Bitcoin

Kaselj, Marina

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku

Sveučilišni diplomski studij matematike
smjer: Financijska matematika i statistika

Marina Kaselj

Bitcoin

Diplomski rad

Osijek, 2015.

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
smjer: Financijska matematika i statistika

Marina Kaselj

Bitcoin

Diplomski rad

Mentor: izv.prof.dr.sc. Ivan Matić

Sažetak:
Bitcoin je sustav elektroničkog plaćanja kojeg je izumio Satoshi Nakamoto. Objavljen je 2008. godine, a 2009. je postavljen kao open-source program. Sustav je peer-to-peer što znači da korisnici mogu trgovati izravno, bez posrednika (treće strane). Transakcije provjeravaju čvorovi (korisnici) u mreži te se one nakon provjere pohranjuju u javno distribuiranu knjigu koja se naziva blokovni lanac. Sustav koristi vlastitu jedinicu koji se naziva bitcoin. Bitcoin ne kontroliraju ni centralne banke, ni državne institucije ni korporacije. Bitcoin kao decentralizirana valuta podrazumijeva da ne postoji središnja organizacija poput banke ili države koja koordinira cijelim sustavom. Valja naglasiti da je Bitcoin prva digitalna valuta izgrađena na decentraliziran način. Bitcoin se često naziva i prvom kriptovalutom, iako su postojale neke kriptovalute prije njega. Može se reći da je Bitcoin prva decentralizirana digitalna valuta, u smislu ukupne tržišne vrijednosti je najveća.

Ključne riječi: kriptovaluta, Bitcoin, adresa, blokovni lanac, transakcija

Abstract:
Bitcoin is a digital store of value and payment system invented by Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009. The system is peer-to-peer which mean users can transact directly without needing an intermediary. Transactions are verified by network nodes and recorded in a public distributed ledger called the block chain. The ledger uses its own unit of account, also called bitcoin. The system works without a central repository or single administrator, which has led to categorize it as a decentralized virtual currency. Bitcoin is often called the first cryptocurrency, although prior systems existed. Bitcoin is more correctly described as the first decentralized digital currency. It is the largest of its kind in terms of total market value.

Keywords: cryptocurrency, Bitcoin, address, blockchain, transaction

Sadržaj

1 Uvod

Posljednjih desetljeća nagli razvoj informatičke tehnolgije i interneta omogućio je početak elektroničkog trgovanja robama i uslugama. U počecima trgovina na internetu se oslanjala gotovo isključivo na financijske institucije koje su bile pouzdani posrednici za obradu elektroničkih plaćanja. Iako sustav elektroničkog plaćanja u kojem ulogu posrednika imaju financijske institucije radi dobro u većini transakcija, postoje još uvijek određene slabosti u pogledu povjerenja.
Potpuno nepovratne transakcije nisu moguće jer financijske institucije ne mogu izbjegavati posredovanja u sporovima između dviju strana. Trošak posredovanja povećava troškove transakcija te ograničava minimalnu veličinu transakcije i mogućnost za manje povremene transakcije.
Isto tako, tu su i veći troškovi uzrokovani gubitkom sposobnosti da se naprave nepovratna plaćanja za nepovratne usluge. Kako se povećava mogućnost povrata, povećava se potreba za povjerenjem.
Trgovci trebaju biti oprezni i od svojih kupaca zahtjevati više informacija nego što je inače potrebno kako bi se umanjila mogućnost prevare. Ipak, određeni postotak prevara je neizbježan. Troškovi i plaćanje zbog neizvjesnosti mogli su se izbjeći korištenjem fizičke valute, ali tada nije postojao mehanizam za plaćanje preko komunikacijskog kanala bez posrednika. Ono što je bilo potrebno je elektronički sustav plaćanja na temelju kriptografskih mehanizma umjesto povjerenja koji dopušta da bilo koje dvije strane trguju izravno jedna s drugom, bez potrebe za posrednikom (tzv. trećom stranom).
Takav skup koncepata i tehnologija koje čine osnovu sustava digitalnog novca stvoren 2009. godine nazvan je Bitcoin i za kratko je vrijeme pobudio zanimanje medija i javnosti.
To će biti tema daljnjeg proučavanja ovog rada. U prvom dijelu rada upoznat ćemo pojam elektroničkog novca, a nakon toga i pojam kriptovalute. Drugo poglavlje donosi kratak općeniti dio o Bitcoinu i najvažnijim činjenicama iz njegove povijesti. S obzirom da se projekt Bitcoina temelji na kriptografskim znanjima, napravit ćemo kratki pregled osnova kriptografije . Treće poglavlje govori o načinu uporabe Bitcoina, dok se u sljedećem upoznajemo s novčanicima i adresama koje rabimo u Bitcoin sustavu. U posljednjem poglavlju objašnjavamo način na koji se odvijaju Bitcoin transakcije.

1.1 Elektronički novac

Spomenuli smo da je nagli razvoj interneta pokrenuo elektroničko trgovanje. Također, doveo je i do razvoja nekih novih oblika imovine, od kojih je svakako najviše pozornosti privukao elektronički novac. Taj pojam se odnosi na sustave plaćanja u realnome i virtualnom svijetu čiji je cilj unaprijediti efikasnost postojećih sustava plaćanja i zamijeniti novčanice i kovanice u maloprodajnim transakcijama.
Elektronički novac jedan je od načina plaćanja na internetu, on je zamjena za gotovinu

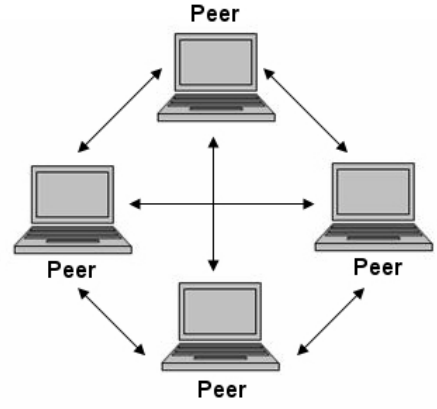
te samo plaćanje elektroničkim novcem podsjeća na obično plaćanje gotovinom.
Postoje brojne definicije elektroničkog novca jer ga je teško jedinstveno definirati zbog različitih tehnoloških i ekonomskih obilježja. Europska centralna banka (ECB) ga je definirala kao elektroničko spremište monetarne vrijednosti na tehničkom uređaju koji se može široko koristiti za plaćanja obveza bez uključivanja bankovnih računa u transakciju, već da služi kao instrument za plaćanje unaprijed.

U Zakonu o elektroničkom novcu (NN, br. 139/2010.) dana je sljedeća definicija: Elektronički novac jest elektronički, uključujući i magnetski, pohranjena novčana vrijednost koja je izdana nakon primitka novčanih sredstava u svrhu izvršavanja platnih transakcija u smislu zakona kojim se uređuje platni promet i koju prihvaća fizička ili pravna osoba koja nije izdavatelj tog elektroničkog novca, a koja čini novčano potraživanje prema izdavatelju.

Sve značajnija uporaba elektroničkog novaca dovela je do razvoja različitih oblika elektroničkog plaćanja kao i do razvoja više vrsta sustava za elektroničko plaćanje. Sustavi za elektroničko plaćanje su sljedeći:

1. notacijski sustav
2. simbolički sustav
3. centralizirani sustav
4. peer to peer sustav

Kako je ranije navedeno, cilj ovoga rada je detaljnije obraditi pojam Bitcoina i njegove karakteristike, stoga nećemo pobliže objašnjavati prva tri sustava, već samo peer to peer sustav koji je usko vezan uz Bitcoin.



Slika 1: Peer to peer sustav

Peer to peer sustavi (skraćeno P2P) sastoje se od međusobno povezanih čvorova koji se mogu samostalno organizirati u mrežu sa svrhom dijeljenja raspoloživih resursa kao

što su korisnički podaci, procesorsko vrijeme, kapacitet za pohranu podataka ili mrežna propusnost, te koji se mogu samostalno adaptirati na ispade funkcionalnosti i nepredvidive dolaske i odlaske čvorova na mreži, uz zadržavanje prihvatljive razine spojenosti i performansi bez potrebe za nadzorom, kontrolom i podrškom iz jednog središnjeg mjesta.

Na Slici 1. može se vidjeti prikaz jednostavnog peer to peer sustava. Uočljivo je da je komunikacija između čvorova izravna (nema poslužitelja). Također, možemo vidjeti i da je svaki čvor ravnopravan i neovisan.
Jedan od najznačajnih primjera korištenja peer to peer sustava su digitalne valute, odnosno njihova podvrsta kriptovalute o kojoj ćemo nešto više reći u sljedećem potpoglavlju.

1.2 Kriptovaluta

Pojam kriptografske valute ili kriptovalute (eng. cryptocurrency) označava da se za njeno stvaranje i bilježenje njenih transakcija koriste kriptografski mehanizmi javnih i privatnih ključeva koji omogućuju različitim korisnicima koje nemaju povjerenja jedni u druge da vjeruju cijelom sustavu. Transakcijska platforma omogućuje provođenje i bilježenje novčanih transakcija kriptovaluta između pojedinih korisnika. Takve transakcije obavljaju se bez posrednika. Naime, kriptografske valute se razmjenjuju izravno između dva korisnika (P2P). U tom slučaju transakcija ne mora putovati preko centralnog servera koji se nalazi pod kontrolom neke banke, kartične kuće ili druge financijske institucije. Ipak, u takvoj mreži postoje razni serveri koji su smješteni na putu između korisnika i trgovca, ali je u osnovi riječ o transakciji između dva korisnika. Dakle, nema visokih naknada koje uzimaju financijske institucije te nema straha da će transakcija pasti zbog isteka kartice ili nekog drugog nepredviđenog razloga. Spomenute transakcije u mreži odvijaju se pseudonimno, bez otkrivanja pravog identiteta korisnika. Da bismo obavili transakciju sve što je potrebno je generirati adresu vezanu uz kriptografsku valutu s odgovarajućim parom javnog i tajnog ključa. Iz sigurnosnih razloga, za svaku se transakciju obično koristi nova adresa. Potrebno je napomenuti kako transakcije nisu posve anonimne budući da se u svakom trenutku svaka transakcija može povezati s odgovarajućom adresom. No, ono što stoji iza tih adresa samo po sebi jest anonimno drugim korisnicima mreže. Tako korisnik s druge strane ne zna tko stoji iza pojedine adrese. Ipak, postoje određene metode kako tajne službe i vladine agencije mogu utvrditi tko je koristio određenu adresu, pa možemo reći da svojstvo pseudonimnosti ipak nije do kraja provedeno.
Digitalne valute postoje već desetljećima i mnogi ih uspješno koriste. Razni novčići i krediti koje kupuju u računalnim i mobilnim igrama su zapravo digitalne valute. No, za razliku od Bitcoina, do njih se može doći samo ako ih se zamijeni za realan novac. One se ne mogu koristiti izvan određene igre te obično nemaju mogućnost konvertibilnosti natrag u dolare, eure ili kune. Što se tiče brojnosti kriptovaluta, u svijetu trenutno postoji 468 kriptovaluta, a od njih svakako je najpoznatija i najrasprostanjenija kriptovaluta Bitcoin, čiju detaljnu analizu donose sljedeća poglavlja.

1.3 Općenito o Bitcoinu

Bitcoin se prvi put spominje 2008. godine u članku "Bitcoin: A Peer-to-Peer Electronic Cash System" izdanom od strane Satoshija Nakamota. O Satoshiju Nakamotu se ne zna ništa osim njegova imena. Postoje mnoge teorije tko je on, a one najpopularnije kažu da je to bio tim stručnjaka koji je izradio ovu valutu, dok druga kaže da je to bila osoba koja se povukla kako bi zaštitila svoju privatnost te je prije povlačenje prepustila vodeću ulogu Gavinu Andersonu koji je sada voditelj projekta Bitcoin.
Početkom 2009. godine, ista organizacija (osoba) pokrenula je projekt pod nazivom Bitcoin-Qt kojim su stvorili svoju vlastitu valutu bitcoin[1] i pustili prve bitcoine u promet. Prvih godina postojanja bitcoin nije imao skoro nikakvu vrijednost, a aktivnosti su bile jako slabe i uglavnom su se svodile na razmjenu bitcoina između ljudi koje je zanimala kriptografija. Sredinom 2011. godine došlo je do značajne popularizacije Bitcoina, pa se posljedično dogodio i prvi veliki skok vrijednosti bitcoina. Broj korisnika kao i broj transakcija počeo je naglo rasti, otvarale su se prve online mjenjačnice kriptovaluta, te su i pojedini trgovački centri počeli prihvaćati bitcoine kao validno sredstvo plaćanja.
Bitcoin je skup koncepata i tehnologije koji čine osnovu elektroničkog sustava plaćanja, uključuje jedinično određenu valutu nazvanu bitcoin, koja se koristi za prijenos i pohranu vrijednosti među sudionicima u Bitcoin mreži. Bitcoin korisnici komuniciraju jedni s drugim pomoću Bitcoin protokola, primarno preko interneta. Bitcoin tehnologija uključuje značajke bazirane na enkripciji i digitalnom potpisu, namijenjene održavanju sigurnosti Bitcoin mreže. Više o tome reći ćemo u sljedećem poglavlju.
Ideja Bitcoina leži u nezavisnosti i decentraliziranosti. Naime, Bitcoin ne kontroliraju ni centralne banke, ni državne institucije ni korporacije. Riječ je o valuti čija vrijednost nije vezana uz neku drugu vrijednost kao ni uz fizičke materijale kao što su zlato ili srebro. Vrijednost bitcoina određuju jedino ponuda i potražnja, odnosno spremnost drugih da ga prihvate kao sredstvo plaćanja. Bitcoin kao decentralizirana valuta podrazumijeva da ne postoji središnja organizacija poput banke ili države koja koordinira cijelim sustavom. Valja naglasiti da je Bitcoin prva digitalna valuta izgrađena na decentraliziran način. Bitcoin sustav je u suštini računalni program koji kontrolira sam sebe pomoću složenih algoritamskih mehanizama.
Stog Bitcoin protokola dostupan je kao softver otvorenog koda te se može izvoditi na velikom broju različitih računalnih uređaja, uključujući prijenosna računala, pametne telefone i druge. To čini cijelu platformu izrazito dostupnom.
Otvoreni kod (eng. open source) znači da je izvorni kod sustava potpuno besplatno dostupan svima za korištenje, prepravljanje te redistribuciju. Cilj softvera otvorenog koda je učiniti izradu softvera sličnu akademskoj istraživačkoj mreži, na način da će zajednica svojim radom moći utjecati na kvalitetu i napredak softvera.

[1] Kada govorimo o valuti pišemo malo slovo b na početku riječi.

Zagovornici Bitcoina tvrde da je riječ o "pravednom novcu" koji će u dogledno vrijeme ukinuti monopol banaka te omogućiti brzo i jednostavno pseudonimno plaćanje svih proizvoda ili usluga.
Također, zagovornici kriptografskih valuta traže načine kako bi iskoristili novonastalu "zlatnu groznicu" i ostvarili zaradu. S druge strane, pojavljuje se i mnoštvo onih koji se bave prijevarama u sustavu, od krađe tuđih računala za izradu Bitcoina pa do najobičnije krađe virtualnih novčanika.

2 Kriptografski mehanizmi vezani za Bitcoin

Kao što smo naveli u uvodnom dijelu, dat ćemo kratak uvod i definicije najvažnijih pojmova vezanih uz kriptografiju.
Znanstvena disciplina koja se bavi analiziranjem i pronalaženjem metoda pomoću kojih je poruku moguće poslati u obliku u kojem ju neće moći pročitati nitko osim onih kojima je namijenjena naziva se kriptografija.

Osnovni zadatak kriptografije je omogućiti dvjema osobama komuniciranje preko nesigurnog komunikacijskog kanala na način da treća osoba, koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke. Poruku koju pošiljatelj želi poslati primatelju zovemo otvoreni tekst. Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni ključ. Taj postupak se naziva šifriranje, a dobiveni rezultat šifrat. Nakon toga pošiljatelj pošalje šifrat preko nekog komunikacijskog kanala. Treća osoba prislukujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primatelj koji zna ključ kojim je šifrirana poruka može dešifrirati šifrat i odrediti otvoreni tekst.

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo prostor ključeva. Kriptosustav se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva. Formalna definicija glasi ovako:

Definicija 1. Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ za koju vrijedi:

1. $\mathcal{P}$ je konačan skup svih mogućih osnovnih elementa otvorenog teksta;
2. $\mathcal{C}$ je konačan skup svih mogućih osnovnih elemenata šifrata;
3. $\mathcal{K}$ je prostor ključeva, konačan skup svih mogućih ključeva;
4. Za svaki $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : P \to C$ i $d_K : C \to P$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki otvoreni tekst $x \in P$.

Postoje 2 vrste kriptosustava, kriptosustavi s tajnim ključem (simetrični) i kriptosustavi s javnim ključem (asimetrični). S obzirom da je važnu ulogu u funkcioniranju Bitcoina imaju kriptosustavi s javnim ključem, reći ćemo nešto više o njima.

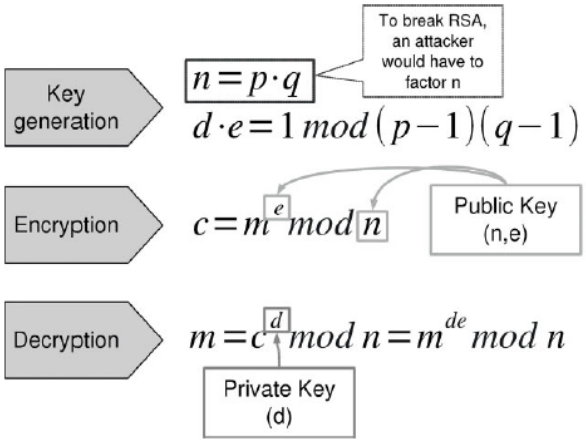
2.1 Kriptografija javnog ključa

Kriptosustav s javnim ključem se sastoji od dva skupa funkcija, funkcija za šifriranje e_K i funkcija za dešifriranje d_K, gdje K prolazi skupom svih mogućih korisnika, koje imaju sljedeća svojstva: za svaki K je d_K inverz od e_K, za svaki K je e_K javan, ali je d_K poznat samo osobi K te za svaki K je e_K osobna jednosmjerna funkcija, funkcija kojoj je teško izračunati inverz bez poznavanja nekog dodatnog podatka. Ključ e_K se zove javni ključ, a d_K se zove tajni ključ.
Diffie i Hellman, matematičari koji se smatraju začetnicima kriptografije javnog ključa predložili su korištenje dva različita, ali matematički povezana ključa. Javni ključ je objavljen i svima dostupan, a služi za šifriranje poruke namijenjene osobi - vlasniku javnog ključa. Dešifriranje poruke obavlja se korištenjem tajnog ključa poznatog samo primatelju poruke. Prije komunikacije nije potrebno obaviti razmjenu ključeva. Tajni ključ se ne može izračunati iz javnog ključa, niti je korištenjem javnog ključa moguće dešifrirati poruku. Asimetričnost je postignuta korištenjem asimetričnih matematičkih algoritama poput na primjer faktorizacije velikih brojeva. Jednostavno i brzo se mogu pomnožiti dva velika prosta broja, ali tako dobiveni broj nije moguće jednostavno ponovno faktorizirati bez poznavanja jednog od faktora. Jedan od faktora bi mogao predstavljati upravo tajni ključ osobe čiji je umnožak javni ključ.
Navedenim konceptom postignute su sljedeće pogodnosti:

- ono to je šifrirano jednim ključem (bilo tajnim ili javnim), može se dešifrirati drugim ključem (javnim ili tajnim)
- asimetrična enkripcija je sigurna
- budući da nije potrebno slati ključ primatelju, asimetrično šifriranje je imuno na presretanje ključa
- broj ključeva koje treba distribuirati je uvijek isti bez obzira na broj sudionika pa tako u asimetričnoj kriptografiji ne postoji problem kompleksnosti distribucije ključeva
- asimetrična kriptografija omogućuje digitalni potpis i neporecivost
- asimetrična enkripcija relativno je spora
- asimetrična enkripcija proširuje šifrirani tekst.

Postoje mnogobrojni algoritmi asimetrične kriptografije koji su vrlo uspješni, a isto tako postoje i oni koji su se prestali koristiti zato što su kriptoanalitičari otkrili njihove propuste. Vjerojatno najpoznatiji i najkorišteniji algoritam kriptografije javnog ključa jest RSA kriposustav koji je dobio ime po prvim slovima prezimena njegovih autora: Rona Rivesta, Adija Shamira i Leonarda Adlemana. RSA se upravo temelji na problemu umnoška velikih prostih brojeva i složenosti faktorizacije rezultata. U nastavku slijedi defincija RSA kriptosustava.

Definicija 2. Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathcal{Z}_n = \{1, 2, ..., n-1\}$, te $\mathcal{K} = \{(n, p, q, d, e) : n = pq, p, q \text{ prosti}, de \equiv 1 \pmod{\varphi(n)}\}$. Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo $e_K(x) \equiv x^e \bmod n$ i $d_K(y) \equiv y^d \bmod n$, $x, y \in Z_n$. Vrijednosti n i e su javne, a vrijednosti p, q i d su tajne.



Slika 2: Shema šifriranja u RSA kriptosustavu

Slika 2. prikazuje postupak šifriranja u RSA kriptosustavu koji ćemo sada opisati.
Izabiremo tajno dva velika prosta broja p i q od oko 100 znamenaka, tako da q ima nekoliko znamenaka više od p. To radimo tako da pomoću nekog generatora slučajnih brojeva generiramo prirodan broj m s traženim brojem znamenaka, a zatim korištenjem nekog testa za testiranje prostosti tražimo prvi prosti broj veći ili jednak m.
Izračunamo $n = p \cdot q$ i $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$.
Izaberemo na slučajan način broj e takav da je $e < \varphi(n)$ i $(\varphi(n), e) = 1$. To se može napraviti slično kao u prvom koraku. Nakon toga tajno izračunamo d tako da je $de = 1 \pmod{\varphi(n)}$, tj. $d = e^{-1} \pmod{\varphi(n)}$ direktno ili pomoću Euklidovog algoritma.
Sljedeće što želimo pojasniti je digitalno potpisivanja poruka, no prije toga moramo definirati pojam *hash-funkcije*.

2.2 Hash-funkcija

Jednostrana hash-funkcija ima veliku praktičnu primjenu u modernoj kriptografiji. U suradnji s ostalim kriptografskim alatima, koristi se za utvrđivanje vjerodostojnosti podataka i njihovog porijekla.Učinkovita funkcija koja preslikava niz proizvoljne duljine u binarni niz fiksne duljine zove se jednostrana hash-funkcija. Binarni niz fiksne duljine se zove hash-vrijednost (engl. hash-value) i uobičajeno je duljine 128 ili 160 bitova.

Važne karakteristike hash-funkcije su sljedeće:

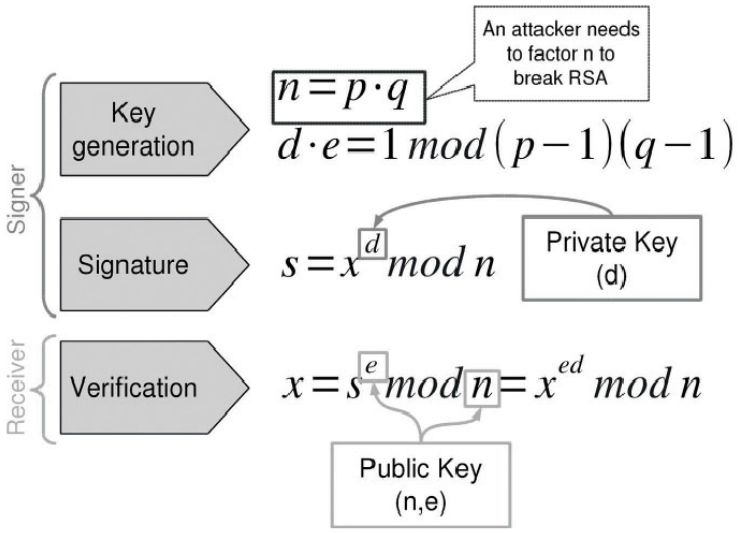
- Sve hash-funkcije su jednosmjerne. Počevši od hash-vrijednosti, vrlo je teško ili gotovo nemoguće doći do originalne poruke.
- Svaki par različitih poruka se treba preslikati u različite hash-vrijednosti, čak i ako se poruke razlikuju za samo jedan bit. U stvarnosti, postoje parovi poruka koje rezultiraju istom hash-vrijednošću, ali vjerojatnost mora biti mala da će taj par biti sastavljen od smislenih podataka (teksta npr.)
- Svaki put kad se ista poruka pusti kroz istu hash funkciju, rezultira točno istom hash-vrijednošću
- Duljina hash-vrijednosti je određena samim hash algoritmom i ne mijenja se s dužinom poruke koja se obrađuje. Najčešće duljine hash-vrijednosti su 128 i 160 bita.

Budući da je algoritam hash-funkcije javan, njena sigurnost leži u jednosmjernosti, jer nije moguće dobiti originalni niz podataka iz same hash-vrijednosti. Najčešće korištenje hash funkcija je u osiguravanju vjerodostojnosti podataka, zaštiti datoteka od promjene, zaštiti elektroničkih financijskih radnji od zlonamjerne manipulacije. U kombinaciji s asimetričnim kriptografskim algoritmima, hash-vrijednost se koristi i za osiguravanje porijekla informacije preko sustava digitalnih potpisa.

2.3 Digitalni potpis

Pojavom asimetrične kriptografije, koncept digitalnog potpisa postao je izvediv. Naime, kao i kod uobičajenog parafa izvedenog rukom, postoji samo jedna osoba koja je sposobna staviti potpis na neki dokument, no mnogo drugih osoba je sposobna pročitati taj potpis.

Digitalni potpis je baziran na konceptu para ključeva. Analogno realnom svijetu, postoji jedan ključ koji je poznat osobi koja potpisuje dokument u vidu tajnog ključa. Pa tako kada osoba potpiše dokument svojim tajnim ključem, jamstvo je da su ti potpisani podaci izričito i jedinstveno povezani s tom osobom. Kako bi se mogao taj potpis identificirati ili verificirati, osoba distribuira svoj javni ključ. Podaci koji se mogu potpisati mogu biti bilo koji digitalni sadržaj te ne ovise o podatkovnoj veličini, jer se za ulaz u funkciju digitalnog potpisivanja uzima fiksna veličina i operacija kriptografske hash-funkcije. Samo potpisivanje se svodi na to da potpisnik pomoću hash-funkcije dobiva iz dokumenta podatak fiksne duljine, a potom primjenjuje enkripciju na dobiveni podatak, koristeći tajni ključ. Ako se želi provjeriti taj potpis, pomoću hash-funkcije se iz dokumenta dobiva podatak fiksne duljine i zatim se ta vrijednost razmatra zajedno s dobivenim potpisom na koji se primjenjuje javni ključ potpisnika. Ako se te dvije vrijednosti poklapaju, potpis je ispravan.



Slika 3: Shema digitalnog potpisa u RSA kriptosustavu

Slika 3. prikazuje proces potpisivanja u RSA kriptosustavu. Možemo vidjeti da se sastoji od 3 dijela: generiranja ključa, potpisivanje i verifikacija. Generiranje ključa se odvija na isti način kao i kod šifriranja u RSA. Potpisivanje se izvodi tako da se poruka zapiše u obliku $s = x^d \mod n$, gdje je x orginalni tekst, a d privatni ključ. Verifikacija je završena kada s^e usporedimo s orginalnom porukom x. Ako je $x = s^e = x^{e \cdot d} = x \mod n$, potpis je točan. RSA koristi se u praksi s ključevima od 1024 ili 2048 bita. Slika 4. prikazuje primjer od 2048-bitni RSA ključ. Suvremeni računalni procesori imaju 32-bitni ili 64-bitni

Slika 4: 2048-bitni RSA ključ, svi brojevi su zapisani u heksadecimalnom sustavu

registare, te operacije nad 2048-bitnim brojevima kao u ovom primjeru treba razdvojiti i izvoditi tijekom više ciklusa. Izvođenje operacija u kojima sudjeluje kriptografija s javnim ključem je relativno sporo.

2.4 Eliptičke krivulje

U ovom potpoglavlju definirat ćemo eliptičke krivulje, navesti primjere nekih eliptičkih krivulja, i dati kratak pregled svojstava te njihovu vezu s kriptografijom.

Neka je K polje. Karakteristika polja K je najmanji prirodni broj n takav da je $1 + 1 + ... + 1 = n \cdot 1 = 0$, gdje su 0 i 1 neutralni elementi za zbrajanje, odnosno množenje u K. Ako je $n \cdot 1 \neq 0$ za svaki prirodan broj n, onda se kaže da je K polje karakteristike 0. Pojam eliptičke krivulje se može definirati nad proizvoljnim poljem K, međutim najvažniji slučajevi su kad je K polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$, polje kompleksnih brojeva $\mathbb{C}$, te konačno polje F_q s q elemenata.
Polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ su karakteristike 0, dok je karakteristika od F_q jednaka p, gdje je p prost broj i $q = p^m$ za neki prirodan broj m.

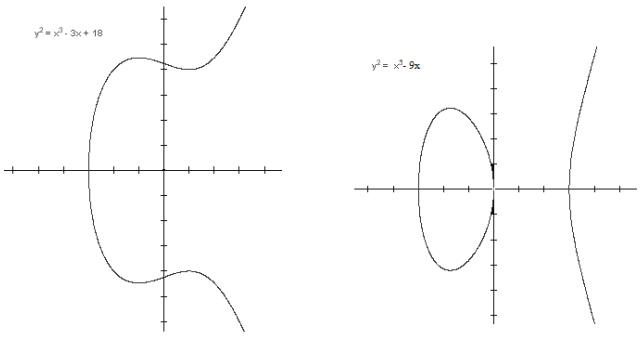
Definicija 3. Neka je K polje karakteristike različite od 2 i 3, te neka je $f(x) = x^3 + ax + b$ (gdje su a, $b \in K$) kubni polinom bez višestrukih korijena. Eliptička krivulja E nad K je skup svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu $y^2 = x^3 + ax + b$, zajedno s još jednim elementom kojeg označavamo s O i zovemo "točka u beskonačnosti".

Slično se može definirati eliptička krivulja i nad poljima karakteristike 2 ili 3. Ako je $K = 3$, onda je pripadna jednadžba $y^2 = x^3 + ax^2 + bx + c$, a ako je $K = 2$, onda imamo dva tipa jednadžbi: $y^2 + cy = x^3 + ax + b$ ili $y^2 + xy = x^3 + ax^2 + b$. Opći oblik jednadžbe je:

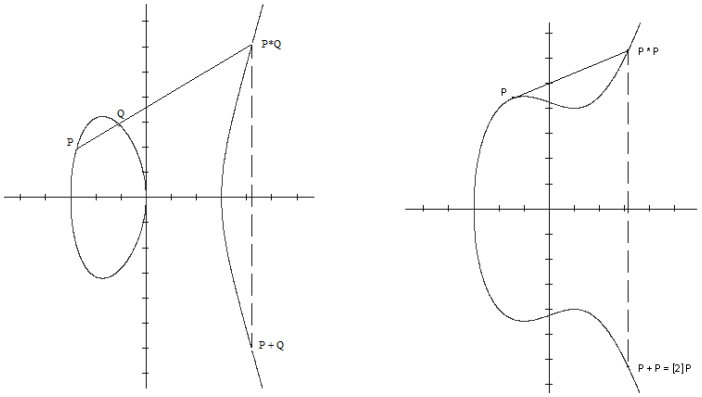
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Ovu jednadžbu zovemo Weierstrassova forma od E i ona se supstitucijom varijabli može transformirati do jedne od gore navedenih jednadžbi, koju onda zovemo kratka Weierstrassova forma od E.

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe. Uzmemo da je $K = \mathbb{R}$ polje realnih brojeva. Tada eliptičku krivulju (bez točke u beskonačnosti) možemo prikazati kao podskup ravnine. Polinom $f(x)$ može imati 1 ili 3 realna korijena. U ovisnosti o tome, graf pripadne eliptičke krivulje ima jednu ili dvije komponente povezanosti, kao što je prikazano na sljedećim slikama.(Slika 5.)
Definirat ćemo operaciju zbrajanja na E. Neka su P, $Q \in E$. Povucimo pravac kroz točke P i Q. On siječe krivulju E u tri točke. Treću točku označiti ćemo s $P * Q$. Sada definiramo $P + Q$ kao osnosimetričnu točku točki $P * Q$ s obzirom na os x (Slika 6). Ako je $P = Q$, onda umjesto sekante povlačimo tangentu kroz točku P. Po definiciji stavljamo da je $P + O = O + P = P$ za svaki $P \in E$.



Slika 5: Grafovi eliptičkih krivulja koje imaju jednu i dvije komponente



Slika 6: Definiranje operacije zbrajanja na eliptičkoj krivulji E

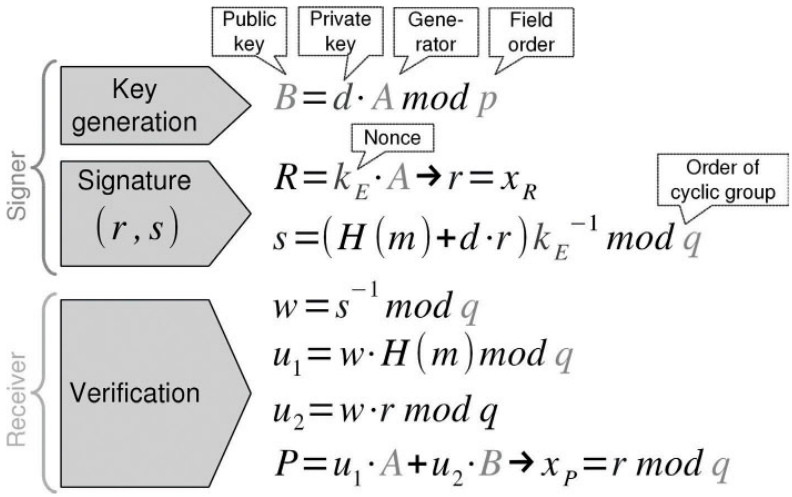
Pokazuje se da skup E uz ovako definiranu operaciju zbrajanja postaje Abelova grupa. Očito je O neutralni element, dok je $-P$ osnosimetrična točka točki P u odnosu na os x. Komutativnost je također očita. Najteže je provjeriti asocijativnost. To se može napraviti korištenjem eksplicitnih formula za zbrajanje, koje ćemo sada navesti. Za $P+P$ koristimo oznaku $[2]P$.
Ako je $P = (x_1, y_1)$ i $Q = (x_2, y_2)$, onda je

$$\begin{aligned} x(P+Q) &= ((y_2 - y_1)/(x_2 - x_1))^2 - x_1 - x_2, \\ y(P+Q) &= -y_1 + (x_1 - x(P+Q))(y_2 - y_1)/(x_2 - x_1), \\ x([2]P) &= ((3x_1^2 + a)/(2y_1))^2 - 2x_1, \\ y([2]P) &= -y_1 + (x_1 - x([2]P))(3x_1^2 + a)/(2y_1). \end{aligned}$$

Jasno je da gore navedene algebarske formule za zbrajanje točaka, koje smo dobili za slučaj eliptičke krivulje nad $\mathbb{R}$, imaju smisla nad svakim poljem (uz malu modifikaciju za slučaj polja s karakteristikom 2 i 3). Pokazuje se da uz operaciju definiranu ovim formu-

lama eliptička krivulja nad proizvoljnim poljem K postaje Abelova grupa.

Nakon kratkog općenitog dijela o eliptičkim krivuljama, slijedi dio o njihovoj primjeni u kriptografiji, odnosno u kriptosustavima koji ih koriste. Jedno od pitanja koje se može postaviti prilikom komunikacije pomoću kriptosustava s javnim ključem jest pitanje vjerodostojnosti ili autentičnosti poruke.
Kako bismo osigurali vjerodostojnost poruke koju šaljemo u digitalnom obliku, koristimo analogon potpisu dokumenta - digitalni potpis poruke. Ideja se sastoji u tome da se pomoću originalne poruke i tajnog ključa osobe A generira digitalni potpis za osobu A. Imajući na raspolaganju poruku, digitalni potpis i javni ključ osobe A, osoba B može verificirati da je potpis autentičan. Korištenje originalne poruke u generiranju digitalnog potpisa često rezultira vrlo dugačkim potpisom. Stoga se umjesto originalne poruke često koristi "sažetak poruke" koji se dobije primjenom neke hash funkcije. Među najpoznatije hash funkcije spadaju MD5 (izlaz od 128 bitova), RIPEMD-160 (izlaz od 160 bitova) i SHA-1 (izlaz od 160 bitova).
Neki kriptosustavi s javnim ključem (RSA) mogu se direktno iskoristiti za potpisivanje poruke. Ipak, najpoznatije metode za generiranje digitalnih potpisa su Digital Signature Algorithm (DSA/DSS) i Elliptic Curve Digital Signature Algorithm (ECDSA). DSA je zasnovan na problemu diskretnog logaritma u multiplikativnoj grupi konačnog polja, dok ECDSA predstavlja njegov analogon i koristi eliptičke krivulje.
Slika 7. prikazuje etape algoritma ECDSA.



Slika 7: Koraci algoritma ECDSA

Koraci ECDSA su sljedeći:

1. ECDSA generiranje ključeva.
E je eliptička krivulja nad F_p, gdje je p prost broj, a P je točka prostog reda q na $E(F_p)$.
Svaki korisnik napravi sljedeće:
a) Izabere slučajan broj d iz skupa $\{1, ..., q-1\}$
b) Izračuna $R = [d]P$;
c) R je javni, a d tajni ključ.

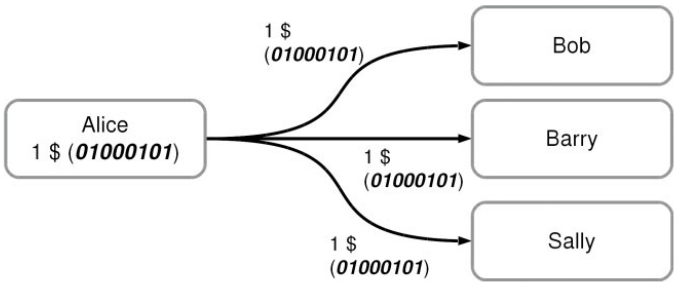
2. ECDSA generiranje potpisa.
Kad želi potpisati poruku m, korisnik radi sljedeće:
a) Izabere slučajan broj k iz skupa $\{1, ..., q-1\}$;
b) Izračuna $[k]P = (x_1, y_1)$ i $r = x_1 \mod n$. Ako je $r = 0$, onda se vrati na korak a);
c) Izračuna $k^{-1} \mod q$;
d) Izračuna $s = k^{-1}(H(m) + dr)$ mod n, gdje je H hash funkcija. Ako je $s = 0$, onda se vrati na korak a);
e) Potpis poruke m je uređeni par prirodnih brojeva (r, s).

3. ECDSA provjera potpisa.
Da bi verificirao potpis (r, s) poruke m drugog korisnika, prvi korisnik treba napraviti sljedeće:
a) Dobiti Alicein javni ključ Q;
b) Provjeriti da su r i s cijeli brojevi iz skupa $\{1, ..., q-1\}$;
c) Izračunati $w = s^{-1} \mod q$ i $H(m)$;
d) Izračunati $u_1 = H(m)w \mod q$ i $u_2 = rw \mod q$;
e) Izraunati $[u_1]P + [u_2]Q = (x_0, y_0)$ i $v = x_0 \mod q$;
f) Prihvatiti potpis kao vjerodostojan ako i samo ako je $v = r$.

Uvjet $r \neq 0$ osigurava da se u potpisivanju stvarno koristi tajni ključ d, dok se uvjet $s \neq 0$ pojavljuje zbog koraka 3.c).

3 Princip rada bitcoina

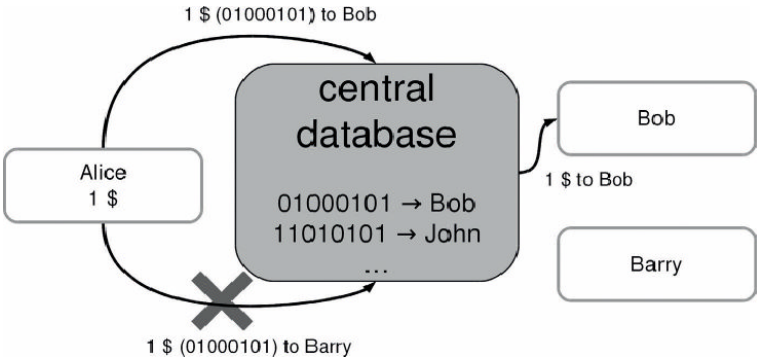
Najjednostavniji način za stvaranje digitalne valute je dodijeljivanje vrijednosti (niza nula i jedinica) određenom uzorku podataka. Problem tog pristupa je taj što je digitalne informacije lako replicirati praktički bez troška. To dovodi do problema "dvostrukog trošenja" koje je prikazano na Slici 8. Recimo da Alice ima digitalni novčić koji je predstavljen bi-



Slika 8: Problem "dvostrukog trošenja"

narnim niz 01000101. Ona može prenijeti tu vrijednost Bobu tako da mu pošalje poruku s tim brojem, pa Bob ima kopiju broja koja predstavlja vrijednost novčića. Problem je očigledno to što ništa ne spriječava Alice da pošalje taj isti novčić drugom korisniku ili više njih.
Stoga, digitalna valuta ne može biti predstavljena samo kao broj zato što se digitalni podaci mogu vrlo jednostavno replicirati mnogo puta, pa znanje tog broja nema nikakvu vrijednost. Dakle, izazov je kako stvoriti sustav korištenjem digitalnih tehnologija koje omogućuju savršeno kopiranje podataka (bez mogućnosti dvostrukog trošenja).

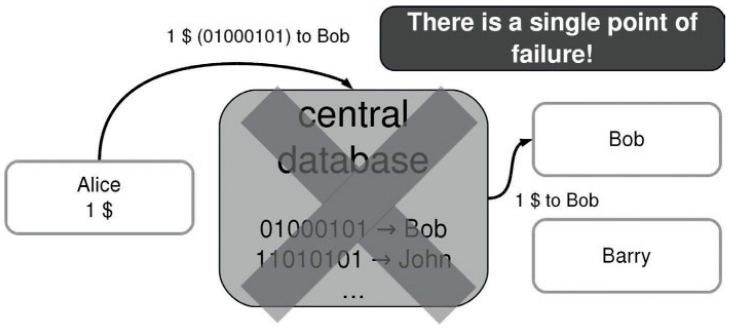
Sljedeći korak naprijed u izgradnji sustava elektroničkog plaćanja je stvaranje centralne baze koja sadrži listu korisnika i sredstava koje oni posjeduju. Sustav je prikazan na Slici 9. Ako Alice želi prenijeti jednu jedinicu valute koja je predstavljena brojem



Slika 9: Sustav elektroničkog plaćanja s centralnom bazom

01000101 Bobu, ona će kontaktirati server koji pokreće centralnu bazu i direktno prebacuje tu jedinicu Bobu. Server ažurira bazu i novčić sada pripada Bobu. Ako Alice pokuša dva puta potrošiti isti novčić, ovaj put šaljući ga Barryju, ona će se opet povezati na server i narediti slanje novčića Barryju. Međutim, za vrijeme provjeravanja baze, server je uočio da taj novčić 01000101 više ne pripada Alice i da ga ona nije ovlaštena potrošiti.

Centralna baza rješava problem "dvostrukog trošenja". Međutim, postoje problemi vezani uz centralnu bazu, a prvi je taj da se svi korisnici moraju prethodno registrirati na centralnom serveru ako žele trgovati. Također, centralna baza zna identitete svih korisnika i skuplja njihovu financijsku povijest, pa je zbog toga laka meta napada (vanjski i unutarnji). Ako napadač preuzme kontrolu nad centralnom bazom, može promjeniti vlasništvo nad svakom imovinom, kradući imovinu od njenih legitimnih vlasnika ili može stvoriti novu imovinu (novce) i pripisati ih sebi.
Možda glavni nedostatak centralnih servera je taj što on ima jednu slabu točku (prikaz na Slici 10.) - sustav plaćanja se može jednostavno srušiti ako se sruši centralni poslužitelj.



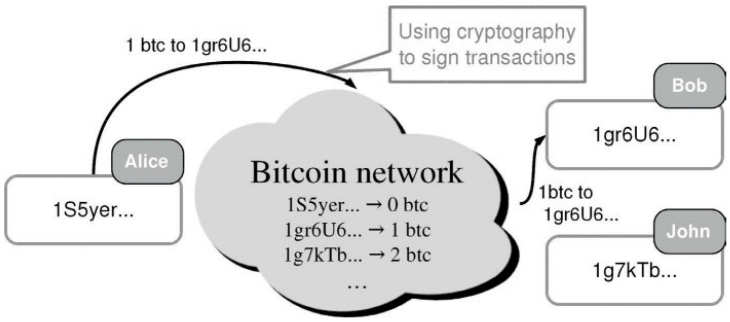
Slika 10: Slaba točka sustava s centralnom bazom

3.1 Bitcoin adrese

U centru Bitcoin mreže je decentralizirana lista koja održava ravnotežu svakog bitcoin korisnika. Bitcoin identificira korisnike po dugačkim nizovima slova i brojeva kao što je na primjer "13mckXcnnEd4SEkC27PnFH8dsY2gdGhRvM". Adresa je javni dio javno - tajnog kriptografskog ključa. Tajni dio ključa je poznat samo korisnika koji izvršava plaćanje.

Slika 11. prikazuje kako korisnik (Alice) šalje neka sredstva drugom korisniku (Bobu): Alice koristi svoj tajni ključ kako bi potpisala poruku: " Želim poslati jedan bitcoin na adresu 1gr6U6..." i to pošalje na mrežu. Primjetimo da Alice nije identificirala korisnika kojem želi poslati jedan bitcoin nego samo adresu koja prima sredstva. Tako Alice mora naći Bobovu adresu na druge načine. Po primitku Alicine poruke, čvorovi (korisnici) u mreži prate nekoliko koraka:

- provjeru je li potpis ispravan. Ako nije, odbiju poruku.



Slika 11: Proces prijenosa sredstava s jednog na drugi korisnički račun

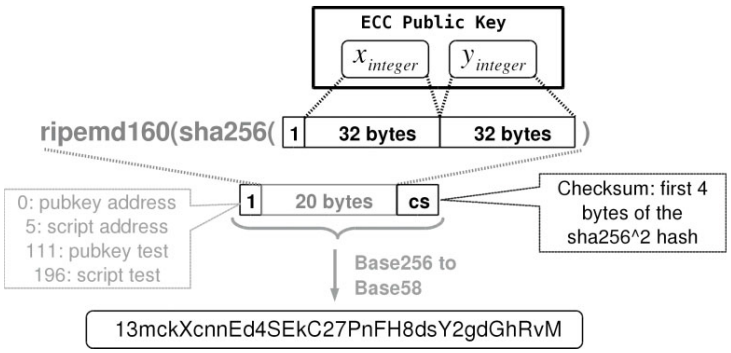
- ima li adresa koja šalje dovoljno sredstava da napravi transakciju. Ako nema, transakcija se smatra nevaljanom.
- Konačno, oni ažuriraju bazu, oduzimaju sredstva s jedne adrese (Alicine) i dodaju ih na drugu adresu (Bobovu).

Važan detalj je da čvorovi u mreži ne znaju identitete ni Alice ni Boba jer su korisnici identificirani samo preko svojih adresa. Bitcoin korisnici se identificiraju pseudonimima, Bitcoin omogućuje pseudonimnost.
Drugi važan detalj je da adrese nisu odobrene na mreži. One su kreirane unutar korisničkih uređaja i kada oni pokrenu Bitcoin softver, generiraju se javni i tajni ključ. Kako su javni i tajni ključ blisko povezani, oni moraju biti generirani povezano te lokalno na korisnikovu uređaju. Proces generiranja adrese je jednostavan i može se izvesti vrlo brzo na bilo kojem uređaju (laptop ili pametni telefon). Također, nema ograničenja na broj adresa koje korisnik može kreirati. Dapače, preporučuje se da korisnici generiraju mnogo adresa kako bi zaštitili privatnost.

Nikakva prethodna registracija nije potrebna da bi se koristio bitcoin. Zapravo, novi korisnici uopće ne trebaju poslati svoje adrese na mrežu da bi bili u mogućnosti primati sredstva. Korisnik (Bob) može generirati adresu i poslati ovu adresu Alice drugim komunikacijskim kanalima, kao što je e-pošta ili putem pametnih telefona. Alice sada može poslati sredstva Bobu na adresu, a mreža će prihvatiti transakcije iako nikada prije nije zabilježila tu adresu.
U centraliziranom sustavu imovinu drži središnje tijelo, što znači da ono kontrolira ta sredstva zapisivanjem promjena u glavnoj knjizi (eng. ledger). Nasuprot tome, u decentraliziranom sustavu, privatni ključevi daju pristup sredstvima isključivo krajnjim korisnicima.

Bitcoin adresa prikazujemo pomoću kriptografije javnog ključa koja koristi eliptičke krivulje. Slika 12. prikazuje korake poduzeti koje je potrebno provesti kako bi se od javnog ključa došlo do bitcoin adrese. Bitcoin koristi OpenSSL za izvođenje kriptografskih rezultata temeljenih na eliptičkim krivuljama. OpenSSL prikazuje točke na eliptičkoj krivulji

pomoću 65 bajtova. Prvi bajt se koristi za pohranu tipa točke na eliptičkoj krivulji. Vrijednost 0x04 ukazuje da je točka nekomprimirana. Vrijednost 0x02 ili 0x03 pokazuje da je točka komprimirana. Kad god prvi bajt ima vrijednost 0x02 ili 0x03 ovisno o parnosti izostavlja y koordinatu.
Točka je nekomprimirana ako su pohranjene x i y koordinata točke. Točka je komprimirana ako je samo x koordinata točke na eliptičkoj krivulji sačuvana: y koordinata odstupa od x i jednadžbe eliptičke krivulje. Nakon vodećeg bajta su dvije koordinate (x, y) točke eliptičke krivulje u slučaju nekomprimirane točka, odnosno x koordinata za komprimiranu točku. Bitcoin koristi eliptičku krivulju duljine 256 bitova, pa tako svaka koordinata zauzima 256 bita = 32 bajta prostora. Nekomprimirana točka zauzima ukupno 65 bajtova, 1 bajt za tip i 32 bajtova za svaku od koordinata.
Sljedeći korak na Slici 12. je hash OpenSSL prikaz točke eliptičke krivulje, najprije pomoću SHA256 funkcije, a zatim RIPEMD160. Prva hash funkcija SHA256 daje hash od 256 bita = 32 bajta. Druga funkcija RIPEMD160 daje hash od 160 bita = 20 bajta. Satoshi je izabrao drugi hash kako bi smanjio veličinu adresu, čineći transakcije manjima, a opet zadržava određenu veličinu adrese kako bi se izbjegla mogućnost da pomoću ovog procesa dvije osobe slučajno odaberu isti privatni ključ i tako dobiju istu adresu.
Konačno, sveukupna provjera (CS na Slici 12.) izračunava se kao SHA256^2 rezultata od hasha RIPEMD160. Samo se prva četiri bajta ovog hasha čuvaju za provjeru. Svrha ove provjere je slična kontroli zapisa na računima banaka ili kreditnim karticama: provodi se radi izbjegavanja pogreške u prijepisu koji bi uzrokovale slanje sredstava na pogrešne adrese. Program koji koristi Bitcoin novčanik provjerava je li adrese točna prije slanja sredstva na tu adresu. Ako je znamenka Bitcoin adrese pogrešno upisana ili kopirana, novčanik će uočiti pogrešku i odbiti slanje sredstva na tu adresu.



Slika 12: Generiranje Bitcoin adrese

Slanje sredstava na adresu koja je nepovezana s tajnim ključem čini ta sredstva nedostupnima, a time ih možemo smatrati i trajno izgubljenima.

U sljedećem koraku stvaranja Bitcoin adrese, niz bajtova je spreman za kodiranje u Base58. Ovaj niz bajtova počinje s bajtom koji predstavlja tip adrese, nakon čega slijedi 20 bajtova koji su rezultat hash funkcije RIPEMD160 i završava s 4 bajta koji služe za

provjeru.

Vrijednost tipa adrese određuje početak adrese kodirane u Base58. Vrsta adresa mogu imati sljedeće vrijednosti:

- 0 (decimala) za adresu s javnim ključem u glavnoj mreži. To će rezultirati kodiranom adresom počevši s 1.
- 5 (decimala) za prijepis adrese u glavnoj mreži. To će rezultirati kodiranog adresom počevši s 3.
- 111 (decimala) za adresu s javnim ključem u alternativnom blokovnom lancu. To će rezultirati kodiranom adresom počevši od m ili n.
- 196 (decimala) za prijepis adrese u alternativnom blokovnom lancu. To će rezultirati kodiranom adresom počevši od 2.

Posljednji korak u postupku je kodiranje s Base58. Base58 je binarno - tekstualni algoritam za kodiranje koji prevodi binarne podatke u tekstualnom formatu. Baza58 je sličan algoritmu Base64. Base64 koristi znakove A-Z, a-z, 0-9 i simbole + i /. Baza58 koristi iste znakove, osim znakova +, /, 0, O, I i 1. Time se izbjegavaju zabune, jer u nekim fontovima 0 i O te I i 1 imaju slične, pa ponekad i identične prikaze. Kodiranje niz bajtova koje tumačimo kao veliki broj sukcesivno dijelimo s 58. Ostatke u svakom koraku dijeljenja kodiramo kao znakove. Ovaj cijeli postupak rezultira Bitcoin adresama koje su između 27 i 34 znakova. Važno je napomenuti da su adrese osjetljive na velika i mala slova.

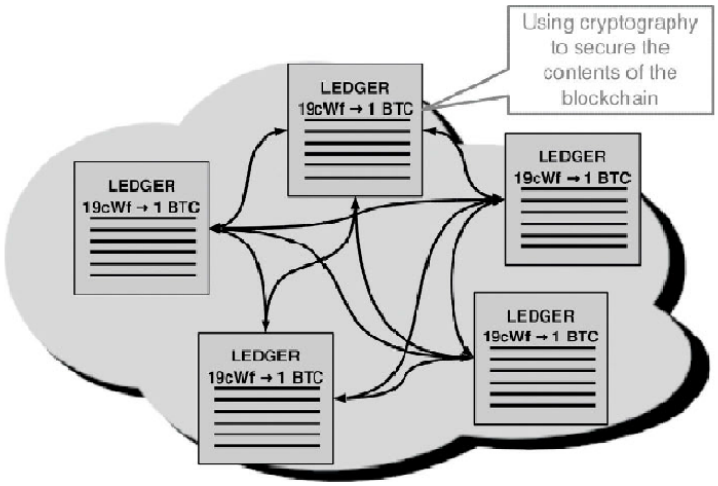
Hashiranje ključa koji koristi eliptičke krivulje čini sustav otpornijim na napade kvantnih računala. Međutim, treba napomenuti da se to odnosi samo na adrese čiji rezultati nikada nisu bili korišteni. ECC javni ključ adrese je objavljen u svakoj transakciji koja se šalje iz te adrese. Nakon izlaz poslan iz adrese, javni ključ ECC objavljuje se u blokovnom lancu, čime adresa postaje osjetljiva na napade kvantnih računala. Mnoge implementacije novčanika generiraju novu adresu prilikom svake transakcije.

3.2 Distribuirana baza podataka, blokovni lanac

Distribuirana baza podataka Bitcoina naziva se blokovni lanac. Transakcije su grupirane u blokove transakcija otprilike svakih deset minuta. Ti blokovi tranaskcija se tada bilježe jedan za drugim u lanac, pa otud potječe naziv blokovni lanac. Ovo izgleda kao neobičan način bilježenja informacija, u usporedbi s uobičajenim relacijskim bazama podataka. Blokovni lanac je stvoren tako da bude otporan u slučaju napada na mreži. Blokovi su povezani tako da tvore zapis transakcija koje su se odvijale u prošlosti i koje ne mogu biti promjenjene. Veza između blokova se ne može krivotvoriti osim ako napadač ima

ogromne računalne resurse na raspolaganju.

Osim lanca transakcija, čvorovi sadrže dodatnu bazu koja se zove Uspent Transaction Outputs cache (kratica: UTXO). UTXO je knjiga koja bilježi dostupna sredstva za svaku adresu, u suštini radi kao priručna memorija (predmemorija) za blokovne lance. Kako dolaze nove transakcije, UTXO se ažurira: sredstva sa adresa koje šalju se oduzimaju te se dodaju na adrese koje primaju novac.
UTXO je najsličniji centralnim bazama koje su središte većine centraliziranih sustava. Slika 13. prikazuje apstrakciju bitcoina: distribuirana knjiga koja sadrži podatke o raspoloživim sredstvima dostupnima za svaku adresu, što ugrubo predstavlja UTXO. Svaki čvor u mreži sadrži kopiju distribuirane knjige. Nadalje, kopije knjige su konzistentne preko čvorova, a nove transakcije imaju isti učinak u svim tim kopijama.

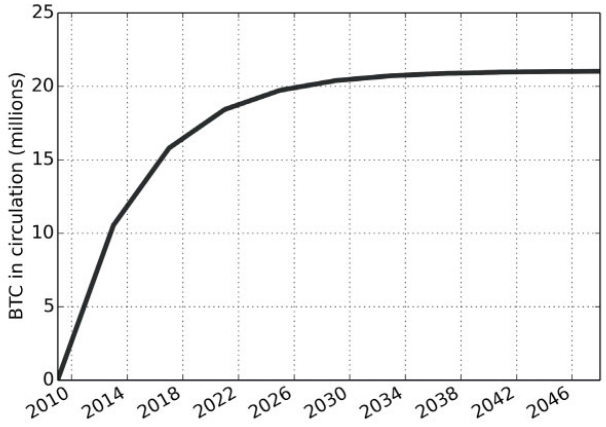


Slika 13: Bitcoin sustav kao distribuirana knjiga

Ono što Bitcoin protokol čini sigurnim i održivim jest izrada i održavanje blokovnog lanca koji treba brzo distribuirati svim sudionicima protokola (čvorovima). Novi blok transakcija uvrštava se u blokovni lanac svakih deset minuta i taj blok treba kriptografski pripremiti za uvrštavanje u blokovni lanac, a priprema se sastoji od izračunavanja kompleksnih hash funkcija (bitcoin-protokol koristi SHA-256). U pripremi bloka sudjeluju svi sudionici protokola koji su mu odlučili dati na raspolaganje svoju procesorsku snagu, nakon čega su nagrađeni novonastalim bitcoinima. Premisa protokola jest da će zajednica korisnika s velikom procesorskom snagom biti snažnija od pojedinih napadača. Kako snaga hardvera iz godine u godinu raste, bitcoin-protokol u skladu s tim mijenja blokovni lanac kako bi otežao pripremu novih blokova tako da bi ta priprema uvijek trajala oko deset minuta.

Čvorovi, odnosno korisnici koji su odlučili dati na raspolaganje svoju procesorsku snagu, nakon čega su nagrađeni novim bitcoinima nazivaju se rudari. Rudari se natječu u stvaranju blokova transakcija koje se pridodaju lancu transakcija. Rudar koji stvori jedan od tih blokova dobiva nagradni blok, koji se sastoji od određenog broja novonastalih

bitcoina.



Slika 14: Raspored stvaranja bitcoina

Slika 14. prikazuje raspored stvaranja bitcoina. Tempo novog izdanja je prepolovljen otprilike svake četiri godine, tako da na kraju će se ukupan broj bitcoina popeti do ukupno oko 21 milijun. Vrijednost bitcoina proizlazi iz njihovog nedostatka, a i zato što će broj izdanih bitcoina na kraju biti fiksan.
Rudari također prikupljaju naknade za transakcija koje su objavljene u blokovnom lancu. Naknade za transakcije su mali dio ukupne naknade rudara, trenutno ispod 1% ukupnog iznosa naknada. Očekuje se da će, kako se izdavanje novih bitcoina smanjuje, naknade za transakcije činiti glavni dio naknada rudara.
Krajem 2013. i početkom 2014. godine došlo je do velikog ulaganja u Bitcoin rudarsku opremu, procjenjuje se da je uloženo više od 200 milijuna dolara. Ovaj "uzlet" investicija u opremu za rudarenje je potaknut povećanjem vrijednosti bitcoina i tehnološkim razvojem.

3.3 Novčanici

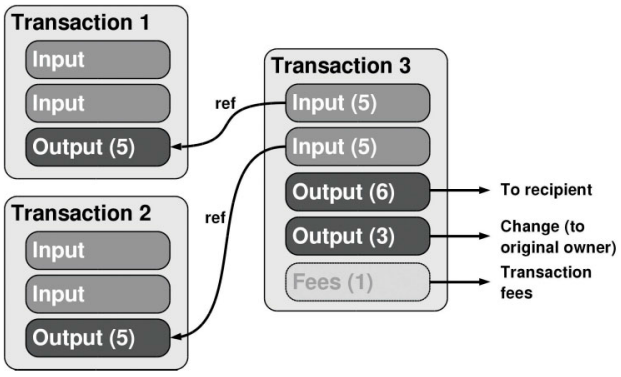
Novčanik je računalni program koji služi za slanje, primanje i skladištenje bitcoina. Novčanik sadrži korisnikove adrese i tajne ključeve, te prikazuje količinu bitcoina koje korisnik posjeduje, te sve transakcije koje je korisnik obavio. Najvažnije funkcije novčanika su čuvanje korisničkog tajnog ključa, kreiranje transakcija koje se šalju mrežom te prikupljanje dolaznih i odlaznih transakcija. Budući da korisnik može posjedovati više adresa, većina programa pruža mogućnost upravljanja višestrukim adresama, agregirajući sredstva između njih. Bitcoin novčanik predstavlja napredniji oblik novčanika u kojem držimo papirnati novac, odnosno kombinaciju standardnog novčanika i bankovnog računa. Bitcoine iz jednog novčanika u drugi prebacujemo bitcoin transakcijama.
Prilikom gubitka ili krađe novčanika, korisnik ostaje bez svih sredstava i u većini slučajeva

ostaje bez mogućnosti povrata sredstava. Međutim, u zadnje vrijeme se javljaju specijalizirane kompanije koje nude usluge povrata podataka putem analiziranja računalne memorije. Također, sve je veći broj kompanija koje nude usluge čuvanja Bitcoin novčanika.

Novčanik je moguće instalirati na stolno računalo, mobitel ili tablet. Novčanici su također dostupni kao web aplikacije, kojima je moguće pristupiti sa svakog računala povezanog na internet. Prema službenoj web stranici Bitcoina iza koje stoji Bitcoin organizacija, postoje 4 tipa Bitcoin novčanika: mobile, desktop, hardware i web. Mobile novčanici instaliraju se na smartphone uređaje, a desktop na osobna ili prijenosna računala. Web novčanici nalaze se na web serverima te im se pristupa putem internet preglednika. Hardware novčanici su specifična vrsta Bitcoin novčanika budući da imaju svoju fizičku izvedbu najčešće u obliku pametnih kartica. Preporučljivo je Bitcoin novčanik smjestiti van mreže, budući da su sustavi u oblacima i specijalizirane web stranice često mete napadačima. Tajni ključ, koji se obično čuva u uređaju, najvažniji element u cijelom Bitcoin konceptu. Gubitkom privatnog ključa korisniku je onemogućen pristup sredstvima. Iako su sredstva i dalje upisana u distribuiranoj knjizi, bez privatnog ključa ne postoji način kako ispravno zaključiti transakciju za njihovo korištenje pa se smatraju izgubljenima. Zbog toga tvrtke koje proizvode programe za novčanike preporučuju izradu digitalne sigurnosne kopije privatnih ključeva. Isto tako, zbog opasnosti od neovlaštenog pristupa uređaju na kojem se nalazi Bitcoin novčanik te kasnije zlouporabe, preporučuje se šifriranje (enkripcija) tajnih ključeva. Na taj se način, prije korištenja tajnog ključa, mora unijeti lozinka za dešifriranje (dekripciju) što otežava posao napadačima. Ipak, najbolje rješenje je čuvanje tajnog ključa u fizičkom obliku poput papira ili pohranivanje na digitalan medij koji nema pristup internetu.

4 Transakcije

Bitcoini nisu smješteni na korisnikovo računalo. Oni su ulazi u distirubiranu bazu koja se naziv blokovni lanac. Za razliku od centraliziranih digitalnih valuta, Bitcoinov blokovni lanac ne pohranjuje račune i iznose, već samo transakcije.
Transakcije čini lista ulaznih transakcija i lista izlaznih transakcija. Svaka izlazna transakcija sadrži dva podatka: količinu novca i adresu primatelja. Adresa je izvedena iz javnog ključa te jedino vlasnik tajnog ključa može otključati sredstva pohranjenja u izlaznu transakciju. Kako bi se otključala sredstva, vlasnik tajnog ključa mora potpisati transakciju kojom šalje sredstva na novu Bitcoin adresu.
Ulazna transakcija sadrži izvješće o prethodnoj ulaznoj transakciji i potpis koji dokazuje da primljena sredstva iz prethodne izlazne transakcije mogu trošiti. Potpis se mora napraviti pomoću tajnog ključa povezanog s javnim ključem u Bitcoin adresi. Ako se potpis ne poklapa, transakcija se smatra nevažećom i mreža ju odbacuje.
Transakcije se sastoje od nekoliko ulaznih i izlaznih transakcija, s tim da svaka mora sadržavati barem jedna ulaznu i jedna izlaznu transakcija. Njihova svrha je distibuirati sredstva među korisnicima. Ulazi transakcija odgovaraju izlazima prethodnih transakcija. Ti izlazi ne smiju biti potrošeni, inače se transakcija smatra nevažećom.
Da bi transakcija bila valjana, zbroj iznosa ulaza mora biti veći ili jednak zbroju iznosa izlaza. Razlika između ulaza i izlaza (ukoliko postoji) je naknada za transakcije. Transakcijsku naknadu skupljaju rudari koji uključuju transakcije u blokove. Izlazi u blokovni lanac mogu biti potrošeni samo jednom te moraju biti potrošeni u potpunosti. Ako je iznos izlaza veći od potrošenog iznosa, transakcija stvara ostatak. Pošiljatelj transakcije može prikupiti ovaj ostatak uključujući adresu ostatka kao dodatnu izlaznu transakciju. Činjenica da ostatak na adresi obično kontrolira pošiljatelj transakcije može se aktivno koristiti u algoritmima za rudarenje podataka primijenjenim na blokovni lanac. Adresa s koje potječu sredstva može se koristiti kao adresa na kojoj će stići ostatak nakon obavljene transakcije, no ipak se preporuča generirati potpuno novu adresu za ostatak pri svakoj transakciji s ciljem povećanja privatnosti.



Slika 15: Primjer transakcije

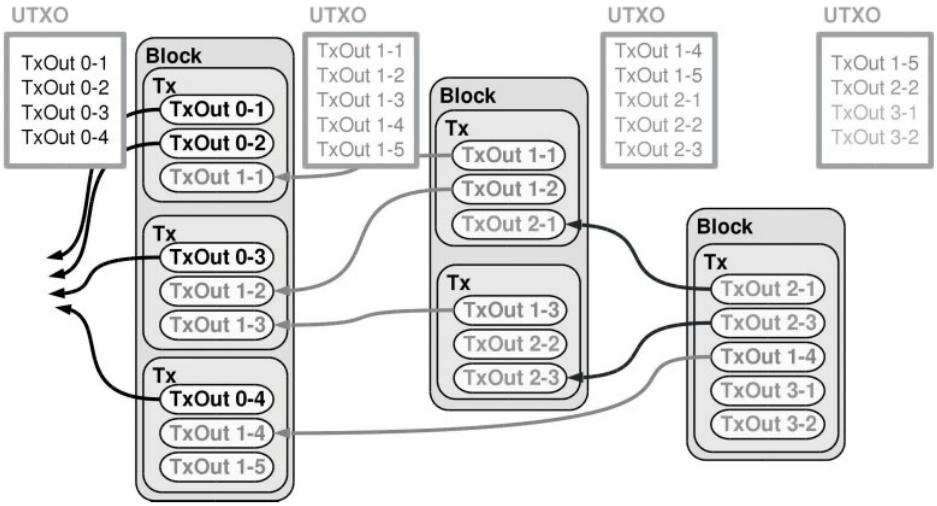
Slika 15. prikazuje primjer transakcije. U ovom primjeru, pošiljatelj želi poslati 6 milibitcoina primatelju. Međutim, pošiljatelj nema na raspolaganju nijednu izlaznu transakciju s iznosom od točno 6 millibitcoina. On kontrolira samo dvije izlazne transakcije, svaku sa po 5 millibitcoina. Stoga, on stvara transakciju grupiranjem ove dvije izlazne transakcije i šalje 6 millibitcoina primatelju. Pošiljatelj uključuje u izlaz adresu koju je ranije stvorio kako bi primao ostatak transakcije (3 millibitcoina). Jedan millibitcoin ostavlja kao naknadu za rudare. Prije slanja transakcije u mrežu, on mora biti potpisati dvije ulazne transakcije kako bi dokazao da kontrolira adrese.
Transakcija se zatim šalje na mrežu. Prvi čvor u mreži koja prima transakcija potvrđuje da je valjana transakcija. Ako je transakcija ispravna, čvor je proslijedi drugim čvorove u mreži. Kako bi bili sigurni da je transakcija valjana, čvor mora slijediti ove korake:

- Provjeriti postoje li dosadašnje promatrane izlazne transakcije te da nisu potrošene. Čvor koji obavlja ovu provjeru koristi UTXO.
- Provjeriti je li zbroj vrijednosti ulaza veći ili jednak zbroju izlaza, odnosno provjerava da transakcija nije provela više od dostupnih outputa. Razlika između zbroja vrijednosti outputa i zbroj vrijednosti inputa smatra se naknadom za rudare što je uključeno u coinbase transakcije.
- Provjeriti je li potpis za svaki ulaz valjan, odnosno da je svaki ulaz potpisan privatnim ključem s odgovajućim javnim ključem povezan s adresom.

Satoshi zahtjeva da izlazne transakcije trebaju biti utrošene u potpunosti jer je to računalno učinkovitije. Bitcoin program čuva unspent transaction outputs predmemoriju (UTXO) kao bazu podataka koja sadrži samo nepotrošene izlazne transakcije. UTXO je vrlo korisna jer se može koristiti za brzu provjeru jesu li nove transakcije valjane. Kad se napravi nova transakcija, njeni ulazi gledaju prema UTXO. Ako se svi ulazi nalaze u UTXO, onda oni odgovaraju prethodno valjanim izlazima, a transakcije se nastavljaju procjenjivati. Ako se bilo koji ulaz ne nalazi u UTXO, transakcija nije valjana i može biti odbačena.

Pretpostavimo da su transakcije grupirane u blokove koje su zajedno potvrđene (uključene su u blokovni lanac istovremeno).
Slika 16. prikazuje UTXO u akciji. U početku postoje četiri neutrošene transakcije u mreži ($0-1$ do $0-4$) i UTXO drži te četiri neutrošene transakcije. U sljedećem koraku stvoren je blok koji uključuje tri transakcije. Tri transakcije potroše četiri izlazne transakcije u UTXO te ih tako uklanjaju.

No, nove transakcije u bloku također uvele nove izlaze ($1-1$ do $1-5$) i ti rezultati su uključeni u UTXO. Sljedeći blok potroši tri od pet izlaznih transakcija u UTXO ($1-1$ do $1-3$) i dodaje tri nova TxOuts ($2-1$ do $2-3$) i tako redom dalje. Pri stvaranju svakog novog bloka, izlazi se troše i uklanjaju iz UTXO, a novi izlazi stvoreni transakcijama u bloku se dodaju u UTXO. Prednost UTXO je ta što je mnogo manji od cjelokupne transakcijske baze podataka (blokovnog lanca). To omogućuje čvorovima zadržavanje UTXO u RAM-u, što znatno ubrzava provjeru valjanosti novih transakcija. Vratimo se na pitanje



Slika 16: Unspent Transaction Outputs Cache (UTXO)

gdje se bitcoini nalaze. Moglo bi se reći da se bitcoini nalaze u nepotrošenim izlazima transakcija u blokovnom lancu.

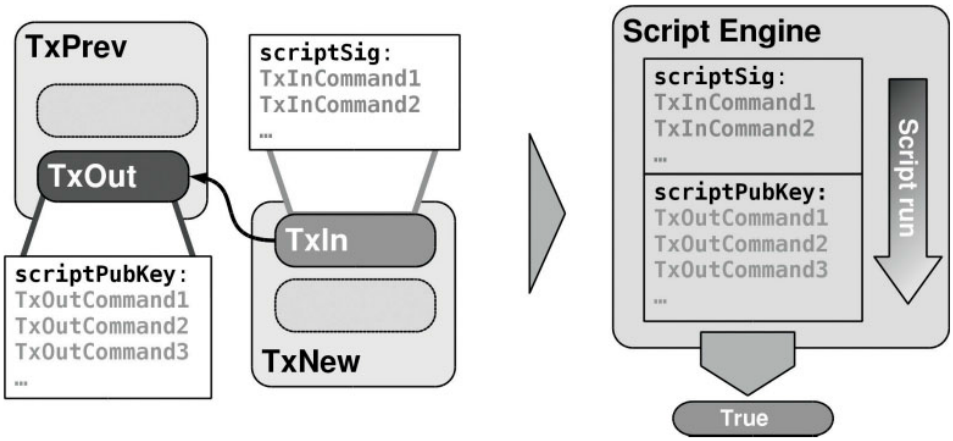
Postoje još neke načini upotrebe bitcoin transakcija osim prijenosa sredstava između adresa. Većina tih načina se oslanjaju na sposobnost za pohranu proizvoljnih podataka u blokovni lanac. Nakon što su podaci u blokovnom lancu, njihova postojanost i valjanost osigurana je računalnom snagom Bitcoin mreže, na isti način su bitcoini i osigurani. Jedan od načina za pohranu podataka u blokovni lanac je korištenje adrese primatelja kao polja podataka. Recimo, da osigura podatke "Thisblobofdata", transakcija mogla biti poslana na adresu 1Thisblobofdata (adresa inače ne izgleda ovako, ali ju uzimamo radi jednostavnosti). Privatni ključ povezan s ovom adresom nije poznat, pa će tako sva sredstva poslana na ovu adresu će biti izgubljena.
Razumljivo, korisnici ove vrste transakcija bi željeli potrošiti što je moguće manji iznos (1 satoshi). Problem je u tome što su ovi izlazi bili uključeni u UTXO i nisu obrisani iz njega jer su nepotrošeni. Kao odgovor ovoj praksi, programeri Bitcoina su odlučili uvesti minimalni prag - iznos ispod kojeg se transakcija smatra nepotrošiva. Rezultat transakcije ispod ovog praga se naziva transakcija prašine jer se kao prašina nakuplja u UTXO. Prag je postavljen trenutno na 546 satoshija (0.0000546 bitcoina). Izračunat je kao iznos izlaza čija minimalna naknada iznosi 1/3 svoje vrijednosti.

4.1 Osnove Bitcoin skripti

Prije no što se detaljnije opišemo kako izgledaju Bitcoin skripte i za što služe, prvo ćemo definirati njih i protokol. Skripte su niz naredbi pisanih u Bitcoinovom skriptnom jeziku Script. Protokoli se mogu definirati kao skup općeprihvaćenih pravila koja se primjenjuju

kod elektroničkog načina prijenosa podataka u nekoj mreži.

Dosada, podrazumijevalo se da su izlazne transakcije poslane na Bitcoin adresu. Međutim, protokol je mnogo fleksibilniji. Svaka izlazna transakcija stvori matematički izraz koji mora biti riješen kako bi se mogao potrošiti iznos izlazne transakcije. Taj izraz za otključavanje sredstava i njegovo rješenje je predstavljeno pomoću dvije skripte. Ona skripta koja stvori novi matematički izraz naziva se <scriptPubKey> zato što dio skripte sadrži javni ključ.



Slika 17: Skriptiranje

Skripta koja rješava izraz <scriptPubKey>, točnije otključava sredstva zove se <scriptSig> zato što je dio skripte koja sadrži potpis.
Slika 17. prestavalja proces trošenja iznosa izlazne transakcije. Izlazna transakcija stvara <scriptPubKey> koji mora biti rješen da se mogla trošiti sredstva iz te izlazne transakcije. Ulazna transakcija pokusašava trošiti iznos u izlaznoj transakciji definiranjem <scriptSig>. Protokol provjerava rješava li <scriptSig> matematički izraz koji je <scriptPubKey> stvorio. Kako bi se to napravilo, protokol stvara cijelu skriptu (čitav niz naredbi) nadovezivanjem <scriptSig> na <scriptPubKey> i pokreće cijelu skriptu. Ako je krajnji rezultat istina, onda se ulaz smatra valjanim. Ako skripta ima grešku u nekom koraku ili krajni rezultat daje neistinu, ulazna transakcija je nevaljana i cijela se transakcija smatra nevaljanom i odbačenom.
Jezik skripte je baziran na stogu i sličan je Forth[2] jeziku. Naredbe koje su prikazane pomoću svojih kodova mogu postavljati podatke na stog ili računati s podacima na stogu. Funkcije koje računaju na stogu mogu uzimati argumente s vrha stoga i postavljati njihove rezultate na vrh stoga. <scriptSig> potiskuje podatke u stogu dok je <scriptPubKey>

[2]Forth je programski jezik koji je strukturan, imperativan, refleksivan, proširiv i zasnovan na reprezentaciji stoga.

kombinacija podataka koji stavljaju podatke na stog i funkcija koje dohvaćaju podatke sa stoga.
Jezik skripte u Bitcoinu je prilično fleksibilan i jak, ali nije Turing-potpun[3]. Tako je odlučeno da bi se izbjegli napadi na mreži. Kada bi jezik skripte bio Turing-potpun, napadač bi mogao smisliti <scriptPubKey> koji nikad ne završava, beskonačna petlja. To preopterećenje bi prouzrokovalo da čvorovi u mreži prestanu procjenjivati skripte te bi došlo do pada mreže. Iz tog razloga je odlučeno da jezik skripte ne sadrži petlje.

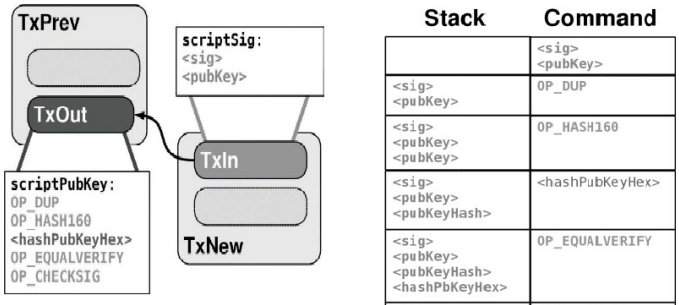
Primjer jedne transakcije:
{
"*hash*" : "7*c*40250...",
"*ver*" : 1,
"*vin_sz*" : 1,
"*vout_sz*" : 1,
"*lock_time*" : 0,
"*size*" : 224,
"*in*" : [
{
"*prev_out*" : {
"*hash*" : "2007*aec*...",
"*n*" : 0
},
"*scriptSig*" : "*signature*"
}
],
"*out*" : [
{
"*value*" : "0.31900000",
"*scriptPubKey*" : "*script*"
}
]
}

4.2 Pay-to-address i pay-to-public-key transakcije

Najčešći tip transakcija je pay-to-address. Slika 18.a) predstavlja izlaz i ulaz takvih transakcija, dok sljedeća Slika 18.b) predstavlja stog nakon što se izvrši svaka od naredbi u <scriptSig>.

Skripta najprije ocjenjuje <scriptSig> ulaza. Taj <scriptSig> stavlja samo dva podataka u stog. Kako je stog podatkovna struktura u kojoj zadnji podatak izlazi prvi van

[3]Turing-potpun jezik ne može simulirati rad Turingova stroja.



a) Pay to Bitcoin address transakcija

b) Stog za skriptu pay-to-address

Slika 18: Pay-to-address transakcija

(LIFO - Last In First Out), podaci koje <scriptSig> prve potisne u stog trebali bi se pojaviti najzadnji u procjeni skripte. Prvi element koji se potisnut je <sig> je potpis na hash nove transakcije s tajnim ključem koji odgovara javnom ključu <PubKey>. Drugi element koji se potiskuje na stog je javni ključ <pubKey>. Treba uočiti da <pubkey> nije Bitcoin adresa, nego javni ključ generiran pomoću eliptičke krivulje iz koje je izvedena Bitcoin adresa.

Nakon postavljanja <scriptSig> na stog, protokol sada ocjenjuje <pubKey> izlaza. OP_DUP je naredba da udvostručuje posljednji element stoga, u ovom slučaju <pubKey>. Sljedeća je naredba OP_HASH160 koja izračunava Bitcoin adresu iz javnog ključa generiranog pomoću eliptične krivulje. Naredba koja slijedi u <scriptPubKey> postavlja <hashPubKeyHex> na stog. To je Bitcoin adresa da je stvaratelj izlazne transakcije odlučio poslati sredstava. Sljedeća naredba u <scriptPubKey> je OP_EQUALVERIFY. Ova naredba provjerava jesu li posljednja dva elementa na stogu jednaka. Ako nisu, transakcija se označava kao nevaljana. Nakon te provjere, ta dva elementa se uklanjaju sa stoga.
Posljednja naredba OP_CHECKSIG provjerava je li potpis transakcije ispravan. Prvo hashira novu transakciju i provjeri je li <sig> ispravan potpis za taj hash. Ako je potpis ispravan, transakcija je valjana i program vrati istina. U suprotnom, program vraća laž te je transakcija odbijena.
Ukratko, tvorac izlazne transakcije postavlja određene uvjete za njeno trošenje: nova transakcija mora biti potpisana tajnim ključem povezanim s Bitcoin adresom <hashPubKeyHex>. Ulaz koji troši ovaj ulaz mora osigurati sljedeća dva elementa:

- javni ključ generiran pomoću eliptičke krivulje <pubKey> koji hashiran mora odgovarati <hashPubKeyHex>.
- potpis <sig> cijele transakcije s ispravnim tajnim ključem. Taj ključ dokazuje vlasništvo nad Bitcoin adresom.

Pay-to-public-key transakcija je slična kao pay-to-address, ali umjesto uključivanja adrese u <scriptPubKey>, uključen je javni ključ generiran pomoću eliptičke krivulje.

<scriptPubKey> i <scriptSig> u slučaju pay-to-public-key transakcija izgledaju na sljedeći način:

scriptSig: <sig>
scriptPubKey: <pubKey> OP_CHECKSIG

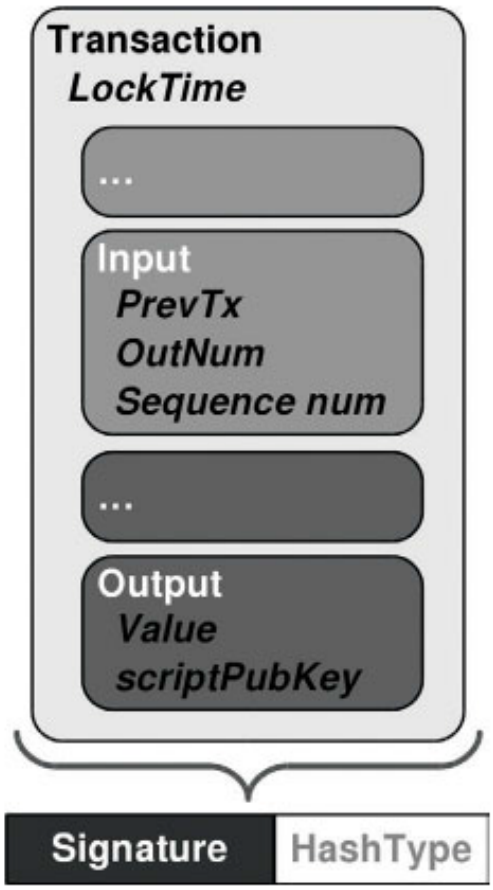
Treba primjetiti da nakon stavljanja <scriptSig> i <scriptPubKey> na stog, sadržaj stoga je jednak onome u posljednjem koraku prikazanom na Slici 18.b).
Pay-to-public-key transakcije imaju potencijalne nedostatke. Sredstva nisu otporna na kvantna računala te je javni ključ generiran pomoću eliptičke krivulje veći od adrese što čini transakciju većom. Zbog toga se rijetko koriste u praksi.

4.3 Potpisi transakcija

Kako bi se potrošila sredstva spremljena u izlazne transakcije, trošenje transakcija mora biti potpisano tajnim ključem povezanim s adresom na kojoj su ta sredstva pohranjena. Potpisivanje transakcije obuhvaća sljedeće korake:

- Pravljenje kopije transakcije tako da se ne ošteti orginalna transakcija.
- Transakcija koja se potpisuje ne sadrži <scriptSig> zato što je potpis dio <scriptSig> i stoga će <scriptSig> biti dodan nakon potpisa.
- Cijela skripta se onda hashira i onda se potpisuje privatnim ključem koji odgovara Bitcoin adresi izlaza koji se troši.

Transakcija sadrži varijablu zaključno vrijeme koja se u kodu označava nLockTime. Također, svaki ulaz u transakciju ima redni broj koji se u kodu označava s nSequence. Transakcija se smatra gotovom kada je dostignuto zaključno vrijeme ili kada je redni broj svih ulaza postavljen na najveću moguću vrijednost.
Zaključno vrijeme dopušta slanje nedovršenih transakcija koje mogu biti zamjenjene u budućnosti tehnikom koja se zove zamjena transakcija. Period zamjene takve transakcije određen je vrijednošću nLockTime-a ili kao broj blokova u vremenskom pečatu. Treba primjetiti kako za transakcije koje mogu biti zamjenjene, barem jedan ulaz mora imati redni broj manji od najvećeg mogućeg.
Transakcija se smatra gotovom kada je dostignuto zaključno vrijeme ili kada svi redni brojevi ulaza postižu maksimalnu vrijednost.
Transakcije čije zaključno vrijeme nije dostignuto ili čiji redni brojevi nisu postavljeni na maksimum zovu se nedovršene transakcije. Nedovršene transakcije nisu uključene u blokovni lanac i čvorovi ih odbacuju kad ih prime. No nije oduvijek bilo tako, prije 2010. godine čvorovi su čuvali nedovršene transakcije, čekajući da zaključno vrijeme bude dostignuto ili nove zamjenske transakcije koje će biti dovršene.



Slika 19: Elementi transakcije

Slika 19. prikazuje vrste hash potpisa. Svaki potpis u <scriptSig> sadrži oznaku koja ukazuje koji ulazi i koji izlazi su potpisani. Ta oznaka se naziva tip hash potpisa i može biti u tri oblika:

- SIGHASH_ALL - potpis obuhvaća sve izlaze, što znači da će promjena bilo kojeg izlaza učiniti transakciju nevaljanom. Promjena bilo kojeg izlaza u transakciji će zahtjevati da se svi izlazi ponovno potpišu.
- SIGHASH_NONE - potpis ne uključuje nijedan izlaz. To znači da pri promjeni bilo kojeg izlaza transakcija je još uvijek valjana. Ovaj oblik dopušta drugim ulazima da ažuriraju svoje redne brojeve.
- SIGHASH_SINGLE - potpis uključuje jedino izlaz koji ima isti indeks kao i ulaz, ako je ulaz na trećem mjestu, potpis jedino pokriva izlaz na trećem mjestu. Ovaj oblik omogućuje drugim inputima da ažuriraju svoje redne brojeve.

Potpisi imaju dodatnu oznaku SIGHASH_ANYONECANPAY koja može biti istinita ili lažna i može se kombinirati s svim prethodnim oblicima. Ako vraća istinu, potpis uključuje samo trenutni potpis. Ako je postavljena na laž, onda potpis uključuje sve ulaze.

5 Zaključak

Bitcoin je specifična valuta koja se po svojim karakteristikama razlikuje od prethodnih digitalnih valuta. Otkako se pojavio 2008. godine Bitcoin je pokrenuo niz rasprava vezanih za pozitivne i negativne strane njegove primjene. Valuta je računalno programirana, ograničena, te za razliku od svojih prethodnika decentralizirana. Koristi peer-to-peer sustav kao i tehnologiju šifriranja podataka kojom se elimira problem dvostrukog plaćanja, krivotvorenje i slične zloupotrebe. To je ujedno i jedan od glavnih razloga zašto se Bitcoin smatra sigurnom valutom.
Transakcijski troškovi su vrlo niski, ali same transakcije nisu reverzibilne što smatramo nedostatkom ove valute. Budući da Bitcoin svojim korisnicima omogućuje anonimnost i netransparentnost njihovih aktivnosti, pojavljuju se kritike da je na taj način stvorena mogućnost za pranje novca, kreiranje crnih tržišta, poreznih oaza te slučajevi različitih zlouporaba kao što su Ponzijeva shema koji su korišteni za krađu elektroničkih novčanika korisnika Bitcoin valute.
Navedeni niz nedostataka doveo je do pitanja nadzora i regulacije Bitcoina. Iako je određen broj zemalja počeo regulirati Bitcoin transakcije i dalje je relativno malo učinjeno po tom pitanju jer ovo pitanje zahtjeva oprez. Naime, bilo koji oblik kontrole i regulacije Bitcoina posljedično bi mogao preusmjeriti korisnike na korištenje nekih drugih kriptovaluta koje još nisu regulirane.
U tom smislu, jedan od najvećih izazova za središnje institucije u budućnosti će se odnositi vrlo vjerovatno na praćenje efekata korištenja Bitcoina i njihovu regulaciju, odnosno poduzimanje adekvatnih mjera u slučaju različitih zloupotreba ili izazivanja nestabilnosti. Vrijednost jednog bitcoina dana 11.10.2015. godine iznosila je 322.93 $. Promatranjem podataka o kretanju cijene bitcoina može se uočiti da u kratkom vremenskom periodu dolazi do velikih promjena u njegove vrijednosti. Možemo zaključiti da je vrijednost bitcoina nestabilna, kao i njegov zakonski status te izgube li korisnici vjeru u njega i padne li potražnja za njim, on će istog trenutka postati bezvrijedan.
No, zagovornici Bitcoina smatraju da će ta kriptovaluta u sljedećih nekoliko desetljeća imati status koji danas u međunarodnim financijskim tokovima ima švicarski franak. Prema procjenama jedne londonske tvrtke, u sljedećih 15 godina Bitcoin će postati šesta valuta po zastupljenosti u deviznim rezervama država.

Literatura

[1] Antonopoulos, A. M.: Mastering Bitcoin Unlocking digital cryptocurrencies. Sebastopol, California O'Reilly Media, Inc. 2014.

[2] Drabik, T.: Novac u oblaku, BUG, 256 (2014), Zagreb.

[3] Dujella, A., Maretić, M.: Kriptografija, Element, Zagreb., 2007.

[4] Franco, P.: Understanding Bitcoin: Cryptography, Engineering and Economics (The Wiley Finance Series), Wiley, 1 edition 2014.

[5] Kućan, B.: Bitcoin podzemlje. Mreža časopis za IT profesionalce, 3 (2014), Zagreb.

[6] Nakamoto, S.: Bitcoin: A peer-to-peer Electronic Cash System, 2008.
dostupno na: https://bitcoin.org/bitcoin.pdf

Životopis

Zovem se Marina Kaselj. Rođena sam 1991. godine u Virovitici. Upisala sam 2006. godine prirodoslovno-matematički smjer Gimnazije Petra Preradovića Virovitica u Virovitici. Tijekom srednjoškolskog školovanja sudjelovala sam na županijskim natjecanjima iz matematike, geografije i hrvatskog jezika. 2010. godine upisala sam preddiplomski studij matematike na Odjelu za matematiku Sveučilišta J.J. Strossmayera u Osijeku. Preddiplomski studij sam završila 2013. s temom završnog rada Testovi prostosti pod mentorstvom izv. prof. dr. sc. Ivana Matića. U listopadu 2013. godine upisujem diplomski studij matematike, smjer Financijska matematika i statistika.