Bitcoin

Dajana Cerovina
studenti drugog ciklusa studija,
Univerzitet u Istočnom Sarajevu, Elektrotehnički fakultet
Istočno Sarajevo, BiH,
dajanacera@yahoo.com

Sadržaj—**U ovom radu je opisan *Bitcoin* sistem. To je elektronski sistem, zasnovan na matematičkom dokazu, koji počinje sve više da se upotrebljava da bi omogućio plaćanje. *Bitcoin* je prvi primjer valute za koji se koristi termin kripto-valuta. *Bitcoins* se stvaraju (*mined*) elektronskim putem korištenjem računarske moći u distribuiranoj mreži. U radu je dat pregled kako kupiti, prodati i čuvati *Bitcoins*. Osnovne karakteristike ovoga sistema su: decentralizacija, jednostavnost, anonimnost, transparentnost, brzina i minimalni porezi na transakcije. Međutim, ovaj sistem posjeduje i neke mane kao što su: sklonosti ka ilegalnim aktivnostima, *mining* troši previše energije i poteškoće pri razmjeni sa drugim valutama.**

Ključne riječi - Bitcoin; mining; block-chain; Bitcoin novčanik;

I. UVOD

Bitcoin je elektronski sistem koji omogućava plaćanje i zasnovan je na matematičkom dokazu. *Bitcoin* valuta se ne printa kao euri ili druge novčanice, ona se generiše pomoću računara na kome ljudi korištenjem određenog softvera rješavaju matematičke probleme. *Bitcoin* je prvi primjer valute za koji se koristi termin kripto-valuta. Koristi se za kupovinu stvari elektronskim putem. U tom smislu je sličan euru, dolaru ili nekoj drugoj valuti. Jedna od glavnih karakteristika koje ga čine drugačijim od svake druge valute je da je ovaj sistem decentralizovan. Nijedna institucija ne kontroliše *Bitcoin* mrežu. Ova činjenica pomaže nekim ljudima jer korištenjem *Bitcoin*, velike banke ne mogu da kontrolišu njihov protok novca. *Satoshi Nakamoto* je predložio upotrebu *Bitcoin* i razvio softver. Ideja je bila da se razvije valuta koja je nezavisna od bilo koga centralnog autoriteta, koja omogućava transponovanje elektronskim putem, bez velikih vrijednosti poreza, nezavisno od banke. Banke mogu da proizvedu više novca da pokriju nacionalne dugove. To smanjuje vrijednost valute. Međutim, *Bitcoin* se kreira digitalnim putem. *Bitcoin* valuta se stvara (*mined*) elektronskim putem korištenjem računarske moći u distribuiranoj mreži. Ova mreža procesuira transakcije i na taj način čini *Bitcoin* sistem efektivnim za izvršavanje plaćanja.

Bitcoin protokol – pravilo po kojem se stvaraju *Bitcoins* omogućava stvaranje samo 21 miliona *Bitcoins*. *Bitcoins* se

mogu dalje podijeliti na manje dijelove (najmanji dio se naziva *Satoshi*).

Konvencionalna valuta je bazirana na zlatu i srebru, za razliku od *Bitcoin* koji je zasnovan na matematičkoj logici. Širom svijeta ljudi koriste softverske programe da bi proizvodili *Bitcoins*. Matematička formula je svima dostupna i svako je može provjeriti jer je softver *open source*. Karakteristike *Bitcoin* mreže su: decentralizacija, jednostavnost pri implementaciji, anonimnost, transparentnost, porezi transakcija su minimalni, brzina, ne mogu se povratiti vrijednosti. [1]

II. KORIŠTENJE BITCOIN SISTEMA

Bitcoin predstavlja digitalni fajl koji sadrži vrijednosti dobara određenog pojedinca. Kopija ovoga fajla se nalazi na svakom računaru koji koristi *Bitcoin* mrežu. Ovi brojevi ne predstavljaju nikakvu fizičku vrijednost, ali omogućavaju ljudima da mijenjaju postojeća dobra i usluge. Da bi se poslao novac, šalje se poruka cijeloj mreži (*broadcast*). Tom porukom se poručuje da bi stanje na korisnikovom računu trebalo da se smanji i poveća stanje na računu prijemnika. Računari ili čvorovi primaju tu informaciju, ažuriraju lokalne kopije i prosljeđuju naredbu drugim kopijama. Ovaj način rada je sličan onome na koji banka održava knjigu glavnih vrijednosti. Razlika je u tome što glavnu knjigu u banci održava jedan entitet, a ne grupa pojedinaca kao što je slučaj sa *Bitcoin*. Za razliku od banke, gdje svaki pojedinac samo zna za svoje transakcije, u *Bitcoin* sistemu, svi znaju sve. Dok se banci može vjerovati ili ne i kriviti je ako dođe do neke greške, *Bitcoin* mreži posluje sa potpunim strancima. [2]

Posebne matematičke funkcije štite svaki aspekt bezbjednosti sistema, zbog toga je *Bitcoin* sistem tako dizajniran da povjerenje nije neophodno. Da bi korisnik, npr. Alisa poslala novac Bobu, ona šalje opštu poruku u kojoj šalje npr. 5 *Bitcoins*. Svaki čvor koji se nalazi u *Bitcoin* mreži tu poruku prima, ažurira svoje informacije i prosljeđuje transakcionu poruku ostalim čvorovima. Međutim, to nije jednostavno jer se postavlja sljedeće pitanje. Kako čvorovi mogu biti sigurni da je transakcija autentična i da pripada pravom korisniku i kojem korisniku je dozvoljeno da preuzme novac? Korisnik u *Bitcoin* mreži zahtijeva posebnu lozinku da bi primio poslati, nepotrošeni novac. Ovu vrstu bezbjednosti omogućava digitalni potpis. Digitalni potpis potvrđuje autentičnost poruke pomoću matematičkog algoritma. [2]

Digitalni potpis koristi dva povezana ključa. Privatni ključ se koristi da kreira potpis dok se javni ključ koristi za provjeravanje pripadnosti poruke. Privatni ključ se smatra pravi ključem. Potpis se koristi da pokaže i dokaže da imamo lozinku bez potrebe da je otkrijemo. Adresa koja služi za slanje novca se obrazuje pomoću prijemnikovog javnog ključa. Da bi prijenik dobio novac, mora dokazati vlasništvo nad javnim ključem. Digitalni potpis se formira od transakcione poruke i privatnog ključa. Potpis zavisi od poruke pa će zato za svaku transakciju biti različit. Ova zavisnost od poruke pokazuje da niko ne može modifikovati poruku dok se šalje jer bilo koja promjena poruke bi izmijenila i potpis.

Umjesto sveukupnog brojčanog stanja na računu, stanje na računu se određuje provjerom vrijednosti *Bitcoins* koji su dobijeni prethodnim transakcijama. Da bi npr. poslala 5 *Bitcoins* Bobu, Alisa mora referencirati druge transakcije gdje pokazuje gdje je dobila 5 ili više *Bitcoins*. Ove transakcije se nazivaju *inputs* ili ulazi. Drugi čvorovi koji verifikuju ove transakcije će provjeriti ove ulaze da bi utvrdili da je Alisa stvarni pošiljalac i da li ima ulaz od 5 *Bitcoins* ili više. Pravilo je da se svaki ulaz mora potpuno koristiti u transakciji. Ako se pokuša poslati količina koja nije jednaka vrijednosti *Bitcoins* na postojećem ulazu računa, već je vrijednost veća, pošiljalac mora poslati preostalu vrijednost sebi samom. Na ovaj način posjedovanje *Bitcoins* se prosljeđuje kroz lanac sa pravilom da svaka transakcija zavisi od prethodnih transakcija. [2]

Bitcoin predstavlja opasnost bankama već od 2008. godine. *Bitcoin* može biti put bez korupcije jer rješava više problema. Prvi od tih problema je povećanje vrijednosti *Bitcoins*. Vrijednost *Bitcoins* se samo povećavaju na određenoj stopi što znači da je rast ograničen. *Bitcoin* je jednostavniji za prenos novca, omogućava da transakcije ostanu privatne. Međutim, *Bitcoin* mreža ima i svoje mane. Transakcije nisu regulisane na način na koji je se to radi u bankama. *Bitcoin* nema regularni status valute. To je razlog zašto vlasti ne mogu brzo da otkriju lopove. U slučaju krađe *Bitcoin* personalnog novčanika, kao posljedica propusta u bezbjednosti u lozinci i šifri, ne postoji nijedan bezbjedan način da se povrate sredstva. Neke banke smatraju digitalnu valutu prijetnjom biznis modelu pa vrše diskriminaciju svega što ima bilo kakvu vezu sa *Bitcoin*. Banke, takođe zatvaraju račune svim koji spominju *Bitcoin*, bez objašnjenja. Te banke nisu prijateljski orjentisane prema ovoj novoj digitalnoj valuti.

Kako kupiti *Bitcoins*? Kako se dobija *Bitcoins* u posjedovanje? Kao jedan od načina da se polako i igrom slučajnosti generišu i distribuiraju *Bitcoins*, formira se nagrada koja se dodjeljuje svakom korisniku koji riješi određeni zadatak. Zadaci se rješavaju matematičkim proračunima. Cijena *Bitcoins* se plaća kroz potrošnju energije. Svake četiri godine nagrada za rješavanje problema *mining* metodom je podijeljena u pola tako da se u budućnosti eventualno više *Bitcoins* neće formirati.

- trenutno dodijeljeno *Bitcoins*: 11.4 miliona,
- ukupno moguće *mining*: 21 milion *Bitcoins*,
- posljednji *Bitcoin* će biti dodijeljen 2140. godine; [4]

Najmanja jedinica razmjene *Bitcoins* je 0.00000001 BTC. *Bitcoins* se mogu dobiti razmjenama ili direktno kupovinom od drugih ljudi. *Bitcoins* se mogu kupiti kešom, kreditnom karticom ili drugim kripto-valutama, zavisno od koga se kupuju i gdje živimo. Međutim, nije lako kupiti *Bitcoins* pomoću kreditne kartice ili *PayPal* zato što transakcije mogu biti vraćene. *US, Coinbase*, *Circle, Trucoin i coin.mx* nude mogućnost kupovine sa karticama. *Bittylicious* i *CoinCorner,* takođe nude ove opcije u *UK*, prihvatajući *3D Secure-enabled cards* na *Visa* i *MasterCard* mrežama. Korisniku je neophodno mjesto gdje će čuvati nove *Bitcoins.* U *Bitcoin* mreži to omogućavaju novčanici (*wallets)*. [2]

Kako prodati *Bitcoins?* Broj opcija raste svakog dana, svakim novim osnovanim biznisom. Opcije za razmjenu zavise od mjesta gdje smo locirani. Razmjene su omogućene u: *Bitfinex (Hong Kong), Bitstamp (US), BTC-e (*nepoznat*), Kraken (US), Huobi (China), OKCoin (China) i BTC China*. *CoinBase* je popularni *wallet* servis koji služi za razmjenu lokalne valute sa *Bitcoins*. Kompanija posjeduje *web* i *mobile (Android) apps*, kao i neoficijalni ali dozvoljeni *iOS wallet. Circle* je nedavni učesnik u *Bitcoin* prostoru, koji nude širom svijeta šansu da se zapamte, pošalju, prime i razmjene *Bitcoins*. *Wallet* i *bitcoin debit card* provajder *Xapo* nudi da se depoziti mogu pretvoriti u *Bitcoins* na računu korisnika. [2]

Za one koji žive u gradu i više vole anonimnost bez povezanosti sa bankama, najpovoljnija opcija za zahtijevanje *Bitcoins* je uspostavljanje razmjena sa lokalnim prodavačem. *LocalBitcoins* je primarni sajt gdje se cijene pregovaraju. Uvijek je bolje sastajati se na javnim mjestima nego u privatnim kućama. Treba imati na umu sve što se može desiti kao kada bi hodali sa velikom količinom keša. Takođe, potrebno je imati pristup *bitcoin wallet*. Bez obzira da li se radi o pametnim telefonima, tabletu ili laptopu, pristup Internetu je neophodan da bi se potvrdile transakcije. Da bi dobili informaciju da li oblast življenja pojedinca posjeduje *Bitcoin meetup* grupu, korisno je provjeriti *meetup.com*. Ove grupe su počele sa razvojem u posljednjoj polovini 2013. godine. Neki veliki gradovi organizuju otvorene događaje, gdje se mogu kupiti *Bitcoins*. Pojedinac koji se nazivaju *Satoshi Squares*. Tu se mogu kupiti *Bitcoins*. Pojedinac sa reputacijom će pregovarati o cijeni prije sastanka, međutim, mnogi neće čekati dugo jer bi vrijednost *Bitcoins* mogla dobiti dramatični pomak. Neki prodavci dozvoljavaju korištenje *PayPal* računa za plaćanje, ali mnogo preferiraju keš. Preporučljivo je da se provjeri da li su takve razmjene legalne u okruženju u kome živimo jer postoji mogućnost da se pojavi policijska sumnja pri razmjeni novca na javnom mjestu.[2]

Kako čuvati *Bitcoins?* Sa tehničke strane gledišta, *Bitcoins* se nigdje ne čuvaju. Ono što se čuva su sigurni digitalni ključevi koji se koriste da se pristupi javnim *Bitcoin* adresama i omogući potpisivanje transakcija. Ove informacije

se čuvaju u *bitcoin wallet* koji postoji u više formi: *desktop, mobile, web i hardware*.

- *Desktop wallets*
  Bitcoin client (*Bitcoin-Qt*) je softver koji omogućava da se kreira *bitcoin* adresa za slanje i primanje virtuelne valute i da bi sačuvala privatni ključ za čitanje transakcija. Postoje mnogi *desktop wallets* sa različitim karakteristikama. *Multibit* se pokreće na *Windows, Mac OSX i Linux. Hive je OSX* baziran novčanik sa jedinstvenim karakteristikama dok *DarkWallet* obezbjeđuje visok nivo bezbjednosti.
- *Mobile wallets*
  Desktop bazirani novčanici nisu mnogo korisni ako pokušavamo da platimo neku robu u prodavnici. U ovom slučaju, najpovoljnije je koristiti *mobile wallet*. Pametni telefoni koriste NFC karakteristiku koja omogućava da se mobilni telefon postavi blizu čitača i izvrši plaćanje sa *Bitcoins* bez potrebe da se upisuju dodatne informacije. Važna karakteristika *mobile wallets* je da oni nisu potpuni *Bitcoin* klijenti. Potpuni *Bitcoin* klijent mora da pothrani cijeli *bitcoin block-chain,*veličine nekoliko gigabajta, koji stalno raste, na svoj lokalni uređaj. Ova činjenica može korisniku da stvori mnogo problema sa *mobile service provider*, jer bi dobio od provajdera veliki račun nakon izvršenog skidanja podataka kroz celularni link. Mnogi telefoni nisu u mogućnosti da čuvaju *block-chain* u memoriji. Umjesto toga, mobilni telefoni su obično dizajnirani sa jednostavnom verifikacijom za plaćanje (SPV). Mobilni telefoni pothranjuju samo mali podskup *block-chain* i oslanjaju se na druge, povjerljive čvorove u *Bitcoin* mreži koji imaju prave informacije. Primjeri *mobile wallets* uključuju *Android* – bazirane *Bitcoin wallet, Mycelium, Xapo i Blockchain*. Neki od njih imaju specijalne karakteristike. *Kipochi*, na primjer dozvoljava ljudima da koriste svoje brojeve telefona kao *Bitcoin* adrese. *Apple* je paranoidan oko *bitcoin wallets*. Međutim, *app Bity* omogućava posebnu uslugu koja se povezuje na korisnikov *wallet* koji je smješten bilo gdje i omogućava prihvatanje i izvršavanje plaćanja preko *QR* koda ili ručni unos ključa za novčanik. Takođe je moguće koristiti *bitcoin* račun korištenjem pretraživača na *iPhone* i *CoinPunk.*
- *Web wallets*
  Ovi novčanici čuvaju privatne ključeve na računaru koji je konektovan na Internet. Nekoliko takvih servisa na Internetu su dostupni i neki od njih su povezani sa mobilnim i desktop novčanicima. Na taj način se repliciraju adrese između uređaja koje posjedujemo. Jedna od prednosti *web* baziranih novčanika je da im možemo pristupiti bilo gdje, bez obzira koji uređaj koristimo. Mana im je što je organizacija koja održava *web* sajt zadužena za privatne ključeve, što znači da može da kontroliše *Bitcoins*. Ovo je jako opasno po bezbjednost, posebno ako čovjek posjeduje mnogo *Bitcoins*. *Coinbase* je integrisani novčanik – *wallet* koji radi sa Internet novčanicima širom svijeta. *Circle* nudi korisnicima širom svijeta šansu da čuvaju, šalju, prime i kupe *Bitcoins*. *Blockchain,* takođe posjeduje popularni *web-based wallet*. *Strongcoin* posjeduje ono što se zove hibridni novčanik jer dozvoljava enkripciju privatne adrese prije nego što se šalje preko servera, enkripcija se izvršava u pretraživaču.
- *Hardware wallets*
  Hardver novčanici su trenutno jako ograničeni u brojnosti. Ovo su uređaji koji čuvaju privatne ključeve elektronski i olakšavaju plaćanja. *Trezor i Mycelium* trenutno posjeduju novčanike u razvoju. [3]

III. BEZBJEDNOST

Bitcoin omogućavaju da se prenose vrijednosti bilo gdje na vrlo lagan način, omogućavajući čovjeku da kontroliše svoj novac. On omogućava visok novo bezbjednosti ako se koristi korektno, ali bitno je da korisnik treba da zaštiti svoj novac. Načini na koji *Bitcoin* sistema obezbjeđuje bezbjednost:

- Obazrivost
  Korisnik treba biti obazriv sa *online* servisima koje koristiti za čuvanje novca. Preporučljivo je dodatno, korištenje dvo-faktorske autentifikacije.
- Male količine za svakodnevne upotrebe
  Generalno, praktično je čuvati malu količinu *Bitcoins* na računaru, mobilnom ili serveru za svakodnevne upotrebe, a preostali dio novca čuvati na bezbjednijem okruženju.
- Ažuriranje novčanika
  Neki novčanici koriste privatne ključeve inicijalno. Ako korisnik ima samo sačuvane privatne ključeve za vidljive *Bitcoin* adrese, moguće je da se nikada ne povrate velike količine novčanih sredstava sa pothranjivanjem.
- Korištenje više bezbjednih lokacija
  Potrebno je koristiti USB ključeve, papire ili CD-ove.
- Regularno pothranjivanje
  Potrebno je da se pothrani novčanik, da se osigura da su sve stare i sve nove *Bitcoin* adrese uključene.
- Enkripcija novčanika
  Enkripcija novčanika ili pametnog telefona dozvoljava da se postave šifre za sve. Ovim se vrši zaštita od lopova, ali ovo ne djeluje na hardver i softver koji snimaju ključeve.
- Nikada ne zaboraviti šifru
  Nikada ne treba zaboraviti šifre ili će novčana sredstva biti zauvijek izgubljena.
- *Offline* novčanik za štednju
  Ovaj novčanik se može čuvati na bezbjednom mjestu koje nije konektovano na mrežu. Korištenje novčanika u *offline* režimu u vezi sa pothranom i enkripcijom je dobra praksa. Ova opcija uključuje dva računara koji dijele neke dijelove istog novčanika. Prvi se mora diskonektovati sa mreže. On

je jedini koji drži cijeli novčanik i dostupan je da potpiše transakcije. Drugi računar je povezan na mrežu i može kreirati samo nepotpisane transakcije. Na ovaj način se mogu bezbjedno izdavati transakcije sa sljedećim koracima:

- kreirati novu transakciju na računaru koji je priključen na mrežu i zapamtiti je na USB,
- potpisati transakcije sa računarom koji nije na mreži,
- poslati potpisanu transakciju sa računara koji je na mreži;

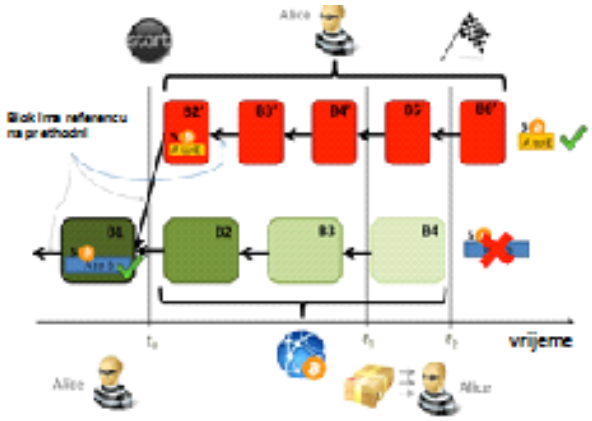
- Održavati softver ažuriran.
  Održavanje najnovije verzije *Bitcoin* softvera omogućava da se dobiju bitne informacije vezane za bezbjednost i stabilnost.
- Hardverski novčanici
  Hardverski novčanici su najbolji balans između visokog nivoa bezbjednosti i jednostavnosti korištenja. Nijedan softver ne može biti instaliran na njima da bi se učinili još bezbjednijim. Oni dozvoljavaju pothranjivanja tako da se mogu povratiti sva novčana sredstva ako se izgubi uređaj.
- Više potpisa u svrhu zaštite od lopova
  Bitcoin uključuje karakteristiku koja omogućava da transakcija zahtijeva više od jednoga privatnog ključa. Trenutno je to samo korisno za korisnike koji imaju dobro razumijevanje tehnike ali veća dostignuća mogu biti očekivana u budućnosti. Na primjer, firma omogućava da 3 od 5 članova potpisuju transakcije.
- Misliti o testamentu
  Potrebno je da porodica zna o kreiranim novčanicima i šiframa tako da ne bi izgubili sva novčana sredstva. [3]

IV. KONTROLA TRANSAKCIJA

Fizički ne postoje *Bitcoins*, samo snimci transakcija koje se izvršavaju. Nije moguće pokazati fizički objekat ili digitalni fajl i reći „ovo je *bitcoin*“. Svaka transakcija koja je ikada izvršena se pamti u *block-chain*. [3]

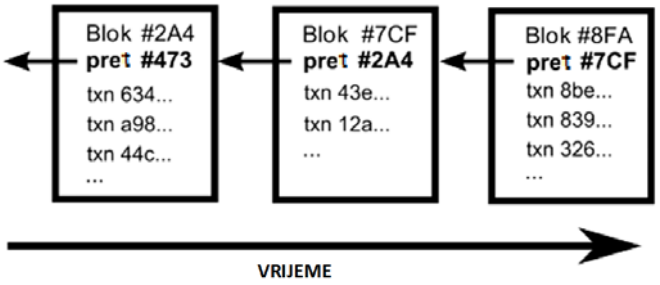
Transakcija u kojoj Alisa šalje određen broj *Bitcoins* Bobu, ima tri dijela informacija: ulaz (zapis koji pokazuje traksakcije kojim je Alisa dobila *Bitcoins* (ono što je dobila od prijateljice Eve), količina (količina *Bitcoins* koje Alisa šalje Bobu), izlaz (Bobova *Bitcoin* adresa). Da bi poslali *Bitcoins*, potrebni su: *bitcoin* adresa i privatni ključ. Oni se generišu slučajno i oni su sekvenca slova i brojeva. Za razliku od *bitcoin* adresa, privatni ključ se čuva u tajnosti. *Bitcoin* adresa je kao sigurna kutija. Svi znaju šta je unutra ali samo privatni ključ može da je otključa, da uzme stvari iz nje ili da je dopuni novim stvarima. Da bi se saznalo Alisino stanje na računu, da li postoji mogućnosti da se pošalje novac, provjerava se svaki neposlat i*nput*.

Ako se podrazumijeva da se transakcije prenose od čvora do čvora kroz mrežu, ne postoji sigurnost da redoslijed u kome primimo poruke predstvalja isti redoslijed u kojima su kreirane. Ne treba vjerovati prikazu vremena kreiranja transakcije jer neko može lagati o tome i zbog toga se ne može objasniti zašto je jedna transakcija došla prije neke druge. Ovo otvara moguću polemiku o prevarama. Tako npr. Alisa bi mogla izvršiti transakciju u kojoj šalje novac Bobu i da čeka da Bob pošalje proizvod koji je ona platila sa tom transakcijom. Kada Bob pošalje proizvod, Alisa može vrati novac kojim je platila proizvod i zadržati proizvod. Grafički prikaz ovoga problema je prikazan na Sl. 1.



Slika. 1. Redoslijed transakcija Alise i Boba

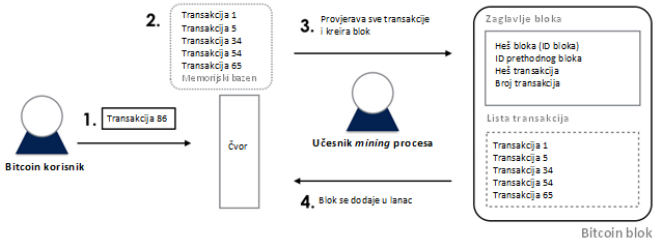
Zbog razlike u propagandnom vremenu, Alisa bi mogla da dobije duplo potrošenu transakciju prije one koja treba doći Bobu. Kada Bobova transakcija stigne ona će se smatrati nevalidnom zato što pokušava da koristi već iskorišteni *input*. Na ovaj način bi Bob ostao i bez novca i bez proizvoda. Takođe, pojavio bi se nesporazum na mreži oko toga da li Bob ili Alisa imaju novca jer nema načina da se dokaže koja je transakcija došla prva. Zbog toga u cijeloj mreži mora postojati način da se usaglasi vrijeme. Sistem kontroliše transakcije tako što ih stavlja u grupe koje se zovu blokovi i povezuje te blokove u lanac bloka. Na Sl. 2. je prikazan jedan takav lanac.



Slika 2. *Block chain.*

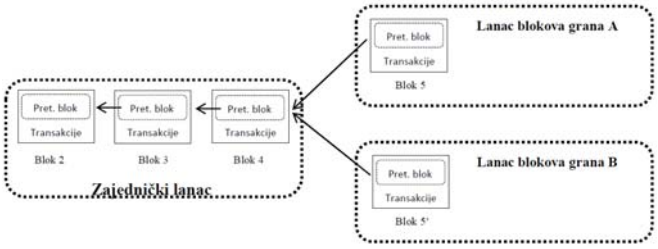
Block-chain služi da rasporedi transakcije dok *transaction-chain* prati kako se posjedovanje mijenja. Svaki blok ima referencu na prijašnji blok. Kada se ide unazad, može se čak doći do prve transakcije koja je napravljena. Sve transakcije u jednom bloku su se desile u isto vrijeme. One transakcije koje

nisu unutar bloka smatraju se nepotvrđene. Bilo koji čvor može sakupiti nepotvrđene transakcije u blok i poslati ga ostatku mreže kao sugestiju sljedećeg bloka u lancu. Na ovaj način bi mnogi mogli kreirati blokove u isto vrijeme. Kao i transakcije, blokovi mogu stići različitim redoslijedom u različite čvorove mreže. Svaki blok mora da sadrži odgovor na matematičke probleme. Računari koriste cijeli tekst bloka i slučajni broj i nad svim tim primjenjuju kriptografski heš sve dok je izlaz manji od određene vrijednosti. Heš funkcija kreira poseban *digest* od bilo koje proizvoljne veličine teksta. Jedan od primjera posebnih heš funkcija koje *Bitcoin* koristi je SHA256. Bitno je da se izlaz ove funkcije mijenja sa svakom dodatnom periodom vremena. Izlaz je potpuno nepredvidiv tako da je jedini način da se pronađe prava vrijednost metoda slučajnih pogodaka. Sl. 3. prikazuje proces izvršavanja transakcija.



Slika 3. Redoslijed izvršavanja transakcija.

Jednom samom računaru je potrebno nekoliko godina da riješi blok. Prva osoba koja riješi matematički problem, uradi *broadcast* svoga bloka i dobije blok prihvaćen kao sljedeći u lancu blokova. Postoji mala vjerovatnoća da će dvoje ljudi riješiti problem u isto vrijeme. Povremeno, više od jednog rješenja se može pojaviti u isto vrijeme što vodi do mogućnosti izgradnje nekoliko mogućih grana kako je i prikazano na Sl 4.



Slika 4. Razdvajanje blokova u više razdvojenih grana.

Vezivanje blokova, nastavljajući na prvu granu koja je prihvaćena. Neki korisnici možda dobiju blokove u različitom redoslijedu ali svaki od njih će dalje graditi lanac na blokove koje prvi dobiju. Ova petlja se razbija kada neko riješi sljedeći blok. Generalno pravilo je da se blok veže za najdužu dostupnu moguću granu. Rezultat koji se dobija je da se lanac blokova brzo stabilizuje, što znači da se svi slažu oko redoslijeda blokova. To posebno važi za nekoliko blokova sa kraja lanca. Često se dešava da se blok koji pripada manjoj grani gubi i vraća ponovo u neformirane blokove. Formacija *Block Chain* može podrazumijevati promjenu redoslijeda na kraju lanca. Sve ovo može izazvati *Double Spend Attack*. *Bitcoin miners* verifikuju transakcije, stavljajući ih u blok transakcija i eventualno rješavajući ih. Protokol je podešen tako da svakom bloku treba oko 10 minuta da se izvrši *mining*.

Nekada, ali ne i uvijek postoje porezi na transakcije. Neki novčanici dozvoljavaju da korisnik postavi transakcioni porez. Bilo koji dio vrijednosti transakcije koji prijemnik nije uzeo ili vratio kao ostatak smatra se porezom. Ova količina dobija *miner* kao nagradu za proračunavanje i provjere. Trenutno, mnogi *miners* procesuiraju transakcije bez poreza. [4]

V. Bitcoin Mining

Ovaj proces omogućava proizvodnju *Bitcoins* i omogućen je jedino ako pojedinac posjeduje jaku grafičku kartu i veliku moć računara. Međutim, pojavljuju se uređaji koji olakšavaju proces proizvodnje *Bitcoins*. U procesu *mining*, u posljednje vrijeme se sve više koriste grupe koje se nazivaju g*uilds* u koje se učešće može kupiti. Svako ko tvrdi da može proizvoditi *Bitcoins* pomoću PC ili grafičke kartice je potpuno neobavješten ili pokušava da proda opremu koja je izgubila rok trajanja. Druga relativna opcija je *cloud mining*, gdje da bi se proizveli *Bitcoins*, osoba plaća da koristi centre kompanije da bi vršila *mining*. Iako relativno novi koncept, *Bitcoin ATMs* se stalno povećavaju brojčano. Oni povećavaju energiju koja je neophodna da se ubrza proizvodnja određene količine *Bitcoins* i omogućavaju direktnu razmjenu. Najpopularniji su: *BitAccess, CoinOutlet, Genesis Coin, Lamassu i Robocoin*. Posao *miners* je da potvrdi ove transakcije i da ih zapiše u glavnu kolekciju podataka koja pretstavlja dugu listu blokova, koja se i drugačije naziva *block-chain*. [4]

Konstantna ažuriranja se šalju svim korisnicima koji učestvuju u lancu, tako da svi znaju šta se dešava. Kada se blok transakcija kreira, *miners* ga procesiraju. Nakon toga se uzimaju informacije iz bloka i nad njima se primjenjuje matematička formula i vrši se njegova transformacija. Ono što je nastalo konverzijom je mnogo kraće i sastoji se od sekvence slova i brojeva i poznato je kao heš. Ovaj heš se pamti zajedno sa blokom i postavlja se na kraj *block-chain*. Lako je formirati heš od podataka koji se nalaze u bloku koji pripada *block-chain*, ali je zato otežan reverzibilan proces koji određuje koji je podatak prethodio heširanom podatku. Svaki heš je jedinstven, ako se promijeni samo jedan karakter u bloku, njegov heš se mijenja kompletno. *Miners* ne koriste samo transakcije u bloku da generišu heš. Oni koriste heš posljednjeg bloka koji se pamti u *block-chain*. Pokušajem lažiranja transakcije mijenjanjem bloka koji je već postavljen u *block- chain*, izazvala bi se deformacija njegovog heša. Kada bi se izvršila heš funkcija radi provjere autentifikacije, uočilo bi se da je blok različit od onoga što se nalazi u lancu blokova i utvrdilo bi se da je blok lažan. Da bi se lažirao blok, potrebno je lažirati i heš toga bloka ali i sekvence blokova iza njega. [4]

Svi računari se takmiče jedni sa drugima koristeći specifični softver da bi se izvršio *mining*. Problem predstavlja lakoća proizvednje heševa od kolekcije podataka. *Bitcoin* protokol otežava ovaj proces uvodeći *proof of work.* On zahtijeva da blok heš izgleda na određen način, mora da ima određen broj nula na početku. Ne postoji način da se sazna kako će heš izgledati prije nego što se proizvede. *Miners* provjeravaju dio podataka koji se naziva *nonce* i taj dio podataka se mora mijenjati da bi se kreirao različit heš sve dok se ne dobije heš koji zadovoljava prethodno spomenuta pravila. *Bitcoin* nije jedina valuta koja se može koristiti u ovom procesu. Jedna vrsta *mining* procesa koja se vrši naziva se *merged mining*. Kod ove metode, blokovi koji su riješeni mogu se također koristiti i za druge valute koje koriste *proof of work* algoritam (na primjer: *namecoin* i *devcoin*). Oni koji po prvi put vrše proces *mining*, a koji imaju nisku hardversku moć bi trebali da razmisle o radu sa *altcoins* prije nego što počnu sa *Bitcoins*. Ovo je preporučljivo zato što je poteškoća rješavanja *Bitcoins* mnogo veća kod procesora koji odgovarju regularnom PC. Kada postoji nesigurnost o tome nad kojom valutom se treba da izvrši proces *mining*, može se koristiti bazen koji se zove *Multipool* koji će automatski da uključi *mining* na najprofitabilniji *altcoin.* [4]

Šta su *Bitcoin Mining Pools?*Jedno od čestih i prvih nedoumica sa kojim se ljudi suočavaju je da li da proces *mining* vrše samostalno ili da se pridruže bazenu (*pool*). Postoji više razloga za i protiv *mining pools.* Kada korisnik vrši sam proces *mining,* ne mora da dijeli nagradu nakon uspješno završenog posla ali i mogućnosti za dobivanje nagrade su znatno smanjene. Iako *pool* ima daleko veće šanse da riješi blok i dobije nagradu, ta nagrada će biti podijeljena između svih članova bazena.

VI. Zaključak

Bitcoin je matematički zaštićena digitalna valuta koja se održava u mreži čvorova. Digitalni potpisi autorizuju individualne transakcije. Posjedovanje *Bitcoins* se mijenja preko transakcionih lanaca, a redoslijed ovih transakcija je zaštićen i održava se u blokovskom lancu. Zbog teških matematičkih problema koje je neophodno riješiti sa svakim blokom, lopovi se izlažu proračunatoj utrci u kojoj je mogućnost da pobijede jako mala.

U posljednje vrijeme, velika prednost *Bitcoin* sistema je što omogućava pokretanje sopstvenog biznisa. Moguće je podesiti *Bitcoin* adresa da bi se dobijao i slao novac i razne usluge bez podmirivanje bankarskih propisa zemalja. *Bitcoins* su danas prihvaćeni širom svijeta, u radovima, donacijama, organizacijama, picerijama, šopovima, serverima, aukcijama, domenima registracije, grafičkom dizajnu kao i u maloprodajnim tržištima. Trenutno *mining* proces uključuje transakcije bez poreza. Međutim u budućnosti, transakcije će se procesuirati sa porezima, neće biti slobodno slanje *Bitcoins*, ali će porezi biti jeftinije nego porezi koje korisnik ima na kreditne kartice.

Zahvalnica

Pri izradi ovoga studentskog rada poslužila sam se radom iz predmeta Elektronsko poslovanje. Zahvalnicu isključivo dugujem mentoru prof. dr Slobodanu Obradoviću koji me je nadgledao i davao savjete u procesu izrade rada.

Literatura

[1] Scott Driscoll. ImponderableThings. [Online]. Available: http://www.imponderablethings.com/, 06.09.2014.

[2] Bitcoin. © Bitcoin Project 2009-2014 Released under the MIT license. [Online]. Available: https://bitcoin.org , 06.09.2014

[3] Danny Bradbury. What's Next for Bitcoin Wallet Security? [Online]. Available: http://www.coindesk.com/whats-next-bitcoin-walletsecurity/,

[4] Martin Tillier. The Economics Of Mining. [Online].Available:http://www.nasdaq.com/article/bitcoin-basics-the-economics-of-mining- cm406845, 28.10.2014.

ABSTRACT

This paper describes the *Bitcoin* system. It is an electronic system, based on a mathematical proof, which begins increasingly to be used to enable payment. *Bitcoin* is the first example of currencies for which the term crypto-currency. *Bitcoins* are created (mined) electronically using a computing power in a distributed network. The paper gives an insight into how to buy, sell and keep *Bitcoins.* Basic features of this system are: decentralization, simplicity, anonymity, transparency, speed and minimum taxes on the transaction. However, this system has some disadvantages, such as susceptibility to illegal activities, mining consumes too much energy and difficulties in trade with other currencies.

Bitcoin

Dajana Cerovina