Elektronski novac

Barić, Borjana

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:797531

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku

Borjana Barić

Elektronski novac

Diplomski rad

Osijek, 2016.

Sveučilište J.J.Strossmayera u Osijeku
Odjel za matematiku

Borjana Barić

Elektronski novac

Diplomski rad

Mentor: izv. prof. dr.sc. Ivan Matić

Osijek, 2016.

Sadržaj

1 Uvod

S početkom informacijskog doba narod je postao sve više ovisan o mrežnoj komunikaciji. Tehnologija zasnovana na računalima znatno utječe na našu sposobnost pristupu, pohrani i distribuciji informacija. Među najvažnijim upotrebama ove thenologije je elektroničko poslovanje. Ključni uvjet za elektronsku trgovinu je razvoj sigurnih i učinkovitih sustava elektronskog plaćanja. Potreba za sigurnošću ističe se razvojem Interneta koji je postao vodeći medij za elektronsko trgovanje. Elektronski sutavi plaćanja dolaze u mnogim oblicima (digitalni čekovi, debitne kartice, kreditne kartice, tokeni). Sigurnosne značajke za takve sustave su privatnost, autentičnost i nemogućnost opovrgavanja transakcije.

Elektronski sustav plaćanja objašnjen u ovom radu je elektronski novac (digitalni novac, elektronska gotovina). Elektronski novac je elektronski sustav plaćanja konstruiran po uzoru na sustav plaćanja tradicionalnim novčanicama i kovanicama. Novčanice i kovanice imaju sljedeća svojstva: prenosivost, pokretnost, prihvatljivost kao zakonsko stredstvo plaćanja, nemogućnost ulaska u trag i anonimnost. Elektronski novac se definira kao elektronski sustav plaćanja koji osim navedenih svojstava sustava omogućuje anonimnost korisnika i nemogućnost ulaska u trag plaćanju. Ovi ciljevi se postižu putem digitalnih potpisa koji se temelje na kriptografiji javnog ključa, no opasnosti od pranja novca i krivotvorenja su mnogo veće u odnosu na tradicionalnu gotovinu.

Rad je organiziran na sljedeći način. U drugom poglavlju opisan je razvoj sustava plaćanja te osnovne karakteristike elektronskog sustava plaćanja. Treće poglavlje prikazuje osnovnu implementaciju elektronskog novca te svojstva i unutarnju strukturu novčanica. U četvrtom poglavlju su opisani osnovni protokoli ovog sustava plaćanja. Tri su osnovna protokola: podizanje novca iz banke, plaćanje i polaganje novca u banku. Dodatni protokol je oporavak koji se provodi ukoliko se prekine protokol podizanja novca zbog pada sustava. Sljedeće poglavlje opisuje shemu koja jamči svojstvo nemogućnosti ulaska u trag, ali omogućuje banci otkrivanje kupaca koji dvostruko troše e-novac. U posljednjem poglavlju opisano je nekoliko poznatih implementacija elektronskog novca. Neke od njih više ne djeluju, no uključene su u rad kako bi se dobio uvid u provedbu elektronskog novca.

2 Elektronski sustav plaćanja

2.1 Povijest sustava plaćanja

Najstariji poznati sustav trgovanja je trampa u kojem se vršila razmjena dobara i usluga. Problem s ovim sustavom je nedostatak standardizacije za količinu i dobra koja bi se mijenjala. Kako bi se riješio ovaj problem, uvedene su kovanice i papirnati novac. Oni imaju tržišnu vrijednost što korisnicima omogućuje razmjenu za sva željena dobra i usluge. Kako bi se dovršila transakcija koristeći ovaj sustav, kupac mora imati dovoljnu vrijednost kovanica i novčanica.

Kako je vrijeme prolazilo, uvedeno je plaćanje putem čekova. Čekovi su izdavani sa suglasnošću banke kao pouzdanog tijela za provjeru valjanosti obveznika i navedenog iznosa. Tako je omogućeno kupcu da obavi veliku količinu transkacija bez nošenja kovanica ili novčanica te je smanjen rizik pljačke. Međutim trgovci su izloženi riziku dobivanja nevažećih čekova bez novca ili nepostojanja računa u banci.

Ubrzo nakon čekova, kartice bankomata (automatic teler machine - ATM kartice) su uvedene kako bi se poboljšao sustav plaćanja. Tako je omogućena prva transkacija elektronskim putem. ATM kartice se izdaju od strane banaka ili trgovačkih lanaca kako bi se omogućila kupovina bez upotrebe kovanica, novčanica ili čekova.

Nakon uspjeha ATM kartica, uvedene su kreditne kartice. Nova metoda zahtijeva da kupci pri svakoj transakciji pozajme novac od izdavatelja kartica. Pri svakoj transakciji izdavatelji plaćaju u ime kupca, zatim kupac mora vratiti iznos izdavatelju unutar zadanog razdoblja ili se rizik naplaćuje s kamatama. Za obje kartice, ATM i kreditne, svatko tko dođe do kartice ilegalno moći će je koristiti jer nema provjere autentičnosti nakon plaćanja osim potpisa koji može biti krivotvoren.

2.2 Karakteristike elektronskog sustava plaćanja

Objasnit ćemo neke od osnovnih karakteristika sustava plaćanja. Iz ovih karakteristika možemo izvoditi mogućnosti za brojne varijacije te zaključiti koji je njihov utjecaj na performanse i fleksibilnost sustava.

Plaćanje prema instrukcijama i plaćanje unaprijed (prepaid) elektronskim novcem

U sustavu plaćanje prema instrukcijama kupac nalaže banci da premjesti iznos novca s njegovog računa na račun trgovca. Primjer za ovaj tip plaćanja su kreditne i debitne kartice, kao i mnogi oblici čekova. Trenutak u kojem se novac prebacuje s računa kupca na račun trgovca ovisi o sustavu, ali u svakom trenutku će banke i izdavatelji kreditnih kartica pokušati spriječiti odstupanja između računa. Središnji sigurnosni aspekt je osigurati da su jedino zakonski nositelji računa u mogućnosti izdavati upute za plaćanje. Digitalni potpisi su rješenje za obavljanje plaćanja preko otvorene mreže. Budući da digitalni potpisi imaju smisla ako postoji infrastruktura za ovjeravanje javnih ključeva, puno truda je posvećeno upravo tomu (npr. suradnja MasterCard, Visa i drugih utjecajnih partnera). Prepaid sustavi su konceptualno blizu elektroničkom ekvivalentu novca (gotovine). Telefonske kartice, pametne kartice kao i elektronski novac pripadaju ovoj kategoriji. Korisnikov račun se tereti čim se na karticu ili uređaj doda e-novac. Tijekom plaćanja e-novac je ponovno "oslobođen", a tek onda uplaćen na račun trgovca. U međuvremenu izdavatelj drži uloženi novac koji označava izvanrednu gotovinu. Središnji sigurnosni aspekt ovog tipa sustava je osigurati da se kartice ili prikazi novca ne mogu krivotvoriti. Kada se to ipak dogodi, uloženi novac će u konačnici

biti dovoljan da podmiri sve račune trgovaca za primljene uplate. Također treba osigurati da samo zakonski nositelji računa mogu učitati novac sa svojih računa. Ovaj sigurnosni aspekt je sada ograničen samo na rijetkom protokolu podizanja novca iz banke, a nije dio češćeg protokola plaćanja.

Online i offline

U području elektronskog sustava plaćanja, online i offline odnose se na određena svojstva protokola plaćanja. Iako je protokol plaćanja funkcionalno između dvije stranke (kupac i trgovac), mnogi sustavi plaćanja zahtijevaju da trgovac kontaktira treću osobu (banka, izdavatelj kreditnih kartica) prije prihvaćanja plaćanja. U ovom slučaju sustav se zove online sustav plaćanja. Za komunikaciju između trgovca i banke može se koristiti bilo koji komunikacijski medij (ne nužno Internet). Ako ovakav kontakt s trećom stranom nije potreban za vrijeme protokola plaćanja, kažemo da se radi o offline sustavu. U ovom sustavu trgovci se trebaju javljati banci na regularnoj osnovi za obračun svih primljenih uplata.

Ovjera autentičnosti tajnim ključem i javnim ključem

Osnovni zahtjev protokola plaćanja je da se omogući trgovcu primanje uplata od bilo kojeg kupca. Plaćanje se može smatrati nekom vrstom ovjere autentičnosti kupca prema trgovcu (dokazivanje da je plaćanje autentično). Ovjera autentičnosti može se temeljiti na kriptografiji tajnog ili javnog ključa. Trgovac samo treba imati javni ključ na raspolaganju kako bi provjerio dolazna plaćanja. Iako se očekuje da će troškovi opremanja pametnih kartica (smart cards) kripto koprocesorima postati marginalni, važno je napomenuti da se svojstvo javne provjere može dobiti samo pomoću pametne kartice pod uvjetom da se odnosi na metodu koju zovemo prijenos potpisa. U takvom sustavu potpise je stvorio izdavatelj, a kasnije su potvrđeni od strane kupca. Trik je u tome da se postigne da dovoljno plaćanja može biti obavljeno između ponovnog učitavanja novca, što zahtijeva optimalnu upotrebu ograničene količine EEPROM-a [1] dostupnog na jednostavnim pametnim karticama. Još jedna prednost je u tome što tajni ključ za stvaranje potpisa koristi samo izdavatelj. U slučaju kada je provjera autentičnosti temeljena na kriptografiji javnog ključa (simetrična), kupac i trgovac moraju imati dostupan zajednički tajni ključ kako bi dovršili plaćanje. Jednostavno rješenje je dati svim korisnicima isti tajni ključ, no to se općenito smatra nesigurnim, jer to bi značilo da će razbijanje jedne pametne kartice (tj. otkrivanje njenog tajnog ključa) biti dovoljno da se razbije cijeli sustav. Standardno rješenje je razbijanje simetrije između kupca i trgovca opremanjem trgovaca vrlo sigurnim kutijama zaštićenim od neovlaštenog pristupa (tamper-proof) koje se zovu SAM i sadrže glavni ključ. Ključevi kupaca su izvedeni iz ovog glavnog ključa u procesu promjene primjenom kriptografske hash funkcije (npr. SHA-1) na povezanost glavnog ključa i broja kartice kupca. Ideja je da je SAM teže razbiti nego pametnu karticu, ali i da je moguće rutinski provjeriti jesu li SAM-ovi mijenjani (u sklopu održavanja). U EMV standardu[2] prvi korak je napravljen prema uključivanju provjere javnim ključem. Kako bi spriječili prijevare u kojima se uvode kartice s lažnim brojevima, svaka kartica nosi fiksni RSA certifikat koji pokazuje valjanost broja kartice. Na početku svake

[1] (engl. Electrically Erasable Programmable Read-Only Memory, električno izbrisiva programibilna ispisna memorija) vrsta je ispisne memorije koja se može brisati i ponovno programirati električnom strujom. To je i vrsta memorije za trajno pohranjivanje podataka pri čemu se jednom upisani podatci mogu izbrisati, ali samo električno, pri čemu se neki memorijski čipovi prije brisanja uklanjaju iz računala, a neki, poput flash memorije, ne.

[2] EMV je thenički standard za plaćanja pametnim karticama te za terminale plaćanja i bankomate. Nastao je 1993. godine kao rezultat zajedničkog rada vodećih svjetskih platnih institucija: Europaya, Mastercarda i Vise.

uplate, certifikat može potvrditi protiv javnog ključa spremljenog u POS terminalu[3]. Ostatak protokola plaćanja ponovno se oslanja na tajni glavni ključ koji je pohranjen u SAM-u POS terminala.

Brojači i novčanice
Izravan način prikaza elektronskog novca je korištenjem brojača pohranjenog na pametnoj kartici. To je učinkovit i fleksibilan način, a svaki iznos može biti plaćen karticom sve dok ne prelazi vrijednost brojača. Drugi način je prikaz elektronskog novca elektronskim novčanicama. Kao i kod običnih novčanica, svaka elektronska novčanica ima fiksnu vrijednost. Svaki iznos može biti plaćen kad god se može dobiti kao zbroj vrijednosti podskupa dostupnih novčanica. Pomoću odgovarajuće raspodjele vrijednosti novčanica pri stavljanju novca na račun, kao funckije očekivanog uzorka potrošnje, može se u većini slučajeva spriječiti da plaćanje ne može biti dovršeno iako je ukpna vrijednost novčanica dovoljna. Projekt CAFE[4] oslanja se na kompromis između ova dva osnovna načina. Za svako plaćanje potrebni iznos se oduzme od brojača, a u isto vrijeme je jedna posebna novčanica iskorištena. Nakon ponovnog stavljanja novca na račun, brojaču se pripiše povučeni iznos i ponuda novčanica se dopuni. Važno svojstvo po kojem se razlikuju novčanice i brojači je da su e-novčanice jedini način za postizanje sigurnosti sustava (u interesu banke), koji istovremeno štiti privatnost korisnika. Niti jedna stranka osim banke nije u mogućnosti stvoriti novčanice. Jedini način da se napadne sustav je da se udvostruči novac koji je već u opticaju, ali to se lako zaustavi praćenjem utrošenih novčanica.

Samo-softver i hardver otporan na "uplitanje"
Uz pretpostavku da je kupcima i trgovcima potreban neki računalni uređaj za sudjelovanje u elektronskom sustavu plaćanja, važna razlika je sadrži li uređaj hardver otporan na uplitanje ili ga ne sadrži. Ako nijedan dio uređaja nije otporan na uplitanje (tj. sigurnost sustava se ne oslanja na takve pretpostavke), tada sustav nazivamo samo-softver. Pametne kartice i SAM kartice su primjeri uređaja otpornih na uplitanje. Neke od prednosti samo-softver sustava su da se može distribuirati lako i po niskoj cijeni, može izvoditi na bilo kojem računalu te korisnici ne moraju imati poseban hardver. Važne prednosti upotrebe hardvera otpornog na uplitanje su da su pohrana i korištenje tajnih ključeva dobro zaštićeni te da kritični dijelovi sustava rade u sigurnom okruženju.

[3]POS (point-of-sale) terminal je računalna zamjena za blagajne POS terminal ima mogućnost snimanja i praćenja narudžbi kupca, obrade kreditnih i debitnih kartica, povezivanja s drugim sustavima u mreži i upravljanja inventarom.

[4]CAFE (Conditional Access For Europe) je projekt Europske zajednice koji je razvio siguran elektronički sustav plaćanja koji štiti privatnost korisnika. Uključilo je trinaest partnera iz nekoliko zemalja, a cilj je bio napraviti elektronske novčanike koji je mogu koristiti za plaćanje, za pristup informacijama i ukoliko je potrebno, za identifikaciju.

3 Elektronski novac

3.1 Uvod u elektronski novac

Internet je povezao ljude širom svijeta te tako omogućio tvrtkama da nude proizvode i usluge bez fizičke prisutnosti pred kupcima ili eventualnim kupcima. Internet je postao dio svakodnevnog života što zahtijeva stvaranje sve više aplikacija i dostupnih usluga. U skladu s online poslovnim transakcijama, elektronski novac je jedna od usluga koja privlači ljude da obavljaju poslovne transakcije elektronskim putem. Elektronski novac je zamjena za tradicionalne kovanice i papirnate novčanice čija upotreba nije moguća za e-trgovinu. Druga alternativa za online plaćanje su kreditne kartice, međutim sheme poput kreditnih kartica zahtijevaju evidentiranje transakcija u pojedinim računima. Ova metoda zahtijeva povjerenje od strane trgovca, što je obično olakšano od strane tijela za provjeru kao što su izdavatelji kreditnih kartica ili payment gatewaya (Internet servis plaćanja). Zbog uvjeta povjerenja, ova metoda eliminira transakcijsku anonimnost trgovac-kupac. Sustav zasnovan na tokenima kao što je elektronski novac ne zahtijeva da transakcije budu zabilježene budući da sam token omogućuje izravnu potvrdu od strane trgovca.

Iako elektronski novac može ostvariti anonimnost u implementaciji, također može biti implementiran tako da mu se može ući u trag zbog sigurnosnih razloga. Može biti implementiran na dva načina, online i offline. Online znači da je e-novac pohranjen od strane banke ili izdavatelja i kupac ga treba zatražiti pri plaćanju. Offline elektronski novac čuva kupac na uređajima poput pametnih kartica ili drugih tipova tokena. Svaka ova implementacija može biti klasificirana kao identificirana (može joj se ući u trag) ili anonimna (ne može joj se ući u trag). Kod identificirane implementacije svaka transakcija zahtijeva verifikaciju i validaciju treće strane kao što je banka. Ova implementacija nudi bolju sigurnost jer koristi šifriranje i digitalni potpis za osiguranje i potvrdu e-novca. Identificirana implementacija omogućuje bankama da pronađu pojednice koji koriste e-novac kako bi se izbjegla dvostruka potrošnja. Pogodna je za veći broj transakcija, a posebno za sustav koji je dostupan na internetu. Međutim, daje kupcima manje slobode u usporedbi s tradicionalnim gotovinskim transakcijama gdje kupci mogu potrošiti novac gdje i kada žele bez potrebe treće osobe za verifikaciju. Anonimna implementacija je bliža tradicionalnom sustavu plaćanja kovanicama i papirnatim novčanicama. Provedba je moguća pomoću slijepog/digitalnog potpisa. Slijepi potpis se koristi za kriptiranje poruka i potpisivanje u svrhu provjere autentičnosti. Kada je potpisan slijepim ili digitalnim potpisom, dokument se šalje u banku. Banka može osigurati autentičnost dokumenta ali ne zna tko ga je poslao te stoga identitet kupca nije otkriven. Zatim banka potpisuje dokument i time ga ovjerava. Ova implementacija je prikladna za mikro plaćanja, međutim može uvesti problem dvostruke potrošnje. Čak i ako banke otkriju problem, teško je ući u trag krivcu.

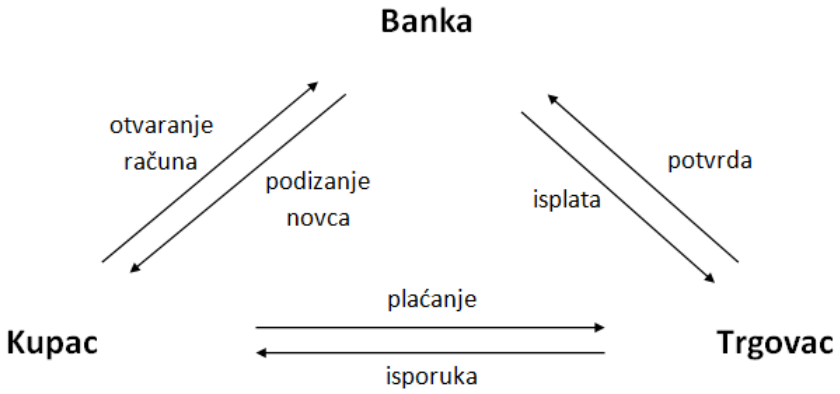
Uvedeno je i razvijeno mnogo sustava e-novca, no osnovna ideja uključuje najmanje tri stranke: izdavatelja koji nije nužno financijska institucija, kupca kao krajnjeg korisnika e-novca i trgovca koji prihvaća e-novac u zamjenu za proizvode ili usluge.

1. Kupac mora otvoriti račun u banci. Trgovac koji želi sudjelovati u transakcijama e-novcem mora imati račune u različitim bankama kako bi bile podržane transakcije kupca koji može koristiti bilo koji bankovni račun. S druge strane, banke će rukovati računima i kupca i trgovca.

2. Kada se kupac odluči za kupnju, prenijet će e-novac sa svog bankovnog računa u elektronički novčanik (online sustav) ili na token (offline sustav). E-novac tada može

biti prenesen trgovcu u zamjenu za njegova dobra ili usluge. Plaćanje se može obaviti putem softwarea ili temeljem tokena. Transakcije putem interneta su obično šifrirane.

3. Po primitku uplate e-novca od strane kupca, trgovac će dobiti potvrdu od banke. Banka će tada potvrditi autentičnost transakcije. U isto vrijeme banka će teretiti račun kupca temeljem ugovorenog iznosa. Trgovac zatim isporučuje proizvode ili usluge i nalaže banci da uplati ugovorenu svotu na njegov račun.



Slika 1: Proces elektronskog novca

3.2 Svojstva elektronskog novca

Kako bi zamijenio kovanice i papirnate novčanice, e-novac bi trebao imati jednako dobra svojstva. Neke važne značajke kovanica i papirnatih novčanica su: prenosivost, prihvatljivost, djeljivost, anonimnost te da im se ne može ući u trag. Dalje su navedena neka važna svojstva za implementaciju e-novca.

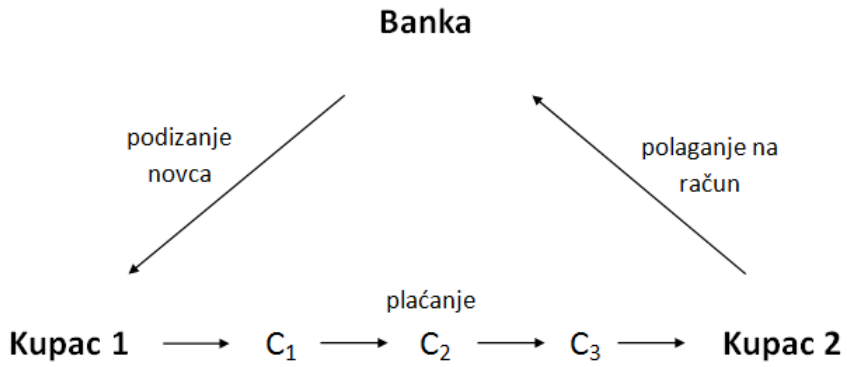
1. Sigurnost
   Kako bi sustav elektronskog novca bio prihvaćen, sigurnost je jedan od glavnih problema koje treba razmotriti. Originalnost poruke koja se prenosi između kupca, trgovca i banke mora biti osigurana kako bi spriječila bilo kakva neovlaštena presretanja ili mijenjanje sadržaja poruke. Kako bi e-novac bio zaštićen od takve ilegalne aktivnosti, sustav mora posjedovati kvalitetu kao što su integritet, mogućnost za provjeru autentičnosti i neosporavanje. Prije uključivanja u transakciju ili izvršenja bilo koje transakcije svi sudionici moraju znati s kim rade. Integritet se postiže tako da poruka poslana od strane kupca, trgovca ili banke mora biti nepromijenjena kada dođe odgovarajućem primatelju. Nakon što su postigli integritet i autentičnost, trgovci, kupci i banke više ne mogu osporiti transakciju.

2. Privatnost
   Privatnost znači postojanje anonimnosti za kupce koji su izvršili plaćanje. Slično kao s kovanicama i papirnatim novcem, ne bi trebao postojati trag ili veza s pojedincem koji koristi e-novac za bilo koju transakciju. Ovo svojstvo je potrebno kako bi se zaštitila

privatnost kupca od praćenja u svrhu financijskog nadzora. Međutim, anonimnost nameće određene opasnosti kao što su krivotvorenje, pranje novca i ucjene. Kupci bi trebali biti svjesni da više anonimnosti pruža manje sigurnosti.

3. Pokretnost
   Elektronski novac treba biti pokretan, slično kao i konvencionalni novac koji ne ovisi o fizičkoj lokaciji. E-novac treba biti prenosiv putem mreže na prijenosne uređaje za pohranu.

4. Prenosivost
   Ova značajka omogućuje korisnicima prijenos e-novca od jedne osobe drugoj bez obraćanja banci. Slično konvencionalnom novcu koji se može lako prenijeti, e-novac bi trebao imati jednaku mogućnost. Međutim ovo svojstvo nameće problem dvostruke potrošnje kojoj se ne može ući u trag jer bi se mogao prenijeti različitim subjektima više puta.



Slika 2: Prenosivost elektronskog novca

5. Djeljivost
   Ovo svojstvo znači da elektronski novac mora posjedovati sposobnost da se podijeli u manje vrijednosti kako bi bile moguće transakcije manjih iznosa (mikroplaćanje). Izazov za djeljive sustave je mogućnost podjele vrijednosti e-novca na manje vrijednosti tako da je ukupna vrijednost manjih jednaka originalnoj vrijednosti.

3.3 Tijek novca

Potrebno je razlikovati banke elektronskog novca (ili izdavatelje) i institucije koje stvaraju elektronski novac (eng. e-cash mint). Takva institucija je komponenta sustava elektronskog novca gdje se stvara novac i održavaju baze podataka o utrošenom novcu. Račun elektronskog novca čini sučelje između banke i kovnice. U praksi, postoji nekoliko načina za prijenos novca s računa i na račun. Na primjer, izdavatelj elektronskog novca može omogućiti kućnu bankarsku aplikaciju koja omogućuje svojim korisnicima da premještaju novac između bankovnih računa i računa elektronskog novca. Druga mogućnost je da banka prihvaća plaćanja kreditnom karticom pomoću koje korisnici mogu vršiti uplate na račune elektronskog novca.

Usredotočit ćemo se na osnovne radnje potrebne za rukovanje elektronskim novcem:

- **Podizanje novca iz banke**
  Pomoću protokola podizanja novca, korisnici su u mogućnosti pretvoriti novac sa svojih računa elektronskog novca (e-računa) u novčanice e-novca. Pristup računu elektronskog novca je moguć samo ako je korisnik u mogućnosti potpisati zahtjev za podizanje novca, gdje se potpis uspoređuje s javnim ključem registriranim za taj račun. Jednostavan način za postavljanje klijenta je pretpostaviti da su softver i javni ključ banke na siguran način dani korisniku. Korisnik dobiva od banke broj računa i PIN kod, te kod kuće instalira klijenta e-novca, generira svoj par privatni ključ/javni ključ i registrira ga sa svojim računom tako da sve zajedno s PIN kodom pošalje banci (sve je šifrirano javnim ključem banke). Korisnikov privatni ključ može biti pohranjen na tvrdom disku i zaštićen šifriranom lozinkom. Podignute novčanice su pohranjene na korisnikovom tvrdom disku. Novčanice su zaštićene kriptiranom zaporkom kako bi se spriječila krađa, tj. kopiranje.

- **Plaćanje**
  Kako bi određeni iznos bio plaćen, odabire se skup novčanica tako da je ukupni zbroj vrijednosti jednak potrebnom iznosu. U online sustavu, ovaj skup novčanica se šifrira za banku koristeći javni ključ banke, kako bi se spriječila krađa ili kopiranje. Trgovac stavlja taj iznos u banku koja ga dodaje na njegov račun tek nakon provjere jesu li novčanice valjane i jesu li prije potrošene. Prihvaćene novčanice se dodaju u bazu podataka utrošenih novčanica tako da dvostruka trošenja mogu biti otkrivena.

- **Polaganje novca u banku**
  U online sustavu ovaj protokol je dio protokola plaćanja koji se izvršava od strane trgovca. U offline sustavu, ovaj protokol se izvršava u neko drugo vrijeme (batch mode - transakcije se akumuliraju tijekom određenog vremenskog razdoblja i obrađuju u redovitim intervalima).

- **Otkup novca**
  Moguće je da se novac vrati izravno izdavatelju bez upotrebe u plaćanju. Broj novčanica koje korisnik otkupljuje ne smije biti veći od broja novčanica koje je podigao iz banke. Ovaj protokol se koristi ukoliko su novčanice zastarjele ili se želi promijeniti raspodjela vrijednosti novčanica.

- **Oporavak**
  Ukoliko žele, korisnici mogu vratiti novčanice koje su izgubili, npr. prilikom pada sustava. Pomoću posebnog protokola oporavka izvršenog između korisnika i izdavatelja, mogu se rekonstruirati sve novčanice koje je korisnik povukao iz banke nakon posljednje točke provjere. Rekonstruirane novčanice su otkupljene od izdavatelja koji odobrava samo one novčanice koje nisu prije utrošene.

3.4 Elektronske novčanice

Promotrit ćemo unutarnju strukturu novčanica elektronskog novca. Za svako generiranje novčanice izdavatelj nasumično generira novi RSA modul $N = pq$, čuvajući proste brojeve p i q tajnima. Privatni ključevi bi se trebali koristiti samo na uređajima koji su otporni na manipuliranje, dok sigurnosne kopije čuva nekoliko subjekata koristeći tehnike tajne podjele. Na taj način su spriječeni, koliko je to moguće, napadi na privatne ključeve iznutra.

Apoeni novčanica su kodirani pomoću različitih javnih eksponenata ali s istim modulom. Neka k označava broj različitih apoena novčanica i neka $\{e_i\}_{i=1}^{k}$ označava prvih k prostih

brojeva, $k \neq 2$. Kako bi svaki e_i bio valjan RSA eksponent, imamo uvjet da je svaki e_i relativno prost s $\varphi(N)$, $(e_i, \varphi(N)) = 1$ za $i = 1, \ldots, k$. Apoen novčanice koja je povezana s javnim eksponentom e_i označili smo s D_{e_i}. Novčanice elektronskog novca su zapravo RSA potpisi malih poruka. Tako imamo sljedeći izraz, gdje se novčanica C apoena D_e sastoji od samo jednog RSA potpisa:

$$C = f(x)^{1/e} \bmod N.$$

Zbog konkretnosti pretpostavljamo da je x duljine 160 bita, i neka $\mathcal{H}$ označava jednosmjernu hash funkciju čija je izlazna vrijednosti duljine 160 bita te $\|$ označava operator ulančavanja[5]. Funkcija f je funkcija redundancije definirana s

$$f(x) = x_t \| \ldots \| x_1 \| x_0$$

gdje je $x_0 = x$ i $x_{i+1} = \mathcal{H}(x_0 || \ldots || x_i)$. Parametar t je fiksan tako da je ukupna duljina od $f(x)$ približno jednaka veličini modula N. Funkcija f može biti definirana s $f(x) = y_t$, gdje je $y_0 = x$ i $y_{i+1} = \mathcal{H}(y_i)||y_i$. Funkcija f očito nije jednosmjerna funkcija jer $f(x)$ sadrži ulaznu varijablu x kao podniz.

U sadašnjim implementacijama e-novca RSA moduli koji se koriste za novčanice su veličine najmanje 768 bita. Za ovu veličinu krivotvorenje se smatra potpuno neisplativim unutar ograničenog vremena u kojem novčanice vrijede. Dakle, potrebno je skladištenje od oko 100 bitova po novčanici na korisnikovoj strani. Uz današnje tvrde diskove i memorijske čipove ne postoji nikakav problem za pohranu bilo kojeg broja novčanica.

Nakon provjere valjanosti potpisa novčanice i provjere da novčanica nije već utrošena, dovoljno je pohraniti samo broj novčanice. Kao što je opisano, veličina broja novčanice je određena na 20 bajta. Jedini uvjet na veličinu brojeva novčanice je da bude dovoljno velik kako bi se spriječilo da se isti broj ponovno generira, tj. dovoljno je da su brojevi novčanica jedinstveni. Po standardnom rezultatu paradoksa rođendana, vjerojatnost da dvije novčanice neće biti jednake kada su brojevi novčanica slučajno odabrani uniformno iz $\{0,1\}^{160}$ je omeđena približno s $e^{-B(B-1)/2^{161}}$, sve dok je generirano najviše B novčanica istog tipa. To pokazuje da je vjerojatnost da se brojevi dviju novčanica podudaraju je zanemariva za bilo koji broj novčanica B. Budući da je broj novčanica po generiranju ograničen, ova analiza prikazuje da veličina brojeva novčanica može biti ograničena na $64-80$ bitova ($8-10$ bajta). Dakle, tvrdi disk kapaciteta 1 GB može pohraniti 100 milijuna brojeva novčanica.

Osim RSA modula, e-novčanica ima sljedeće atribute: identitet izdavatelja, slijed denominacija, valutu i datum isteka. Privatni ključ može biti uklonjen čim se podizanje novca iz banke deaktivira, dok javni ključ mora biti dostupan sve dok je novčanica važeća.

Postoje dva razloga zašto se novčanice redovito obnavljaju, npr. svakih šest mjeseci. Prvo, standardni razlog je da se ograniči rizik ugrožavanja tajnog ključa. Postoje dva izravna načina za ugrožavanje. U prvom, napadač će pokušati pronaći tajni ključ samo iz javnog ključa, vjerojatno koristeći potpis izdavatelja. U drugom načinu, napadač jednostavno pokuša doći do tajnog ključa provaljivanjem u banku ili na svojoj računalnoj mreži, eventualno uz pomoć iznutra.

Drugi razlog je da se ograniči baza podataka "potrošenih novčanica". Potrošene novčanice se prvo pohrane na disk kako bi se omogućila brza provjera duplikata. Nakon nekog vremena se uklone iz baze podataka ali i dalje je moguće provjeriti duplikate korištenjem sporije procedure (dostupna samo da korisnici mogu vratiti novčanice kada nisu koristili svoj e-novac duže vrijeme). Na kraju novčanica postane nevažeća i bude potpuno uklonjena.

[5]U matematici je ulančavanje spajanju dvaju brojeva po njihovim znamenkama. Ulančavanje od 123 i 456 je 123456. Ulančavanje brojeva a i b označava se s $a\|b$.

Osim podjele u vremenu, gdje se novčanice obnavljaju svakih šest mjeseci, možemo koristiti i podjelu u prostoru. Umjesto da gledamo na sve korisnike kao jedan veliki skup korisnika, podijelimo korisnike u klastere. Svaki klaster je dovoljno velik tako da ponašanje pojedinih korisnika nije vidljivo. Ograničavanjem veličine klastera koji odgovaraju dijelovima baze potrošenih novčanica, klasteri su neovisni jedan o drugom, što poboljšava fleksibilnost sustava.

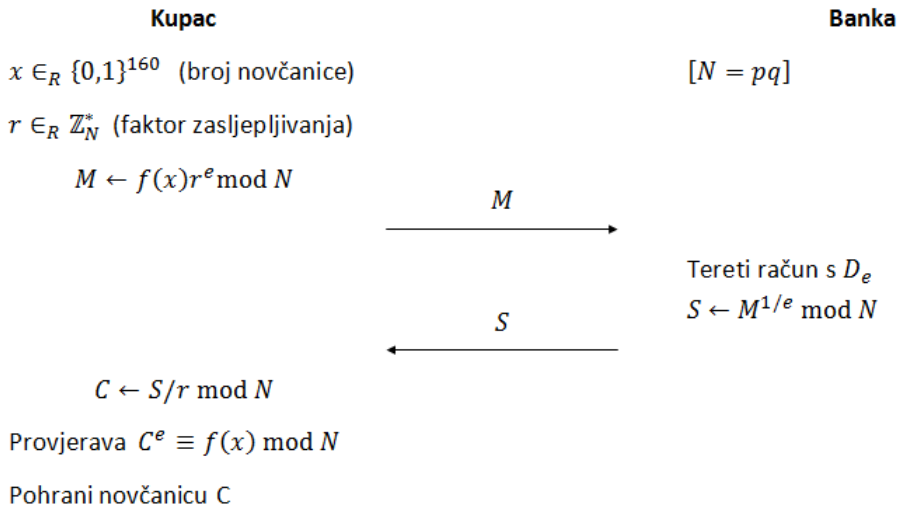
Način na koji banka dijeli korisnike u klastere treba biti javno provjerljiv, a ne prema nahođenju banke (kako bi se spriječilo da banka uvodi nekoliko malih klastera). Postoji mnogo načina za postizanje takve poštene podjele u klastere. Jednostavna ideja je da se prvo uzme kriptografski hash identitet korisnika, a zatim definira 2^t klastera, $t \geq 0$, gledajući prvih t bita hash vrijednosti. Pod pretpostavkom da banka ne može utjecati na korisnički identitet (tj. zastupljenost), korisnici su ravnomjerno raspoređeni po klasterima.

4 Protokoli

4.1 Podizanje novca iz banke

Za povlačenje svake novčanice s korisnikovog bankovnog računa, korisnik i izdavatelj izvršavaju Chaumov protokol slijepog potpisa. Ovaj protokol se izvodi paralelno onoliko puta koliko je potrebno da bi se podigao željeni iznos.

Osim slučajnog odabira broja novčica x, korisnik bira i broj $r \in \mathbb{Z}_N^*$ [6], čija se $e-$ta potencija koristi za slijepi potpis "poruke" $f(x)$. Kako inverz $1/r$ postoji, faktor zasljepljivanja može biti uklonjen kako bi se dobila novčanica $C = f(x)^{1/e} \bmod N$. Potpuni protokol podizanja novca ovisi o dva koraka. Korisnik šalje ovjeren zahtjev za podizanje novca banci, koji sadrži između ostalog popis $M-$poruka, jedan za svaku novčanicu koji bi podigao. Uz prepostavku da je na korisnikovom računu dovoljno novca, banka odgovara porukom koja sadržu odgovrajući popis $S-$poruka.



Slika 3: Podizanje novčanice $C = f(x)^{1/e} \bmod N$ apoena D_e

Što se tiče sigurnosti ovog dijela sustava, važno je odgovoriti na pitanje je li neisplativo dobiti više novčanica od propisanog u protokolu na slici. Prema analizi sigurnosti (u razumnom modelu), ukoliko se na bilo koji način dobije više nego je propisano protokolom, radi se o razbijanju RSA pretpostavke (RSA pretpostavka otprilike kaže da je neisplativo izračunati $y^{1/e}$ za nasumično odabrani $y \in \mathbb{Z}_n^*$). Objasnit ćemo dva aspekta ove analize koji su specifični za sustav e-novca.

Prvo, činjenica je da ne koristimo samo jedan nego niz javnih eksponenata s istim RSA modulom za kodiranje različitih apoena novca. Postavlja se pitanje, mogu li se novčanice nižih vrijednosti kombinirati u novčanice viših vrijednosti. Formalnije je li za nasumično odabrani $M \in \mathbb{Z}_N^*$ moguće izračunati M^{1/e_k} iz vrijednosti $M, M^{1/e_1}, \ldots, M^{1/e_{k-1}}$, pri čemu su e_i relativno prosti. Za različite svrhe, ali primjenjivo na ove postavke, pokazano je da je odgovor na ovo pitanje negativan: obzirom na vrijednosti $M, M^{1/e_1}, \ldots, M^{1/e_{k-1}}$ izračunavanje je jednako teško kao da te vrijednosti nisu ni dane.

[6] $\mathbb{Z}_N^*$ je skup svih invertibilnih elemenata u $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ kojeg nazivamo sustav najmanjih nenegativnih ostataka modulo N.

Sljedeća činjenica je da će banka samo prihvatiti bilo koju poruku M i vratiti $S = M^{1/e} \bmod N$ korisniku ali svaki put teretiti korisnikov račun s D_e, čak i kada korisnik preuzme poruku M u pogrešnom obliku. Dakle, ne postoji jamstvo da je poruka M u propisanom obliku $f(x)r^e$, gdje korisnik zna x, r, što je u suprotnosti sa standardnim postavkama RSA potpisa, gdje potpisnik osigurava da je svaka potpisana poruka oblika $f(m)$. U stvari, pomoću primjera ćemo pokazati da je moguće dobiti valjan novac, iako se odstupa od propisanog protokola. Ipak, korisnikov račun se tereti ukupnom vrijednošću dobivenog novca tako da ne postoji problem sigurnosti.

Pretpostavimo da želimo podići dvije novčanice $C_1 = f(x_1)^{1/e_1}$ i $C_2 = f(x_2)^{1/e_2}$ redom apoena D_{e_1} i D_{e_2}. Učinit ćemo sljedeće:

1. Tražiti od banke da potpiše $M_1 = f(x_1)^{e_2} f(x_2)^{e_1}$ za apoen D_{e_1}, što daje $S_1 = M_1^{1/e_1}$.

2. Nakon toga, tražiti od banke da potpiše $M_2 = S_1$ za apoen D_{e_2}, što daje $S_2 = M_2^{1/e_2} = M_1^{1/e_1 e_2} = f(x_1)^{1/e_1} f(x_2)^{1/e_2}$

3. Konačno, koristeći činjenicu da je $(e_1, e_2) = 1$, postoje cijeli brojevi t_1, t_2 tako da $t_1 e_1 + t_2 e_2 = 1$, možemo izdvojiti C_1 i C_2 iz S_2

$$S_2^{t_2 e_2} f(x_1)_1^t f(x_2)^{-t_2} = f(x_1)^{(t_2 e_2 + t_1 e_1)/e_1} = C_1$$

$$S_2^{t_1 e_1} f(x_1)^{-t_1} f(x_2)^{t_2} = f(x_2)^{(t_1 e_1 + t_2 e_2)/e_2} = C_2.$$

Dakle, iako ne slijedimo prethodno opisani protokol, u mogućnosti smo dobiti dvije valjane novčanice. Međutim dobili smo dvije novčanice ukupne vrijednosti $D_{e_1} + D_{e_2}$, ali i račun je terećen točno tim iznosom. Odstupanjem od propisanog protokola nećemo ništa dobiti. Ovakve devijacije mogu se koristiti za poboljšanje protokola. Potpuno je sigurno da će koraci 1 i 2, gdje banka izda potpis obzirom na eksponent $e_1 e_2$ i naplati $D_{e_1} + D_{e_2}$ za ovu uslugu, biti neuspješni. To dvostruko smanjuje troškove komunikacije s bankom, a poštedi banku obavljanja jednog potpisivanja.

4.2 Plaćanje

Prije nego što se plaćanje izvrši, kupac i trgovac se moraju dogovoriti što je objekt koji će biti kupljen i za koji iznos X. Neka je rezultat tog pregovaranja zabilježen u nizu `pay-spec`. Glavno svojstvo protokola plaćanja je da banka neće saznati ništa o `pay-spec` osim njegove hash vrijednosti. Kako bi se spriječilo da su moguće vrijednosti niza `pay-spec` ograničene na mali skup (a time i da je banka u mogućnosti pogoditi vrijednost `pay-spec` iz hash vrijednosti), potrebno je da `pay-spec` bude slučajno odabran (uključujući neke slučajno odabrane nizove, često se spominje "salt" ili "začinjavanje"). Zatim će kupac odabrati skup novčanica $C_1, \ldots, C_l$ tako da je ukupna vrijednost jednaka traženom iznosu X. Kako bi platio trgovcu s identiteton ID_{shop}, kupac sastavlja poruku za plaćanje koja se sastoji od niza `pay-spec` i šifriranu poruku za banku:

$$Y = E_{PK_{bank}}(ID_{shop} || \mathcal{H}(\texttt{pay-spec}) || C_1 || \ldots || C_l),$$

gdje $E()$ označava hibridnu RSA metodu šifriranja (pomoću trostrukog korištenja DES kriptosustava). Nakon primitka ove poruke, trgovac će potpisati i proslijediti poruku koja se sastoji od $\mathcal{H}$(`pay-spec`) i šifriranu poruku Y banci. Banka dešifrira Y, provjerava vrijednosti ID_{shop} i $\mathcal{H}$(`pay-spec`) te na kraju provjerava valjanost novčanica $C_1, \ldots, C_l$. Kada su

sve novčanice prihvaćene, plaćanje je potvrđeno, što znači da su novčanice dodane u bazu podataka o utrošenom novcu te je na račun trgovca dodan iznos X.

Važno je da ni trgovac ni prisluškivač ne mogu izvući novac iz poruke plaćanja. U ovom slučaju javni ključ je potreban jer banka i kupac ne mogu koristiti zajednički tajni ključ kako bi kupac ostao anoniman. Iako niz `pay-spec` nije poznat banci, trgovac je siguran da kupac koristi isti niz jer banka uspoređuje hash vrijednosti kupca i trgovca. Na taj način detalji transakcije ostaju skriveni banci. Kasnije, ako je potrebno, kupac ili trgovac mogu otkriti `pay-spec` kako bi se usporedio s podacima pohranjenim u banci.

Zbog problema s mrežom, protokol plaćanja može biti prekinut u nekoliko faza, a kupcu je važno samo znati što se od sljedećeg dogodilo:

- plaćanje nije obrađeno od strane banke ili nije uplaćeno na račun trgovca
- plaćanje je obrađeno od strane banke i uplaćeno na račun trgovca.

Kako bi otkrio status plaćanja, kupac može otkupiti novac $C_1, \ldots, C_l$ pojedinačno, ili saznati o potpunoj uplati slanjem poruke Y banci. Tada kupac dokazuje da je on vlasnik uplate otkrivajući vrijednost `pay-code`, na koju se korisnik opredijelio uključujući $\mathcal{H}$(`pay-code`) u poruci Y (ovo opredjeljenje je izostavljeno u gornjem opisu). Ako je uplata na račun trgovca izvršena, banka potpisuje takvu izjavu da je korisnik može pokazati trgovcu i tako dokazati da je iznos uplaćen.

4.3 Oporavak

Slično kao što postoje načini za dobivanje prekinutih plaćanja natrag, postoje i mjere za vraćanje prekinutog podizanja novca. Na primjer, u slučaju kada su sve informacije na korisnikovom tvrdom disku oštećene, protokol oporavka omogućuje korisniku da počne ispočetka s novcem koji je pohranjem na disku u trenutku pada. Ovo je moguće pod uvjetom da su slučajno odabrani brojevi novčanica i faktori zaslјepljivanja korišteni u protokolu podizanja novca generirani pseudo-slučajno. Na početku korisnik e-novca dobije niz znakova za oporavak koje je potrebno pohraniti na sigurno mjesto. Kao dio oporavka, korisnik i izdavatelj novca surađuju kako bi rekonstruirali sve novčanice koje su povučene nakon prethodne točke provjere. Nakon toga, sve rekonstruirane novčanice su otkupljene i korisniku se nadoknade novčanice koje nisu utrošene.

Jasno je da niz znakova za oporavak mora biti dovoljno dug (najmanje 16 bajta) kako bi bilo neisplativo doći do njega iscrpnom potragom. Zatim, važno je i da izdavatelj osigura da protokol oporavka ne daje novac koji zapravo nikada nije ni bio povučen od strane korisnika. U tu svrhu izdavatelji vode dodatne evidencije za podizanje novca. Uočimo da kada god korisnik zatraži oporavak, dio privatnosti je narušen jer banka sazna koje su novčanice potrošene od posljednje točke provjere.

5 Elektronski novac kojemu se ne može ući u trag

Generiranje elektronskog novca bi trebalo biti teško za bilo koga, osim ako je učinjeno u suradnji s bankom. Shema RSA digitalnog potpisa može se koristiti za dobivanje e-novca kojemu se ne može ući u trag. Taj novac može biti u obliku $(x, f(x)^{1/3} \bmod N)$ gdje je N složeni broj čija je faktorizacija poznata samo banci i f je odgovarajuća jednosmjerna funkcija. Protokol za izdavanje i trošenje takvog novca može se sažeti na sljedeći način:

1. Kupac odabire nasumice x i r, banci daje $B = r^3 f(x) \bmod N$.
2. Banka izračuna treći korijen od B modulo N: $r \cdot f(x)^{1/3} \bmod N$ i povlači jedan dolar s računa kupca.
3. Kupac izvede $C = f(x)^{1/3} \bmod N$ iz B.
4. Kako bi kupac platio trgovcu 1 dolar, daje mu $(x, f(x)^{1/3} \bmod N)$.
5. Trgovac odmah nazove banku koja potvrđuje da ova elektronska novčanica još nije položena.

Svatko može lako provjeriti ima li novčanica pravu strukturu i je li potpisana od strane banke, dok banka ne može povezati određenu novčanicu s kupcem. Ovaj pristup uklanja potrebu da trgovac mora kontaktirati banku za svaku transakciju. Ako kupac koristi novčanicu samo jednom, njegova privatnost je bezuvjetno zaštićena, ali ako je ponovno koristi, banka može pratiti njegov račun i dokazati da ju je koristio dva puta.

5.1 Novčanice kojima se ne može ući u trag

Banka inicijalno objavljuje RSA modul N čija je faktorizacija tajna i za koji $\varphi(N)$ nema malih neparnih faktora. Banka također postavlja neki parametar sigurnosti k. Neka su f i g funkcije dva argumenta bez kolizije, tj. za bilo koju takvu funkciju je neisplativo naći dvije ulazne varijable koje se preslikavaju u istu točku. Zahtijevamo da f bude "slučajno predvidiva" (eng. random oracle[7]). Kako se novčanicama bezuvjetno ne bi moglo ući u trag zahtijevamo da g ima svojstvo da fiksiranje prvog argumenta daje bijekciju s drugog argumenta na kodomenu.

Kupac ima bankovni račun numeriran s u te banka ima brojač v povezan s njim. Neka operator $\oplus$ označava isključivo ili te $\|$ operator ulančavanja. Kako bi dobio elektronsku novčanicu, kupac provodi sljedeći protokol s bankom:

1. Kupac odabire a_i, c_i, d_i i $r_i, 1 \leq i \leq k$, nezavisno i uniformno nasumično iz skupa ostataka pri dijeljenju s N.
2. Kupac formira i šalje banci k zaslijepljenih kandidata (pod nazivom B)

$$B_i = r_i^3 \cdot f(x_i, y_i) \bmod N, \quad 1 \leq i \leq k,$$

gdje je

$$x_i = g(a_i, c_i) \quad y_i = g(a_i \oplus (u \,\|\, (v+i)), d_i).$$

3. Banka odabire slučajni podskup $k/2$ indeksa zaslijepljenih kandidata $R = \{i_j\}, 1 \leq i_j \leq k$ za $1 \leq j \leq k/2$ i šalje ga kupcu.

[7] za svaki ulaz je izlaz slučajno na uniforman način odabran iz kodomene

4. Kupac pokaže vrijednosti r_i, a_i, c_i i d_i za svaki $i \in R$ i banka ih provjeri. Uočimo da je $u \parallel (v+i)$ poznato banci. Radi jednostavnosti, pretpostavit ćemo da je $R = \{k/2+1, k/2+2, \ldots, k\}$.

5. Banka kupcu daje
$$\prod_{i \notin R} B_i^{1/3} = \prod_{1 \le i \le k/2} B_i^{1/3} \bmod N$$
i tereti njegov račun jednim dolarom. Banka također poveća brojač v za k.

6. Kupac tada može jednostavno izvesti novčanicu
$$C = \prod_{1 \le i \le k/2} f(x_i, y_i)^{1/3} \bmod N.$$
Kupac ponovno indeksira kandidate u C tako da vrijedi $f(x_1, y_1) < f(x_2, y_2) < \cdots < f(x_{k/2}, y_{k/2})$. Kupac također poveća svoj primjerak brojača v za k.

Za bilo koji fiksni ϵ, ako manje od $1-\epsilon$ od ukupno k zaslijepljenih kandidata B_i ima odgovarajući oblik $(r^3 f(g(a_i, c_i), g(a_i \oplus (u \parallel (v+i)), d_i)))$, tada će kupac biti uhvaćen s vjerojatnosti $1 - exp(-c\epsilon k)$ za neku konstantu c.

Kako bi trgovac dobio dolar, kupac i trgovac postupaju na sljedeći način:

1. Kupac šalje trgovcu C.

2. Trgovac bira nasumično binarni niz $z_1, z_2, \ldots, z_{k/2}$.

3. Za svaki $1 \le i \le k/2$ kupac odgovara na sljedeći način

   a) Ako je $z_i = 1$, kupac šalje trgovcu a_i, c_i i y_i

   b) Ako je $z_i = 0$, kupac šalje trgovcu $x_i, a_i \oplus (u \parallel (v+i))$ i d_i.

4. Trgovac provjerava je li C odgovarajućeg oblika i odgovaraju li odgovori kupca.

5. Trgovac kasnije šalje C i odgovore kupca banci. Banka zatim provjerava ispravnost i dodaje novac na račun trgovca.

Banka mora pohraniti C, binarni niz $z_1, \ldots, z_k$ i vrijednosti a_i za $z_i = 1$ te $a_i \oplus (u \parallel v)$ za $z_i = 0$.

Ako kupac iskoristi istu novčanicu C dva puta, tada postoji velika vjerojatnost da mu se uđe u trag. Dva različita trgovca će poslati komplementarne binarne vrijednosti za najmanje jedan bit z_i za koji B_i ima odgovarajući oblik. Banka može jednostavno pretražiti svoje evidencije kako bi utvrdila da C nije bio korišten prije. Ako kupac koristi C dva puta, banka s velikom vjerojatnošću posjeduje i a_i i $a_i \oplus (u \parallel (v+i))$. Stoga, banka može izolirati u i pratiti plaćanja računa kupca.

Mogući problem je dosluh između kupca i drugog trgovca. Nakon transakcije s prvim trgovcem, kupac opiše transakciju drugom trgovcu, i oba trgovca pošalju banci iste informacije. Banka s velikom vjerojatnošću zna da jedan od njih laže, ali ne postoji način da otkrije koji niti da poveže novčanicu s računom kupca.

5.2 Dokazivanje dvostrukog trošenja

Prethodno objašnjena shema ima svojstvo da banka može optužiti kupca za višestruko trošenje, ali takva shema ne može imati nikakav pravni značaj. Kako bi se spriječilo lažno optuživanje pretpostavljamo da kupac ima shemu digitalnog potpisa i ovjerenu kopiju svog javnog ključa. Budući da koristimo digitalni potpis, kupac je zaštićen od zavjere samo računski, a ne bezuvjetno. Ipak, privatnost kupca ostaje bezuvjetno zaštićena.

Umjesto upotrebe istog broja računa u za sve novčanice dane kupcu, u će se razlikovati za svaku novčanicu i za svakog zaslijepljenog kandidata. Opisat ćemo izmjene osnovne sheme.

Kupac bira nasumično dva cijela broja z'_i i z''_i za svaki i. Tada u_i može biti odabran u obliku "Broj računa kupca"$\| z' \| z''$. Zajedno sa zaslijepljenim kandidatima (B_i vrijednosti) kupac isporučuje banci digitalni potpis na

$$g(z'_1, z''_1) \parallel g(z'_2, z''_2) \parallel \cdots \parallel g(z'_k, z''_k).$$

Provedbom metode "podijeli i izaberi" (eng. cut and choose), banka potvrđuje da svaki od $k/2$ B_i-ova koje ispituje generiraju odgovarajuće u_i. Banka ima pravni dokaz da kupac ponovno koristi novčanicu svaki put kada može izvesti prasliku najmanje $k/2 + 1$ od $g(z'_i, z''_i)$.

Kupac nema nade ako banka može razbiti shemu potpisa koju je izabrao. Pod pretpostavkom da banka ne može krivotvoriti potpis, tada čak i ako može razbiti g, njegovo ranije spomenuto bijektivno svojstvo osigurava, s velikom vjerojatnošću, da banka može dokazati da je g razbijena pokazivanjem (z'_i, z''_i) za bilo koji razbijeni $g(z'_i, z''_i)$. Ovo je dokaz, jer je pretpostavka da samo banka, a ne kupac, može razbiti g.

5.3 Čekovi kojima se ne može ući u trag

Sljedeća shema oponaša koncept čekova, ali osigurava da im se ne može ući u trag. Kupac zatraži skup čekova, pri čemu može koristiti svaki ček za bilo koji iznos do svog limita i kasnije može zatražiti povrat novca za razliku (limit - stvarni iznos). Banka neće znati gdje je novac potrošen, niti će znati tko je nositelj transakcije.

Kupac može generirati nekoliko čekova u jednoj interakciji s bankom. Čekovi su slični osnovnoj verziji opisanoj u 5.1, ali prvih j faktora koristi se za šifriranje iznosa kupovine dok se sljedećih $k - j$ faktora kako bi se spriječilo da kupac koristi ček više puta. Banka izdaje dva različita RSA modula, N i N', koji se koriste za dvije različite vrste digitalnog potpisa. Kupčev u može se koristiti na jedan od dva prethodno opisana načina, te neka je kao i prije v osobni brojač kupca.

Kupac šalje t parova većih i manjih kandidata. Za svaki veći kupac odabire nasumično b, c, d i a. Veći kandidat M_i je oblika $f(x, y)$ gdje je $x = g(a \parallel b, c)$ i $y = g(a \oplus (u \parallel (v+i)), d)$. Svaki manji kandidat je oblika $g(b, e)$ gdje je e izabran nasumično. Kupac generira nekoliko većih kandidata $M_1, M_2, \ldots, M_t$ i s njima povezane manje kandidate $m_1, m_2, \ldots, m_t$. Kupac ih zaslijepi prije nego pošalje u banku.

Zaslijepljeni veći kandidati su oblika $B(M_i) = r^{3^k} \cdot M_i \bmod N$, gdje je r odabran nasumično. Zaslijepljeni manji kandidati su oblika $B(m_i) = r^{3^k} \cdot m_i \bmod N'$. Ako banka da neki 3^i-ti korijen zaslijepljenog većeg (manjeg) kandidata, $i \leq k$, tada kao i prije kupac može izračunati odgovarajući korijen.

Kupac šalje zaslijepljene M_i i m_i u banku. Slično kao u prethodnom poglavlju, banka obavlja operaciju "podijeli i odaberi", potvrđujući da je polovina parova odgovarajućeg oblika. Tada banka slučajno permutira ostale, grupirajući ih u određene skupove veličine k.

Neka je jedan takav skup radi jednostavnosti označen s $B(M_1), B(M_2), \ldots, B(M_k)$. Banka izračuna sljedeće korijene.

$$F_i = B(M_i)^{1/3^i} \bmod N \quad \text{za} \quad 1 \leq i \leq k,$$

$$D_i = B(m_i)^{1/3^i} \bmod N' \quad \text{za} \quad 1 \leq i \leq k.$$

Sada banka vraća produkt k korijena od zaslijepljenih većih kandidata ($\prod_{i=1}^{k} F_i$), a odgovarajući korijeni j zaslijepljenih manjih kandidata su vraćeni pojedinačno. Kupac izdvaja ček

$$C = \prod_{i=1}^{k} M_i^{1/3^i}$$

i $E_1, E_2, \ldots, E_j$ gdje je $E_i = m_i^{1/3^i}$.

Banka sada poveća brojač kupca v za t, kupac isto učini sa svojim. Za obavljanje kupnje ovakvim čekom, kupac šifrira iznos kupnje smatrajući prvih j od M_i lokacija apoenima čekova $1, 2, \ldots, 2^{j-1}$. Ako je i-ti apoen dio u ukupnom iznosu kupovine, tada kupac otkriva trgovcu odgovarajući y_i i prasliku od x_i. Ako i-ti apoen nije dio u ukupnom iznosu kupovine, kupac otkriva x_i i y_i. Dakle, kasnije predstavljanje E_i i unutarnje strukture M_i banci za povrat je sigurno kada taj apoen nije potrošen.

Ukoliko je dan korijen oblika $x^{1/3^i}$, lako je izračunati korijen oblika $x^{1/3^j}$ za $j \leq i$. Stoga je kupac mogao koristiti apoen 2^j, ne koristiti 2^i, $j < i$, i banci dati

$$E_i^{i-j} = (m_i^{1/3^i})^{i-j} = m_i^{1/3^j} = g(b, e)^{1/3^j} \bmod N'$$

tvrdeći da je to potpisani manji kandidat za neiskorišten apoen 2^j. Banka nema traga odgovorajućoj b vrijednosti i odobrit će povrat. Srećom, to ne bi bilo u interesu kupcu, budući da bi dobio manji povrat nego što ima pravo.

Posljednji $k - j$ veći kandidati sprječavaju kupca da koristi ček više od jednom, čak i ako je iznos kupovine jednak. Kupac međutim ima dobre šanse za uspješno varanje banke s obzirom na povrat novca. Potrebna su samo dva nepovezana veća i manja kandidata. Ipak, ova vrsta varanja je daleko manje opasna nego posjedovanje otvorenog čeka koji se može iznova koristiti. Banka može kazniti kupca poništavanjem očekivane dobiti kupca kada otkrije pokušaj varanja.

5.4 Sumnjiva podizanja novca iz banke

Ukoliko kupac koristi novčanicu dva puta, banka može staviti na crnu listu sve novčanice koje je kupac podigao. To znači da sve novčanice kupca moraju biti povezane na neki način. Ideja je šifrirati neke redundanciju u "nasumičnom" izboru kupca koja može biti prepoznata samo kada kupac troši novčanicu više od jednom.

Razmotrimo osnovnu shemu: Kupac šalje banci k zaslijepljenih kandidata oblika

$$r^3 f(g(a, c), g(a \oplus (u \parallel (v + i)), d)),$$

gdje a, c i d bira kupac nausmično, v je kupčev brojač, i je serijski broj kandidata i u je broj računa kupca. Modificirat ćemo protokol tako da kupac generira b elektronskih novčanica istovremeno.

Kupac šalje banci bk zaslijepljenih kandidata u obliku matrice

$$\begin{pmatrix} B_{11} & B_{12} & \dots & B_{1k} \\ B_{21} & B_{22} & \dots & B_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ B_{b1} & B_{b2} & \dots & B_{bk} \end{pmatrix}.$$

Banka zahtijeva da vidi $k/2$ stupaca u cijelosti. Svaki B_{ij} mora biti oblika

$$r_{ij}^3 f(g(a_{ij}, c_{ij}), g(a_{ij} \oplus (u \parallel k_{ij} \parallel (v + ki + j)), d_{ij})).$$

Kupac odabire r_{ij}, a_{ij} nasumično za zaslijepljen član i k_{ij} nasumično po stupcu.

Neka je h_i familija jednosmjernih funkcija. Svaki c_{ij} je oblika $h_{ij}(c'_{ij}) \parallel c'_{ij}$, a svaki d_{ij} je oblika $h_{ij}(d'_{ij}) \parallel d'_{ij}$. Kupac odabire c'_{ij} i d'_{ij} nasumično za zaslijepljene članove.

Banka može jednostavno provjeriti jesu li $k/2$ stupaca koje vidi odgovarajućeg oblika. Zbog jednostavnosti oznaka, pretpostavimo da banka želi vidjeti stupce $k/2+1, \dots, k$. Zatim banka daje kupcu b produkata

$$P_i = \prod_{1 \le j \le k/2} B_{ij}^{1/3} \bmod N$$

i tereti njegov račun s b dolara.

Kupac tada može jednostavno izvesti

$$C_i = \prod_{1 \le j \le k/2} f(g(a_{ij}, c_{ij}), g(a_{ij} \oplus (u \parallel l_j \parallel (v + ki + j)), d_{ij}))^{1/3} \bmod N, \quad \text{za } 1 \le i \le b.$$

Kupac raspoređuje faktore u leksikografski poredak. Ove novčanice su korištene kao u osnovnoj shemi, samo što trgovac ima skup indeksa s crne liste L. Ako trgovac pošalje $e_j = 1$, kupac mora otkriti odgovarajuće a, c, i y. Trgovac izračuna $f(g(a, c), y)$ i provjerava zadovoljava li $c = c''$ izraz $c'' = h_l(c')$ za svaki $l \in L$. Slično, ako trgovac pošalje $e_j = 0$, kupac mora otkriti odgovarajuće $x, a \oplus (u \parallel h_j \parallel (v + ki + j))$ i $d = d'' \parallel d'$. Ponovno, trgovac provjerava vrijedi li $d'' \neq h_l(d')$ za svaki $l \in L$.

Ako kupac koristi bilo koju novčanicu više od jednom, banka dodaje odgovarajuće k_j na crnu listu koja je dostupna trgovcima.

6 Primjeri implementacije elektronskog novca

6.1 First Virtual

First Virtual Holdings osnovao je Lee Stein krajem 1994. godine te je to prva tvrtka koja omogućuje prijenos elektronskog novca putem Interneta. Sustav ovisi o elektronskoj pošti kao sredstvu komunikacije između kupca, trgovca i First Virtual. Kupci moraju dati svoje brojeve kreditnih kartica u zamjenu za First Virtual e-novac. First Virtual sustav radi na sljedeći način:

1. Kupac otvara račun u First Virtual te mora imati račun elektronske pošte i kreditnu karticu. First Virtual će dati kupcu identifikacijski broj kao zamjenu za njegovu kreditnu karticu.

2. Kada kupac želi kupiti nešto od trgovca koji prihvaća First Virtual identifikacijski broj, kupac će pregovarati o cijeni s trgovcem. Nakon dogovorenog, kupac će dati trgovcu svoj First Virtual identifikacijski broj.

3. Trgovac šalje e-mail serveru plaćanja First Virtual koji sadrži ID trgovca, ID kupca i opis transakacije (ugovorena cijena).

4. Po primitku trgovčevog e-maila, server šalje e-mail za potvrdu kupcu.

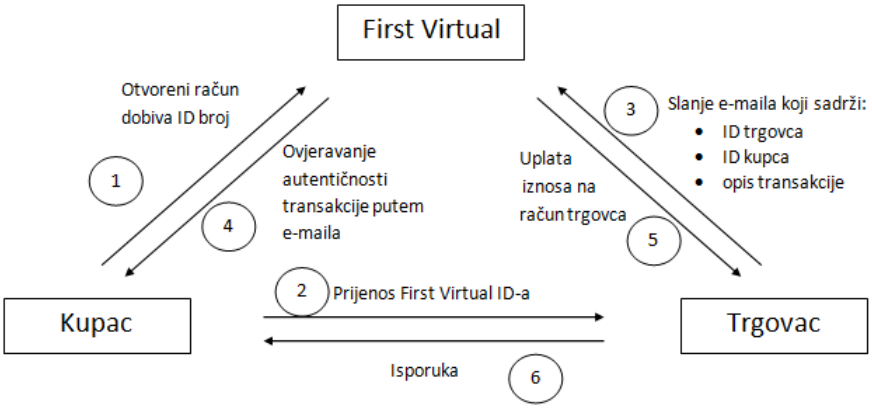
5. Kupac mora odgovoriti na e-mail jednim od sljedećih odgovora:

   - DA, što znači da se kupac slaže s transakcijom i omogućuje da First Virtual uputi banku da tereti njegovu kreditnu karticu navedenim iznosom.
   - NE, što znači da se kupac ne slaže s transkacijom i stoga plaćanje neće biti obavljeno. First Virtual snima sve odbijene transkacije kako bi se izbjeglo iskorištavanje trgovca. Kupci koji prečesto odbijaju transakcije, bit će suočeni s mogućnosti ukidanja računa.
   - PRIJEVARA, kupac nije pokrenuo transkaciju. First Virtual će provesti istragu kako bi se utvrdila istina.

6. Kada First Virtual prizna da je plaćeno kreditnom karticom kupca, iznos će biti dodan na račun trgovca.

First Virtual se može kategorizirati kao online implementacija gdje se svaka transkacija bilježi i prati s potrebom ovjere od strane treće osobe. To znači da sustav ne osigurava privatnost kupca. Uz transakcije kupac-trgovac, First Virtual nudi i prijenos e-novca od osobe do osobe. Stoga je e-novac prenosiv. Ovaj sustav je pokazao da je upotrebom elektronske pošte e-novac više prenosiv budući da kupci mogu obaviti transakciju bilo kada i bilo gdje, sve dok postoji pristup elektronskoj pošti.

Ovaj sustav ne koristi ni šifriranje ni digitalni potpis prilikom slanja e-maila kupca trgovcu, trgovca First Virtalu, First Virtuala kupcu i obrnuto. Iako sustav tvrdi da se sigurnost postiže tako što se ne vrši prijenos brojeva kreditnih kartica putem Interneta, ali prijenos First Virtual identifikacijskog broja od kupca do trgovca nije osiguran i može biti presreten. Također naglašavaju da je verifikacija kupca putem e-maila dovoljna da osigura transakciju, no e-mail poruka je prenesena na otvorenu mrežu u obliku otvorenog teksta gdje se e-mail može presresti. Iako First Virtual ne koristi šifriranje, moguće je da sve uključene strane



Slika 4: Tijek First Virtual sustava

zaštite svoje e-mailove i transakcije. Kupci mogu šifrirati svoje e-malove prije slanja (npr. PGP[8]), trgovci mogu razviti sigurnu komunikacijsku aplikaciju za kupce pomoću protokola poput SSL za prijenos First Virtual ID-a i trgovci mogu koristiti zaštićen e-mail za slanje podataka banci.

6.2 CyberCash

CyberCash je američko poduzeće koje su osnovali Bill Melton i Daniel Lynch 1994. godine. CyberCash koristi takozvani "Novčanik" kao medij za rukovanje kreditnim karticama, valutama, čekovima i CyberCoin-ima. CyberCoin je sustav za obradu mikroplaćanja manjih od 10 $. Osim usluga kupac-trgovac, sustav podržava i usluge kupac-kupac. CyberCash radi na sljedeći način:

1. Kupac zatraži "Novčanik " preuzimanjem besplatnog softvera s CyberCash internetskog poslužitelja. Softver će uspostaviti veze između kupca, trgovca i banke. Kupac će tada dobiti 768-bitni RSA ključ i koristiti lozinku kako bi osigurao ključ.

2. Nakon što se kupac odluči za kupnju, šalje svoj "Novčanik" putem softvera za komunikaciju pritiskom na gumb "PAY". Sustav će tada aktivirati CyberCash softver trgovca. Trgovac šalje kupcu elektronski račun s detaljima transakcije.

3. Po primitku računa, kupac će potpisati račun dodavanjem svog broja kreditne kartice, imena s kreditne kratice i datuma isteka kartice. "Novčanik" će šifrirati potpisani dokument s CyberCash javnim ključem i poslati ga CyberCash-u i trgovcu.

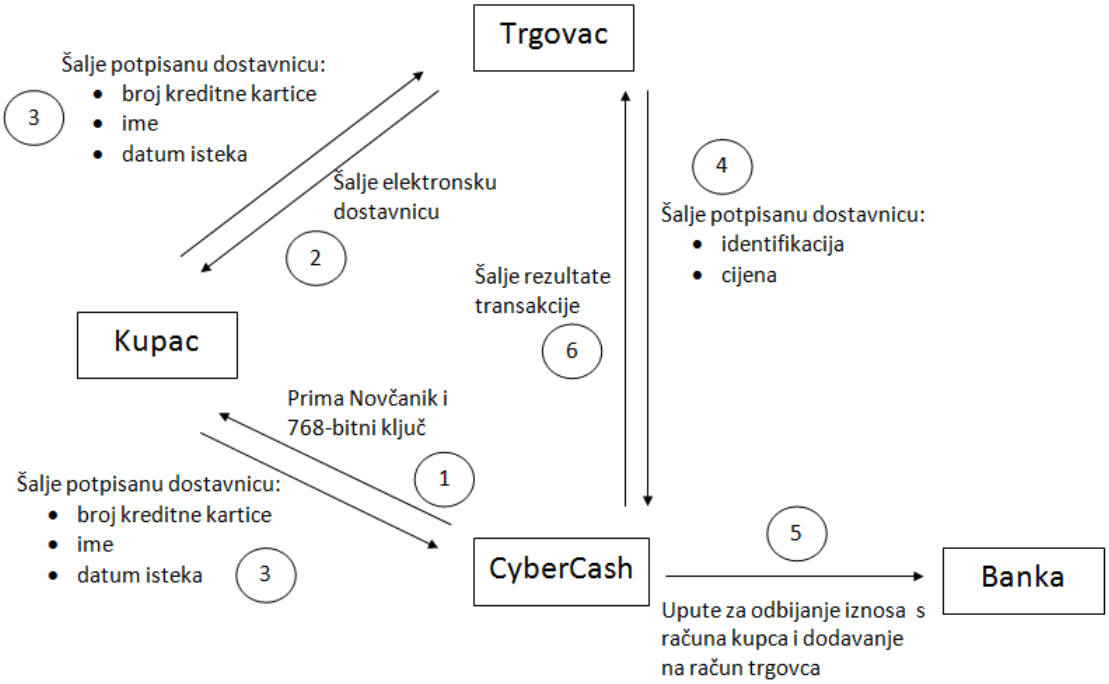
4. Trgovac koji je dobio potpisani dokument će zatim dodati svoje identifikacijske podatke i cijenu prije potpisivanja i proslijediti dokument CyberCash-u.

5. CyberCash je dobio potpisane dokumente od kupca i trgovca te će ih otkriti (eng. unblind) i usporediti navedenu cijenu. Ako je navedena cijena ista, CyberCash će

[8]PGP (Pretty Good Privacy) je računalni program za kriptografsku zaštitu podataka koji je 1991. godine razvio Phil Zimmermann. PGP je svojevrsna sigurnosna nadogradnja sustava elektroničke pošte, koji korisnicima omogućuje da izmjenjuju datoteke ili poruke vodeći računa o povjerljivosti, autentičnosti i praktičnosti.

uputiti banku na oduzimanje dogovorenog iznosa s kreditne kartice kupca, te dodavanje istog iznosa na račun trgovca. Zatim će detalje transakcije poslati trgovcu.

6. Konačno, trgovac će isporučiti kupljeni proizvod ili uslugu.



Slika 5: Tijek CyberCash procesa

CyberCash temelji se na online implementaciji elektronskog novca. Svaka transakcija se bilježi, može se ući u trag i potrebna je potvrda treće strane. Upotreba šifriranja omogućuje da dokumenti budu ovjereni. Sustav podržava svojstvo djeljivosti uvođenjem CyberCoin-a. Međutim, CyberCash ne štiti privatnost kupca jer su identiteti kupca i trgovca otkriveni prije izvršenja transakcije. U smislu prenosivosti, "Novčanik" se može instalirati samo na računalo kupca. Stoga on može obavljati transakcije samo s računala na kojem je "Novčanik" instaliran.

6.3 DigiCash

DigiCash osnovao je David Chaun 1994. godine i nalazi se u Amsterdamu. Sustav je osmišljen na temelju Chaumovog digitalnog sustava plaćanja. DigiCash sustav koristi digitalni potpis za šifriranje i slijepi potpis za provjeru autentičnosti kako bi se osigurala sigurnost transakcija i zaštitili kupci, trgovci i banka od nezakonitih aktivnosti. DigiCash je dizajniran tako da pruža mogućnost plaćanja s jednog računala na drugo putem Interneta. Elektronski novac koji je uveo DigiCash zove se "ecash" i koristi RSA algoritam za šifriranje. Sustav radi na sljedeći način:

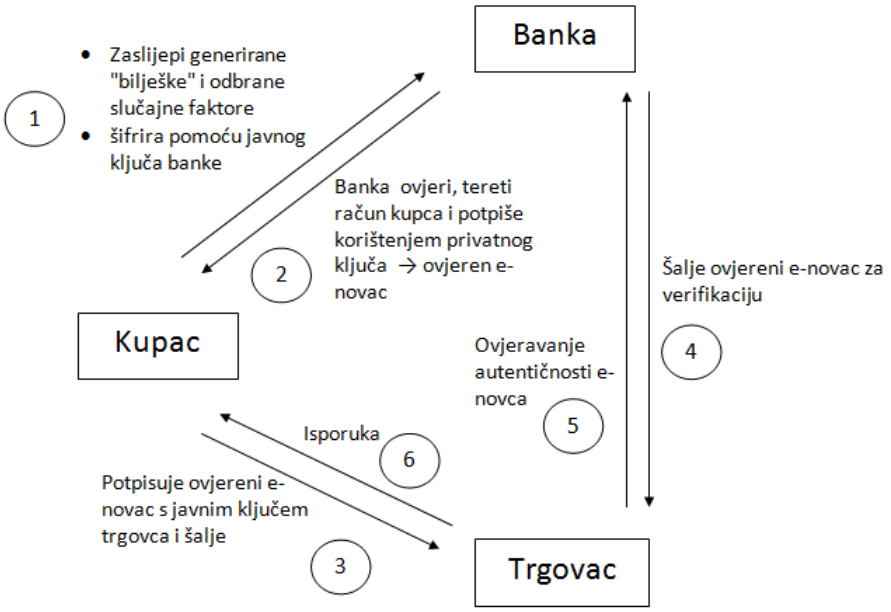
1. Kupac koji želi koristiti DigiCash mora otvoriti račun u banci koja pruža online DigiCash sustav.

2. Kada kupac prvi put na računalu pokrene ecash softver, generirat će par ključeva, javni i tajni. Kupac će zadržati tajni ključ koji se koristi za potpisivanje transakcije. Javni ključ će biti na raspolaganju bankama, trgovcima i drugima za provjeru poruka ili e-novca prenesenog od kupca.

3. Kada se kupac odluči na kupnju, njegovo računalo će odrediti vrijednosti potrebnih novčanica i generirati slučajne serijske brojeve koji se ponašaju kao "bilješke" za svaku vrijednost novčanice. Računalo će generirati i odabrani slučajni faktor za zaslijepljivanje vrijednosti novčanica, tj. slučajnih serijskih brojeva. Zaslijepljeni slučajni serijski brojevi ili zaslijepljene "bilješke" su onda šifrirane javnim ključem banke prije slanja banci na ovjeravanje.

4. Banka dešifrira poruku koristeći svoj tajni ključ. Nakon što je poruka dešifrirana, banka će teretiti račun kupca iznosom iz poruke. U zamjenu za terećeni iznos, banka tada potvrdi zaslijepljene "bilješke " pronađene u poruci svojim tajnim ključem. Potpisane zaslijepljene "bilješke" se šalju natrag kupcu koji će izvući zaslijepljeni faktor prije upotrebe "bilješki" u plaćanju. Slučajni serijski brojevi ("bilješke") i potpisi (kupca i banke) čine potvrđeni elektronski novac.

5. Nakon uplate, potvrđeni e-novac se šalje trgovcu koji će ga poslati u banku na provjeru. Banka će provjeriti je li e-novac važeći i je li već korišten.



Slika 6: Tijek DigiCash procesa

DigiCash sustav pruža anonimnost za online i offline usluge te omogućuje i transfere od kupca do kupca. Ovjereni e-novac je prenosiv. Budući da fizički ne postoji, može se pohraniti i prenijeti na druge uređaje, što ga čini jednostavnim i praktičnim za korištenje. Također štiti privatnost kupca preko slijepog potpisa. Banka ne može napraviti nikakvu vezu s onim tko je potpisao taj dokument jer samo kupac zna slučajni faktor korišten u

slijepom potpisu. Sljedeće svojstvo je djeljivost koje dolazi uvođenjem CyberCoina za rukovanje mikroplaćanjima. DigiCash pruža i bolju sigurnost korištenjem digitalnog potpisa za autentifikaciju poslanih i primljenih poruka. Korištenjem ovog pristupa, javni ključ banke je dostupan i kupcu i trgovcu, što omogućuje objema stranama provjeru autentičnosti poruke. Međutim, nijedna strana ne može krivotvoriti potpis banke jer samo banka ima odgovarajući tajni ključ za potpisivanje (potvrđivanje) e-novca. Kupac je također zaštićen od ilegalnih aktivnosti trgovca.

6.4 Mondex

Razvoj Mondexa počeo je u ranim 90.-im godinama prošlog stoljeća. Briga o sigurnosti dovela je Mondex (aplikacija za e-novac) i Multos (pametna kartica) do najvišeg postignuća u prepoznavanju sigurnosti, razinom E6 nagrađeni su 1999. od strane UK IT security Evaluation and Certification (ITSEC). Priznanje je dokazalo da je Mondex jedna od najsigurnijih aplikacija e-novca koje su dostupne danas. Mondex se temelji na pametnim karticama gdje je e-novac pohranjen u čipu na kartici.

Koncept Mondexa je sličan DigiCash-u. Kupac zatraži e-novac od banke. Kada se odluči za kupnju, e-novac kupca će biti prenesen trgovcu koji ga zatim šalje u banku na provjeru i isplatu. Po primitku e-novca, banka će provjeriti i potvrditi e-novac. Istovremeno će račun kupca biti terećen istim iznosom koji će biti dodan na račun trgovca. Konačno, trgovac će isporučiti proizvode ili usluge kupcu.

Mondex nudi anonimnost u obje svoje usluge, online i offline. Za offline transakcije, trgovac može napraviti provjeru nakon transakcije (to može izložiti trgovca dvostrukom trošenju kojem je teško ući u trag). Osim transakcija potrošač-trgovac, omogućuje i transfer kupac-kupac. Ukratko, Mondex zadovoljava gotovo sva svojstva elektronskog novca. Sigurnost se temelji na digitalnom potpisu, gdje može biti provjerena svaka poruka između banke, trgovca i kupca. Sustav je prijenosan uz korištenje pametnih kartica. Mondex također štiti privatnost kupca pomoću slijepog potpisa. U smislu djeljivosti, sustav je u mogućnosti rukovati mikroplaćanjima od tek jedan cent.

7 Zaključak

Za kupca je elektronski novac više nego prikladan način nošenja gotovine. Kupac mora samo imati pametnu karticu poput uređaja za pokretanje transakcije, bilo online ili offline. Za neke implementacije e-novac može biti pohranjen na računalu za jednostavan prijenos preko Interneta. Provedba anonimnosti daje kupcu privatnost za korištenje e-novca baš kao i konvencionalne kovanice i novčanice. Kupci su također u mogućnosti obavljati transakcije bez provjere treće strane. E-novac omogućuje kupnju malih predmeta putem Interneta, što je nespretno u drugim implementacijama poput kreditnih kartica. Za trgovca, e-novac pruža priliku da proširi svoje poslovanje diljem svijeta bez ograničenja različitim valutama. Korištenjem pristupa identificiranja, trgovac se može zaštiti od prijevare jer svaka transakcija mora biti potvrđena od financijskih institucija ili banaka. Za banke uvođenje e-novca smanjuje trošak držanja novca u banci i time se povećava učinkovitost banke te su u mogućnosti pružiti lakše svoje usluge u svijet putem Interneta.

Jedan od nedostataka e-novca je postojanje krivotvoritelja koji mogu ponovno stvoriti e-novac. Sve uključene strane, kupci, trgovci i banke ili izdavatelji su pogođeni ovim krivotvorenjem. Mogućnost gubitka e-novca na oštećenoj pametnoj kartici ili srušenom računalu na koje je instaliran e-novac također je problem. Iako je broj korisnika Interneta u porastu, postoji mnogo ljudi koji nemaju mogućnost posjedovanja računala ili pristup Internetu. Kupac također mora učiti nove stvari kao što je instaliranje softvera na računalo te mora razumjeti kako softver radi. Broj tvrtki koje sudjeluju je još uvijek nizak a čini se kako tvrtke nisu spremne prihvatiti ovaj sustav kako bi privukli više kupaca. Ova pojava se može odnositi na činjenicu da postoji dodatna naknada kao troškovi obrade banke za trgovca i kupca. Ovi dodatni troškovi nisu problem u konvencionalnom sustavu plaćanja. Problem s e-novcem je praćenje od strane vlade. S konvencionalnim kovanicama i novčanicama vlada može pratiti tijek novca za stabilizirano gospodarstvo. S e-novcem ne može predvidjeti i kontrolirati tijek e-novca u i iz zemlje. Problem je i kako vlada može određivati i prikupljati porez od e-novca kojem se ne može ući u trag.

Kriptografski algoritmi kao što su šifriranje, digitalni potpis i slijepi digitalni potpis imaju važnu ulogu u implementaciji e-novca. Šifriranje omogućuje svim sudionicima (kupcima, trgovcima i bankama) da potvrde izvornost primljene poruke. Rezultat digitalnog potpisa, potvrđenog e-novca, uspostavlja povjerenje između kupca i trgovca. Bilo kakve ilegalne aktivnosti kao što su krivotvorenje od strane kupca ili trgovca mogu biti spriječene jer su samo banke ili izdavatelji u mogućnosti potvrditi ovjereni e-novac. Uvođenje koncepta slijepog potpisa, koji je sličan digitalnom potpisu (osim što se izostavlja identitet kupca), daje kupcima slobodu i privatnost (anonimnost) da potroše svoj e-novac bez praćenja. Kupci imaju izbor da koriste ili slijepi potpis ili digitalni potpis kako bi se osigurala razina sigurnosti sklopljene transakcije, pogotovo kada uključuje makroplaćanje. Najveće priznanje ikada primljeno u području sigurnosti dodijeljeno je Mondexu. Priznanje dokazuje predanost radu na uspostavi sigurnosti kako bi se osiguralo da implementacija e-novca postane stvarnost i bude prihvaćena. Također ukazuje na mogućnost da e-novac postane sustav plaćanja budućnosti.

Literatura

[1] D. Chaum, A. Fiat, M. Naor, *Untraceable Electronic Cash*, Proceedings on Advances in Cryptology, Springer-Verlag New York, USA, 1990.

[2] S. Goldwasser, M. Bellare, *Lecture Notes on Cryptography*, Summer course on cryptography, MIT, 2008.

[3] R. Razali, *The Overview of E-cash: Implementation and Security Issues*

[4] B. Schoenmakers, *Basic Security of the ecash Payment System?*, State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography, Belgium, 1997.

Sažetak

Elektronski novac je sustav plaćanja dizajniran i implementiran za kupovanje preko otvorene mreže kao što je Internet. U radu je osnovna ideja elektronskih novčanica objašnjena u detalje te su opisani osnovni protokoli za rukovanje novčanicama. Osim poznavanja načina naplate, važno je i poznavanje sigurnosti pri obavljanju transakcija elektronskim novcem. Zaštita uključuje kriptiranje podataka između strana koje su uključene u transakciju, provjeru autentičnosti i sprječavanje zlouporabe sustava.

Ključne riječi: *elektronski sustav plaćanja, elektronski novac, RSA kriptosustav, slijepi potpis*

Summary

E-cash is a payment system designed and implemented for making purchases over open networks such as the Internet. In this paper the central notion of electronic coin is treated in detail and the basic protocols are described. Besides from knowing the ways of payment via the Internet, it's also important to know how to safely carry out e-cash transactions. Methods of protection include encrypting the informations between the parties involved in e-cash transactions, checking the authenticity of both parties and preventing the abuse of the system.

Keywords: *electronic payment system, e-cash, RSA cryptosystem, blind signature*

Životopis

Rođena sam 10. prosinca 1991. godine u Kotor Varošu, u Bosni i Hercegovini. 1998. godine sam upisala osnovnu školu u Kutjevu. 2006. godine sam upisala prvi razred prirodoslovno-matematičke gimnazije u srednjoj školi Gimnazija Požega. Nakon završetka srednje škole, 2010. godine, sam upisala Preddiplomski studij matematike na Odjelu za matematiku u Osijeku, te 2013. godine Diplomski studij matematike, smjer Financijska matematika i statistika.