Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 621.313
DOI: https://doi.org/10.24867/17BE24Mutavdzic

DIGITALNI POTPISI I NJIHOVA ULOGA U BLOCKCHAIN TEHNOLOGIJI

DIGITAL SIGNATURES AND THEIR ROLE IN BLOCKCHAIN TECHNOLOGY

Ana Mutavdžić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – KRIPTOZAŠTITA INFORMACIJA

Kratak sadržaj – *Digitalni potpis postao je jedan od najvažnijih kriptografskih alata koji je danas u širokoj upotrebi. Njegova osnovna uloga je da potvrdi identitet pošiljaoca poruke, kao i da obezbedi dokaz da je originalni sadržaj poruke ostao nepromenjen. U ovom radu dat je opis nastanka i funkcionisanja digitalnih potpisa, kao i njihova primena u blockchain tehnologiji.*

Ključne reči: *Kriptografija, Digitalni potpis, Blockchain tehnologija*

Abstract – *Digital signature has become one of the most important and broadly used contemporary cryptographic tools. Its main purpose is to verify the identity of the sender of the document, as well as to provide evidence that the original content of the sent message is unchanged. This paper describes the origin and basic principles of digital signatures, as well as their application in blockchain technology.*

Keywords: *Cryptography, Digital signature, Blockchain technology*

1. UVOD

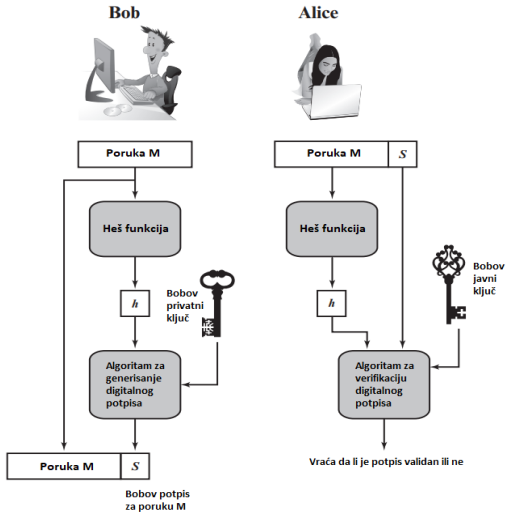
Potreba za komunikacijom je jedna od glavnih sociogenih potreba čoveka. Veći deo čovečanstva dnevno ulazi u komunikaciju sa drugim ljudima. Neki od njih provode sate razgovarajući i razmenjujući informacije, dok neki to rade samo par minuta dnevno. Jako je bitno znati ko šalje poruku i biti siguran da tokom slanja poruke niko nije uspeo da promeni njen sadržaj. Ovo se postiže autentifikacijom. Jedan od najvažnijih kriptografskih alata koji se koristi da potvrdi identitet pošiljaoca poruke kao i činjenicu da je poslata poruka nepromenjena naziva se *digitalni potpis*.

2. DIGITALNI POTPIS

Digitalni potpis je jedan od najvažnijih kriptografskih alata koji danas ima široku primenu. U mnogim slučajevima, oni pružaju sloj provere valjanosti i sigurnosti porukama poslatim putem nebezbednog kanala. Pravilno sproveden, digitalni potpis daje primaocu razlog da veruje da je poruku poslao pošiljalac koji se potpisao. Digitalni potpisi su u mnogim aspektima ekvivalentni tradicionalnim ručno napisanim potpisima, ali je pravilno primenjene digitalne potpise teže falsifikovati nego ručno pisane.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio doc. dr Mladen Kovačević.

Na Slici 1. predstavljen je generički model procesa izrade i upotrebe digitalnih potpisa. Pretpostavimo da komuniciraju dve strane koje nazivamo Alice i Bob. Ukoliko Bob želi da pošalje poruku Alice, on želi da Alice bude sigurna da je poruka zaista od njega. Algoritam potpisa je funkcija Bobovog privatnog ključa te pod pretpostavkom da on zaista drži svoj ključ privatnim, jedino Bob može potpisati poruku M u svoje ime. Poruka M predstavlja ulaz u algoritam za potpis u cilju njenog povezivanja sa potpisom. Bob najpre formira sažetak poruke *h* korišćenjem određenog algoritma za heširanje. Zatim se sažetak poruke, koji je obično dužine 128 ili 256 bita, šifruje korišćenjem Bobovog privatnog ključa i tako nastaje digitalni potpis *S*. Digitalni potpis se dodaje na kraj poruke pa se par (M, S) šalje Alice. Važno je napomenuti da digitalni potpis sam po sebi nije od koristi osim ako nije propraćen porukom. Potpis je koristan samo ako postoji način da Alice proveri je li važeći ili ne. Za ovo je potrebna funkcija verifikacije koja uzima sažetak poruke i potpis kao ulaze. Da bi se potpis povezao sa Bobom, funkcija takođe zahteva njegov javni ključ. Njen jedini izlaz je binarni izraz *true* ili *false*. Ako je poruka potpisana privatnim ključem koji odgovara javnom ključu za verifikaciju, izlaz je *true*, u suprotnom je *false*.



Slika 1. *Generički model procesa izrade i upotrebe digitalnih potpisa*

Najčešće korišćeni digitalni potpisi u *blockchain* tehnologiji su digitalni potpisi bazirani na eliptičnim krivama ECDSA (*eng. Eliptic Curve Digital Signature Algorithm*) i *Schnorrovi* potpisi čiji će način rada biti objašnjen u taljem tekstu.

2.1. Eliptične krive

Eliptične krive imaju nekoliko prednosti u odnosu na druge vrste digitalnih potpisa. Konkretno, u kripto-sistemima baziranim na eliptičnim krivama, ključevi dužine 160–256 bita pružaju sigurnost ekvivalentnu 1024–3072-bitnim RSA i šemama baziranim na problemu diskretnog logaritma. Kraća dužina često rezultira kraćim vremenom obrade i kraćim potpisima. Iz ovih razloga, algoritam digitalnog potpisa eliptične krive standardizovan je u SAD od strane Američkog instituta za standarde (ANSI) 1998. godine.

ECDSA standard zasnovan je na problemu diskretnog logaritma konstruisanog u grupi eliptične krive. Generisanje ključeva za ECDSA izgleda ovako:

1. Koristiti eliptičnu krivu E sa modulom p, koeficijentima a i b, i tačkom A koja generiše cikličnu grupu osnovnog reda q.
2. Odabrati slučajni ceo broj d takav da je $0 < d < q$.
3. Izračunati $B = d\ A$.

Ključevi su sada $k_{pub} = (p, a, b, q, A, B)$ i $k_{pr} = (d)$. ECDSA potpis se sastoji od para celih brojeva (r, s). Svaka vrednost ima istu bitsku dužinu kao q, što čini prilično kompaktne potpise. Koristeći javni i privatni ključ, potpis za poruku x izračunava se na sledeći način:

1. Odabrati ceo broj kao slučajni efemeralni ključ k_E takav da važi $0 < k_E < q$.
2. Izračunati $R = k_E\ A$.
3. Neka je $r = x_R$.
4. Izračunati $s \equiv (h\ (k) + d \cdot r)\ k_E^{-1} \bmod q$.

Poruka x mora biti heširana pomoću funkcije h da bi se izračunalo s. Izlazna dužina heš funkcije mora biti najmane iste dužine kao q, a proces verifikacije potpisa je sledeći:

1. Izračunati pomoćnu vrednost $w \equiv s^{-1}\ mod\ q$.
2. Izračunati pomoćne vrednosti $u_1 \equiv w \cdot h(x)\ mod\ q$ i $u_2 \equiv w \cdot r\ mod\ q$.
3. Izračunti $P = u_1\ A + u_2 B$.
4. Verifikacija $ver_{k_{pub}}(x, (r, s))$ sledi iz:

$$x_P \begin{cases} = r\ mod\ p \Longrightarrow validan\ potpis \\ \neq r\ mod\ p \Longrightarrow invalidan\ potpis \end{cases}$$

Glavni analitički napad na ECDSA pokušava da reši problem diskretnog logaritma eliptične krive. Kada bi napadač bio sposoban za to, mogao bi izračunati privatni ključ d i/ili efemeralni ključ. Takođe, na početku verifikacije mora se proveriti da li su $r, s \in \{1,2,\dots,q\}$ kako bi se sprečio određeni napad. Ponovna upotreba efemeralnog ključa takođe se mora sprečiti.

2.2. Schnorr digitalni potpis

Schnorr šema potpisa zasnovana je na problemu diskretnog logaritma. Ona minimizuje broj potrebnih izračunavanja pri generisanju potpisa. Prvi deo ove šeme jeste generisanje privatnog i javnog ključa, koje se sastoji od sledećih koraka:

1. Odabrati proste brojeve p i q, tako da važi $p - 1 \equiv 0\ mod\ q$.
2. Odabrati ceo broj a, tako da je $a^q = 1\ mod\ q$.
3. Odabrati slučajni ceo broj s tako da je $0 < s < q$.
4. Izračunati $v = a^{-s}\ mod\ p$. Ovo je javni ključ korisnika.
5. Vrednosti a, p i q pedstavljaju javni ključ koji može biti zajednički za grupu korisnika. Privatni ključ korisnika je s a javni ključ korisnika je v.

Za vrednosti p i q obično se uzima $p \approx 2^{1024}$ i $q \approx 2^{160}$. Dakle, p je 1024-bitni broj, a q je 160-bitni broj, što je ujedno i dužina SHA-1 heš vrednosti. Korisnik pomoću privatnog ključa s generiše potpis na sledeći način:

1. Odabrati slučajni ceo broj r tako da je $0 < r < q$ i izračunati $x = a^r\ mod\ p$. Ovo izračunavanje je faza predprocesiranja nezavisna od poruke M koju treba potpisati.
2. Spojiti poruku M sa x i heširati rezultat kako bi se izračunala vrednost $e = H\ (M \parallel x)$
3. Izračunati $y = (r + se)\ mod\ q$. Potpis se sastoji od para (e, y).

Svaki korisnik može da verifikuje potpis na sledeći način koristeći javni ključ.

1. Izračunti $x' = a^y v^e\ mod\ p$
2. Proveriti da li je $e = H(M \parallel x')$. Treba primetiti da važi sledeće

$$x' \equiv a^y v^e \equiv a^y a^{-se} \equiv a^{y-se} \equiv x\ mod\ p$$

Dakle, $H(M \parallel x') = H(M \parallel x)$.

Schnorrovi potpisi izgledaju kao slučajni brojevi. Konkretno, vrednosti r i s su slučajni brojevi. $H(M \parallel x)$ takođe treba da bude slučajan broj jer predstavlja izlaz heš funkcije, a spajanje više slučajnih brojeva daje nasumičan broj. Verovatnoća vrednosti potpisa jednaka je verovatnoći nasumice izabranog broja, bez obzira na sadržaj poruke i na to ko je potpisuje. Ukoliko potpišemo dve različite poruke istim ključevima, procuriće ceo privatni ključ. Ukoliko imamo dve poruke M1 i M2 potpisane privatnim ključem s i istim vrednostima r i x tada napadač može da oduzme dve vrednosti i nasumične izmene koje skrivaju privatni ključ će se poništiti. Iz tog razloga je ponovna upotreba vrednosti r i x zabranjena.

Sada kada imamo bolji uvid u način funkcionisanja digitalnih potpisa u daljem tekstu biće reči o revolucionarnoj *blockchain* tehnologiji i primeni digitalnih potpisa u ovoj oblasti.

3. BLOCKCHAIN TEHNOLOGIJA

Blockchain predstavlja revolucionarnu tehnologiju koja je u velikoj meri uticala na različite industrije. Na tržištu je predstavljena svojom prvom modernom aplikacijom *bitcoin*. *Blockchain* tehnologija omogućava svim učesnicima u mreži da postignu dogovor, opšte poznat kao konsenzus. Svi podaci uskladišteni na *blockchain-u* snimaju se digitalno i imaju zajedničku istoriju koja je dostupna svim učesnicima na mreži. Na ovaj način se eliminišu šanse za bilo kakvu lažnu aktivnost ili dupliranje transakcija bez potrebe za trećom stranom.

Postoje tri vrste *blockchaina* a to su javni, privatni i hibridni *blockchain*. Javni *blockchain* o kom će se govoriti u ovom radu je otvorena, decentralizovana mreža računara dostupna svima koji žele da zatraže ili potvrde transakciju. Sve transakcije koje se odvijaju na javnom

blockchainu su potpuno transparentne, što znači da svako može pregledati pojedinosti transakcije. Javni *blockchain* koristi mehanizme konsenzusa dokaza o radu (*eng. proof-of-work*) ili dokaza o ulogu (*eng. proof-of-stake*) i oni koji potvrđuju transakcije dobijaju nagrade. Dva uobičajena primera javnog blockchaina su *bitcoin* i *ethereum*.
Blockchain se kao što mu samo ime govori sastoji od blokova. Blok je struktura podataka u kojoj su zapisane digitalne informacije koje se dele putem blockchaina. Blokovi su organizovani linearno, a nove transakcije se konstantno procesuiraju od strane rudara (*eng. miner*) u nove blokove koji se nadodaju na kraj lanca. Blok takođe sadrži podatke o svojoj veličini, zapise koji prikazuju sadržaj podataka skladištenih u datom bloku i njihov broj. U strukturi bloka takođe se nalazi i zaglavlje, koje sadrži metapodatke.

3.1. Sistem ravnopravnih partnera

Sistem ravnopravnih partnera, odnosno sistem građen prema modelu ravnopravnih partnera (*eng. peer-to-peer*) sastoji se od velikog broja procesa, takozvanih partnera (*eng. peer*). Partneri obavljaju zadatke prema potrebama svojih korisnika. U javnom *blockchainu* partneri se razlikuju prema funkcijama koje obavljaju. Vrste partnera su:

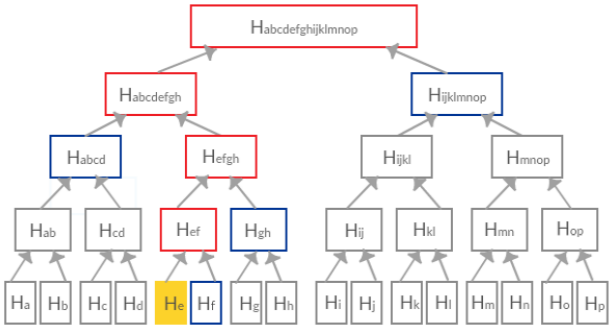
- Potpuni partner
- Rudar
- Novčanik
- Blockchain partner

3.1.1. Novčanik

U javnim sistemima koji koriste *blockchain* zbog velike količine podataka nema svaki korisnik mogućnost da skladišti podatke u čitav *blockchain*. Takav korisnik tada u sistemu sudeluje kao jednostavan novčanik.

Glavni zadatak koji jednostavni novčanik obavlja jeste kreiranje novih zapisa u skladu sa protokolom koji propisuje sistem. U svrhu potvrde vlasništva nad digitalnim novcem ili nekom drugom digitalnom informacijom čiji integritet želimo zaštititi stavljanjem na *blockchain*, novčanici skladište parove javnih i privatnih kriptografskih ključeva. Budući da nemaju punu sliku transakcija koje su se dogodile pre one koju žele da validiraju oslanjaju se na ostale partnere koji im na njihov zahtev mogu pružiti uvid u deo *blockchaina*. Jednostavni novčanici proveravaju dubinu transakcija. Binarno heš stablo pruža partnerima novčanicima proveru kom bloku pripada određena transakcija, to je prikazano na Slici 2.

U blok čije binarno heš stablo vidimo na slici, zapisano je 16 transakcija i jednostavni novčanik želi proveriti pripada li tom bloku transakcija *e*. Budući da poznaje sadržaj transakcije *e* partner lako može odrediti heš H_e. Kako bi proverio pripadnost transakcije bloku potrebno je da primi od nekog od svojih susednih partnera koji održavaju celu kopiju *blockchaina* heš vrednosti H_f, H_{gh}, H_{abcd} i $H_{ijklmnop}$. Ove heš vrednosti na Slici 2. označene su plavim pravougaonicima i nazivaju se *autentifikacijski put*. Nakon što jednostavni novčanik poseduje autentifikacijski put on može izračunati heš vrednosti H_{ef}, H_{efgh}, $H_{abcdefgh}$ i konačno koren binarnog heš stabla $H_{abcdefghijklmnop}$ označen crvenim pravougaonikom. Izračunat koren stabla partner tada upoređuje sa korenom binarnog heš stabla zapisanog u zaglavlju bloka, ako se ti podaci podudaraju transakcija *e* pripada bloku sa Slike 2.



Slika 2. *Proces potvrde pripadnosti transakcije određenom bloku*

3.1.2. Blockchain partner

Glavna funkcija blockchain partnera je da održava ceo lanac sa podacima u njemu, krenuvši od prvog do poslednjeg bloka u *blockchainu* koji u tom određenom trenutku postoji. Ukoliko je potrebno validirati neku određenu transakciju ili proveriti verodostojnost neke transakcije koja je zapisana u *blockchainu*, tada *blockchain* partner može proveriti jesu li sredstva koja su deo transakcije stvarno od tog korisnika.

3.1.3. Rudar

Funkcija rudara je da prihvata nove zapise koji su napravljeni od strane novčanika, kreira blokove zapisa i smešta ih u *blockchain*. Na primeru *bitcoina*, način kako se upisuju novi zapisi u lanac potrebno je korišćenje računarskih resursa. Pod korišćenjem računarskih resursa, misli se na rešavanje algoritma koji se zove *proof-of-stake*. Dakle, novi blokovi se dodaju u blockchain pomoću rešavanja algoritma, kada se izvrši validacija transkripcije rudar koji je obavio taj zadatak i utrošio svoje resurse na izvršenje iste, biva nagrađen sa određenim udelom *bitcoina*.
Treba napomenuti da potpuni partner može obavljati funkcije svih prethodno navedenih partnera.

3.2. Uloga digitalnog potpisa u blockchain tehnologiji

Digitalni potpisi su temelji *blockchain* tehnologije, pružaju ključne prednosti skladištenja i prenošenja i garantuju integritet. Tehnički, poslati podaci mogu se promeniti a da to ne učini haker. Čak i da se to dogodi, u slučaju podataka koje prati digitalni potpis, potpis bi podrazumevano postao nevažeći. Prema tome, digitalno potpisani podaci, koji su šifrovani, ne samo da su sigurni već će i u slučaju da su podaci falsifikovani to otkriti i učvrstiti njihovu koruptivnost.
Kada korisnici podnose transakcije, moraju dokazati svakom čvoru u sistemu da su ovlašćeni da troše ta sredstva, dok sprečavaju i druge korisnike da troše ta sredstva. Svaki čvor u mreži će proveriti uslove poslate transakcije i proveriti rad svih ostalih čvorova kako bi se dogovorili o ispravnom stanju. Ovo se postiže u okviru tri osnovne faze, to su heširanje, potpis i verifikacija.
Faza 1: Pre svega, *blockchain* hešira poruku ili digitalne podatke putem algoritma heširanja. Algoritam pomaže u generisanju heš vrednosti kako bi različine poruke imale

heš vrednosti istih dužina. Kao što već znamo, ovo je osnovna osobina heš funkcije i pokazuje jasan uticaj na digitalne potpise. Heširanje je obavezno u većini *blockchain* aplikacija zbog fleksibilnosti u korišćenju sažetka poruke fiksne dužine.

Faza 2: Sledeći korak u radu digitalnog potpisa u *blockchainu* odnosi se na potpisivanje. Nakon heširanja informacija pošiljalac poruke mora da je potpiše. U ovom trenutku procesa, kriptografija javnog ključa igra ključnu ulogu. Mnogi algoritmi za digitalni potpis nude jedinstvene mehanizme, iako sa jedinstvenim pristupom asimetrične kriptografije. Pošto su digitalni potpisi direktno povezani sa sadržajem svake poruke, digitalno potpisane poruke će imati različite digitalne potpise.

Faza 3: Poslednji korak u korišćenju digitalnog potpisa odnosi se na verifikaciju. Primaoci su lako mogli da provere valjanost digitalnih potpisa upotrebom javnog ključa. Potpis bi mogao funkcionisati kao jedinstveni digitalni otisak date poruke. Međutim, takođe je važno obratiti pažnju na sigurno skladištenje i upravljanje ključevima kako bi se izbegle neželjene okolnosti.

Dakle, ako Alice želi da pošalje jedan *bitcoin* Bobu, mora potpisati transakciju koristeći svoj privatni ključ i poslati ga čvorovima na mreži. Rudari, koji znaju njen javni ključ, zatim će proveriti uslove transakcije i potvrditi autentičnost potpisa. Nakon što se potvrdi valjanost, blok koji sadrži tu transakciju biće spreman za finalizaciju od strane validatora/rudara.

3.3. Šeme potpisa koje se koriste u blockchainu

Šema potpisa koja se trenutno koristi u *bitcoinu* je ECDSA. U poređenju sa RSA, ECDSA koristi kraće ključeve i ima manje računarskih zahteva, a da pritom održava jaku bezbednost. Zamislimo grupu eliptične krive kao konačnu grupu tačaka na krivoj gde je neku operaciju lako izvesti u jednom smeru, ali je teško izvesti u drugom smeru. Osim toga, ECSDA se oslanja na problem diskretnog logaritma umesto na teškoću primarne faktorizacije radi sigurnosti. *Bitcoin* je imao problema sa implementacijom ECDSA u kojoj su identifikatori transakcije mogli biti izmenjeni promenom potpisa transakcije, što je kasnije popravljeno. Implementacija ECDSA takođe može biti sklona raznim drugim napadima.

Uprkos problemima, ECDSA je godinama generalno dobro služio *bitcoinu*. Međutim, ECDSA nema ključno poželjno svojstvo: ne postoji efikasan način za komprimovanje i proveru potpisa zajedno. Poslednjih godina došlo je do pritiska za prelazak na novu šemu potpisa radi poboljšanja skalabilnosti, efikasnosti i privatnosti *bitcoina*: *Schnorr* potpisi.

Svojstvo linearnosti koje poseduju *Schnorrovi* potpisi ima dve prednosti za *bitcoin*. Prvo, linearnost u transakciji sa više potpisa omogućava potpisnicima da kombinuju svoje javne ključeve u jedan agregatni ključ (agregacija ključeva). *Schnorrovi* potpisi omogućavaju da se lista i broj učesnika sakriju objedinjavanjem javnih ključeva i stvaranjem jedinstvenog objedinjenog potpisa koji se ne razlikuje od normalnog potpisa. Ovo svojstvo bi dodatno smanjilo opterećenje blokova i povećalo privatnost omogućavanjem izgradnje pametnog ugovora, tehnike koja čini složene skripte nerazlučivim od normalnih transakcija.

Schnorrovi potpisi dodatno omogućavaju agregaciju unakrsnog unosa. *Bitcoin* transakcije često imaju mnogo ulaza za koje su potrebni pojedinačni potpisi i mogu zauzeti veliku količinu prostora u bloku. Omogućavaju da se pojedinačni potpisi u transakciji objedine i stoga dopuštaju da se svi ulazi u transakciji predstave jednim potpisom. Ova mogućnost kombinovanja potpisa ostavlja više prostora za podatke o transakcijama u blokovima i procenjuje se da će povećati kapacitet za 20-40%.

4. ZAKLJUČAK

Karakteristike šeme digitalnog potpisa imaju kaskadne efekte na funkcionalnost blockchaina. Kao takav, odabir šeme je fundamentalni deo procesa razvoja protokola. Postoje kompromisi i nijedno rešenje neće ostati zlatni standard. Nove optimizacije za poboljšanje upotrebljivosti potpisa se stalno dešavaju kako bi se poboljšala veličina potpisa, vreme verifikacije ili bezbednost. Gore opisane šeme potpisa postoje decenijama i verovatno će biti prisutne u doglednoj budućnosti. Ipak, neizbežno je da će ih na kraju zameniti novije šeme razvijene iz istraživanja koja se danas sprovode.

5. LITERATURA

[1] C. Paar and J. Pelzl, *"Understanding Cryptography"*, Springer, 2010.

[2] W. Stallings, *"Cryptography and Network Security"*, 7th ed., Pearson, 2017.

[3] S. Vaudenay, *"A Classical Introduction to Cryptography"*, Springer, 2006.

[4] https://suredbits.com/introduction-to-schnorr-signatures/

[5] https://bisontrails.co/digital-signatures/

[6] https://101blockchains.com/hashing-and-digital-signature-in-blockchain/

[7] https://www.cryptomathic.com/news-events/blog/how-digital-signatures-and-blockchains-can-work-together

[8] https://www.investopedia.com/terms/b/blockchain.asp

[9] A. Lewis, *"The Basics of Bitcoins and Blockchains"*, Mango Publishing, 2018.

[10] D. Tapscott and A. Tapscott, *"Blockchain Revolution"*, Penguin, 2016.

Kratka biografija:

Ana Mutavdžić rođena je u Šapcu 1997. godine. Osnovne studije na Fakultetu tehničkih nauka, odsek Biomedicinsko inženjerstvo, završila je 2020. godine, a master studije na istom fakultetu, odsek Energetika, elektronika i telekomunikacije, studijski modul Obrada signala, 2021. godine.
kontakt: ana.mutavdzic.97@gmail.com