pojavljuju se u trenutku kada su svetske finansije ušle u krizu i probleme 2008. godine, a posebno je intrigantna i karakteristična njihova primena kao sistema potpuno anonimnog i decentralizovanog sistema plaćanja. Tako se te iste 2008. godine pojavljuje rad Satoši Nakamota sa idejom pravljenja kripto valuta. Ono što izaziva zainteresovanost je da u tom trenutku niko ne zna ko je dotični autor ove ideje i predložene tehnologije (a to se ne zna ni do danas), ali je karakteristično da je javnost kroz medije brzo i masovno informisana o pojavi kripto valute, koja je potpuno anonimna i nije pod kontrolom bilo kog autoriteta, što navodi na razmišljanje da iza ove tehnologije stoji neko dovoljno moćan da promoviše ovu ideju. Realizacija ovog projekta je završena 2009. godine i BitCoin se pojavljuje a prve transakcije su obavljene 2010. godine. Ubrzo posle Bitcoina se pojavljuje "Litecoin" a zatim i niz drugih kripto valuta. Od 2010. godine do 2017. razvijeno je 720 kripto valuta dok u februaru 2021. godine njihov broj dostiže 8413 različitih sistema plaćanja. Drugi značajan datum u pojavljivanju ove tehnologije je 2013. godina kada se pojavljuje Ethereum. Danas (2023. god) se na "CoinMarketCap" može naći 25400 kripto valuta sa kojima se trguje na 636 berzi (Market Cap: €1,071,925,331,351 na dan 04.06.2023. god).

Tehnologija lanca blokova (Blockchain) je u javnosti prepoznata kao revolucionarna nova tehnologija koja se primenjuje u poslovima sa kriptovalutama. Međutim, potencijalne primene ove tehnologije mogu se naći u različitim sektorima društvenih delatnosti i različitim industrijama. Primena ove tehnologije posebno je značajna u obezbeđivanju novog načina poslovanja i koordinacije koja je neophodna za obavljanje onlajn transakcija. To ovu tehnologiju čini blagovremenim pronalaskom u doba kada napredovanje i digitalizacija poslovanja iziskuje potrebu za efikasnošću i bezbednošću onlajn transakcije.

Ovako dobro osmišljena tehnologija nije mogla da ostane neprimećena i ubrzo su počeli da se pojavljuju radovi u kojima se analiziraju primene u drugim oblastima. Prvobitno razvijena kao tehnologija za obavljanje transakcija kriptovaluta, Blockchain tehnologija je brzo evoluirala u veliki broj aplikacija, kao što su državna uprava, bankarstvo, finansijska tržišta, računovodstvo, lanci snabdevanja, sistemi glasanja i vladine usluge itd.

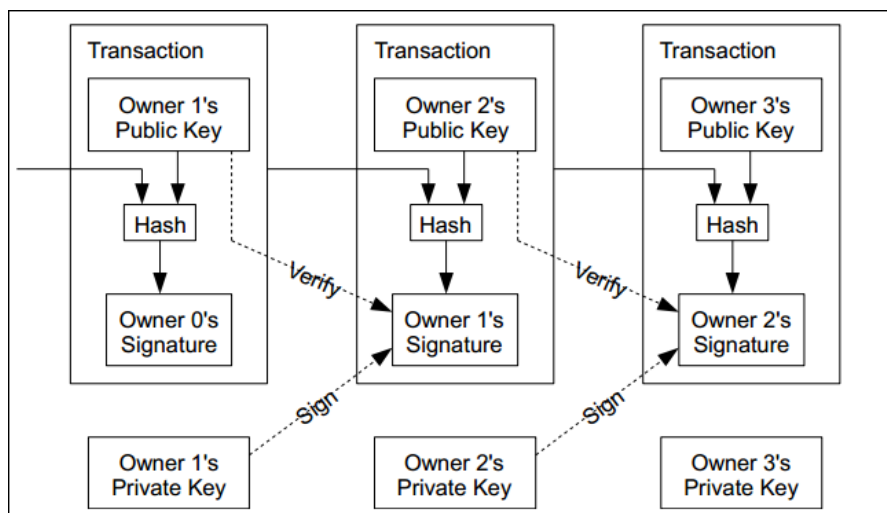
Tehnologija lanca blokova (blockchain) je baza podataka transakcija koja sadrži informacije o svim transakcijama koje su ikada izvršene u prošlosti (od prvog do poslednjeg registrovanog) i radi na Bitcoin protokolu. To je u stvari digitalna knjiga transakcija i omogućava svim učesnicima na mreži da mogu da uređuju tu glavnu knjigu na siguran način a ona se deli preko distribuirane mreže računara.



Slika 1: Prikaz distribuirane mreže računara

Tehnologija lanca blokova (blockchains) u suštini predstavlja mehanizam koordinacije između učesnika. To je skup tehnologija koji je zasnovan na kriptografskim mehanizmima [1] koji je razvijen na osnovu koncepta distribuirane knjige. Termin se odnosi na lanac blokova informacija uskladištenih na decentralizovanom uređaju mreže računara, koja verifikuje i beleži svaku transakciju u zajedničku i šifrovanu knjigu. Svaki novi blok informacija se verifikuje konsenzusom protokola i povezan je sa onim koji mu prethode, formirajući tako lanac. Jednom stvorena, blok (tj. informacije sadržane u njemu) se ne može promeniti, dajući lancu blokova kvalitet nepromenljivosti (promena je moguća samo ako se svi prethodni blokovi takođe zamene). Korišćenje konsenzus protokola zamenjuje posrednike pružanja usluga ispunjenja ugovora (banke, berze,..) sa peer-to-peer kliring sistemom, gde se bilo šta što je vredno može preneti na mrežu.

Tehnologija lanca blokova se zasniva na tri osnovne tehnologije i to su: Kriptografski mehanizmi, peer to peer mreže i blockchain protokol.



Slika 2: Prikaz šeme izvođenja Blockchains transakcije (Originalna šema koja je objavljena od strane Satoši Nakamota 2008.)

Na šemi se jasno vidi na koji način se formira lanac blokova preko korišćenja sistema javnih i tajnih ključeva.

Blockchain može da bude organizovan kao:

- Javni lanac blokova (blockchain).

Ovaj lanac blokova ne zahteva dozvolu za pristup mreži i u njemu može učestvovati svako ko ima računar ili mobilni uređaj. Ovaj blockchain se uglavnom zasniva na konsenzus metodi dokazivanja rada (PoV), za dodavanje novih unosa informacija u mrežu. U javnom lancu blokova, svaki čvor može da učestvuje u procesu konsenzusa. Transakcije u javnom lancu blokova su vidljive na mreži. Što se nepromenljivosti tiče treba napomenuti da se zapisi čuvaju na velikom broju računara učesnika, tako da je skoro nemoguće manipulirati transakcijama u javnom lancu blokova. Efikasnost rada u njemu je u zavisnosti od broja učesnika i broja transakcija koje se obrađuju ovim protokolom. Poznato je da potvrda Bitcoin transakcije može da traje dosta dugo ukoliko je veliki broj transakcija koje u je u datom vremenskom intervalu potrebno izvršiti.

- Privatni lanac blokova (blockchain).

Ovaj lanac blokova zahteva centralni organ koji upravlja pristupom učesnika na mrežu i pristupi privatnom lancu blokova su ograničeni, tako što centralna vlast (operater sistema, vlasnik lanaca blokova) mora da izabere učesnike za dodavanje u mrežu na osnovu određenih specifikacija (ovlašćenja). Privatni blockchain se smatra centralizovanom mrežom pošto ga u potpunosti kontroliše jedna organizacija. Kod privatnog lanaca blokova on je u potpunosti kontrolisan od jedne

organizacije i ona utvrđuje konačan konsenzus. Kada je u pitanju privatni blockchain ili blok lanac konzorcijuma odluku o vidljivosti donosi centralni organ koji vodi posao. Kada je u pitanju nepromenljivost transakcija u privatnom blockchain-u ili blockchain-u konzorcijuma postoji mogućnost da se zapisi menjaju jer postoji ograničen broj učesnika. Efikasnost privatnih i konzorcijskih blockchain-a je znatno bolja jer je ograničen broj korisnika i transakcija. Privatan blockchain je potpuno centralizovan jer ga kontroliše pojedinačna grupa koja ga je i implementirala.

- Lanac blokova konzorcijuma.

To je kombinacija privatnog i javnog blokčejna i uključivanje novog učesnika zahteva od centralne institucije odobrenje celog konzorcijuma. Stručnjaci iz oblasti, predviđaju budućnost koja obećava za hibridne tipove uključujući različite tipove blok lanaca. Konzorcijum blockchain koji je konstruisalo nekoliko organizacija je delimično decentralizovan pošto bi samo mali deo čvorova bio izabran da utvrdi konsenzus. Blockchain konzorcijuma je delimično centralizovan.

Prednosti blockchain tehnologije

Tehnologija lanca blokova se u velikom broju slučajeva pokazala kao odlično rešenje.

Osnovne prednosti su [1]:

1. Sve je decentralizovano što znači da se knjiga zapisa nalazi na više ili na svim računarima u zavisnosti kako je sistem organizovan.
2. Obezbeđena je transparentnost.
3. Zasnovano je na open source-u.
4. Potpuno je autonomno što podrazumeva da svaki čvor može da ažurira ceo sistem i niko ne može da interveniše ili nešto promeni.
5. Obezbeđena je nepromenljivost: znači da će svi zapisi ostati trajno upisani u neizmenjenom obliku.
6. Sve je anonimno (pre se može reći pseudo anonimno)

Problemi Blockchain tehnologije

Od samog pojavljivanja ove tehnologije mnogo je onih koji zagovaraju primenu Blockchain tehnologije ali ima i dosta kritičara. Interesantno je da se pojavljuju implementacije ove tehnologije u najrazličitijim situacijama, pa se ozbiljno postavlja pitanje racionalnosti primene, bez analize koliko je zaista potrebna u pojedinim slučajevima.

Pošto se ovde radi o decentralizovanoj obradi to znači da se svaka transakcija registruje na svim čvorovima koji su u mreži. Kada uzmemo u obzir samo kripto valute, svaka transakcija se upisuje na preko milion čvorova (Bitcoin). Tako se ispostavlja da su transakcije u javnom Blockchain-u (Bitcoin i slični) toliko skupi da se postavlja pitanje racionalnosti njihovog korišćenja. [13] Da bi funkcionisala mreža svaka transakcija potroši određenu količinu električne energije i to su nenadoknadiivi gubici. Ako se zna da transakcije Bitcoina u najvećem delu predstavljaju špekulativni posao (80%-90%) trošenje energije na ovaj posao predstavlja čist gubitak resursa. Kada se govori o pametnim ugovorima u javnim mrežama pitanje je ko će snositi trošak održavanja sistema. Sa druge strane kada su u pitanju ugovori transakcije osetljivog i poverljivog sadržaja ne bi smele da budu vidljive ostalim učesnicima na mreži.

Blockchain mreže mogu biti spore i neefikasne zbog visokih računarskih zahteva potrebnih za validaciju transakcija. Kako se broj korisnika, transakcija i aplikacija povećava, sposobnost blockchain mreža da ih obrađuju i validiraju na vreme postaje problematična. Ovo čini blokčejn mreže teškim za korišćenje u aplikacijama koje zahtevaju velike brzine obrade transakcija. Kao primer može se navesti Ethereum blockchain koji može da obavi oko 20 transakcija u sekundi

što u masovnoj primeni predstavlja veliko ograničenje. Ako se zna da VISA obrađuje oko 30000 transakcija u sekundi, postavlja se pitanje kako će u ovako punom opterećenju čitav sistem Blockchain obrade da funkcioniše.

Sigurnost Blockchain tehnologije nije u potpunosti dokazana. Ovo je relativno nova tehnologija koja je još uvek, može se reći u fazi eksperimentisanja u mnogim oblastima. Blockchain-ove bezbednosne mere su često proglašavane kao ključne prednosti tehnologije, ali, bezbednost mreža blockchain nije bez problema. Bilo je slučajeva kršenja bezbednosti i hakerskih napada na blockchain mreže, a ovi problemi mogu dovesti do velikih gubitaka i oštećenja integriteta mreže. Postoji hipotetička mogućnost da kada neko preuzme 50% mreže može da dođe do manipulacije. Kada je u pitanju javni blockchain kao što je Bitcoin koji ima više miliona umreženih čvorova tako da je preuzimanje 50% mreže gotovo nemoguće.

Oblasti primene blockchain tehnologije

Interesantno je kojom brzinom su blockchain tehnologiju masovno prihvatili korisnici. Teško je naći neku oblast poslovanja gde nisu započele analize i primene ove tehnologije.

Tabela 1: Oblasti primene Blockchain tehnologije.

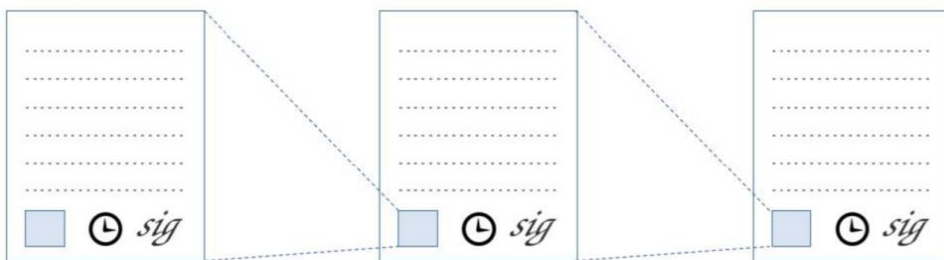
	Oblast primene	Primeri
1.	Javna uprava [1]	Izdavanje dokumenata, (vozačke dozvole, lične karte, pasoši, biračke registracije) Glasanje, Notarski poslovi, Vlasništvo nad nekretninama, Upravljanje identitetima
2.	Javna evidencija	Zemljišta i vlasništvo, registracije vozila, poslovne dozvole, venčani listovi, umrlice
3.	Opšti poslovi	Ugovori, Arbitraža, Transakcije sa više potpisa,
4.	Potvrda vlasništva	Intelektualna svojina, Osiguranje, Sprečavanje falsifikata
5.	Finansije [7]	Finansijski servisi, Kripto valute, Međubankarski transferi, Upravljanje rizicima, DeFi- Decentralizirane finansije, akcije, privatni kapital, crowdfunding, obveznice, fondovi, derivati, anuiteti,
6.	Zdravstvo [11]	Zdravstveno osiguranje, Praćenje zdravstvenog stanja pacijenata, Potrošnja lekova, Medicinska dokumentacija
7.	Obrazovanje [14]	Registrowanje sertifikata - diploma Registrowanje uspeha studenata
8.	Poslovanje [9]	Pametni ugovori, Praćenje snabdevanja, Upravljanje kadrovima, marketing.
9.	Privatna evidencija	Zajmovi, ugovori, opklade, potpisi, testamenti,
10.	Industrija [8]	Projektovanje, Upravljanje energetskim sektorom
11.	Upravljanje podacima [5]	Praćenje unosa i distribucije podataka Smart multisignature escrow (garancije)
12.	Internet of things [6]	Praćenje podataka sa mreže Upravljanje uređajima u distribuiranoj mreži
13.	Sigurnost i privatnost [12]	Poboljšanje bezbednosti, Vlasništvo nad podacima Kontrola pristupa, Zaštita privatnosti
14.	E-poslovanje [5]	Social networking, Crowdsourcing, Igre na sreću - kockanje na internetu
15.	Ključevi fizičkih sredstava	Stanovi, Hotelske sobe, automobili za iznajmljivanje, pristup automobilima

Analiza dostupne literature pokazuje da je ova tehnologija našla primenu u mnogim oblastima. Može se reći da se trenutno rade eksperimenti u mnogim oblastima. Tako se mogu naći podaci da više stotina banaka radi eksperimente (a neke su počele da koriste) ovu tehnologiju. Već su poznati projekti koji su u toku na nivou država. Tako se u Kini eksperimentiše sa kriptoumanom, u Rusiji na kriptorubljom; u Venecueli je kriptovaluta petro. Ozbiljno se razmatraju mogućnosti da se platni promet obavlja putem kriptovaluta.

Decentralizovane finansije (DeFi)

DeFi je skraćenica fraze decentralizovane finansije koja se uopšteno odnosi na digitalnu imovinu i finansijske pametne ugovore, protokole i decentralizovane aplikacije (DApps) izgrađene na Ethereum platformi. To je finansijski softver izgrađen na blockchain tehnologiji.

U svom najjednostavnijem obliku, decentralizirane finansije su sistem po kojem finansijski proizvodi postaju dostupni na javnoj decentraliziranoj blockchain mreži, što ih čini otvorenima za svakoga za korišćenje, umjesto da prolaze kroz posrednike kao što su banke ili brokeri. Za razliku od bankarskog ili brokerskog računa, ID koji je izdala vlada, broj socijalnog osiguranja ili dokaz o adresi nisu neophodni za korišćenje DeFi-ja. Tačnije, DeFi se odnosi na sistem po kojem softver napisan na blockchainima čini da je moguće da se omogući kupcima, prodavačima, uzimaocima kredita, i pozajmljivačima interakcija sa strogo softverom baziranim posrednikom, a ne kompanijom ili institucijom koja olakšava transakciju.



Slika 3. Lanac blokova dokumenata [1]

Decentralizirane finansije, ili DeFi, imaju za cilj da koriste tehnologiju za uklanjanje posrednika između stranaka u finansijskoj transakciji. One koriste tehnologiju za distribuirane modele i omogućavaju pružanje finansijskih usluga bilo gde za bilo koga bez obzira na etničku pripadnost, starost ili kulturni identitet. Decentralizirane finansije imaju za cilj stvaranje finansijskog sistema koji je otvoren za sve i minimizira nečiju potrebu da se veruje i da se pouzda u centralne vlasti. Tehnologije poput interneta, kriptografije i blockchajna daju solidne alate za kolektivnu izgradnju i kontrolu finansijskog sistema bez potrebe za centralnim vlastima.

Pametni ugovori pružaju okvir za funkcioniranje DeFi aplikacija jer kodiraju uslove i aktivnosti potrebne za funkcionisanje ovih usluga. Na primer, šifra pametnog ugovora ima specifičnu šifru koja uspostavlja tačan uslov i odredbe zajma između pojedinaca. Ako se ne ispuni određena odredba ili uslovi, kolateral bi se mogao likvidirati automatski. Sve to provodi se putem određenog koda, a ne ručno od strane banke ili druge institucije.

Zaključak

Tehnologija lanca blokova se pojavila 2008. godine i od tada ubrzano se razvijaju mogućnosti njene primene u različitim oblastima života. U početku primena je bila samo u obliku kripto valuta (Bitcoin i slični) ali su u međuvremenu unapređeni algoritmi što je omogućilo da se primeni i u drugim oblastima poslovanja. Blockchain tehnologija je pokazala svoj potencijal za transformaciju poslovanja kroz decentralizaciju, postojanost, anonimnost i dostupnost.

Činjenica je da se masovno eksperimentiše i uvodi ova tehnologija u različitim oblastima poslovanja, mada se mora priznati da je u nekim slučajevima potpuno neracionalna. Problemi sigurnosti ove tehnologije još uvek nisu dovoljno istraženi i u literaturi se pojavljuju radovi gde se analiziraju mogući napadi.

Tehnologija lanca blokova zahteva visok nivo znanja i tehničkih veština za implementaciju i održavanje i to može da uspori primenu ovih tehnologija. Drugi problem koji se javlja u primeni ove tehnologije je da postoji veliki broj različitih blockchain platformi sa različitim protokolima i standardima i prilikom razmene podataka može doći do problema interoperabilnosti sistema.

Sa druge strane svaka transakcija korišćenjem blockchain-a zahteva znatno veću potrošnju električne energije koja je inače deficitarna u svetu. Posebno što se električna energija još uvek većinom proizvodi sagorevanjem fosilnih goriva to onda ima značajnog ekološkog uticaja.

Bibliografija

- [1] Zheng, Z, Xie, S., Dai, HN., Chen, X., Wang, H.: An overview of Blockchain technology: architecture, consensus, and future Trends. In: 978-1-5386-1996-4/17 6th International Congress on Big Data PP557-564 IEEE (2017).
- [2] Porru, S., Pinna, A., Marchesi, M., Tonelli, R.: Blockchain-oriented software engineering: challenges and new directions. In: 39th IEEE International Conference on Software Engineering Companion PP169-179 IEEE/ACM (2017)
- [3] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2009) <https://bitcoin.org/bitcoin.pdf>
- [4] Hassan, F.U., Ali, A., Latif, S., Qadir, J., Kanhere, S.S., Singh, J., & Crowcroft, J.A. (2019). Blockchain And The Future of the Internet: A Comprehensive Review. ArXiv, abs/1904.00733.
- [5] Ethereum Whitepaper, (2023), www.ethereum.org
- [6] T. M. Fernández-Caramés, P. Fraga-Lamas: Review on the Use of Blockchain for the IoT, VOLUME 6, 2018, IEEE ACEES.
- [7] Горан Радивојац, Милош Грујић (2018) ACTA ECONOMICA. Година XVI, број 29 /.ISSN 1512-858X, e-ISSN 2232-738XУДК: 336.76:330.322.14 DOI: 10.7251/ACE1829079R
- [8] Kahn, M.T.E. (2021). Review of Blockchain Technology: Enhancing the Services of Distributed Energy Systems. Academia Letters, Article 4237. <https://doi.org/10.20935/AL4237>.
- [9] Abderahman Rejeb, John G. Keogh, Horst Treiblmaier,. (How Blockchain Technology Can Benefit Marketing: Six Pending Research Areas , Frontiers in Blockchain | www.frontiersin.org, February 2020 | Volume 3 | Article 3
- [10] Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich,. Regulating Blockchain. Techno-Social and Legal Challenges, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich, Oxford University Press, 2019, 3-24. <https://global.oup.com/academic/product/regulating-blockchain-9780198842187>
- [11] Ivan Homoliak, Sarad Venugopalan, Qingze Hum, Pawel Szalachowski,.A Security Reference Architecture for BlockchainsSingapore University of Technology and Design
- [12] Marten Risius • Kai Spohrer (2017), A Blockchain Research Framework, What We (don't) Know, Where We Go from Here, and How We Will Get There, Bus Inf Syst Eng, <https://doi.org/10.1007/s12599-017-0506-0>
- [13] Zibin Zheng and Shaoan Xie, (2018), Blockchain challenges and opportunities: a survey, Int. J. Web and Grid Services, Vol. 14, No. 4, 2018
- [14] Grech, A. and Camilleri, A. F. (2017) Blockchain in Education. Inamorato dos Santos, A. (ed.) ; doi:10.2760/60649

Datum prijema rada:09.05.2023.

Datum prihvatanja rada:10.06.2023.