# BITCOIN

5902

***Rezime:***

*U ovom seminarskom radu reći ću nešto o digitalnom novcu Bitcoin-u, kako je nastao, koje su njegove prednosti i nedostatci i kako doći do svog prvog bitcoina.*

*Bitcoin je oblik digitalnog novca stvoren i čuvan elektronički. Ova valuta nastaje u procesu koji se naziva „rudarenje" (mining). Reći ću šta je to sve što je potrebno da bi i Vi počeli sa „rudarenjem". Prvi Bitcoin pojavio se u januaru 2009. godine, a njegov tvorac je čovjek koji se predstavlja kao Satoshi Nakomato, ali još uvijek njegov identitet i lokacija nisu poznati. U ovom istraživanju zainteresovao me je napredak tehnologije i sve veća upotreba digitalnog novca. Da li Bitcoin ima svoju budućnost i kakve još novosti možemo da očekujemo u budućnosti?*

Kjučne riječi: Bitcoin, Satoši Nakomato, „rudarenje".

## Uvod

Povijest Bitcoina počela je krajem 2008.godine, tačnije 31.oktobra na internetu se pojavljuje dokument „Bitcoin: A Peer-to-Peer Electronic Cosh System". Dokument je sastavljen od osam strana, na kojima se potpuno opisuje jedna nova vrsta novca. [1] Autor tog članka se predstavlja kao Satoshi Nakomato, čiji identitet još uvijek nije poznat. Neki čak smatraju da se iza imena Satoshi Nakomato krije određena grupa ljudi.

Prve jedinice Bitcoina puštene su u promet u januaru 2009. godine. Njegova vrijednost bila je 0,002 centa. U prvih 16 mjeseci nije imao velikog napretka, vrijednost mu se nije značajno promjenila. Sva aktivnost se svodila na međusobno razmjenjivanje Bitcoina među malim brojem korisnika. 22.maja.2010 godine obavljena je prva kupovina Bitcoinom. Tog dana je programer gospodin Loso za dvije pizze platio 10.000 Bitcoina. Od tada Bitcoin zajednica 22.maj slavi kao „Bitcoin pizza dan". Do kraja 2009. godine stvoreno je preko milion i po Bitcoina, i kako je te godine samo četvrtina njih promjenila vlasnika procjenjuje se da bi Satoshi mogao imati oko milion Bitciona. Početkom 2011. godine on prestaje da radi na ovom projektu.

Danas se u svijetu više od osam miliona ljudi služi ovom digitalnom valutom.

Bitcoin nastaje u procesu koji se naziva „rudarenje". Ovo „rudarenje" se izvodi na standardnim računarima ili specijalizovanom hardveru, i to tako što ti računari i specijalizovani hardveri rješavaju kompleksnu seriju matematičhik algoritama. Efikasnost i brzina „rudarenja" zavise od akumulirane snage računarskog sistema, odnosno od brzine rješavanja algoritama. To je automatski proces koji računar obavlja kontinualno, najbolje da radi 24 sata 7 dana u sedmici. „Rudarenjem" se može baviti svako, bez obzira ma mjesto i državljanstvo.

Najznačajnija karakteristika Bitcoina i ujedno njegova najveća razlika od ostalih valuta jest što je decentralizovan. Ova valuta nema zemlju porijekla, iza nje ne stoji nijedna država niti bankarska organizacija. [2]

## Bitcoin

Bitcoin je oblik digitalne valute, kreiran i čuvan elektronski. BTC je kriptografska valuta iza koje ne stoji ni jedna institucija i ni jedan pojedinac. Bitcoin ima svoje karakteristike po kojima se razlikuje od ostalih valuta. Najznačajnija karakteristika Bitcoina i ujedno njegova najveća razlika od ostalih valuta je ta što je decentralizovan. To znači da Bitcoin mrežu ne kontrolira nijedna vlast ili država. On je prva valuta izgrađena na decentraliziran način. Bitcoin je anoniman,  tačnije on je pseudo – anoniman. Korisnik može posjedovati više Bitcoin adresa i one nisu povezane sa ličnim podatcima. Moramo znati da Bitcoin mreža pohranjuje sve podatke o svakoj transakciji koja se dogodila unutar mreže. Ako posjedujete adresu svako može vidjeti koliko je Bitcoinova pohranjeno na njoj, ali niko ne zna kome oni pripadaju. Otvaranje Bitcoin računa je jednostavno. U tradicionalnim bankama otvaranje računa podrazumijeva mnogo papirologije. Za Bitcoin račun (adresu) potrebno je nekoliko minuta, još sve bez troškova i dodatnik pitanja. Napomenimo još jednu bitnu karakteristiku a to je brzina Bitcoin mreže. Ova mreža je jako brza pa mi novac možemo slati bilo gdje, i on će stići nekoliko minuta kasnije, ćim Bitcoin mreža procesira plaćanje. [3]

## Rudarenje bitcoina

Slika 1. Izgled digitalne valute Bitcoin [4]

Digitalnim putem uz pomoć računara u procesu koji se naziva mining odnosno „rudarenje“ stvara se Bitcoin. Ovaj način izrade podrazumijeva korištenje kriptografskih algoritama. Da bi razumjeli sam proces „rudarenja“ mi moramo znati šta je to kriptografija i šta su kriptografski algoritmi. Naučna disciplina koja se bavi analiziranjem i pronalaženjem metoda pomoću kojih je poruku moguće poslati u obliku u kojem je neće moći pročitati niko osim osobe kojoj je poslana naziva se kriptografija. Osnovni zadatak kriptografije je da u nesigurnom

komunikacijskom kanalu omogući komunikaciju između dvije osobe na taj način da treća osoba koja može nadzirati komunikacijski kanal ne može razumjeti njihove poruke. Kriptografiju kraće možemo definisati kao znanost šifriranja podataka. Poruku koju pošiljatelj želi poslati nekoj drugoj osobi zovemo otvoreni tekst. Pošiljatelj koristeći već unaprijed dogvoreni ključ ulazne podatke tj.otvoreni tekst pretvara u šifrirani izlaz (šifrat). Nakon šifriranja šifrt se šalje preko nekog komunikacijskog kanala drugoj osobi. Treća osoba može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Samo osoba koja zna ključ kojim je šifrirana poruka može dešifrovati šifrat i odrediti otvoreni tekst. [5]

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Radi se o dvije funkcije koje preslikavaju elemente otvorenog teksta u elemente šifrata i obrnuto.

Sada kada znamo šta su to kriptografski algoritmi koji se koriste za stvaranje Bitcoina, možemo reći šta je sve potrebno za proces „rudarenja“.

Slika 2. „Rudarenje“ Bitcoina [6]

Da bi počeli sa „rudarenje“ prvo moramo investirati u odgovarajuću opremu, jer u ovom postupku mi trošimo snagu svog računara kako bi on radio na algoritmu i pri tom „kopao“ Bitcione. Klasičan računar nije dovoljan za uspješno „rudarenje“, on se može koristiti ali ako i šta zaradimo napravit ćemo sebi veći trošak za električnu energiju. Dok „rudarite“, na svom klasičnom računaru nećete moći raditi ništa drugo. U ovom procesu brzina procesora ne igra nikakvu ulogu. Bez obzira da li imate najnoviji ili neki stari procesor razliku nećete ni vidjeti.

Efikasnost tzv.hash rate može se povečati dobrom grafičkom karticom. Hash rate je broj obračuna koje naša oprema može izvesti svake sekunde dok pokušava da riješi matematičke probleme. [7]. Brzina obrade se izražava u hashevima po sekundi (h/s), mada se češće koriste mjere Mh/s ili Gh/s. GPU-u su projektovani za rješavanje matematičkih problema pa se one mogu iskoristiti za ovaj proces. Jedna bolja grafička karta je 80 puta efikasnija od procesora.[8]

Sklapanje mašine koja će uz pomoć „rajzera“ omogućiti da se na ploču prikači 4 ili 5 grafički karti, zajedno sa odgovarajućom pločom i procesorom, 8 GB RAM-a i kvalitetno napajanje koštat će nas oko 1600 eura. Takva mašina može se isplatiti već nakon nekoliko mjeseci. Budući da vlada veliko interesovanje za „rudarenje“ Bitciona došlo je do nestašice grafičkih karti. To je navelo i proizvođaće da počnu sa proizvodnjom grafičkih karti namjenjenih samo za „rudarenje“. Prva takva kartica je MINING P106-6G, koju je predstavio ASUS. Da je namjenjena samo za „rudarenje“ vidi se iz tog što nema video izlaze i potrošnja je optimizirana. Napredniji način „rudarenja“ koji donosi veću zaradu podrazumijeva upotrebu FPGA (Filed Programmable Gate Array) opreme. Jedan FPGA čip je 10 puta efikasniji od GPU-a i samim time brzina „rudarenja“ je 10 puta brža.

Pored sve navedene opreme sada na tržištu postoje ASIC (eng.“Application Specific Integrated Circuit) specijalizovani uređaji namjenjeni samo za „rudarenje“. Ovaj posao obavljaju 10 do 100 puta brže od FPGA opreme. [9]. Pojavom ACIS specijalizovanog hardwera regularni računari i komponente su potpuno potisnute iz Bitcoin trke. Naprimjer grafička karta visokih perfomansi može ostvariti do 1 Gh/s dok pojedini ASIC hardweri idu do 1000 Gh/s, pri tom trošeći manje struje nego GPU. Trenuta cijena ASIC uređaja je previsoka.

Ukoliko imamo svu potrebnu opremu i spremni smo na strpljenje koje „rudarenje“ traži ovo su koraci koje trebamo poduzeti:

- Instalirati digitalni novčanik
- Pridružiti se pulu
  Pulovi su mreže računara koje su uvezane sa ciljem zajedničkog „rudarenja“ kako bi se što prije matematičke operacije pretvorile u novac. Najcjenjeniji pul je Sluhs's Pool. Mada mi možemo „rudariti“ i sami, i u tom slučaju nagradu ne djelimo sa drugima ali vjerovatnoća da dobijemo nagradu se smnanjuje.
- Instalirati Bitcion „rudara“ na svoj računar.
  U pitanju je softwer koji rješava pomenute matematičke operacije kako bi došao do svojih Bitcoina.
- Ulogovati se u svoj nalog na pulu i unijeti adresu svog novčanika
- Registrirati svoje „radnike“
  Radnici su softweri koji prate rad naših „rudara“ i prijavljuje nam kako napreduje „rudarenje“ i da li je negdje došlo d problema.
- Unesite podatke o svom „radniku“ u softwer za „rudarenje“, zatim unesite URL adresu svog pula i „rudarenje“ može početi. [10]

Digialni novčanik

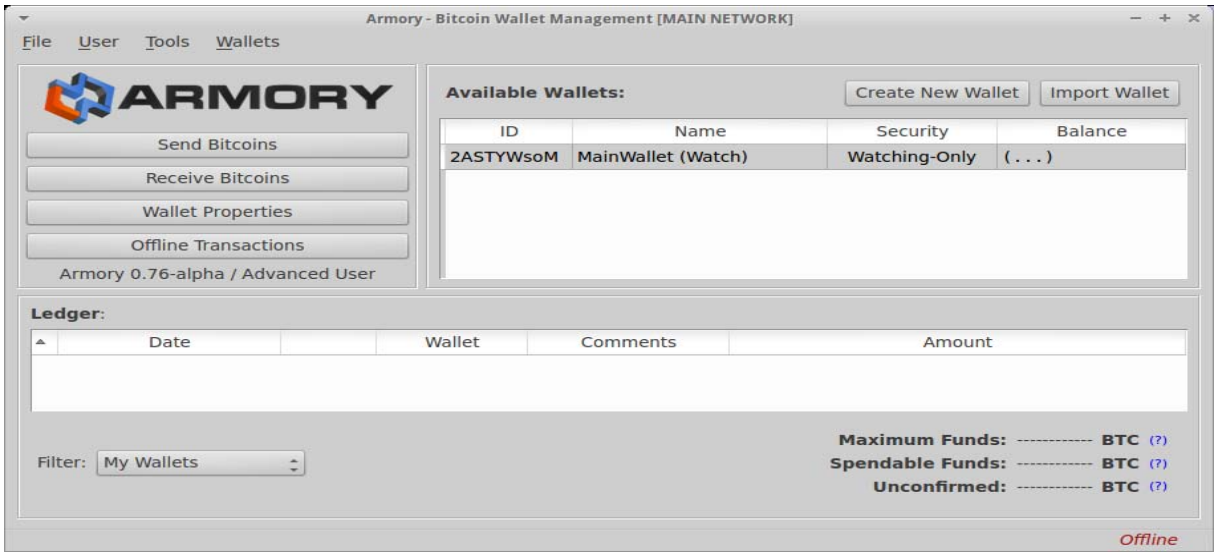
Digitalni novčanik je program koji služi za slanje, primanje i skladištenje Bitcoina, on sadrži korisnikove adrese, tajne ključeve te prikazuju količinu Bitcoina koje korisnik posjeduje i sve tansakcije koje je obavio. Transakcija je zapis u Bitcoin mreži kojim se određeni iznos Bitcoina prenosi sa jedne adrese na drugu. Bitcoin adresa se genriše nasumično, i to je jednostavan niz slova i brojeva, a privatni ključ je dugi niz slova i brojeva, i on je tajan za raliku od adrese. Najvažnija funkcija novčanika je čuvanje korisničkog tajnog ključa. Novčanik je moguće instalirati na mobitel, računar i tablet. Najpopularnija platforma za novčanike je CoinBase.

Prema službenoj stranici Bitcoina iza koje stoji Bitcoin organizacija postoje 4 tipa Bitcoin novčanika:

- mobile
- desktop
- hardwere
- web

Na smartphone instalira se mobil, a na računare desktop novčanik. Web novčanik se nalazi na serverima te mu se pristupa preko internet preglednika. Specifična vrsta su hardwere novčanici. Oni su posebno pravljeni za skladištenje i osiguravanje valuta. Ovi uređaji se mogu povezat sa internetom da bi se obavljale transakcije, a onda se može raskačiti sa mreže zbog sigurnosti. Preporučljivo je da se Bitcoin novčanik smjesti van mreže, jer su web stranice često meta napadačima.

Tajni ključ koji se čuva u novčaniku je najvažniji element u cijelom Bitcoin konceptu. Gubitkom privatnog ključa korisniku je onemogućen pristup, zbog toga se preporučuje šifriranje ključeva. Na taj način prije korištenja tajnog ključa mora se unjeti lozinka za dešifrovanje što otežava posao napadačima. Ipak najbolje rješenje za čuvanje tajnog ključa je da se on pohrani na neki digitalni medij koji nema pristupa internetu ili jednostavno da ključ ispišemo na papira i sačuvamo. [11]




Slika 3. Izgled desktop novčanika[12]


Slika 3. Izgled mobile novčanik [13]

## Kako funksioniše „rudarenje“?

Ljudi jedni drugima Bitcoine šalju širom Bitcoin mreže, ali ako niko ne vodi evidenciju o tim transakcijama, niko ne bi mogao da prati ko je šta platio. Zato Bitcoin mreža vodi evidenciju i to na sljedeći način, u listu se spremaju sve obavljene transakcije tokom određenog perioda. Ta lista se naziva blok. Na rudarima je da potvrde te transakcije i da ih upišu u glavni registar transakija. Registar transakcija je duga lista blokova, poznata kako blockchain. Kad god se novi blok transakcija napravi dodaje se u blockchain praveći tako sve dužu listu transakcija koje se odigraju na Bitcoin mreži. Transakcije su javne, transparentne i pseudoanonimne. Historija transakcija može se pratiti unazad od trenutka kada je Bitcoin proizveden. Da bi svi učesnici znali šta se dešava data im je ažurirana kopija bloka.

Kada se blok transakcija kreira rudari ga procesiraju. Uzimaju informaciju iz bloka, primjenjuju matematičke formule i pretvaraju u nešto drugo mnogo kraće, naizgled nasumična sekvenca brojeva i slova poznata kao hash. Hash se čuva zajedno sa blokom na kraju blok lanca. Hash ima interesantna svojstva. Lahko se proizvodi iz informacija bloka, ali kada vidimo hash, nemoće je vidjeti koje su to informacije bile prije obrade. On je unikatan. U slućaju da u bloku promijenimo bar jedan karakter njegov hash će biti potpuno drugačiji. Rudari ne koriste samo transakcijski blok kako bi generisali hash, već kosriste i hash zadnjeg bloka pohranjenog u lancu blokova. Zbog toga što je hash svakog bloka napravljen pomoću

hasha predhodnog, taj blok postaje digitalni oblik pečata. On potvrđuje da je taj blok, i svaki blok poslije njeg legitiman i ukoliko biste ga dirali svi bi to znali. Svi rudari su jedni drugima konkurencija. Kada god neko proizvede hash dobije 12.5 Bitcoina, blockchain se ažurira i svi u mreži znaju za to.[14]

Algoritam garantuje da će biti samo 21 milion Bitcoina, i da će se svi „iskopati“ do 2014. godine. Budući da je u posljednje vrijeme „rudarenje“ postalo ne isplativo, jer je hardwer koji je potreban veoma skup, a potrošnja struje prevelika mnogi se odlučuju da nabave svoj prvi Bitcoin na drugi način.

## Načini kako da nabavite svoj prvi Bitcoin

- Kupiti Bitcoin od online trgovca
  Stranice kako što su Coinbase dopušaju da se kupe Bitcoini vašom lokalnom valutom. Samo se morate registrirati i potvrditi vaš bankovni račun i odmah možete početi sa kupovinom. Ovo je najlakši način nabavljanja Bitcoina.

- Kupovina od lokalnog trgovca
  Ako baš ne volite svoje finansijske podatke davati online servisu, uvjek možete koristi web mjesta kao što je LocalBitcoins gdje možete naći osobu od koje će te kupiti Bitcoin za gotovinu.

- Pronađie bitcoin bankomat
  Ovdje se radi o dvosmjernom bankomatu kanadske kompanije Bitaccess. Dvosmjerni bankomat znači da osim što je moguće kupovati Bitcoine za svoju valutu (npr.kuna, euro), moguće je i prodavati Bitcione za valute.

- Kupite hardwer koji će za vas rudariti
  Ako se ne želite baviti održavanjem „rudarenja“ i bukom hardwera prilokom vlastitog rudarenja, uvijek računarsku snagu za sudjelovanje u „rudarenju“ možete kupiti online u rudarstvu poput Genesis rudarstva.

- Bitcoin „slavine“
  Ako ste spremni izdvojiti dosta vremena onda je ovo idealno za vas. Ovdje se radi o tome da određene tvrtke plaćaju Bitcoinima da vi radite određene stvari kao što su na primjer gledanje oglasa, ankete, posjete web stranica i još mnogo toga.

- Djelite savjete
  Changetip korisnicima omogućuje da daju savjete ljudima na društvenim mrežama i za uzvrat one najbolje i najažurnije plaćaju Bitcoinima. Trenutno možete savjetovati na Twitteru, Google+, Facebooku.

- Prodaja stvari za bitcoine
  Crypto Thrift omogućuje podaju za Bitcoine, funkcionira kao Ebay. Možete i prodavati i kupovati.

- Oglašavajte svoju  bitcoin adresu
  Bitcoin zajednica ima brojne priče o ljudima koji su puno novca zaradili tako što su svoje Bitcoin adrese stavljali na neka vidljiva mjesta. Student je na sportskom

događaju svog fakulteta  mahanjem transparenta na kome se nalazila njegova Bitcoin adresa zaradio 24.000$. Zanimljiv i lagan način. [15]

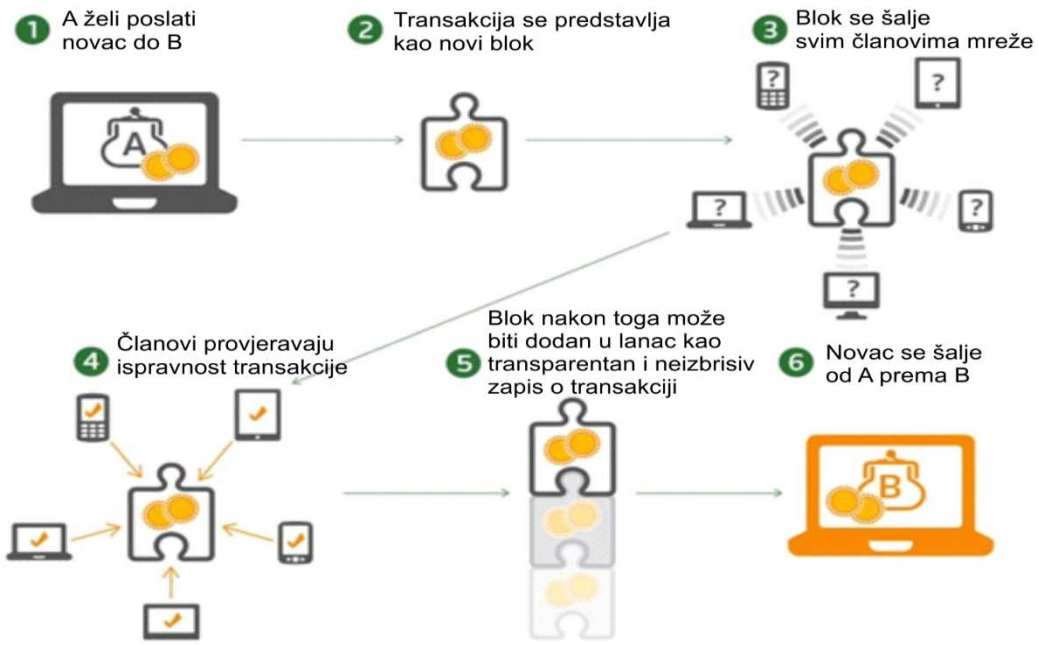
## Upotreba Bintcoina

Bitcoin se najčešće upotrebljava za:

- Kupovina
  Plaćanje Bitcoinima je jednostavno, sigurno i brzo pa je sve veći broj trgovaca koji prihvaćaju ovu metodu plaćanja. Prihvaćenost Bitcoina iz dana u dan raste. Postoje sajtovi koji nude razne proizvode od namještaja, do elektronike i omogućuju plaćamje u Bitcoinima. Napomenimo još da u svijetu postoje brojna mjesta na kojima je usluge moguće platiti Bitcoinima. Pa tako ako ste u Beogradu, svoje bitcoine možete potrošiti u restoranu Appettite. [16]


Slika 5. Izgled prvog Bitcoin bankomata u Beogradu[17]

- Slanje novca
  Za slanje novca na daljinu najčešće koristimo bankovne transfere, poštanske uplatnice, Western Union ili PayPal. Svaka od ovih metoda ima svojih prednosti ili mana, no svima im je zajedničko da: traju neko vrijeme (od dana do tjedan dana) i koštaju. Ako želimo nekom poslat novac Bitcoin mrežom potrebno je učiniti sljedeće:
  pošiljatelj valutu (npr. kunu, euro) promjeni u Bitcoin, zatim pošalje Bitcoin i na karaju primtelj Bitcoine zamjeni u drugu valutu. Kao što vidimo, slanje novaca koristeći Bitcoin mrežu je brže, jefitnije i jednostavnije nego klasičnim metodama.[18]




Slika 6. Ilustracija slanja novca Bitcoin mrežom [19]

## Zaključak

Bitcoin je prvi primjer kripto valute, prvi put pojavljuje se 2009. godine. Tvorac ove kriptografske valute je čovjek koji se predstavlja kao Satochi Nakomato. Od tada pa do danas Bitcoin bilježi svoj veliki napredak. Postoji više načina kojima možemo doći do svog prvog Bitcoina. Lakši od načina je kupovina Bitcoina od online trgovca ili mijenjanje valauta u Bitcoine na posebnim bankomatima. Teži način je „rudarenje“ gdje mi trošeći snagu svog računara „kopamo“ svoje Bitcoine. Danas u svijetu veliki broj ljudi bavi se „rudarenjem“, Bitcoin mreža broji više od 8 milijona korisnika.

## Literatura


[1] https://bitcoin.org/bitcoin.pdf (dostupno 1.12.2017)

[2] http://digre.pmf.unizg.hr/4370/1/diplomski_franciskovic.pdf(dostupno 1.12.2017)

[3] https://crobitcoin.com/15-nacina-kako-da-dodete-do-svog-prvog-bitcoina/(dostupno 7.12.2017)

https://lopp.net/pdf/princeton_bitcoin_book.pdf(dostupno 7.12.2017)

[4]https://www.google.ba/search?q=slika+bitcoin&rlz=1C1GGRV_enBA752BA752&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjPxfaqpITYAhUJalAKHYHlCo0Q_AUICigB&biw=1366&bih=613#imgrc=bZX-q1aDr-prVM: (dostupno 10.12.2017)

[5] http://digre.pmf.unizg.hr/4370/1/diplomski_franciskovic.pdf(dostupno 10.12.2017)

[6] http://blog.mtel.ba/kako-se-rudari-bitcoin/(dostupno 8.12.2017)

[7]http://kako-zaraditi-bitcoin.nr.rs/sve-o-bitcoinu/sve-sto-ste-zeleli-da-znate-o-bitcoinu-pitanja-i-odgovori/(dostupno 11.12.2017)

[8] http://kako-zaraditi-bitcoin.nr.rs/sve-o-bitcoinu/sve-sto-ste-zeleli-da-znate-o-bitcoinu-pitanja-i-odgovori/(dostupno 11.12.2017)

[9] https://pcpress.rs/sve-sto-bi-trebalo-da-znate-o-trgovini-kriptovalutama/(dostupno 11.12.2017)

[10] http://blog.mtel.ba/kako-se-rudari-bitcoin/(dostupno 11.12.2017)

[11] http://digre.pmf.unizg.hr/4370/1/diplomski_franciskovic.pdf(dostupno 11.12.2017)

[12] https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/(dostupno 11.12.2017)

[13] https://crobitcoin.com/kako-poceti-bitcoin/bitcoin-novcanici-wallets/(dostupno 11.12.2017)

[14] https://ecd.rs/pages/dgs?r=V001 (dostupno 11.12.2017)

[14] https://crobitcoin.com/(dostupno 11.12.2017)

[15] https://crobitcoin.com/bitcoin/kako-kupiti-bitcoin/(dostupno 11.12.2017)

[16] http://stojebitcoin.com/cemu-sluzi/(dostupno 11.12.2017)

[17] http://www.novosti.rs/vesti/naslovna/tehnologije/aktuelno.236.html:672910-U-Beogradu-poceo-sa-radom-prvi-dvosmerni-Bitkoin-bankomat(dostupno 11.12.2017)

[18] http://stojebitcoin.com/cemu-sluzi/(dostupno 11.12.2017)

[19]https://www.google.ba/search?q=bitcoin+slanje+novca+slika&rlz=1C1GGRV_enBA752BA752&biw=1366&bih=613&tbm=isch&source=iu&ictx=1&fir=vhHZBANBaCsNfM%253A%252CMA6ZWg04pkoDJM%252C_&usg=__BzIYmMVmB2Pe735kULMO8DkWDfc%3D&sa=X&ved=0ahUKEwjsytHrrITYAhXHKFAKHR6CBo8Q9QEIMDAC#imgrc=vhHZBANBaCsNfM: (dostupno 11.12.2017)