FBIM Transactions
DOI 10.12709/fbim.09.09.02.07

TEHNOLOGIJE ZA ZAŠTITU PODATAKA U DIGITALNIM POSLOVNIM PROCESIMA

DATA PROTECTION TECHNOLOGIES IN DIGITAL BUSINESS PROCESSES

Zoran G. Pavlović
ATUSS-Visoka železnička škola, Beograd, Srbija
https://orcid.org/0000-0001-6076-1811

Veljko Radičević
ATUSS-Visoka železnička škola, Beograd, Srbija

Dragan Nikolić
Univerzitet „Union - Nikola Tesla", Fakultet primenjenih nauka, Niš, Srbija

JEL kategorija rada: **L86, M21**

Apstrakt

Razvojem Interneta dolazi do primene novih tehnologija u poslovanju kako preduzeća tako i kod pojedinaca. Preduzeća koja se bave trgovinom ili pružanjem usluge, već koriste internet mogućnosti za svoje potrebe i to podrazumeva realizaciju finansijskih transakcija. Može se izdvojiti jedan bitan parametar koji može da predstavlja problem preduzećima i korisnicima. Taj parametar se odnosi na sigurnost slanja i dobijanja novca putem internet mreže. Pored algoritama za sigurno poslovanje putem internet mreže, blokčejn tehnologija je trenutno najzastupljenija tehnologija koja se koristi u rudarenju kripto valuta. Blokčejn tehnologija se može posmatrati kao nova mogućnost, alat za ugradnju u informacione sisteme i tehnologije sa primenom u digitalnom bankarstvu. Primena novih mogućnosti blokčejn tehnologija donosi brzi razvoj u okruženju. Svetski moćnici već ulažu veliki novac u blokčejn tehnologiju, jer se nadaju i velikoj zaradi. U Srbiji, u poslednjih 10 godina upotreba elektronskog plaćanja je u porastu ali je i dalje na niskom nivou. Najveći uticaj na upotrebu ima sumnja korisnika (učesnika) u sigurnost celokupnog procesa koji se odvija u mreži. U radu će biti objašnjeni potencijal blokčejn tehnologija, upotreba kriptografije kao zaštitnog mehanizma, kao i primena algoritma. Kriptografske tehnike omogućavaju pošiljaocu da maskira podatke, tako da ako neko pokuša da ih presretne, ne dobije nikakve informacije koje može da zloupotrebi. To istovremeno podrazumeva da je primalac u stanju da izvuče poslate originalne podatke koji su maskirani od strane pošiljaoca.

Ključne reči: *blokčejn tehnologija, kriptografija, sigurnost mreže, digitalni poslovni procesi, algoritmi zaštite*

Adresa autora zaduženog za korespodenciju:
Zoran Pavlović
zoran.g.pavlovic@gmail.com

Abstract

With the development of the Internet, new technologies are being applied in the business of both companies and individuals. Companies that trade or provide services already use Internet opportunities for their needs, and that means the realization of financial transactions. One important parameter can be singled out, which can be a problem for companies and users. This parameter refers to the security of sending and receiving money via the internet network. In addition to algorithms for secure online business, blokčejn technology is currently the most common technology used in cryptocurrency mining. Blokčejn technology can be seen as a new feature, a tool for embedding in information systems and technologies with application in digital banking. The application of new possibilities of Blokčejn technology brings rapid development in the environment. The world's powerful are already investing a lot of money in Blokčejn technology because they hope to make a lot of money. In Serbia, in the last 10 years, the use of electronic payment is on the rise, but still at a low level. The greatest influence on the use has the suspicion of the user (participant) in the security of the entire process that takes place in the network. The paper will explain the potential of Blokčejn technologies, the use of cryptography as a protection mechanism as well as the application of algorithms. Cryptographic techniques allow the sender to mask the data, so that if someone tries to intercept, they do not get any information that they can misuse. This means that the recipient can retrieve the sent original data that is masked by the sender.

Keywords: *Blockchain technology, cryptography, network security, digital business processes, security algorithms*

1 UVOD

Realizacija poslovnih procesa putem internet mreže podrazumeva primenu tehnologija (Pavlović, Banjanin, Vukmirović, & Vukmirović, 2020) (Pavlović, Bundalo, Bursać, & Tričković, 2021) (Subotić, Radičević, Pavlović, & Ćirović, 2021).Jedna od osnovnih definicija digitalnog novca da je to specifični monetarni podatak koji se elektronskim putem prenosi od korisnika usluge do ponuđača u realnom vremenu. Digitalni novac se može podeliti na:

- Digitalni novac koji se zasniva na karticama i
- Digitalni novac koji je zasnovan na softveru gde je omogućen transfer između dve strane putem mreže.

Osnovni principi digitalnog bankarstva podrazumevaju kontrolu svih komponenata sistema i zaštitu na svim nivoima mreže, veb servera, aplikacije i korisnika usluge. Među najvažnijim su (Backović, Radenković, Đelošević, & Novičić, 2009) :

- Poverljivost podataka, koji moraju biti zaštićeni od presretanja tokom procesa prenosa i da ne budu dostupni neautorizovanim licima.
- Integritet, koji se odnosi na podatak i njegovu sadržinu koja ne sme biti izmenjena tokom prenosa.
- Dostupnost, koja se ogleda u dostupnosti podataka u određenom vremenskom trenutku.
- Autentičnost, gde postoji mehanizam kojim se utvrđuje identitet korisnika usluge pre traženja podataka.
- Neporecivost, gde korisnik usluge ne može da porekne slanje poruke, a naravno i primalac ne poriče prijem.
- Enkripcija podrazumeva da podaci moraju da budu enkriptovani i dekriptovani od strane autorizovanog korisnika.
- Praćenje koje podrazumeva snimanje svih podataka u sistemu kako bi se pratila dešavanja u procesu transakcije.

Navedene forme funkcionišu preko interneta radi bezbednosti mreže. U daljem radu biće prikazani osnovni principi kriptografije, sigurnosti, sa tehnologijama koje se primenjuju stavljajući akcenat na blokovno šifriranje.

2 OSNOVNI PRINCIPI KRIPTOGRAFIJE

Osnovni principi u ovom radu zasnovani su na kriptografskim tehnikama. Kriptografskom tehnikom je obuhvaćeno blokovno šifriranje i ulančano blokovno šifriranje koje se koristi u *blokčejn* tehnologiji. Blokovno šifriranje podrazumeva da se neka poruka koja treba da se

šifruje obrađuje u blokovima koji se sastoje od bitova. Na primer, ako se poruka sastoji od 64-bitnih blokova, nakon razbijanja poruke svaki blok se šifruje nezavisno. Kada se šifruje jedan blok, vrši se preslikavanje jedan na jedan i preslikava se jedan bitni blok otvorenog teksta u bitni blok šifriranog teksta. Kod ovakvog preslikavanja kod svakog ulaza postoji različit izlaz. Blokovno šifriranje omogućava veliki broj preslikavanja i takođe veliki broj kombinacija koje mogu nastati. Svako preslikavanje predstavlja jedan ključ. Ako pošiljalac i primalac poruke znaju određeno preslikavanje oni imaju mogućnost da šifruju i dešifruju poruke koje međusobno razmenjuju. Za blokovno šifriranje u ovom slučaju ima veliki broj kombinacija. Znači da pošiljalac i primalac moraju da imaju šemu sa toliko mogućih preslikavanja (Kurose & Ross, 2013).

Zbog mogućih presretanja poruke za šifrovanje se koriste mnogo veći blokovi od 64 bita. Prilikom eventualnog napada od strane zlonamerne osobe moraju se isprobati sva moguća preslikavanja kako bi se pronašao odgovarajući ključ. Ako se pronađe pravo preslikavanje u „oblaku“ mogućih kombinacija, tj. ključ, postoji mogućnost dešifrovanja šifriranog teksta. Za blokovno šifriranje u ovom slučaju kod promene šifre i pošiljalac i primalac moraju da menjaju sva preslikavanja koja su unapred određena i zato je teško implementirati ovaj model.

Nakon prikaza nefunkcionalnosti blokovnog šifriranja gde su unapred određena preslikavanja, pristupamo modelu gde šifre bloka koriste funkcije koje simuliraju slučajno permutovane tabele. Ovaj model podrazumeva da funkcija razdvaja blok od 64 bita na osam kriški. Svaka kriška ima osam bitova. Posle razbijanja funkcije na osam kriški, sastavlja se u 64 bitni izlaz gde se pozicije razbacuju kako bi se dobio 64 bitni izlaz. Sa tog izlaza ponovo se vraća na ulaz od 64 bita. Ovo predstavlja jedan ciklus. Takvi ciklusi isporučuju 64 bitni blok šifriranog teksta. U svakom ciklusu bitovi utiču na većinu, a postoji mogućnost i na sve izlazne bitove.

U praksi postoji dosta popularnih algoritama za blokovno šifriranje kao što su DES (Data Encryption Standard) 3DES i AES (Advanced Encryption Standard). U ovim modelima kao ključ se koristi niz bitova. Ključ jednog algoritma omogućava preslikavanje mini tabele i permutacije. Prilikom napada zlonamerna osoba mora da isproba sve moguće ključeve i primeni algoritam za dešifrovanje podataka. U realnom životu mogućnost razbijanja i dešifrovanja je nemoguća.

Prilikom šifrovanja dužih poruka mora da se primeni „ulančano blokovno šifriranje“. Postupak je isti, poruka se iseče na bitne blokove i šifrira se svaki blok zasebno. Kod ovakvog ulančanog blokovnog šifriranja postoji mogućnost da dva ili više blokova budu identični. Da bi se izbegla identičnost blokova mora da se upotrebi slučajnost u šifriranom tekstu gde identični blokovi otvorenog teksta proizvode različite blokove šifrovanog teksta. Potrebno je da pošiljalac napravi slučajan bitni broj za bilo koji bitni blok. Posle pošiljalac šalje sve blokove do primaoca koji ima ključ za izračunavanje i može da rekonstruiše svaki blok otvorenog teksta kako bi saznao sadržinu poruke. Ovaj model je pouzdaniji ali zbog slanja svakog šifrovanog bita, pošiljalac mora da pošalje i slučajni bit. Na ovaj način potreban je udvostručeni propusni opseg gde je veći broj bitova koji moraju da se prenesu. Ulančavanje šifrovanih blokova podrazumeva da se samo jedna slučajna vrednost šalje samo uz prvu poruku gde pošiljalac i primalac upotrebljavaju već izračunate šifrovane blokove i u narednim slučajnim brojevima.

Ulančavanje šifrovanih blokova funkcioniše na sledeći način (Kurose & Ross, 2013):

- Pre početka šifrovanja poruke generiše se slučajan niz bitova koji ima naziv inicijalizacioni vektor i šalje se primaocu kao otvoreni tekst.
- Kada pošiljalac izračunava prvi blok koristi prvi blok otvorenog teksta sa inicijalizacionim vektorom. Dobijeni rezultat uz pomoć algoritma blokovnog šifriranja koristi za dobijanje odgovarajući blok šifriranog teksta. Dobijeni rezultat kao šifrirani blok šalje primaocu.
- Dalje, pošiljalac za svaki blok generiše šifrirani blok teksta kao ključ.

Na ovaj način primalac može uvek da obnovi originalnu poruku. Ako napadač presretne poruku koja je poslata za inicijalizacioni vektor nema mogućnost da dešifruje šifrovani blok jer ne poseduje ključ. Ovaj model koristi slanje samo još jednog dodatnog bloka inicijalizacionog vektora

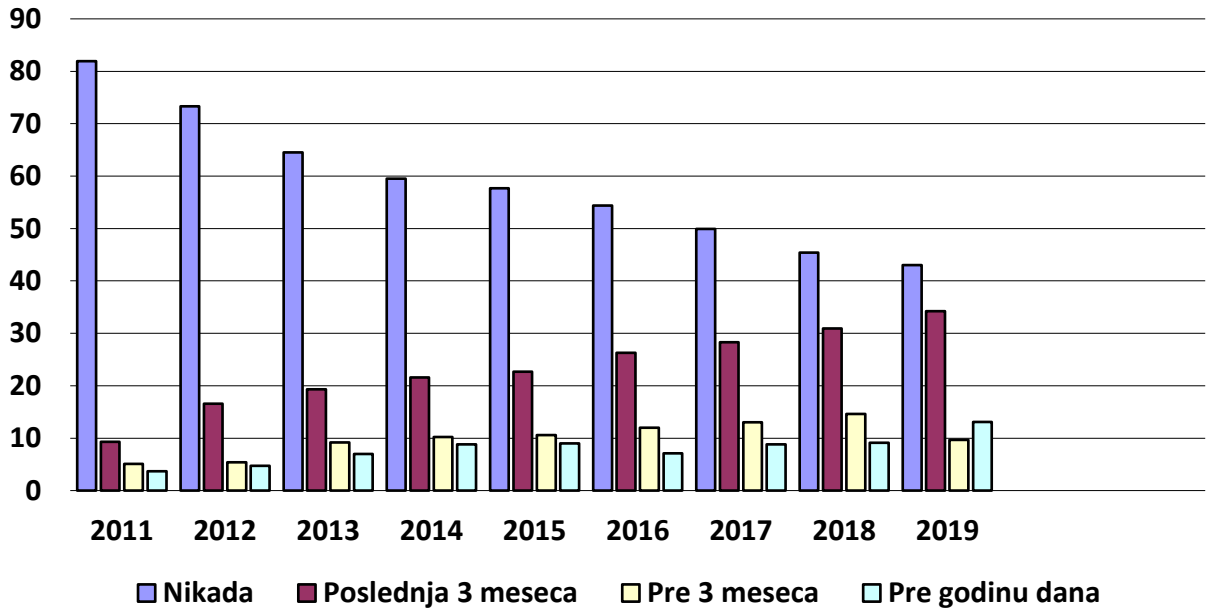
tako da se malo povećava propusni opseg prilikom slanja lanaca blokova.

3 UPOTREBA ELEKTRONSKE TRGOVINE KOD KORISNIKA

Pružanje usluge u elektronskom bankarstvu pojedincima ili organizacijama putem interneta omogućava da se brže, tačnije, pouzdanije izvrši proces plaćanja i naplate. Zavod za statistiku je prikazao upotrebu elektronskih servisa za trgovinu putem interneta u periodu od 2011. do 2019. godine (RZS, 2020). U poslednjih 9 godina korisnici sve više koriste mogućnosti elektronskog plaćanja. Na grafikonu 1 prikazan je porast upotrebe elektronske trgovine kod pojedinaca u Republici Srbiji.

U grafikonu 1 korisnik 1 predstavlja kategoriju koja nikada nije koristila elektronsko plaćanje. Navedeni trend je u opadanju od 81,9% čak na 43,0% 2019. godine. To je jedan od pokazatelja da pojedinci sve više koriste mogućnost trgovine putem interneta. Korisnik 2 je koristio uslugu u poslednja tri meseca, gde se može videti drastično povećanje od 9,3 % u 2011. godini do 34,2% 2019. godine. Korisnik 3 je koristio uslugu pre tri meseca a manje od godinu dana. I ovde se može videti povećanje od 4,6% do 12% 2016. godine. Korisnik 4 je koristio uslugu pre više od godinu dana, gde je povećanje od 3,7% do 13,1% 2019. godine.

Da bi ovaj trend bio u porastu mora se obratiti velika pažnja na sigurnost. Korisnici usluge najveću strepnju i odbojnost imaju prema elektronskom bankarstvu zato što nemaju dovoljno informacija koliko su sigurne transakcije putem interneta. U današnjem vremenu sve više procesa i sistema funkcioniše na osnovu digitalnih informacija, koje su izložene nizovima nula i jedinica odnosno bajtovima (Radenković, Despotović-Zrakić, Bogdanović, Barać, & Labus, 2015).



Grafikon 1. Trgovina putem interneta- pojedinci

Pomoću savremenih informacionih i komunikacionih tehnologija (IKT), mobilno bankarstvo kao novu vrstu finansijskih usluga i može da obezbedi efikasne i efektivne finansijske usluge za korisnika. Implementacija bežične komunikacije tehnologije može dovesti do složenije informacione bezbednosti. Mobilno bankarstvo može da korisnicima pruži bolji kvalitet i više usluga uz smanjenje troškova. Mobilni uređaji predstavljaju mnoge iste rizike kao Internet bankarstvo. Karakteristike mrežnih finansijskih usluga su meta svih vrsta tehnoloških napada. Mnoge tehnologije su zbog bezbednosti šifrovane. Implementacija šifrovanja je neophodna za zaštitu podataka gde postoji sigurnosni mehanizma za bežične komunikacije u mreži. Trenutno mere za šifrovanje i autentičnosti zahtevaju punu snagu računara i kapacitet za skladištenje podataka. Klijenti Internet bankarstva imaju veoma moćan računar

koji omogućava složeno šifrovanje i proveru identiteta kako bi se obezbedila sigurnost. Mobilni uređaji moraju da primenjuju algoritam za simetrično šifrovanje AES i asimetričnost algoritma ECC. Upotreba ECC za šifrovanje, osigurava bezbednost podataka, ali i povećava brzinu dešifrovanja. AEC i ECC je tehnologija najmoćnija za zaštitu od hakera.

4 PREGLED TEHNOLOGIJA U POSLOVNIM PROCESIMA

Sistem mora da spreči nepotpunost podacima koji su nastali u procesu komunikacije. Sistem mobilne komunikacije je sistem koji treba da obezbedi i spreči pojavu ne-integriteta. Mobilni terminali i serveri stalno se suočavaju sa opasnošću od zlonamernih virusa koji napadaju. Mobilni bankarski sistem sa odgovarajućim merama bezbednosti, kao što su zaštitni zidovi, sistem za detekciju upada, mora da ima brze mehanizme za oporavak bezbednosti podataka. Mehanizmi integriteta moraju da čuvaju integritet sistema i osiguraju integritet mobilnog bankarskog sistema. Tokom procesa prenosa podataka, eventualni nepotpuni prenos podataka treba pratiti i pronaći rupu u sistemu. Mobilno bankarstvo može da pruži usluge koje se ne ograničavaju vremenom i prostorom. To će se sa razvojem i zrelošću mobilnih telekomunikacionih tehnologija poboljšati. Ako banke mogu integrisati mobilne bankarske trenutne usluge koje se tiču bezbednosti mogu dobro iskoristiti prednosti bežične komunikacione tehnologije (Jin & Xianling, 2008).

Blokčejn je tehnologija je uvedena za realizaciju Bitkoin, digitalne gotovine. Ona privlači veliku pažnju, posebno u oblastima finansijskih i pravnih aplikacija. Blokčejn tehnologija potvrđuje postojanje digitalne imovine (npr. novčiće, kao u slučaju Bitkoin), gde postoji kontrola za svaku od tih mreža. Ta kontrola se potpuno distribuira, i jedan (ili oni) koji imaju kontrolu mogu da menjaju stanje na sredstvima bez dozvole od svake centralne uprave. Blokčejn od nedavno privlači veliku pažnju industrije, posebno u finansijskim i pravnim sektorima. Uvedena je blokčejn tehnologija za upravljanje privatnim transakcijama sa hartijama od vrednosti od 2015 godine. Poduhvat je uspostavljen od strane konzorcijuma međunarodne banke 2015. godine koja je počela eksperimentisanje sa blokčejn za upravljanje međubankarskim transakcijama. Osnovne osobine blokčejn tehnologije nikada nisu dovedene u pitanje.

Blokčejn podrazumeva da svaki blok sadrži kriptografski nastavak prethodnog bloka, osim prvog bloka koji se ponekad naziva geneza blok. Takav nastavak mora da ispuni određeni kriterijum; treba da bude manji od ili jednak prethodnom i od strukture skladišta ili izračunatog bloka (ova je struktura varenje lanca u nastavku). Pošto se varenje izračunava u jednom pravcu funkcijom čiji su izlazi ravnomerno raspoređeni, niko ne može namerno konfigurisati blok da zadovolji kriterijum. Umesto toga, oni treba da učestvuju u ponavljaju za promenu vrednosti u bloku i oni se stvaraju dok ne dobiju pravi nastavak za varenje. Stvaranje bloka je proces verovatnoće. Učesnici učestvuju u održavanju lanaca blokova prema sledećem (Saito & Yamada, 2016):

- Učesnik sakuplja podatke onako kako ih prima, i pokušava da stvori važeći blok gde se sadržaju dodaju u nastavci u lancu za varenje.
- Ako je učesnik uspešan, onda emituje stvoren blok.
- Ostali učesnici dobijaju blok, i pokušaju da potvrde. Ako se uspešno potvrđen, oni priznaju da je poslednji blok u lancu varenja, i dalje prvi.

Blokčejn tehnologija je pokazala svoju znatnu prilagodljivost u poslednjih nekoliko godina u nizu tržišnih sektora gde je najveći deo fokusa u sektoru finansijskih usluga. Blokčejn izaziva optimizam koji je retko viđen u istoriji tehnologije. On je nova tehnološka revolucija, koja će imati veliki uticaj na društvo kao izum interneta. U izveštaju Svetskog ekonomskog foruma koji je objavljen u septembru 2015. godine, 58 % svih istraživanja i ispitanika su pokazali da očekuju da do 2025, 10% globalnog bruto domaćeg proizvoda bude sačuvano korišćenjem blokčejn tehnologije (Mettler, 2016). Stoga ne čudi da blokčejn privlači slabe investitore koji su intenzivno ulažu u blokčejn tehnologiju. Pristup, ciljevi i potencijali blokčejn još uvek su u velikoj meri nepoznati društvu. Blokčejn je prvobitno razvijen za kriptovanje Bitkoina. Prvi put je opisan u 2008. godine gde se posebno bavi izazovom vlasništva u vezi sa digitalnom valutom i predlaže se rešenje pomoću Blokčejn tehnologije prilikom

novčanih transakcija. Funkcionalnost principa Blokčejn može se objasniti koristeći koncept Bitkoin transakcija. Ako je Bitkoin transakcija, na primer, od novčanika A do novčanika B, ove informacije se istovremeno dele u osnovni Bitkoin blokčejn. Informacije o Bitkoin transakciji kombinuju se u blok informacija označenim sa vremenskim markerom i dodaje kao novi blok na postojeći Bitkoin blokčejn. U isto vreme, transakcija je verifikovana i potvrđuje sve uključene novčanike. Informacije u vezi sa svim transakcijama u prošlosti, u bilo kom trenutku su potpuno transparentne. Sadržaj ove decentralizovane baze podataka je dostupan svim uključenim stranama. Osim toga, pošto su sve transakcije obrađene od strane korisnika preko određenog pseudonima, informacije o sadržaju Bitkoin su potpuno anonimne. Primer jasno pokazuje da blokčejn tehnologija predstavlja pristup kako se postiže vlasništvo digitalnih dobara gde je osnovni princip decentralizovanog, transparentnog i trenutnog pristupa informacijama koje predstavljaju polaznu tačku za mnoge tržišne sektore. Blokčejn je nastavio da se razvija unutar i izvan finansijskog sektora. Shodno tome, postoji neki zanimljivi primeri izvan finansijskog sektora.

Bitkoin dobija mnogo pažnje i značaj akademskog istraživanja. Jedna od njegovih tehničkih karakteristika je da omogućava pouzdane transakcije bez mehanizma centralizovanog upravljanja čak i ako postoje nepouzdani učesnici u mreži. Struktura jednog blokčejna je takva da je blok koji se sastoji od više transakcija povezan sa prethodnim blokom u obliku povezanih lanaca blokova da bi se obezbedila pouzdanost. Kada je novi blok generisan, dodaje se prethodnom bloku. Kao alternativni metod obezbeđivanja, blokčejn je dokaz akcija koji je predložen u Bitkoin zajednici još 2011. godine. Da bi se uspešno izvršio napad na blokčejn tehnologiju, napadač mora da kontroliše više od 50% resursa na celoj mreži (poznat kao napad na 51%). Kada napadač pokuša da prisvoji novčiće učesnici mreže će ga otkriti, a vrednost novca koji imaju će biti značajno smanjena. Ovo radi na principu odvraćanja napadača od napada. Veruje se da blokčejn tehnologija ima veliki potencijal za upravljanje ugovorima, kao što je upravljanje digitalnim pravima, jer je blokčejn jak protiv napada i teško je promeniti tok digitalne valute gde sistem radi bez centralnog organa. Tehnologija stvara mogućnost spuštanja naknada za korisnike (Watanabe, Fujimura, Nakadaira, & Miyazaki, 2016).

Tvorac koncepta, Satoshi Nakamoto, pronalazač blokčejn objavio je rad krajem 2008. godine, pod nazivom „Bitkoin: Elektronski novčani sistem Peer-to-peer“ u kome je predložio sistem elektronskog novca. Uvođenje Blokčejn tehnologije i uz pomoć blokova moguće je pratiti sav novac u sistemu. Nakamoto je dao odgovor kroz blokčejn gde napominje da je to rastući lanac brojeva koji sadrži istoriju svakog Bitkoin ikada napravljenog. Trgovina se obavlja u virtualnom prostoru. Čak i ako se vrednost Bitkoina smanji, blokčejn može da živi. Bitkoin blokčejn aplikacije mogu ugradili svoju vlastitu informaciju koja je nastala u transakcijama često se koristeći delom zapisa transakcije izgrađenom za skladištenje suvišnih informacija. Ako više ljudi pokušava da skladišti i blokčejn raste. Njegova priroda je da se stari podaci ne mogu arhivirati neznano gde. Svaki deo lanca se zasniva na njegovom prethodnom. Posle pete godine svog postojanja Bitkoin blokčejn se udvostručio u 2014. godini do 26GB. Tokom prve dve godine, je bilo potrebno 1MB prostora. Možemo posmatrati blokčejn kao digitalni neboder. Svaki sprat je 'blok' podataka, koji sadrži informacije o transakcijama koje su se dogodile u mreži dok je blok bio napravljen. U Bitkoinu, novi blok se kreira svakih 10 minuta pri čemu se stvara stalno produženje kule spratova ili lanaca blokova (Bradbury, 2015).

Blokčejn je tehnologija u razvoju za decentralizovana i transakciona deljenja podataka preko interneta. To omogućava nove oblike distribuirane softverske arhitekture. S obzirom da blokčejn može da se posmatra kao softver konektor koji prati rezultate performanse i kvalitet atributa sistema (na primer, bezbednost, privatnost, skalabilnosti i održivost). Učesnici treba da veruju svakoj komponenti u sistemu. Struktura blokčejn podataka je sa vremenskim oznakama lista blokova, koja snima podatke o transakcijama koje su bilo kada dogodile u blokčejn mreži. Zato blokčejn obezbeđuje skladištenje podataka koje omogućava ubacivanje transakcije bez ažuriranja ili brisanja postojećih transakcija na blokčejnu. Čitava mreža dostiže konsenzus pre transakcija koje su

uključene u nepromenljivo skladištenje podataka (Xu, et al., 2016).

5 ZAKLJUČAK

Blokčejn se razlikuje od ostalih tehnologija. Radi sa nepoznatim brojem učesnika bez pokušaja da ih odredi. Blokčejn ima mogućnosti za korišćenje u svim finansijskim a i ostalim sektorima. Banke u finansijskom pogledu očekuju nove mogućnosti prenosa finansijskih sredstava, digitalnog novca primenom blokčejn tehnologija gde je mreža zaštićena od trećih lica koja mogu da izvrše napad. Ogroman potencijal ove tehnologije je u stalnom razvoju i sve više zauzima vodeću poziciju na tržištu internet usluga. Zbog toga u budućnosti blokčejn tehnologija otvara nove mogućnosti u pogledu novog načina poslovanja. Realizacija primene blokčejn tehnologija u digitalnom bankarstvu putem Interneta omogućiće jednostavnije i bezbednije procese trgovine kako građanima tako i organizacijama.

CITIRANA DELA

Backović, N., Radenković, S., Đelošević, I., & Novičić, M. (2009). *Elektronsko poslovanje i Internet marketing.* Leposavić: Visoka ekonomska škola strukovnih studija Peć u Leposaviću.

Bradbury, D. (2015). In blocks [SecurityBitcoin]. *Engineering & Technology (Volume: 10, Issue: 2, March 2015),*, 68-71.

Jin, N., & Xianling, H. (2008). Mobile Banking Information Security and Protection Methods. *2008 International Conference on Date of Conference: 12-14 Dec.* Computer Science and Software Engineering.

Kurose, J., & Ross, K. (2013). *Umrežavanje računara, od vrha do dna* (6. izd.). Beograd: CET Computer Equipment and Trade.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here, . *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on, Date of Conference: 14-16 Sept. 2016.*

Pavlović, Z., Banjanin, M., Vukmirović, J., & Vukmirović, D. (2020). Contactless ICT Transaction Model Of The Urban Transport Service. *Research journal TRANSPORT, ISSN: 1648-4142 / eISSN: 1648-3480, Vol 35 No 5, https://doi.org/10.3846/transport.2020.12529*, 500-510.

Pavlović, Z., Bundalo, Z., Bursać, M., & Tričković, G. (2021). Use of information technologies in railway transport. *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2021,,https://ieeexplore.ieee.org/document/9400521* (str. 1-4). East Sarajevo, Bosnia and Herzegovina,: IEE.

Radenković, B., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., & Labus, A. (2015). *Elektronsko poslovanje.* Beograd: FON.

RZS. (2020). Preuzeto sa Upotreba informaciono-komunikacionih tehnologija u Republici Srbiji, 2020: http://publikacije.stat.gov.rs/G2018/Pdf/G201816013.pdf

Saito, K., & Yamada, H. (2016). What's So Different about Blockchain? Blockchain is a ProbabilisticState Machine . *Distributed Computing Systems Workshops (ICDCSW), 2016 IEEE 36th International Conference on , Date of Conference: 27-30 June.*

Subotić, M., Radičević, V., Pavlović, Z., & Ćirović, G. (2021). Development of a New Risk Assessment Methodology for Light Goods Vehicles on Two-Lane Road Sections. *Computer and Engineering Science, Symmetry 2021, Vol.13, Iss.7,https://doi.org/10.3390/sym13071271* , 1271.

Watanabe, H., Fujimura, S., Nakadaira, A., & Miyazaki, Y. (2016). Blockchain contract: Securing a blockchain applied to smart contracts,. *Consumer Electronics (ICCE), 2016 IEEE International Conference on, Date of Conference: 7-11 .*

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The Blockchain as a Software Connector. *13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182-191). Venice, It: IEEE Computer Society.

Received for publication: 26.09.2021.
Revision received: 30.09.2021.
Accepted for publication: 10.10.2021.

Kako citirati ovaj rad? / How to cite this article?

*Style – **APA** Sixth Edition:*

Pavlović, Z. G., Radičević, V., & Nikolić, D. (2021, 10 15). Tehnologije za zaštitu podataka u digitalnim poslovnim procesima. (Z. Čekerevac, Ur.) *FBIM Transactions, 9*(2), 63-70. doi:10.12709/fbim.09.09.02.07

*Style – **Chicago** Sixteenth Edition:*

Pavlović, Zoran G, Veljko Radičević, i Dragan Nikolić. 2021. „Tehnologije za zaštitu podataka u digitalnim poslovnim procesima.“ Urednik Zoran Čekerevac. *FBIM Transactions* (MESTE) 9 (2): 63-70. doi:10.12709/fbim.09.09.02.07.

*Style – **GOST** Name Sort:*

Pavlović Zoran G, Radičević Veljko i Nikolić Dragan Tehnologije za zaštitu podataka u digitalnim poslovnim procesima [Časopis] // FBIM Transactions / ur. Čekerevac Zoran. - Beograd : MESTE, 15 10 2021. - 2 : T. 9. - str. 63-70.

*Style – **Harvard** Anglia:*

Pavlović, Z. G., Radičević, V. & Nikolić, D., 2021. Tehnologije za zaštitu podataka u digitalnim poslovnim procesima. *FBIM Transactions,* 15 10, 9(2), pp. 63-70.

Style – **ISO 690** Numerical Reference:

Tehnologije za zaštitu podataka u digitalnim poslovnim procesima. **Pavlović, Zoran G, Radičević, Veljko i Nikolić, Dragan.** [ur.] Zoran Čekerevac. 2, Beograd : MESTE, 15 10 2021, FBIM Transactions, T. 9, str. 63-70.