Tehnologija iza kriptovaluta

Švigač, Matea

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2018./ 2019.

Matea Švigač

Tehnologija iza kriptovaluta

Završni rad

Mentorica: dr. sc. Vjera Lopina

Zagreb, srpanj 2019.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Zahvaljujem svojoj mentorici dr. sc. Vjeri Lopini na strpljivosti i susretljivosti koju mi je pružila tijekom izrade ovog završnog rada, kao i polaganja ispita iz kolegija Zaštita podataka i Kriptologija. Također se zahvaljujem i svim ostalim profesorima s Odsjeka za informacijske i komunikacijske znanosti, Filozofskog fakulteta u Zagrebu, koje sam imala priliku slušati, a koji su mi izašli u susret u polaganju kolegija s kojima sam zaostala tijekom akademske godine 2017./18. zbog bolesti.

Sadržaj

Sadržaj iv
1. Uvod 1
2. Sociološki aspekti razvoja Blockchain tehnologije 2
2.1. Globalizacija 2
2.2. Moderne institucije 3
2.2.1. (Re)produkcija strukture Blockchain tehnologije 4
3. Kriptografija 6
3.1. Distribuirani sustav 7
4. Blockchain tehnologija 8
4.1. Asimetrična kriptografija 9
4.1.1. Privatni ključ 12
4.1.2. Javni ključ 13
4.1.3. Multiplikacija eliptične krivulje 13
4.1.4. Bitcoin adresa 13
5. Rudarenje 15
5.1. Dokaz rada 16
5.2. Dokaz o udjelu 18
5.2.1. Usporedba dokaza rada i dokaza o udjelu 19
6. Novčanik 20
6.1. Adresa u obliku niza znakova 20
6.2. Adresa u obliku QR koda 21
7. Eko-sistem kriptovaluta 22
7.1.1. Namecoin 22
7.1.2. Litecoin 23
7.1.3. Peercoin 23

7.1.4. Dogecoin 24
7.1.5. QuadrigaCX 25
8. Zaključak 26
9. Literatura 27
Popis oznaka i kratica 29
Popis tablica 30
Popis ilustracija 31
Popis dijagrama 31
Popis grafikona 31
Popis slika 31
Sažetak 32
Summary 33

1. Uvod

Kriptovalute (eng. *cryptocurrencies*) potpuno su nov pojam i koncept koji nastoji promijeniti dosadašnje doživljavanje financijskih sistema i općenit pogled na novac. Može se reći da je njihova pojava jedna od ključnih značajki globalizacije u 21. stoljeću. Globalizacija sa sobom nosi velike prednosti, ali s druge strane i velike mane. Krucijalna posljedica globalizacije, koja je dovela do razvijanja tehnologije koja bi podržavala ideju kriptovaluta, je upravo jaz između institucija s jedne strane te individue s druge strane.

Počinje se buditi refleksivna svijest ljudi koja uviđa negativne strane funkcioniranja odnosa banaka i korisnika (i u nekim slučajevima medija između). Posljedično, razvila se ideja o stvaranju takvog sustava koji bi imao sposobnost povezivati strance na globalnoj razini, a ujedno i (re)producirati povjerenje. Navedeno je zapravo bila i fundamentalna ideja iza banaka, kao financijskih institucija koje osiguravaju ljudima određene funkcionalnosti (npr. transakcije) te im garantira njihovu anonimnost koja će izgraditi povjerenje između svih njenih korisnika. No, financijske institucije počele su zakazivati u tom pogledu, a neki od najvećih problema su njihova sporost, cijena te ranjivost na moguće napade izvana.

Blockchain tehnologija (hrv. *lanac blokova*) nadilazi sve te probleme, a načini na koji to postiže bit će predstavljeni u nadolazećim poglavljima. Za sada je bitno shvatiti samu srž ideje iza tehnologije kriptovaluta, a to je da korisnici mreže sami kreiraju njenu strukturu rudarenjem (eng. *mining*), odnosno provedbom transakcija (njihovim potvrđivanjem i dodavanjem). Jednom kada se mreža kreira, ona ne ostaje nepromjenjiva, nego podliježe konstantnim promjenama koje ovise o aktivnosti korisnika na mreži (npr. aktivnost rudarenja nagrađuje korisnika nagradom od 12,5 bitcoina, ali smanjuje broj ukupno dostupnih bitcoina za rudarenje). Te se nove aktivnosti zatim dodaju u „glavnu knjigu“ (eng. *ledger*), a koja je zapravo lanac blokova, odnosno Blockchain tehnologija. Primjer toga je vrijednost određene kriptovalute, npr. Bitcoina, koja doživljava fluktuacije između njegovog pada i rasta. Ovaj zavisan proces između akcije (eng. *action; agency*) korisnika i strukture (eng. *structure*) mreže kriptovaluta najbolje se objašnjava teorijom strukturacije (eng. *structuration theory*) sociologa Anthony Giddensa.

2. Sociološki aspekti razvoja Blockchain tehnologije

Živimo u svijetu transformacija koje utječu na svaki aspekt onoga što činimo, stoga našu današnjicu najbolje opisuju brzina promjena te poteškoće koje dolaze vezano uz kontrolu i kretanje tih promjena. Neki od najvažnijih sociooloških aspekata koji stoje iza ideje i razvoja Blockchain tehnologije su proces globalizacije te rastući problem nepovjerenja u moderne društvene institucije. Izumitelji Blockchain tehnologije smatraju da bankovni sistem nikako ne uspjeva držati korak sa stalnim društvenim promjenama. Svi pokrenuti procesi koje korisnik zatraži (npr. transakcija) rezultiraju s nekoliko dana čekanja kako bi se transakcija provela, što zbog birokratskih problema oko papirologije, što zbog nedovoljno razvijene tehnološke strukture.

2.1. Globalizacija

Iako globalizacija sa sobom nosi mnogo prednosti i potencijala za razvoj modernog društva, globalizacija iza sebe ostavlja i neke negativne posljedice po moderno društvo. Giddens (2003) smatra da su posljedice globalizacije proizašle iz problema vezanih uz povjerenje (kako vjerovati u svijet, odnosno institucije), znanje (kako uskladiti naša znanja i vjerovanja koja imamo sa kontinuirano promjenjivim svijetom), anksioznost (kako braniti ono što osjećamo) te moral (kako najbolje upravljati sobom u svijetu). Najvažniji aspekt razvijanja Blockchain tehnologije i mreže korisnika kriptovaluta je upravo radikalno rastući problem (ne)povjerenja u moderne institucije, konkretnije u bankovni, financijski sustav.

Za Giddensa (2003) globalizacija ima veze s tezom da svi živimo u jednome svijetu. Ona je revolucionarna, jer obuhvaća političku, tehnološku, kulturnu i ekonomsku sferu života svih nas, a na njen razvoj je utjecalo niz izuma vezanih za informacijske i komunikacijske sisteme koji datiraju od kasnijih 60-ih godina 20. st.

Bilo bi krivo misliti da globalizacija utječe samo na velike sisteme unutar društva. Ona ne predstavlja nešto izvanjsko što ne dotiče individuu, već je ujedno i „unutarnji“ fenomen koji izravno utječe na intimne i osobne aspekte individue. Prema Giddensu (2003), globalizacija kreira nove ekonomske i kulturne zone unutar i izvan pojedinih nacija, stoga ona nije potpuno „benigna“ u svojim posljedicama.

Globalizacija kreira svijet pobjednika i gubitnika – onih koji su na putu blagostanja i prosperiteta, te onih koji su na putu mizerije i očaja. Živimo u svijetu u kojem globalizacija „trese“ i zadire u svaku postojeću sferu našega života, bez obzira gdje se nalazili. Takvo stanje društva nije sređeno niti sigurno, već prepuno anksioznih stanja i strahova od dubokih razdvojenosti. Mnogi posjeduju neobjašnjivi osjećaj da su pod utjecajem sila nad kojima nemaju kontrole niti moći.

2.2. Moderne institucije

Pitanje moderniteta se ponovno pojavilo kao fundamentalni sociološki problem 21. stoljeća. Moderne institucije razlikuju se od njihovih prijašnjih formi društvenog poretka po pitanju njihove dinamičnosti – stupanj u kojem su „srezale“ tradicionalne navike i običaje te njihov globalni utjecaj. Modernost radikalno utječe na prirodu našeg svakodnevnog života i utječe na većinu osobnih aspekata naših svakodnevnih iskustava. Ona direktno utječe na naš individualni život (eng. *individual life*) i na našu ličnost (eng. *self*). Jedna od distinktivnih značajki modernosti je rastuća povezanost dva ekstrema: ekstenzionalnosti (eng. *extensionality*) i intencionalnosti (eng. *intentionality*) – globalnih utjecaja s jedne strane i osobnih dispozicija s druge strane.

Moderni društveni život, osim institucionalne refleksivnosti, karakteriziraju i procesi reorganizacije vremena i prostora, koji se ponašaju tako da transformiraju sadržaj i prirodu svakodnevnog društvenog života. Blockchain tehnologija ima sposobnost transformiranja sadržaja prema prirodi svakodnevnog društvenog života, jer funkcionira na refleksivnosti relacije korisnik – mreža (drugi korisnici), a što je veliki nedostatak bankovnog sustava kao medija između dva ili više korisnika.

Modernost proizvodi različitosti, izdvojenosti i marginalizaciju. Iako zadržavaju mogućnost emancipacije, moderne institucije istovremeno proizvode mehanizme supresije, umjesto aktualizacije ličnosti. To je zapravo paradoksalno, jer bi modernost trebala otvoriti mnoge puteve samoaktualizacije pojedinca, sa svim pravima i slobodama koje sa sobom donosi, ali to ne čini. Primjer još jednog nedostatka banaka je njihova nedostupnost u siromašnijim zemljama (npr. većina afričkih i siromašnijih azijskih zemalja). Blockchain tehnologija

nadilazi i taj problem, jer na bazičnoj razini, dostupna je svima koji posjeduju osobno računalo.

2.2.1. (Re)produkcija strukture Blockchain tehnologije

Giddens (2003) smatra kako društvene institucije prakticiraju radnje koje su postale rutinizirane, a koje ponavlja većina agenata kroz vrijeme i prostor (npr. rudarenje). Prema tome, društvene institucije proizlaze iz činjenice da jedno te isti ljudi ponavljaju stalno jedno te iste radnje. Socijalna struktura nastaje na sličan način, odnosno proizlazi iz već učinjenih akcija agenata, a koja struktura omogućava ili ograničava buduće akcije mogućim (npr. nakon izrudarenog jednog bloka transakcija, ograničava se druge rudare na način da im se smanjuje dostupan broj bitcoina), što predstavlja dualnost strukture (eng. *the duality of structure*).

No, treba se naglasiti kako struktura nije odvojena od akcije. Struktura ne reproducira samu sebe, u pitanju su uvijek agenti i njihove akcije koji reproduciraju strukturu iznova. Na konkretnom slučaju Blockchain tehnologije, korisnici svojom aktivnošću na mreži formiraju vrijednost kriptovalute, ovisno o njenoj potražnji, a ujedno što su korisnici aktivniji, to produciraju veće povjerenje kod ostalih korisnika.

Osim toga, ta mreža je vrlo transparentna te omogućava djelovanje na ravnopravnoj bazi (eng. *peer-to-peer*). Npr. ako korisnik *E* želi poslati 200 kuna korisniku *F*, on neće morati prvo zadati nalog banci da umanji stanje računa za zadani iznos. Jednostavno će zatražiti od mreže da provede transakciju za iznos *a*. Ta transakcija će biti enkriptirana u elektronički zapis tako da izgleda kao nasumičan niz slova i brojeva, npr. *FF26BO228abZ4,* ali je zapravo kodirana po zadanom ključu te u sebi sastoji podatke o pošiljatelju *E,* iznosu *a* koji se šalje te primatelju *F*. Obzirom da se radi o elektroničkom zapisu, tj. signalu, računala u blizini potvrdit će da stanje računa odgovara u potpunosti (ili za veći iznos) zatraženom iznosu te će omogućiti izvršenje transakcije, a što je najbitnije bez provizije, što u većini banaka neće biti slučaj. Iako se čini da izvršenja transakcije putem Blockchain tehnologije ima nekoliko koraka, što nas navodi na zaključak da taj proces potraje, zapravo se radi o svega nekoliko sekundi. Osim toga, korisnik *E* će u svakoj fazi transakcije imati uvid u to što se događa te u trenutak kada je transakcija konačno završena.

Banke još uvijek rješavaju takve zadatke na vrlo birokratski način te predstavljaju posrednika između korisnika *E* i korisnika *F*. S bankovnog stajališta, korisnik *E* prvo mora zadati nalog za izvršenje transakcije, a nakon zadavanja naloga za prijenos iznosa *a* sa računa broj *e* na račun broj *f*, banka kao medij mora proći nekoliko koraka.

Prvi korak bio bi provjeriti da li je račun broj *e* validan te ako je da li ima dovoljan iznos sredstava kako bi se stanje umanjilo za zadani iznos *a*. Ako posjeduje dovoljan iznos sredstava, drugi korak bio bi kontaktiranje banke korisničkog računa broj *f* kako bi se utvrdilo da li je račun valjan i otvoren za primanje sredstava. Jednom kada banka korisnika *f* potvrdi dostupnost za uplate, stanja računa se ažuriraju na način da se račun broj *e* umanji za 200 kuna, a stanje računa broj *f* uveća za 200 kuna.

Ovaj proces uobičajeno potraje minimalno jedan dan, a pri čemu korisnik nema informaciju o tome što se događa nakon zadavanja naloga.

3. Kriptografija

Kriptologija (grč. *cryptos;* grč. *logos*) je, kao što joj i sam naziv govori, znanost o tajnom sporazumijevanju. Dijeli se na dvije grane: kriptografiju (hrv. *kritopis*) te kriptoanalizu (hrv. *kritorazglob*).

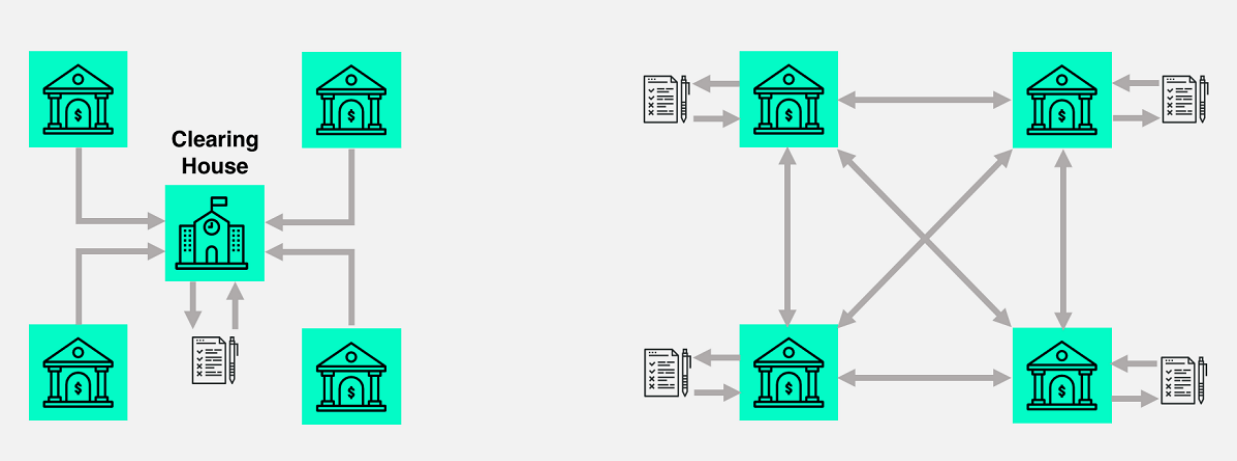
Naziv kriptografija dolazi od grčkih riječi *kripto* (hrv. *tajno*) i *grafein* (hrv. *pisati*) što bi u prijevodu značilo „*tajno pisanje*“. Njen zadatak je oblikovanje kritopisnih sustava, odnosno priprema metoda kojima će se zakriti jasnopis (poruka u originalnom obliku), a koja metoda je poznata samo osobi koja posjeduje ključ za zakrivanje. Prema Krešimiru Bagiću (2018), kriptografija istodobno označava znanstvenu disciplinu koja proučava tehnike šifriranja i slanja tajnih poruka te samo umijeće šifriranja. Ona je odvojena grana matematike koja se znatno koristi u očuvanju računalne sigurnosti, a temelji se na tajnom pisanju, odnosno enkripciji. Osim toga, može se koristiti i za utvrđivanje autentičnosti podataka (eng. *digital fingerprint*). Druga grana kriptologije je kriptoanaliza koja se bavi otkrivanjem metoda koje stoje iza kritopisnih sustava. Kriptoanalitičari nemaju posjed ključa za razotkrivanje poruke te se bave probijanjem kritopisnih sustava.

Prema Alan T. Norman (2017), Blockchain tehnologija ima veći potencijal u uspješnoj provedbi provjera i ovjera veza, ugovora i transakcija, u usporedbi sa financijskim institucijama. Banke su zaštitile privatnost korisničkih računa (i njihovih sprovedenih transakcija) ograničavanjem dostupnosti informacija samo onim strankama koje su direktno uključene. Glavna knjiga banaka (eng. *ledger*) bazirana je na internim dokumentima, a što omogućava osobi *E* da uvidom u provedene transakcije vidi samo one transakcije u koje je osobno umješana.

Za razliku od glavne knjige koju koriste financijske institucije, Blockchain tehnologija se koristi kriptografijom koja omogućava da se svi podaci o provedenim transakcijama saberu u jedan skup podataka (blok). Pod podacima o transakciji misli se na vrijeme i datum provedbe transakcije, iznos, ID transakcije, adrese pošiljatelja i primatelja.

3.1. Distribuirani sustav

Distribuirani sustav (eng. *distributed ledger*) predstavlja bazu podataka koja je rasprostranjena na više lokacija. Točnije, ona sadrži podatke o mnogim korisnicima, ali ne u jednom središnjem mjestu. Dakle, ključna karakteristika ovakvog sustava je decentralizacija. Banke se koriste centraliziranim sustavom, odnosno one su središte koje prikuplja i pohranjuje podatke o svim korisnicima te predstavlja medij kroz koji moraju proći provjere i odobrenja svih transakcija. Za razliku od banaka, distributini sustav funkcionira decentralizirajuće na način da svaki korisnik ima ulogu banke za sebe, odnosno svaki korisnik pohranjuje u svoju internu bazu podatke o sebi i svojim transakcijama, kao što ih i osobno kontrolira. Na taj način, distributivni sustav stvara mrežu svojih korisnika, bez medija (banke) kao posrednika za izvršenje transakcija. Na priloženoj Slici 1 moguće je uvidjeti razliku između mreže koju gradi centralizirani sustav od mreže distributivnog sustava.



Centralizirani sustav glavne knjige

Distributivni sustav glavnih knjiga

Slika 1. Razlika između centraliziranog i distributivnog sustava

Izvor: Belin, O. (n. d.) *The Difference Between Blockchain and Distributed Ledger Technology.* Preuzeto s: https://tradeix.com/distributed-ledger-technology/

Blockchain tehnologija funkcionira kao distributivni sustav te se u literaturi ta dva pojma često koriste kao sinonimi. Takvo shvaćanje je krivo. Blockchain tehnologija predstavlja skup blokova (popis transakcija) koji su lančano povezani, kao što i sam naziv kaže. Distributivni sustav, s druge strane, ne mora nužno spajati skupove podataka na lančani način, niti ih mora nužno imati u blokovima, što je karakteristično za Blockchain tehnologiju.

4. Blockchain tehnologija

Andreas M. Antonopoulos (2017) navodi kako je vlasništvo nad kriptovalutama uspostavljeno kroz digitalne ključeve (eng. *digital keys*), adrese (eng. *addresses*) i digitalne potpise (eng. *digital signatures*). Digitalni ključevi se ne pohranjuju u mrežu, već u korisnikovu datoteku/bazu koju nazivamo korisničkim novčanikom (eng. *wallet*) te su potpuno nezavisni od protokola, odnosno moguće ih je generirati i organizirati bez pozivanja na glavnu knjigu, čak i bez pristupa internetu.

Kako bi se transakcije mogle provesti i uključiti u glavnu knjigu, potrebno je imati važeći digitalni potpis. Digitalni potpis može se kreirati jedino pomoću digitalnog ključa. Antonopoulos (2017) ističe kako posljedično tome, svatko tko ima posjed nad digitalnim ključem nekog korisnika, može imati kontrolu nad njegovim bitcoinima, odnosno cjelokupnim novčanikom. Digitalni potpis poistovjećen je sa terminom svjedoka (eng. *witness*), koji se često koristi u kriptografiji u kojoj predstavlja svjedočenje o vlasništvu nad novčanikom prilikom transakcije, odnosno pravo na korištenje (trošenje) sredstava iz vlasničkog novčanika.

Ključevi koji omogućavaju transakcije sastoje se od parova privatnog, odnosno tajnog, i javnog ključa. Antonopoulos (2017) navodi odličnu usporedbu ključeva sa principom na koji banke funkcioniraju. Uspoređuje javni ključ sa brojem bankovnog računa i privatni ključ kao tajni PIN ili potpis na čeku koji omogućavaju djelovanje nad bankovnim računom.

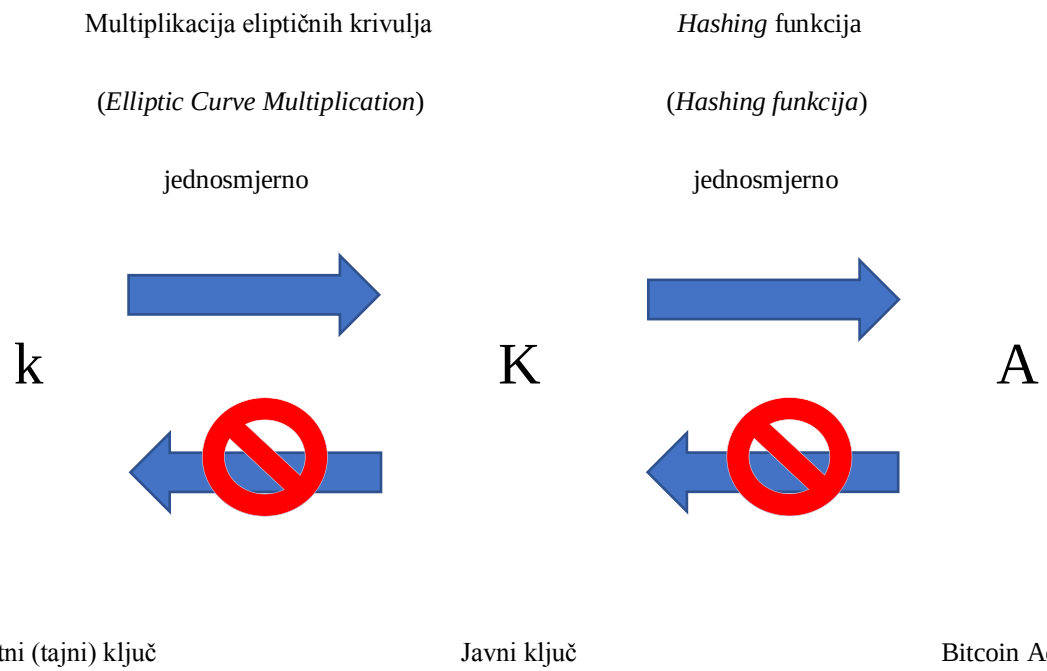
Kriptografija javnih ključeva matematički je temelj računalne i informacijske sigurnosti koji datira iz 1970-ih godina. Ključno obilježje matematičkih funkcija koje se koriste u kriptografiji za enkripciju je njihova nepovratnost. Možda je lako izračunati (enkriptirati) vrijednost ključa primjenom različitih matematičkih funkcija, no jednom kada je ključ definiran, gotovo ga je nemoguće izračunati u suprotnom smjeru, odnosno izvršiti njegovu dekripciju.

Matematička povezanost javnog i privatnog ključa omogućuje javnom ključu da proizvodi digitalne potpise. Ona ujedno daje mogućnost digitalnom potpisu da bude potvrđen od strane javnog ključa, ali bez da se otkrije tajni ključ. Kada korisnik želi izvršiti transakciju, on mora prezentirati javni ključ i svoj digitalni potpis, koji se mijenja od transakcije do transakcije temeljem istog tajnog ključa.

Kakogod, ti ključevi su rijetko viđeni od strane korisnika bitcoina. Oni su većinski pohranjeni unutar novčanika te su kontrolirani od strane bitcoinovog softvera za novčanike (eng. *bitcoin wallet softwer*). Adresu bitcoina (eng. *bitcoin address*) prilikom transakcije bitcoina predstavlja primateljev javni ključ. Ona izriče u čiju korist da se isplati iznos te je vjerojatno jedina reprezentacija ključa koju će korisnik rutinski viđati, zato što ju je nužno podijeliti sa ostatkom mreže kako bi se znalo tko isplaćuje ili kome se isplaćuje određeni iznos.

4.1. Asimetrična kriptografija

Antonopoulos (2017) navodi kako se novčanik sastoji od kolekcije parova ključeva (privatnih i javnih ključeva), pri čemu je privatni ključ *k* nasumično odabrani broj. Korištenje asimetrične kriptografije za dobivanje javnog ključa predložili su 1976. godine Whitfield Diffie i Martin Hellman. Javni ključ *K* dobiva se upotrebom jednosmjerne kriptografske funkcije, multiplikacije eliptičnih krivulja, nad privatnim ključem *k*. Nadalje, iz javnog ključa *K* jednosmjernom kriptografskom *hash* funkcijom dobivamo bitcoin adresu *A*.

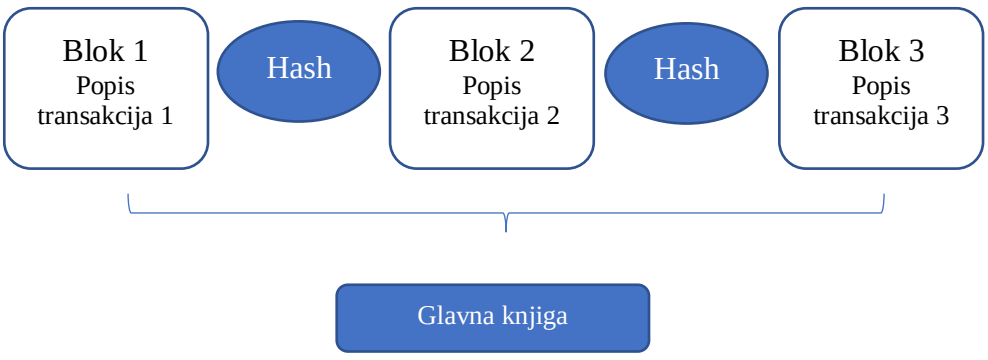


Dijagram 1. Relacija privatni ključ, javni ključ, bitcoin adresa

Iz priloženog dijagrama može se zaključiti da se pri kreiranju javnog ključa i bitcoin adrese koristi asimetrična kriptografija. U literaturi se često spominju imena Alice, Bob i Eve, koja imena se odnose na pošiljatelja, primatelja i protivnika (kriptoanalitičara), retrospektivno. Asimetrična kriptografija omogućava Alice i Bobu da razmjenjuju poruku (u ovom slučaju transakcije) bez da svaki put razmjenjuju tajni ključ putem posredničkog kanala. Na taj način smanjuje se mogućnost da će Eve, protivnik, moći dešifrirati ili iskoristi u svoju korist transakciju, bez obzira da li je upoznata sa funkcijom šifriranja kojom su se Alice i Bob koristili. Točnije, Eve nikako neće moći otkriti funkciju dešifriranja zakritka, zahvaljujući jednosmjernoj funkciji (eng. *trapdoor one-way functions*) poput multiplikacije eliptičnih krivulja.

Antonopoulos (2017) tvrdi da se asimetrična kriptografija ne koristi zbog enkriptiranja transakcije (pretvaranje transakcije tajnom), već zbog njene sposobnosti da stvori digitalne potpise. Jedino osoba koja poznaje tajni ključ može producirati digitalni potpis i posljedično imati kontrolu nad svojim novčanikom.

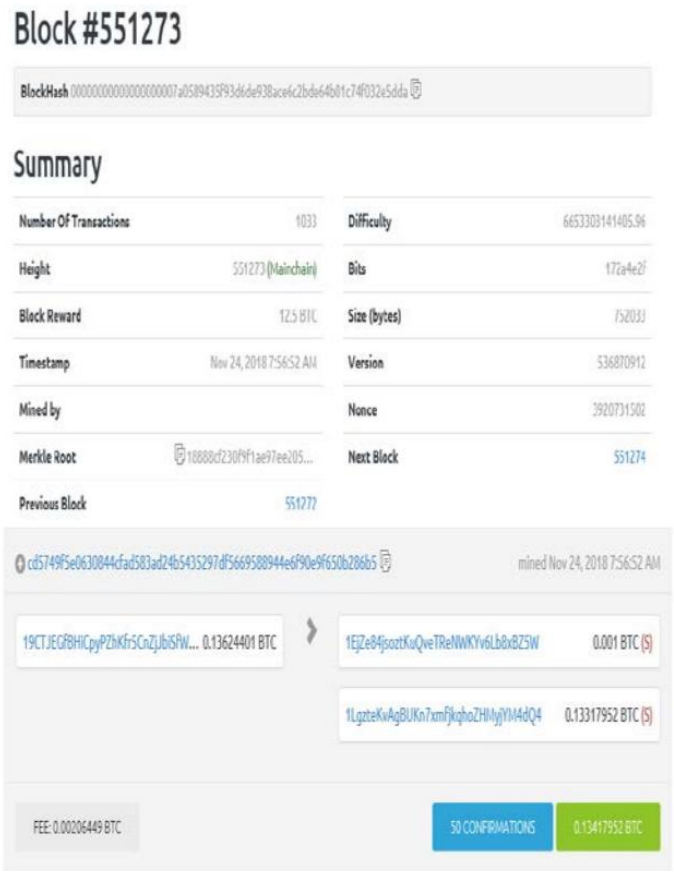
Prema samom nazivu Blockchain tehnologije (lanac blokova), može se zaključiti da se ova tehnologija sastoji od skupa podataka koji se nazivaju blokovima. Blokovi zapravo predstavljaju skup transakcija koje su provedene u nekom vremenskom periodu. **Kriptografski potpis** (eng. *hash*) dobiva se istoimenom *hash* funkcijom koja omogućava da se blokovi međusobno povežu te formiraju glavnu knjigu kao što je prikazano u Dijagramu 2.



Dijagram 2. Formiranje glavne knjige

A.T. Norman (2017) ističe kako hash funkcija skraćuje i standardizira broj znakova u opisu transakcije na način da više transakcija može biti poslano kroz mrežu u bilo koje vrijeme. Primjer kako bi izgledao skup informacija o transakciji nakon enkriptiranja hash funkcijom:

aca178e2918e72ce93b68e9a0c3c1c706ca8f39wa561df12588e90nd778293eacf



Slika 2. Bitcoin Transakcija

Izvor: Izgled prave Bitcoin transakcije prikazane na računalu. Preuzeto s: https://blockexplorer.com

Očigledno je da se prostim pogledom na listu transakcija (blok) sa Slike 2, od kojih bi sve transakcije izgledale kao nasumičan niz slova i brojeva, ne može zaključiti apsolutno ništa o pošiljatelju, primatelju ili iznosu transakcije. Dakle, kriptografski potpis garantira sigurnost i anonimnost korisnika mreže, a što je omogućeno asimetričnom kriptografijom.

Norman (2017) ističe kako obzirom da je bitcoinov standard enkripcije javno dostupan, moguće je dekriptirati transakcije i saznati detalje kao što su javni ključ pošiljatelja, javni ključ primatelja i iznos koji je poslan. Posljedično, noviji oblici kriptovaluta nastoje bolje zamračiti transakcijske informacije na način da je nemoguće izvući informacije o bilo kojoj transakciji jednom kada postane dijelom glavne knjige.

4.1.1. Privatni ključ

Posjedovanje privatnog ključa srž je korisnikove kontrole nad njegovim sredstvima povezanih sa odgovarajućom bitcoin adresom. On nužno mora ostati tajan kako neovlaštene strane ne bi dobile ovlast nad kreiranjem digitalnih potpisa, a što bi rezultiralo preuzimanjem potpune kontrole nad sredstvima, odnosno novčanikom. Jednim dijelom se može poistovjetiti sa PIN kodom određene kartice bankovnog računa, jer on daje ovlast pristupu računu. Za razliku od PIN koda, jednom ako se izgubi privatni ključ, nemoguće ga je povratiti pa tako i financijska sredstva koja su bila vezana za njega.

4.1.1.1. Kreiranje privatnog ključa

Privatni ključ (eng. *private key*) predstavlja niz nasumičnih brojeva. Antolopoulos (2017) ističe kako je krucijalno za stvaranje privatnog ključa pronaći sigurni izvor entropije (eng. *entropy*) ili nasumičnosti (eng. *randomness*), koja će osigurati da se ključ ne ponavlja, niti da se može lako pretpostaviti. Također, preporuča se korisniku da prilikom kreiranja privatnog ključa ne piše sam kod od 256 bitova, niti da koristi jednostavne generatore nasumičnih brojeva. Antolopoulos (2017) tvrdi da je ispravna implementacija kriptografski sigurnog generatora pseudoslučajnih brojeva krucijalna za sigurnost ključeva. Posljedično, potrebno je dobro proučiti dokumentaciju riječnika programskog jezika koji će se koristiti za generiranje ključa, kako bi se utvrdilo da je kriptografski siguran za korištenje.

Privatni ključevi zapisani su u 256-bitnom obliku, što je ogromna količina nasumično povezanih brojeva koja bi zauzela velik dio ovog rada, stoga će se prikazati primjer privatnog ključa u heksadecimalnom obliku:

2BS73HSJVHCGSKAU73BS8XKW79SBNF7W81LBSK391LVBOSZC194JB35L84DZ17D8

4.1.2. Javni ključ

Javni ključ (eng. *public key*) dobiva se pomoću privatnog ključa korištenjem funkcije multiplikacije eliptične krivulje prema formuli *K=k*G*, gdje je *k* privatni ključ, *G* je konstantna točka, odnosno točka generacije, a *K* je rezultat – javni ključ.

4.1.3. Multiplikacija eliptične krivulje

Multiplikacija eliptične krivulje (eng. *elliptic curve multiplication*) je tzv. zamka (eng. *trapdoor*) funkcija koja omogućava lako izračunavanje u jednom smjeru, ali povratno ju je gotovo nemoguće dobiti. U praksi to znači da će korisnik lako moći kreirati i podijeliti cijeli niz javnih ključeva, bez opasnost da će netko reverzibilnom funkcijom moći doći do njegovog privatnog, tajnog ključa i dovesti u opasnost sredstva na njegovom računu.

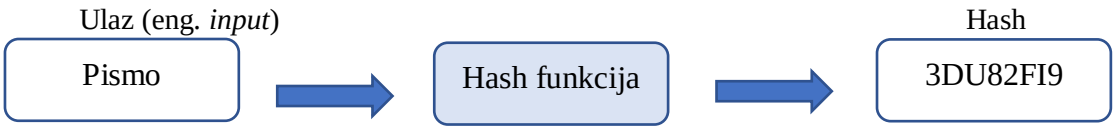
4.1.4. Bitcoin adresa

Bitcoin adresa (eng. *bitcoin address*) je ništa više od niza znamenki i slova koji se koristi za dijeljenje ostalim korisnicima na mreži, a kako bi se izvršila transakcija novca.

Dobiva se iz javnog ključa te započinje znamenkom „*1*“, npr.

1*bjs72kb85lc910sVUQwtzc749gb866hc12*

Adresa se dobiva iz javnog ključa temeljem već spomenute jednosmjerne kriptografske hashing funkcije, odnosno hashing algoritma. A. T. Norman (2017) navodi kako hash funkcija uzima niz znakova, bez obzira na njihovu dužinu, i transformira ga u niz nasumično odabranih znakova standardizirane duljine, a što je prikazano u Dijagramu 3.



Dijagram 3. Hash funkcija

SHA (eng. *Secure Hash Algorithm*) najčešće je korišteni kriptografski hash algoritam, objavljen od strane Agencije za nacionalnu sigurnost (eng. *National Security Agency*). Norman (2017) ističe kako je SHA-256 algoritam prikladan za rudarenje kriptovalutama dokazom rada (eng. *proof-of-work mining*) te je u vrijeme dizajniranja Bitcoina predstavljao najsnažniji kriptografski algoritam. Broj „*256*“ u nazivu algoritma predstavlja 256-bitno stanje i izlaz (eng. *output*) koji daje. Stanje je podijeljeno u osam 32-bitnih riječi. U svakoj iteraciji se određeni broj riječi oduzima te se ponovno dodaje zajedno uz mod 32. Nakon toga se cjelokupno stanje pomiće udesno. Ova radnja se zatim ponovno ponavlja kroz 64 jednake iteracije.

5. Rudarenje

Korisnici su ključni dio funkcioniranja mreže Blockchain tehnologije. Aktivne korisnike koji potvrđuju transakcije, kreiraju blokove i spajaju ih u glavnu knjigu nazivamo rudarima (eng. *miners*). Rudari (re)produciraju mrežu svojim djelovanjem, odnosno akcijama, za koje bivaju nagrađenim s određenom svotom kriptovaluta. Takvo djelovanje korisnika naziva se rudarenjem (eng. *mining*).

Narayanan, Bonneau, Felten, Miller i Goldfeder (2016) uspoređuju rudarenje Bitcoinom sa fenomenom tradicionalne zlatne groznice (eng. *gold rush*), tijekom koje mnogo mladih ljudi žuri kako bi pronašlo blago i obogatilo se, a što često završi time da izgube svu imovinu koju su imali.

Također, navode stavke koje mora zadovoljiti svaki rudar kako bi ostvario zaradu:

1. Rudar mora obratiti pažnju na transakcije na mreži, odnosno treba ih potvrditi (eng. *validate*) na način da se provjerava točnost potpisa i izlaza (sredstava; npr. iznos od 100 kn namijenjen isplati na račun *y*).
2. Rudar treba održavati glavnu knjigu.
3. Rudar sastavlja vlastite blokove potvrđivanjem tuđih i prikupljanjem transakcija za koje je čuo, ali uz naglasak da prije izvrši provjeru da li su uključene transakcije potvrđene od strane drugih korisnika na mreži.
4. Rudar mora pronaći arbitrarni broj (eng. *nonce*) kojeg je moguće upotrijebiti samo jednom, a koji će potvrditi njegov kreirani blok.
5. Iako uspije sastaviti transakcijski blok, to ne znači da će njegov blok biti priznat kao dio općeg konsenzusa mreže. Ovdje je sve stvar sreće da li će ostali rudari naići na rudarev blok, prihvatiti ga i nastaviti s rudarenjem na temelju njega ili će odabrati blok nekog drugog rudara koji predstavlja suparnika.
6. Rudar ostvaruje zaradu tek onda kada rudari prihvate njegov blok unutar mreže. Time dobiva nagradu (eng. *block reward*) koja je tijekom 2015. godine iznosila 25 bitcoina (otprilike 10.000,00 USD).

5.1. Dokaz rada

Obzirom da je Blockchain tehnologija ovisna o konsenzusu korisnika mreže, potrebno je nagrađivati ili sankcionirati svoje korisnike te uvesti određene sustave koji će regulirati opću suglasnost na mreži. Iskreni korisnici koji se trude oko potvrđivanja transakcija bivaju nagrađeni već spomenutom nagradom. S druge strane, oni koji stvaraju lažne transakcije kako bi ih potvrđivali, trebaju biti kažnjeni. Također, potvrđivanjem novih blokova transakcija smanjuje se broj dostupnih bitcoina za rudarenje, stoga je bilo potrebno uvesti regulaciju koja će smanjiti brzinu kreiranja novih blokova, a kako bi svi korisnici imali ravnopravne šanse u potvrđivanju transakcija prije nego je novi blok kreiran.

A. T. Norman (2017) objašnjava najuvaženije rješenje za ovaj problem, tzv. princip dokaza rada (eng. *proof-of-work*). Ovaj princip podrazumijeva da se svim računalima na mreži da jednako težak zadatak (eng. *puzzle*) koji treba biti riješen. Računala koja odaberu da će se natjecati nazivamo već objašnjenim rudarima. Njihov zadatak je potvrditi transakciju (ili više njih) i kreirati blok. Svaki put kada rudar uspije sastaviti jedan blok koji potvrđuju ostali rudari, dobiva određenu svotu bitcoina kao nagradu. Taj određeni iznos bitcoina se zbraja u totalnu sumu izrudarenih bitcoina.

Potrebno je naglasiti kako se obogaćivanje Bitcoinom ne može ostvarivati u nedogled. Tvorac Bitcoina, Satoshi Nakamoto, odredio je pravila Bitcoin protokola na način da je ograničio maksimalan iznos opskrbe bitcoinima na 21.000.000 bitcoina. Svaki put kada rudar bude nagrađen sa npr. 25 bitcoina, prostor za rudarenje se smanjuje za 25 bitcoina. Posljedično tome, Nakamoto je odredio da se nagrada za stvoreni blok smanjuje za 50% svakih 210.000 kreiranih blokova (eng. *halving event*). 99BITCOINS (2019) navodi kako je prosječno šest blokova otkriveno svakih sat vremena, a obzirom da se smanjenje nagrade za 50% događa svakih 210.000 blokova, zaključuju da bi se otprilike svake 4 godine trebao dogoditi događaj umanjenja nagrade za 50%. Konkretnije, trenutna nagrada iznosi 12,5 bitcoina, a bitcoinblockhalf (2019) procjenjuje da će 20. svibnja 2020. godine pasti za 50% na 6,25.

Glavni razlog zašto je Nakamoto definirao ovakav protokol je kako bi spriječio prebrzo gomilanje bitcoina, a obzirom da je maksimalan mogući iznos bitcoina ograničen na

21 milijun, to bi rezultiralo drastičnim padom njegove vrijednosti. Ovakvav protokol, omogućio je Nakamotou održavanje inflacije[1] pod kontrolom.

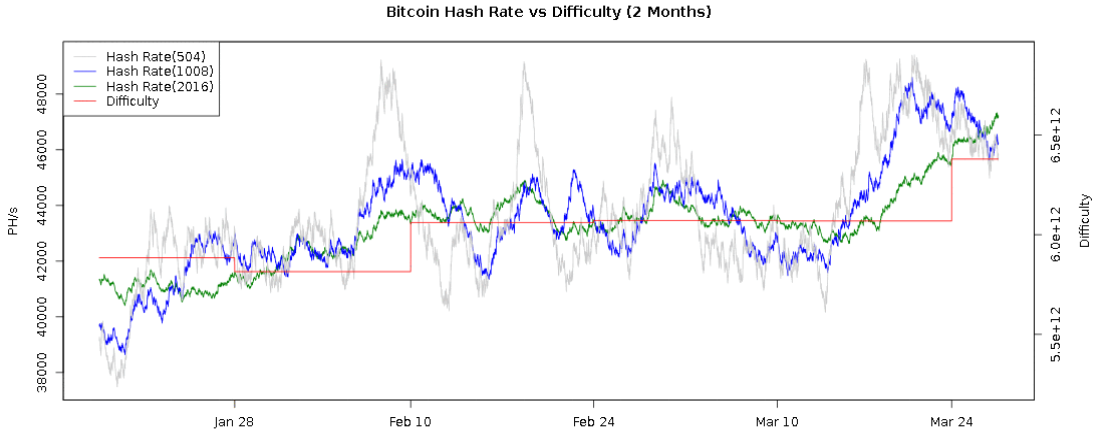
Narayanan i sur. (2016) naglašavaju koliko je teško pronaći važeći blok, a koji već nije otkriven i postao konsenzusom mreže, zbog čega je princip dokaza rada (eng. *proof-of-work*) dobio takvo ime. Tijekom 2015. godine ta težina rudarenja u heksadecimalnom zapisu iznosila je:

00000000000000000a955000000000000000000000000000000000000000000000,

što bi značilo da je manje od 1 na 2^{68} isprobanih apstraktnih brojeva uspjelo potvrditi neki blok. Težina rudarenja mijenja se svakih 2.016 blokova ovisno o uspješnosti rudara u prethodnom periodu izrudarenih 2.016 blokova prema formuli:

sljedeća težina = (prethodna težina x 2016 x 10 minuta) / (vrijeme potrebno za rudarenje prethodnih 2016 blokova)

Na priloženom Grafikonu 1 i Tablici 1 prikazane su fluktuacije težine rudarenja tijekom perioda 28. siječanj – 24. ožujak 2019. godine te trenutno stanje dostupnih bitcoina za rudarenje, stopa inflacije, težina rudarenja, itd.; retrospektivno.



Grafikon 1. Fluktuacija težine rudarenja tijekom 2019. godine

Izvor: Bitcoin Wisdom (2019) *Bitcoin Hash Rate vs Difficulty (2 months).*
Preuzeto s: https://bitcoinwisdom.com/bitcoin/difficulty

[1] *"Inflacija je jedan od najvažnijih ekonomskih pojmova i predstavlja općenito povećanje cijena proizvoda i usluga unutar jednog gospodarskog područja (pojava rasta cijena). Inflacija je zapravo stopa po kojoj su se cijene proizvoda i usluga povećale u određenom vremenskom razdoblju.",* Ekonomski Rječnik (2016) *Inflacija*. Preuzeto s: http://www.ekonomskirjecnik.com/definicije/inflacija.html

Tablica 1. Procjene vrijednosti i inflacije Bitcoina u 2019. godini

Procjene vrijednosti i inflacije Bitcoina u 2019. godini	
Ukupno Bitcoina u opticaju	17.791.675,00
Maksimalna količina Bitcoina koji mogu biti proizvedeni	21.000.000,00
Postotak ukupno izrudarenih Bitcoina	84.72%
Cijena Bitcoina u USD	$ 10.419,00
Generirano Bitcoina po danu	1.800,00
Godišnja stopa inflacije Bitcoina u USD	3.76%
Blokova do sljedećeg *halving eventa*	46.666,00
Okvirno vrijeme potrebno za generaciju bloka	10 minuta
Okviran broj blokova generiranih na dnevnoj bazi	144,00
Težina	7.934.713.219.631,00

Izvor: Bitcoin Block Half (2019) *Bitcoin Block Reward Halving Countdown*.
Preuzeto s: www.bitcoinblockhalf.com

5.2. Dokaz o udjelu

Naravno, Bitcoin nije jedini oblik Blockchain tehnologije. Ethereum je dobar primjer još jedne takve decentralizirane aplikacije. Za razliku od Bitcoina, Ethereum se ne koristi nagrađivanjem svojih korisnika po principu dokaza rada. On je odbacio tu metodu i uveo sistem dokaza o udjelu (eng. *proof-of-stake*).

Za razliku od sistema dokaza o radu koji svim računalima na mreži istovremeno daje priliku da riješe zadatak i time šansu za kreiranjem bloka, sistem dokaza o udjelu određuje novog stvaratelja bloka na temelju postotka (udjela od ukupnog broja) posjedovanja novčića.

Korisnik koji ima 15% svih novčića na svijetu, ima 15% šanse da postane novi stvaratelj bloka. Tek kada dođe red na određenog korisnika, on ima šansu potvrđivati transakcije i tako kreirati blokove. Ovaj sistem ne nudi nagradu za stvaranje blokova kao sistem dokaza o radu, no korisnik koji je na redu za stvaranje blokova ima pravo na sve provizijske iznose koji čine udio u transakcijama koje je uključio u blok.

Također, ovaj sistem je bolje razradio kažnjavanje svojih korisnika koji dolaze u napast za stvaranjem i potvrđivanjem lažnih transakcija kako bi zaradili na temelju provizija. Svaki korisnik kojeg zajednica mreže ulovi, gubi pravo na sve svoje zarađene novčiće.

5.2.1. Usporedba dokaza rada i dokaza o udjelu

Oba dva sistema, i dokaz o radu i dokaz o udjelu, imaju zajednički glavni cilj, a to je osigurati opće suglasje (eng. *consensus*) na mreži. Sistem dokaza rada je efikasniji u vidu stvaranja novih blokova, jer tijekom natjecanja omogućava brojnim računalima da brzo i efikasno rade na rješavanju zadatka, a posljedično se transakcije brže potvrđuju i blokovi brže stvaraju. Za razliku od njega, dokaz o udjelu je mnogo sporiji, jer omogućava samo jednom korisniku da radi na mreži, dok su ostali korisnici ograničeni.

Iako je dokaz o udjelu još uvijek slabo rasprostranjena tehnologija i nije još usvojena u funkcioniranju nekih snažnijih oblika kriptovaluta, npr. Bitcoin, dokaz o udjelu efikasnije provodi sankcije nad korisnicima koji varaju na mreži te unose neravnopravnost u težinu rudarenja.

6. Novčanik

Izrudareni bitcoini moraju se negdje i pohraniti. Pohranjivanje bitcoina vrti se oko pohranjivanja i organizacije ključeva. Narayanan i sur. (2016) navode tri glavna cilja koja se trebaju uzeti u obzir pri pohrani i organizaciji ključeva: dostupnost, odnosno mogućnost da se troše bitcoini onda kada želite; sigurnost, tj. osiguravanje da nitko osim vas ne može trošiti vaša sredstva; i posljednje udobnost korištenja koja karakterizira lakoću organiziranja vlastitih ključeva. Iako se sva tri cilja čine prilično jednostavnim, održavanje sva tri cilja na potrebnoj razini zahtjeva mnogo uloženog vremena i truda.

Najjednostavniji način pohrane i organizacije ključeva je pohrana u datoteku na nekom od vlastitih uređaja, poput računala. Iako je ovaj način odličan što se tiče udobnosti prilikom organizacije ključeva, Narayanan i sur. (2016) upozoravaju da ovakav način pohrane nije adekvatan zbog njegove dostupnosti i sigurnosti u slučaju kvara ili gubitka uređaja. Izgubite li mobitel ili računalo na kojem su pohranjeni vaši privatni ključevi, znači automatski gubitak svih bitcoina koje ste ikada izrudarili, jer su privatni ključevi nepovratni.

Stoga, predlažu korisnicima uporabu softvera za organiziranje novčanika (eng. *wallet softver*) – programa koji prati provedene transakcije te organizira informacije o privatnim ključevima. Novčanik (eng. *wallet*) sadrži jednostavno sučelje koje obavještava o trenutnom stanju u novčaniku, a kada korisnik poželi potrošiti dio svojih sredstava, vodi računa o tome koji ključ koristiti te kako generirati nove adrese. Naravno, kako bi jedan korisnik zaprimio bitcoine od drugog korisnika, mora s njime podijeliti svoju adresu, a to je moguće ili putem teksta u obliku niza nasumičnih znakova ili u obliku QR koda (eng. *QR code*).

6.1. Adresa u obliku niza znakova

Zakrivanje adrese (eng. *encription*) u obliku niza znakova vrši se na način da se uzmu bitovi ključa i konvertiraju se iz binarnog broja u 58-bazični broj (eng. *base-58 number*), prilikom čega se koristimo skupom od 58 znakova kako bi enkriptirali svaku brojku kao znak. Koristi se 58 znakova jer je to ukupan broj dostupnih znakova pisanih velikim i malim slovima, kao i brojki, umanjen za nekoliko zbunjujućih ili sličnih karaktera, poput 0 i O.

1A83hdbA72hbu910B47dGZT4b71jbz811bBc

Primjer adrese u obliku niza znakova

6.2. Adresa u obliku QR koda

Adrese u obliku QR koda (eng. *QR code*) imaju veliku prednost prilikom korištenja mobilnih uređaja, jer je samo potrebno uslikati kod kako bi softver novčanika automatski iz njega izvukao odgovarajuću bitcoin adresu na koju će se uplatiti sredstva. Na taj način moguće je otići u kupovinu i u samo nekoliko sekundi kupiti određeni proizvod bez potrebe za gotovinskim plaćanjem.

QR kodovi najčešće se generiraju putem različitih aplikacija, odnosno softverskih alata u koje se unesu podaci o primateljevoj adresi, a neki od alata traže i podatke o iznosu koji se šalje. Pritiskom na gumb „*Generiraj kod*“ automatski se dobiva QR kod poput prikazanog na slici ispod, a koji je odmah spreman za uplate. Dobiveni QR kod moguće je pohraniti u novčanik kao sliku u obliku .jpg datoteke.

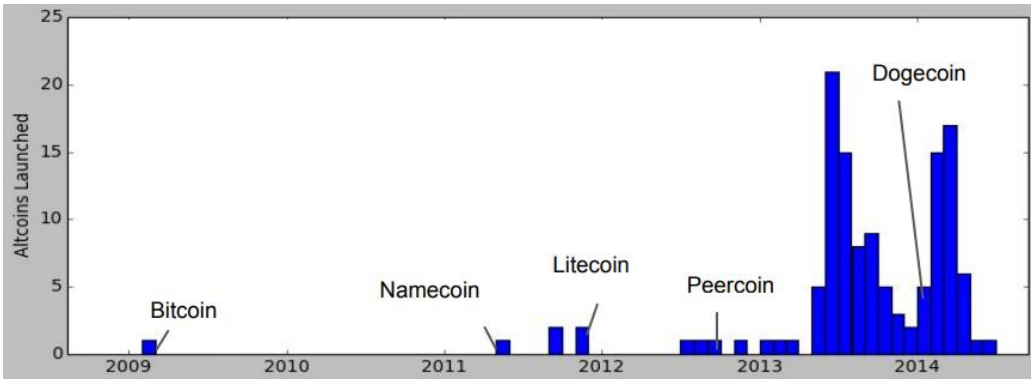
Slika 3. Adresa u obliku QR koda

Izvor: StackExchange (2014) *QR code*.
Preuzeto s: https://bitcoin.stackexchange.com/questions/8111/what-are-qr-codes-and-how-do-you-use-them-as-request-payment-from-wallet

7. Eko-sistem kriptovaluta

Blockchain tehnologija je objašnjena u ovom radu kroz funkcioniranje Bitcoin mreže. Bitcoin je preteča razvijanja ostalih oblika tehnologija koje su slijedile istu viziju decentralizacije financijskog sustava. Postoje mnogi alternativni oblici kriptovaluta (eng. *altcoins*) koji čine cijeli eko-sistem kriptovaluta. Teško je procijeniti ukupan broj alternativnih kriptovaluta, jer se zna samo za one nad kojima se aktivno rudari.

Nakon pokretanja tehnologije Bitcoina 2009. godine, slijedila je stagnacija s pojavom novih kriptovaluta, no u periodu 2013. – 2014. godine uočen je drastičan porast pojave novih oblika kriptovaluta, a što je vidljivo iz priloženog Grafikona 1.



Grafikon 2. Pojava novih oblika kriptovaluta u periodu 2009. – 2014. godine

Izvor: Miller, A. (2015) *Bitcoin and Cryptocurrencies and what they mean for cybersecurity research*. Preuzeto s: http://cyber.umd.edu/sites/default/files/documents/symposium/Bitcoin-Tutorial-Dec2015.pdf

7.1.1. Namecoin

Namecoin je prva tehnologija lansirana nakon Bitcoina, 2013. godine. Bazirana je na Bitcoinovoj tehnologiji te poboljšava decentralizaciju, otpornost na cenzuru, privatnost, zaštitu te brzinu pojedinih dijelova Internetske infrastrukture kao što je domenski sustav imena (eng. *Domain Name System (DNS)*).

Namecoin (2019) na svojim stranicama navodi primjenu svoje tehnologije kao:

1. Online zaštitu prava na slobodu govora, na način da web stranicu čini otpornijom na cenzuru.
2. Provjeru valjanosti certifikata za decentralizirani TLS (eng. *Transport Layer Security*) (HTTPS).
3. Priloženje podataka o identitetu kao što su GNU Privacy Guard (infrastruktura javnih/privatnih ključeva) i OTR (eng. *off the record*) ključevi i e-mail, Bitcoin, itd.

7.1.2. Litecoin

Nakon Namecoina pojavila se valuta Litecoin. To je internetska valuta koja omogućava transakciju sredstava unutar nekoliko sekundi bilo kome u svijetu uz gotovo nikakve provizije. Kao i Namecoin, Litecoin (2019) na svojoj web stranici navodi kako predstavlja otvorenu, globalnu mrežu za prijenos sredstava s računa na račun te je neovisna od bilo koje vrste središnjih, centralnih institucija posrednika. Dakle, Litecoin je također decentralizirajuća tehnologija.

Litecoin (2019) tvrdi da je dokazano komplementaran Bitcoinu. Štoviše, tvrdi da podržava čak veći volumen transakcija nego Bitcoin, a što je rezultat češće generacije blokova. Posljedično tome, trgovcima koji su njihovi korisnici su transakcije brže potvrđene.

Kao i korisnici Bitcoina, korisnici Litecoina svoja sredstva mogu pohraniti u novčanik (eng. *wallet*), a koji omogućav pregled svih izvršenih transakcija i stanje računa.

Rudari Litecoina nagrađivani su trenutno sa 25 litecoina za svaki kreirani blok, a iznos nagrade se također umanjuje za pola otprilike svakih 4 godine. Kapacitet ukupno moguće izrudarenih litecoina (84.000.000) je čak četiri puta veći od ukupno moguće izrudarenih bitcoina (21.000.000).

7.1.3. Peercoin

Stvaratelji Peercoin tehnologije (2019) tvrde da su 2012. godine bili prvi u svijetu koji su uspjeli kreirati učinkovitu i održivu javnu Blockchain tehnologiju. Peercoin je jedna od

Blockchain tehnologija koja kao konsenzusni sistem ne koristi dokaz o radu, u ovom slučaju kovača (eng. *minter*), a ne rudara, već koristi sistem dokaza o udjelu. Ističu kako konsenzusni sistem dokaza o radu omogućava ekonomsku kompetenciju i održava ravnotežu u distribuciji pomoću energije kao zastrašujućeg resursa, dok zakazuje po pitanju očuvanja glavne knjige i zaštite svojih korisnika, a što pruža konsenzusni sistem dokaza o udjelu pomoću vremena kao zastrašujućeg faktora.

Vrijeme kao zastrašujući faktor predstavlja potrebno vrijeme da jedna transakcija dozrije (eng. *coin age*). Nakon trideset dana od transakcije, transakcija dozrijeva, a njeni peercoini postaju spremni za kovanje (eng. *minting*). Nakon većeg broja prikupljenih peercoina, oni mogu formirati blok, a određen udio od tog bloka bit će ponovno vraćen kovaču. Isti ti peercoini dozrijevat će ponovno 30 dana te dati priliku ostalim kovačima da iskuju novi blok. Ovakva iteracija se ne može ponavljati u nedogled, već nakon devedeset dana ona doseže svoju maksimalnu zrelost, a vjerojatnost za kovanjem je na najvišoj razini.

7.1.4. Dogecoin

Dogecoin je lansiran 2013. godine te se kao i svi njegovi prethodnici kriptovaluta temelji na decentraliziranoj Blockchain tehnologiji. Također omogućava online transakciju novčanih sredstava. Ova kriptovaluta specifična je po svojoj maskoti Doge (hrv. *pas*), pasmine Shiba Inu, a koji je već postao globalno popularan na društvenim mrežama.

Glavna strategija koju Dogecoin koristi za privlačenje novih korisnika je upravo Doge. Obzirom da je slika Dogea proširena po Internetu, pogotovo socijalnim mrežama, Dogecoin na taj način komunicira da su zabavna i prijateljski otvorena zajednica dostupna na Redditu[2], baš kao i njihova maskota. Tako se i službeno predstavljaju, kao zabavna i prijateljska internetska valuta.

Ono što je karakteristično za Dogecoin je činjenica da valuta nije lansirana iz namjere da postane ozbiljna valuta sposobna komparirati Bitcoinu, no postala je toliko popularna na društvenim mrežama i forumima da je razvila cijelu zajednicu ljudi koji su velikim brzinama počeli rudariti dogecoine.

[2] Reddit je američka društveno-informativna internetska stranica (www.reddit.com).

7.1.5. QuadrigaCX

QuadrigaCX kriptovaluta se ne nalazi na Grafikonu 2 u kojem je vidljiv porast novih oblika kriptovaluta u periodu 2013. - 2014. godine, no i ona je lansirana tijekom 2013. godine od strane osnivatelja Geralda Cottena i Michaela Patryna. Quadriga je najveća kanadska kriptovaluta koja je u 2019. godini proglasila bankrot nakon neočekivane smrti glavnog izvršnog direktora i osnivača Geralda Cottena u 2018. godini. Nešto manje od 200 milijuna kanadskih dolara ostalo je zauvijek zaključano u novčanicima Quadriga korisnika/rudara. Preminuli osnivač bio je zadužen za sve fondove i coinove koji su proticali stranicom. Njegova žena tvrdi da je na svom računalu u novčaniku imao pohranjene ključeve koji su davali ovlasti za kontrolu nad njegovim novčanikom.

Obzirom da nitko ne zna koji ključ je Cotten koristio, njegova sredstva, kao i sredstva svim korisnika mreže su nepovratno izgubljena. Priča iza ove kriptovalute odlično potvrđuje sigurnost decentraliziranog sustava koji se koristi asimetričnom kriptografijom, a što je jedna od glavnih prednosti nad centraliziranim bankovnim institucijama.

8. Zaključak

Entuzijasti Blockchain tehnologije nadaju se da će naše društvo doći do utopijskog stanja u kojem će institucije konačno izgubiti svoju funkciju, čime bi moglo doći do potpunog sloma centraliziranog financijskog sustava. Jedan od argumenata koji doprinosi toj ideji je činjenica da pojedine oblike osiguranja, ugovora i novca koje trenutno posjedujemo već možemo pohranjivati u digitalnim novčanicima na svojim uređajima. Drugi od argumenata je taj što Blockchain tehnologija omogućuje efikasne transakcije, u vrlo kratkom roku, gotovo uz nikakve provizije. Treći argument se odnosi na pitanje sigurnosti pohranjenih podataka. Banke kao posrednici nude zaštitu samo u vidu limitiranja pristupa informacijama onim strankama koje su uključene u transakcije u koje se traži uvid. Blockchain tehnologija asimetričnom kriptografijom omogućuje gotovo neprobojnu zaštitu korisnikovih računa. U konačnici, banke kao središta centraliziranog sustava gube povjerenje svojih klijenata upravo iz prethodno navedenih razloga. S druge strane, povjerenje u Blockchain tehnologije poput Bitcoina, drastično raste.

Kakogod, Blockchain tehnologija osim dobro razrađene softverske implementacije i ideje u teoriji, je daleko od praktične upotrebe. Teško je zamisliti da će velike korporacije i institucije kao centralizirana središta tek tako odustati od svojih profita. Nadalje, čak i da odustanu, još uvijek nije pronađena solucija u kojoj bi pomoću kriptovaluta mogli platiti npr. račun za vodu.

Stoga, Alan T. Norman (2017) smatra kako se Blockchain tehnologija nalazi negdje u sredini između ova dva stajališta. Iako trenutno postoji mogućnost pohranjivanja i slanja ugovora putem nekih Blockchain tehnologija, još uvijek se nije pronašao dovoljno efikasan sistem koji bi osiguravao sigurno sklapanje ugovora bez uključivanja odvjetnika i banaka, a koji bi zaštitio obje ugovorne strane.

Postoji veliki potencijal ove tehnologije u tome da će decentralizirati povjerenje, ali teško je predvidjeti u kojem smjeru će se dalje kretati njen razvoj i primjena te kako će se regulirati.

9. Literatura

1. 99BITCOINS (2019) *Bitcoin Halving – A Beginner's Guide.* Preuzeto s: https://99bitcoins.com/bitcoin-mining/halving/ (20.06.2019.)
2. Antonopoulos, A. M. (2017) *Mastering Bitcoin: Programming the open Blockchain.* 2. Izdanje. O'Reilly Media.
3. Bagić, K. (2018) Kriptogram – Vrlo kratak uvod. *Croatica*, 42 (62), str. 343-364.
4. Bitcoin Block Half (2019) *Bitcoin Block Reward Halving Countdown.* Preuzeto s: www.bitcoinblockhalf.com (25.06.2019.)
5. Bitcoin Wisdom (2019) *Bitcoin Hash Rate vs Difficulty*. Preuzeto s: https://bitcoinwisdom.com/bitcoin/difficulty (21.06.2019.)
6. BlockExplorer (n. d.) Preuzeto s: https://blockexplorer.com (02.07.2019.)
7. Dogecoin (n. d.) *What is Dogecoin?*. Preuzeto s: https://dogecoin.com (02.07.2019.)
8. Ekonomski Rječnik (2016) *Inflacija*.
   Preuzeto s: http://www.ekonomskirjecnik.com/definicije/inflacija.html (21.06.2019.)
9. Giddens, A. (2003) *Runaway world : how globalisation is reshaping our lives*, New York: Routledge.
10. Litecoin (n. d.) *WHAT IS LITECOIN?.* Preuzeto s: https://litecoin.org (02.07.2019.)
11. Miller, A. (2015) *Bitcoin and Cryptocurrencies: and what they mean for cybersecurity research.*
    Preuzeto s: http://cyber.umd.edu/sites/default/files/documents/symposium/Bitcoin-Tutorial-Dec2015.pdf (27.06.2019.)
12. Namecoin (n. d.) *What can Namecoin be used for?*. Preuzeto s: https://namecoin.org (02.07.2019.)
13. Narayanan, A. i sur. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Oxfordshire: Princeton University Press.
14. Norman, A. T. (2017) *Blockchain Technology Explained: The Ultimate Beginner's Guide about Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts.* CreateSpace Independent Publishing Platform.
15. Peercoin (n. d.) *Introduction to Peercoin*. Preuzeto s: https://docs.peercoin.net/#/comparison-with-other-blockchain-networks (02.07.2019.)

16. Stack Exchange (2014) *What are QR codes and How do you use them as request payment from Wallet?*. Preuzeto s: https://bitcoin.stackexchange.com/questions/8111/what-are-qr-codes-and-how-do-you-use-them-as-request-payment-from-wallet (22.06.2019.)
17. Belin, O. (n. d.) *The Difference Between Blockchain and Distributed Ledger Technology*. Preuzeto s: https://tradeix.com/distributed-ledger-technology/ (20.06.2019.)

Popis oznaka i kratica

.jpg	format fotografije
A	bitcoin adresa
a	iznos transakcije
DNS	domenski sustav imena
E	pošiljatelj
e	račun pošiljatelja
eng	engleski
F	primatelj
f	račun primatelja
G	kontantna točka
GNU Privacy Guard	infrastruktura javnih/privatnih ključeva
hrv	hrvatski
HTTPS	protokol nastao kombinacijom protokola HTTP i SSL/TSL
ID	identifikacija
K	javni ključ
k	privatni ključ
OTR	izvan zapisa
PIN	osobni identifikacijski broj
QR	brzi odgovor
SHA	algoritam za provjeru autentičnosti datoteka/poruke
TLS	protokol, omogućava povjerljivost komunikacije putem mreže
USD	američki dolar

Popis tablica

Tablica 1. Procjene vrijednosti i inflacije Bitcoina u 2019. godini 18

Popis ilustracija

Popis dijagrama

Dijagram 1. Relacija privatni ključ, javni ključ, bitcoin adresa 9

Dijagram 2. Formiranje glavne knjige 10

Dijagram 3. Hash funkcija..... 13

Popis grafikona

Grafikon 1. Fluktuacija težine rudarenja tijekom 2019. godine 17

Grafikon 2. Pojava novih oblika kriptovaluta u periodu 2009. – 2014. godine 22

Popis slika

Slika 1. Razlika između centraliziranog i distributivnog sustava..... 7

Slika 2. Bitcoin Transakcija..... 11

Slika 3. Adresa u obliku QR koda 21

Tehnologija iza kriptovaluta

Sažetak

Živimo u svijetu transformacija koje utječu na svaki aspekt onoga što činimo pa tako i na način na koji trošimo novac. Unazad nekoliko godina, kriptovalute postale su globalni fenomen. Ljudi se najčešće po prvi puta susreću s pojmom kriptovaluta kroz medije i to Bitcoinom kao prvom kriptovalutom u povijesti. Iako je prije Bitcoina postojalo i drugih digitalnih oblika novca, Bitcoin je prvi digitalni oblik novca koji za prijenos vrijednosti koristi kriptografske algoritme, odnosno konačan niz svrhovitih uputa koje u određenom broju iteracija dovode do rješenja (npr. kreiranje bitcoin adrese).

Kontekst spominjanja kriptovaluta najčešće je ekonomske prirode, pri čemu ljudi najčešće ostanu zadivljeni njegovom protuvrijednošću u nekoj drugoj valuti. Neke od manje spominjanih kriptovaluta koje još nazivamo i altcoinima su: Litecoin, Dogecoin, Namecoin i Peercoin. Ono što ljudi manje znaju po pitanju kriptovaluta je otkuda potječe ideja o kriptovalutama te kako funkcionira tehnologija iza njih. Upravo vizija financijske decentralizacije te funkcioniranje Blockchain tehnologije bit će detaljnije objašnjeni u ovome radu na temelju funkcioniranja Bitcoin tehnologije.

Ključne riječi: kriptovalute, blockchain, rudarenje, tehnologija, mreža

Technology behind Cryptocurrencies

Summary

We live in the world of transformations, which affects every aspect of what we do, therefore also on the way we spend money. Cryptocurrencies are becoming a global phenomenon. Usually people confront with the conept of cryptocurrencies through the media, especially with Bitcoin as the first cryptocurrency in the history. Although there were other digital forms of currencies before Bitcoin, Bitcoin is the first digital form of money that uses cryptographic algorithms (a final set of purposeful instructions that leads to solution through numoreous iterations) for money transfers (eg. the process of creating a bitcoin adress).

When people talk about cryptocurrencies, the talk is usually of an economic nature – surprised by its value in another currency. Some of the less mentioned cryptocurrencies, which are called Altcoins, are: Litecoin, Dogecoin, Namecoin and Peercoin. What is less known about cryptocurrencies is the origin of the idea behind cryptocurrencies and how the technology behind them operates. Therefore, the vision of financial decentralization and the way Blockchain technology functions will be explained further in this paper, based on the Bitcoin technology structure.

Key words: cryptocurrencies, blockchain, mining, technology, network