CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Elektronički novac

NCERT-PUBDOC-2010-09-311

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U današnje doba ubrzanog razvoja informatičkih tehnologija, elektroničko poslovanje širi se Internetom i uključuje velikim dijelom prodaju roba i usluga. Elektroničko poslovanje je vrlo prikladno jer kupci i trgovci mogu biti udaljeni i poslovanje traje dvadeset četiri sata dnevno, sedam dana u tjednu. Zbog toga se javlja potreba za brzim, jeftinim i jednostavnim načinom plaćanja preko Interneta. Postojeći načini plaćanja imaju ozbiljne nedostatke jer se radi o klasičnim naplatnim metodama prilagođenim novoj sredini, koji ne zadovoljavaju sigurnosne zahtjeve niti jednako pokrivaju potrebu za velikim, srednjim i mikro novčanim transakcijama.

Elektronički novac je jedan od načina ostvarivanja plaćanja na Internetu. No elektronički novac je i mnogo više od toga. On je zamjena za novac, i plaćanje elektroničkim novcem nalikuje na obično plaćanje gotovinom. Kako se transakcije elektroničkim novcem odvijaju preko Interneta, potrebno je ostvariti visoku razinu sigurnosti takvih transakcija te razviti posebne metode zaštite. Postupci zaštite uključuju kriptiranje prometa između strana koje sudjeluju u novčanim transakcijama, provjeru autentičnosti obiju strana te sprečavanje zlouporabe sustava. Podlogu spomenutim postupcima pružaju kriptografski algoritmi te dodatno razvijeni protokoli koji osiguravaju zaštitu elektroničkog novca, kao i sudionika transakcija. Privatnost i autentičnost su bitne osobine elektroničkog sustava plaćanja.

U ovom dokumentu opisan je elektronički novac, metode plaćanja elektroničkim novcem te sustavi plaćanja. Također, opisani su protokoli koji se primjenjuju kod plaćanja elektroničkim novcem te dani primjeri nekih komercijalnih sustava plaćanja. Razmatrani su i mogući sigurnosni problemi koji se javljaju u elektroničkom poslovanju, te utjecaj elektroničkog novca na ekonomiju i cjelokupno društvo.

2. Što je elektronički novac?

Elektronički novac ili elektronička gotovina jedan je od načina ostvarivanja elektroničkog oblika plaćanja. Spomenuti oblik plaćanja pojavio se kao posljedica širenja Interneta i sve većih mogućnosti koje pružaju računalne mreže. U današnje doba vrlo je jednostavno obavljati kupovinu preko Interneta upotrebom kreditnih i bankovnih kartica, kao i elektroničkog novca. Stalno se povećava broj transakcija putem raznih vrsta bankomata, te pristup uslugama od kuće, telefonom ili osobnim računalom. Smanjuje se važnost poslovnica, a povećava se promet putem informatičkih mreža. Ovakvi trendovi povećavaju zadovoljstvo korisnika, a cijena transakcija se znatno smanjuje. Zanimljiv je podatak da su troškovi transakcije putem Interneta i do 50 puta niži od troškova te iste transakcije u poslovnici banke.

Transakcije je moguće podijeliti na:

- velike – rijetke su i u većini slučajeva korisnik odlazi izravno u banku,
- srednje – ostvaruju najveći promet, jeftine su i brze
- mikro – transakcije ispod 5$, jednostavne i brze

Iako su novčane transakcije putem Interneta vrlo povoljne, svaka se obrada broja kreditne kartice naplaćuje trgovcima oko 10$, što znači da banka na web stranici koja nudi uslugu kupovine preko Interneta s milijun kupaca može zaraditi barem 10 milijuna dolara. Takav način trgovine nije povoljan za trgovce niti za potencijalne kupce koji također ovom prigodom ostave u posredničkoj banci dio novca. Kako bi trgovina na Internetu, odnosno elektronička trgovina, bila što povoljnija za sve stranke osmišljen je elektronički novac. Dakle, razvoj elektroničkog novca potaknut je potrebom za obavljanjem novčanih transakcija preko Interneta uz što manje dodatnih troškova i u što kraćem vremenskom roku.

Ideja kod razvoja elektroničkog novca jest zadržavanje svih prednosti gotovine (papirnatog novca) uz istodobno uklanjanje svih njezinih nedostataka. Prednosti gotovinskog novca su:

- univerzalno je prihvaćen,
- prihvaćen je i od fizičkih i od pravnih osoba,
- kupac ostaje anoniman,
- verifikacija novčanica je jednostavna,
- ne treba imati račun u banci,
- osoba ne treba biti poslovno sposobna (npr. punoljetna),
- lako je prenosiv.

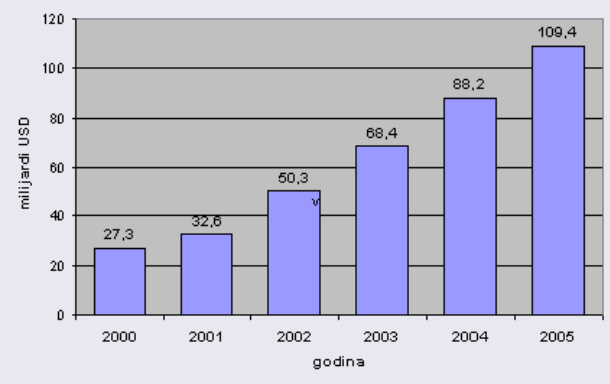
S druge strane, nedostaci su:

- može se krivotvoriti,
- nije praktično nositi velike količine,
- visoki troškovi distribucije i proizvodnje,
- na raspolaganju je ograničen broj nominacija i
- postoji više od jedne valute.

U stvarnosti nije lako zadržati sve prednosti i ukloniti sve nedostatke gotovine. Elektronički novac, za razliku od papirnatog novca, nije prenosiv. Obična novčanica primljena u jednoj od prethodnih transakcija može se ponovno upotrijebiti u nekoj od sljedećih. Ona je prenosiva i traje više od jedne transakcije. Takvo bi svojstvo bilo vrlo poželjno za elektroničke novčanice jer se pri svakoj transakciji novčanica ne bi trebala pohranjivati u banku, smanjujući tako broj interakcija s bankom, a time i troškove sustava. U elektroničkom novčanom sustavu korisnik novčanice bi trebao svakoj novčanici (zapravo skup bitovnih podataka) dodati podatke o svojoj identifikaciji, čime bi veličina novčanice (količina bitovnih podataka pohranjenih u virtualnoj novčanici) rasla svakom transakcijom koja je njome obavljena. Prema tome, broj mogućih transakcija takvom novčanicom bio bi ograničen maksimalnom veličinom novčanice. Zbog takvih nedostataka nisu razvijeni prenosivi sustavi elektroničkog novca i svaka elektronička novčanica ima životni vijek od jedne transakcije.

Elektronički novac, kao i papirnati novac čuva anonimnost osobe koja njime plaća i nije ga moguće pratiti. To znači da osoba koja prima elektroničku novčanicu ne može saznati identitet osobe koja je upotrijebila elektroničku novčanicu, isto kako ni banka koja nije u stanju saznati identitet osobe kojoj je izdala novčanicu, osim u slučaju višestrukog korištenja novčanice, tj. prijevare.

Danas su kreditne kartice standard za kupnju preko Interneta. Nedovoljna sigurnost koja prati uporabu kreditnih kartica rezultira velikim troškovima korištenja. Za plaćanja kreditnim karticama banke naplaćuju tipično 4-6% provizije, dok oko 3% gube zbog prijevara i zlouporaba. Postotak zlouporaba kartica na Internetu znatno je veći nego u klasičnim trgovačkim kanalima. Na primjer, od ukupnog prometa na globalnoj razini najveće svjetske organizacije za plaćanje karticama - VISA-e, svega 2% čine transakcije preko Interneta dok se na njih odnosi više od 50% svih registriranih prijevara i zlouporaba. Ukupna šteta od prijevara na kreditnim karticama 2000. g. iznosila je 1,6 milijardi USD (za usporedbu u 2005. g. oko 15,5 milijardi USD).



Slika 1. Promet ostvaren elektroničkim poslovanjem, procjena do 2005. godine. Izvor: FER

Jedna od najvažnijih uporaba ove nove tehnologije je elektroničko poslovanje - obavljanje financijskih transakcija razmjenom informacija elektroničkim putem. Ključnim za uvođenje elektroničkog poslovanja pokazuje se razvoj sigurnih i učinkovitih elektroničkih sustava plaćanja. Protok elektroničke informacije, kao što je elektronički novac, između dviju strana koje komuniciraju putem Interneta omogućuje njeno nesmetano promatranje i eventualnu zlouporabu od treće strane. Da bi se takve neželjene aktivnosti neutralizirale ili spriječile, koristi se zaštita kriptiranjem te provjera autentičnosti sudionika u transakciji. Podloga takvim postupcima su različiti kriptografski algoritmi i mehanizmi te dodatno razvijeni protokoli više razine koji osiguravaju zaštitu elektroničke informacije kao i privatnost sudionika transakcije. Upravo su privatnost i autentičnost bitne osobine potencijalnog sustava elektroničkog plaćanja.

3. Elektroničko plaćanje

Elektroničko poslovanje je, po definiciji, svaka financijska transakcija koja koristi podatke razmijenjene elektroničkim putem. Elektroničko plaćanje je zaseban dio elektroničke trgovine. Protokol elektroničkog plaćanja čini niz međukoraka na čijem kraju je plaćanje obavljeno. Plaćanje se može obaviti korištenjem tzv. žetona (eng. token), objekata koji sadrže vrijednost i koje je izdao posrednik. Ni osoba koja plaća ni osoba kojoj je plaćena roba ili usluga ne izdaje žeton kojim je plaćanje obavljeno, već obje prihvaćaju žeton kojeg je izdala banka, organizacija ili država kao valjano platežno sredstvo.

Primjer usluge temeljene na istom konceptu je korištenje telefonske kartice. Žetone kojima se plaćaju impulsi izdaje pravna osoba koja je njima i plaćena (telekomunikacijska tvrtka).

U postupku elektroničkog plaćanja postoje tri vrste sudionika:

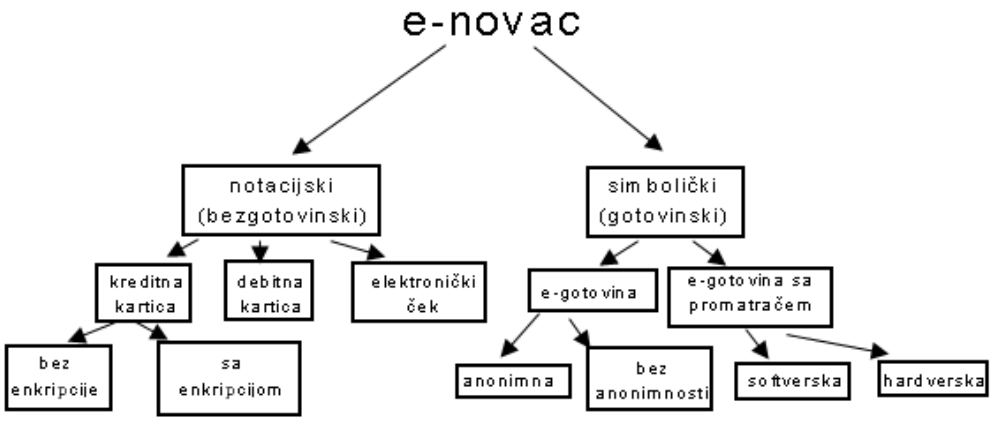
- osoba koja plaća elektroničkim novcem (Kupac),
- osoba koja je plaćena elektroničkim novcem (Trgovac) i
- izdavač elektroničkih novčanica (Banka).

Osnovni protokol elektroničkog plaćanja čine tri koraka:

1. podizanje novca (eng. *withdrawal*) - osoba A u zamjenu za pravi novac dobiva neki oblik elektroničkog novca.
2. plaćanje (eng. *payment*) –osoba A prenosi dio elektroničkog novca osobi B.
3. polaganje novca (eng. *deposit*) - osoba B šalje elektronički novac dobiven od osobe A banci i banka mu zauzvrat povećava stanje na njegovom računu (ili isplaćuje gotovinu).

Elektronička plaćanja po svojoj su funkcionalnosti ekvivalent nekog od klasičnih ne-elektroničkih plaćanja. Vrste plaćanja mogu se podijeliti na dvije skupine:

- notacijsko ili bezgotovinsko i
- simboličko ili gotovinsko.



Slika 2. Elektroničke vrste plaćanja.
Izvor: FER

Razlika između ova dva sustava je u načinu na koji i trenutku kada novac mijenja vlasnika. Notacijski sustav temelji se na dokumentu (nalogu, čeku, kartici) koji sam za sebe nema vrijednost, već je svojevrsni nalog banci gdje je novac pohranjen. Kada se banci predstavi nalog, ona prebacuje novac s računa kupca na račun trgovca. Simbolički sustav se temelji se na simbolu koji nosi u sebi vrijednost (npr. novčanica ili kovanica).

4. Elektronički novčani sustavi

U tehničkom smislu, elektronički novac je virtualna reprezentacija, ili sustav debitnih i kreditnih kartica, koje se koriste za razmjenu vrijednosti s nekim drugim sustavom ili sa samim sobom kao zasebnim sustavom.

Elektronički novčani sustavi se mogu podijeliti na:

- **notacijske sustave,**
- **simboličke sustave,**
- **centralizirane sustave i**
- **decentralizirane sustave.**

S obzirom na tip veze sustavi plaćanja e-novcem mogu se podijeliti u dvije skupine:

- ***online*** sustave – podrazumijeva postojanje stalne komunikacijske veze između osobe koja plaća i banke te se provjera valjanosti novčanice obavlja prije isporučivanja plaćene robe (npr. obavljanje kupovine kreditnim karticama) i
- ***offline*** sustave – podrazumijeva povremenu vezu između osobe koja plaća i banke te se provjera valjanosti novčanica obavlja naknadno, nakon isporuke robe (npr. kupovina čekovima). Nakon obavljene transakcije serijski broj novčanice zapisuje se u bazu podataka banke, te se svaka daljnja novčanica s istim serijskim brojem dospjela na depozit odbija kao krivotvorina.

4.1. Notacijski sustavi

Kod notacijskog sustava kupac koji ima otvoren račun u banci koristeći jedan od oblika bezgotovinskog plaćanja zapravo trgovcu predaje nalog za prebacivanje sa svog računa na račun trgovca. U našem je slučaju to elektronički nalog. To može biti e-ček, kreditna kartica, debitna kartica i slično.

Kod ovih sustava transakcija je izravno ili neizravno vezana uz vrijednost pohranjenu negdje drugdje. Razlikuju se tri potkategorije notacijskih sustava:

1. narudžbe za elektroničko plaćanje prenošene preko mreže,
2. naplata kreditne kartice preko mreža i
3. notacijski sustavi temeljeni na pametnim karticama.

Kod narudžbi za elektroničko plaćanje koje se prenose preko računalne mreže transakcija je izravno povezana s vrijednošću pohranjenom negdje drugdje (uobičajeno na bankovnom računu). Ovakvi sustavi se još nazivaju „plati odmah“ sustavi jer prebacuju polog „odmah“' nakon inicijalizacije zahtjeva za plaćanje. Primjeri takvih sustava su čekovi, debitne kartice i prijenos kredita.

Kod naplata kreditnom karticom preko računalne mreže transakcija je izravno vezana uz vrijednost. Kada se kartica koristi, korisnik prihvaća odgovornost za iznos transakcije. Takav se sustav još naziva i „plati poslije“ sustav. Korisnik može koristiti kriptirane kreditne kartice ili autorizacijske brojeve treće strane za obavljanje transakcija. Ukoliko se koriste kriptirane kreditne kartice, podaci kartice se kriptiraju prije nego se šalju preko otvorene računalne mreže. Autorizacijski brojevi se koriste kod postupka provjere tijekom financijskih transakcija. U ovakvim sustavima postoji i posrednik koji skuplja i odobrava uplate od jednog klijenta prema drugom upotrebom autorizacijskih brojeva.

Notacijski sustavi temeljeni na pametnim karticama koriste tehnologije pametnih kartica. Pametna kartica je plastična kartica veličine kreditne kartice koja ima u sebi ugrađeni čip (mikroprocesor) koji je čini „pametnom“. Pametne kartice su nezavisno razvijene u Njemačkoj (1967), Japanu (1970), SAD-u (1972) i Francuskoj (1974). Kartica omogućuje pohranjivanje, pristup i obradu znatnih količina podataka.

Slika 3. Građa pametne kartice.
Izvor: Tiresias

Pametne kartice se mogu podijeliti prema tipu kontakta:

- kontaktne – podaci i/ili aplikacija pohranjena na čipu prenosi se preko elektroničkog modula koji je spojen na terminal ili čitač kartice,
- bezkontaktne – ovakva kartica posjeduje antenu koja komunicira s antenom za primanje prilikom prijenosa podataka.

Jedan od najznačajnijih događaja u povijesti pametnih kartica je izum programiljive pametne kartice. One omogućuju dodavanje izvršnog koda (programa) pametnoj kartici. U usporedbi s običnom karticom s magnetskom trakom, pametne kartice pružaju povećanu sigurnost, praktičnost i ekonomske koristi. Uz to, sustavi temeljeni na pametnim karticama su vrlo prilagodljivi pojedinačnim potrebama korisnika. Višestruka funkcionalnost, sredstvo plaćanja, aplikacijski i mrežni uređaj čine pametne kartice savršenim korisničkim sučeljem u mobilnoj, mrežnoj ekonomiji.

Pametne se kartice primjenjuju na različitim područjima:

- telefonske kartice,
- mobilne komunikacije,
- satelitska televizija,
- bankarstvo,
- kartično plaćanje,
- za identifikaciju te
- u sustavima elektroničkog plaćanja.

Primjena u sustavima elektroničkog plaćanja je posebno zanimljiva. Sklopovska građa pametne kartice onemogućava neovlašteno čitanje podataka i pruža korisniku mogućnost upotrebe raznih kriptografskih funkcija. Upravo se zbog toga pametne kartice koriste u sustavima elektroničkog plaćanja.

4.2. Simbolički sustavi

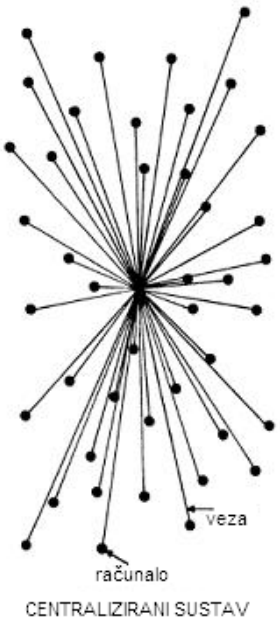
Za razliku od notacijskog sustava gdje novac zapravo nikada ne napušta banku, postoje sustavi kod kojih sama reprezentacija novca nosi njegovu vrijednost. To znači da se iznos na računu umanjuje čim se elektronička novčanica podigne iz banke. Ako se elektronička novčanica izgubi, vlasnik je bez nje ostao trajno. Ova vrsta elektroničkog novca analogna je klasičnoj gotovini i zato se obično naziva e-gotovina.

4.3. Centralizirani sustavi

Centralizirani sustavi se temelje na „plaćanju unaprijed“ i mogu koristiti žetone, tj. objekte koji sadrže vrijednost. Korisnici moraju kupiti žetone od središnjeg autoriteta prije nego što mogu započeti transakciju. Postoje dvije potkategorije sustava sa žetonima:

- **elektronički novac** – pokušava zamijeniti papirnati novac kao glavno sredstvo *online* plaćanja i
- **sustavi elektroničkog novčanika** – temelje se na pametnim karticama (kartice s pohranjenom vrijednosti) koje koriste integrirane čipove za pohranu elektroničkog novca.

Slika 4 prikazuje dijagram centraliziranog sustava. Na slici je moguće uočiti da su sva računala, odnosno korisnici (klijenti) vezani uz jedno središte (poslužitelja) preko kojeg teku sve transakcije. Poslužitelj također nadzire i upravlja svim transakcijama.



Slika 4. Dijagram centraliziranog sustava.
Izvor: Google

Mnogi sustavi, kao što su PayPal, WebMoney i cashU prodaju svoju elektroničku valutu izravno krajnjim korisnicima, dok drugi prodaju samo preko treće stranke.

PayPal, tvrtka čiji je vlasnik eBay, je jedna od najpoznatijih alternativa kreditnim karticama, čekovima i gotovini. Korisnici koji koriste PayPal za plaćanje preko Interneta ne moraju odavati osjetljive podatke, kao što su broj kreditne kartice ili bankovnog računa. Umjesto davanja spomenutih podataka izravno prodavaču, korisnik kaže PayPal aplikaciji da prebaci korisnikovu uplatu na prodavačev račun. Pri tome PayPal identificira korisnika prodavaču isključivo preko adrese elektroničke pošte.

PayPal pruža svoje usluge trgovcima, na aukcijama, te ostalim komercijalnim korisnicima kojima naplaćuje proviziju. Katkad također naplaćuje transakcijsku proviziju za primanje novca. Provizija se naplaćuje ovisno o:

- tome koja se valuta koristi,
- odabranom tipu plaćanja,
- državi u kojoj se korisnik nalazi,
- državi u kojoj je primatelj,
- iznosu novca i
- tipu računa primatelja.

WebMoney je također sustav za plaćanje elektroničkim novcem. Osnovan je 1998. godine i njegovo središte se nalazi u Belizu (Središnja Amerika). U početku su ciljani korisnici bili ruski klijenti, no sada je dostupna svim korisnicima diljem svijeta. Svaki se račun vodi u valuti koja je ekvivalent zlatu, američkim dolarima, rubljima, eurima ili hrivnjama (ukrajinska valuta). Računi se identificiraju prema nizu znakova zvanim WM-ID. Vlasnici računa su međusobno potpuno anonimni. Primanje i slanje WM-jedinica (novca koji je ekvivalent jednoj od nabrojanih valuta) između korisnika je besplatno. Slanje WM-jedinica na druge račune uključuje proviziju od 0.8%. Sredstva se mogu staviti ili povući s WebMoney računa upotrebom naloga za prijenos novca, prijenosom preko banke (eng. *wire transfer*), pretvorbom iz drugih elektroničkih valuta ili gotovinskim transakcijama u ovlaštenim mjenjačnicama (naravno uz određenu proviziju). WebMoney transakcije ne zahtijevaju upotrebu kreditnih kartica ili bankovnih računa.

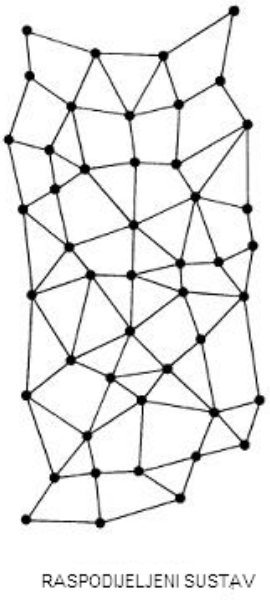
CashU je način elektroničkog plaćanja dostupan na Srednjem istoku i u Sjevernoj Africi, u regiji u kojoj velika populacija mladih ima ograničen pristup kreditnim karticama. Korisnici ju uglavnom koriste za plaćanje Internet igara, VoIP (eng. *Voice over Internet protocol*), Internetskih usluga i slično.

4.4. Raspodijeljeni sustavi

Jedan od najčešćih pristupa izgradnji raspodijeljene mreže je izgradnja partnerske mreže (eng. peer-to-peer – P2P). Rast popularnosti partnerskih računalnih mreža dogodio se pojavom alata i servisa za slobodnu globalnu razmjenu datoteka. Jedna definicija raspodijeljenih sustava [13] glasi: "...Raspodijeljeni sustavi sastoje se od međusobno povezanih čvorova koji se mogu samostalno organizirati u mrežne topologije 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 prospojenosti i performansi bez potrebe za nadzorom, kontrolom i podrškom iz jednog središnjeg mjesta." Iz definicije je vidljivo da partnerski način rada mreže čvorova ima slijedeće osobine:

- svaki čvor je ravnopravan, uključujući mogućnosti prihvaćanja upita o podacima od korisnika ili drugih čvorova,
- komunikacija između čvorova je izravna (bez međukoraka kao što su poslužitelji),
- čvorovi samostalno prikupljaju informacije o dostupnosti drugih čvorova,
- pojedinačni čvorovi imaju u svom lokalnom sustavu za pohranu na raspolaganju samo dio podataka, odnosno podskup ukupnih podataka dostupnih na mreži.

Navedene osobine su suprotne osobinama centraliziranih (klijentsko-poslužiteljskih) sustava, u kojima postoji jasna razlika između čvorova (poslužitelja) koji pohranjuju i nude sadržaj (podatke) te čvorova koji podatke potražuju, obrađuju ili stvaraju (klijenti). Na slici 5, koja prikazuje dijagram raspodijeljene mreže, moguće je uočiti različitu strukturu od centralizirane mreže.



Slika 5. Dijagram raspodijeljenog sustava.
Izvor: Google

Primjeri raspodijeljenih novčanih sustava uključuju Bitcoin i monetarni sustav Ripple.

Bitcoin je *peer-to-peer* mreža namijenjena rukovanju elektroničkim novcem. *Peer-to-peer* (P2P) označava mrežu u kojoj nema središnjeg autoriteta koji izdaje novi novac ili prati transakcije. Zadacima u takvoj mreži rukuju kolektivno čvorovi mreže. Prednosti takvog sustava su:

- jednostavan prijenos novca preko Interneta, bez posrednika,

- treća stranka ne može spriječiti ili upravljati korisnikovim transakcijama,
- transakcije su vrlo jeftine i
- ograničena inflacija novca u sustavu Bitcoin je raspoređena jednako u cijeloj mreži.

Bitcoin je projekt otvorenog koda (eng. *open source*) i trenutno je u *beta* razvojnom stanju, što znači da je dostupan korisnicima, ali je još uvijek u postupku testiranja.

Ripple je programski projekt otvorenog koda namijenjen razvoju i primjeni protokola za otvorenu raspodijeljenu platežnu mrežu. Projekt je još uvijek u fazi razvoja. Kao završeni projekt, Ripple mreža će biti P2P socijalna mrežna usluga uz monetarni sustav temeljen na povjerenju koje već postoji među ljudima u socijalnim mrežama stvarnog svijeta. U ovakvom obliku financijski je kapital poduprt društvenim kapitalom. Temeljna ideja Ripple projekta je omogućavanje platnog puta kroz otvorenu, proizvoljnu mrežu temeljenu na povjerenju (slično kao što mrežni podatkovni paketi putuju Internetom preko otvorenih proizvoljnih računalnih mreža). Prednosti takvog sustava su da se ne oslanja na jedno središte koje odlučuje o postavljanju monetarne politike za jednu državu. Umjesto toga, sustav bi bio demokratske prirode i u teoriji prilagodljiviji potrebama regije i zajednice. Uz takav sustav ne bi bilo potrebe za čvrsto reguliranom institucijskom hijerarhijom za kontrolu ponašanja sudionika u blizini središta. Ripple je zapravo sustav besplatnog bankarstva koji odvaja platežni put od prikupljanja kredita (novca).

Na primjer, neka se Bob nalazi u Kanadi i on želi poslati novac Anji u Švedskoj. Bob se prijavljuje na uslugu Internet bankarstva i unosi Anjin Ripple ID (identifikacijski niz znakova, kao adresa elektroničke pošte) te iznos koji želi poslati. Bankovni Ripple poslužitelj komunicira sa Anjinim Ripple poslužiteljem i oni se koordiniraju kako bi pronašli platežni put između Boba i Anje. Novac završava u jednom od Anjinih računa nekoliko sekundi kasnije.

Ono što je nevidljivo korisnicima je put kojeg je pronašao sustav Ripple kako bi obavio transakciju iz Bobove banke, preko Kanadske izvozne korporacije do banke u Švedskoj i Anjinog bankovnog računa.

Krajnji rezultat je da taj da je vrijednost „tekla“ s Bobovog bankovnog računa do Anjinog računa preko nekoliko posrednika koji nisu znali ništa o transakciji osim o tome tko je sljedeći u lancu. Čak štoviše, niti primatelj i pošiljatelj ne znaju tko su posrednici u komunikaciji.

5. Osnovni protokoli

5.1. Slijepi potpis

Slijepi potpis uveo je David Chaum kao oblik digitalnog potpisivanja dokumenta bez uvida ili s djelomičnim uvidom u sadržaj dokumenta. Potpuno slijepi potpis ne daje nikakav uvid u sadržaj dokumenta.

Digitalno potpisivanje poruke moguće je samo ako potpisnik ima pristup izvornoj poruci. U situacijama kada potpisnik ne smije vidjeti originalnu poruku koju potpisuje, primjenjuje se slijepi digitalni potpis.

Danas su u uporabi dva osnovna oblika kriptosustava:

- simetrični kriptosustavi i
- asimetrični kriptosustavi.

Asimetrični kriptosustavi upotrebljavaju dva različita ključa, poseban ključ za kriptiranje i poseban ključ za dekriptiranje. Takva dva ključa nazivaju se javni i tajni ključ. Javni ključ je poznat i dostupan svima, dok je tajni ključ poznat samo jednoj osobi. Za kriptiranje se, kao i za dekriptiranje, mogu koristiti i javni i tajni ključ, ovisno o potrebi. Prednost ovog sustava je u jednostavnosti stvaranja sigurnog komunikacijskog kanala između dvije osobe. Kriptosustavi su u potpunosti opisani u literaturi [9].

Slijepi digitalni potpis razlikuje se od običnog digitalnog potpisa u tome što se prije potpisivanja originalna poruka "prikriva" množenjem sa slučajnim brojem *r* (faktor sljepoće) potenciranim s javnim ključem banke. Nakon potpisa privatnim ključem banke, poruka se "otkriva" dijeljenjem sa slučajnim brojem *r*. Sada je ostatak poruke potpisan privatnim ključem banke. Ovo je moguće zato što su funkcija prikrivanja i funkcija potpisivanja komutativne.

Neka je *n* prirodni broj (*n* = *pq*, *p* i *q* su veliki prosti brojevi), *e* javni ključ, *d* tajni ključ, *m* elektronička novčanica i *r* faktor sljepoće. Slijedi opis protokola slijepog potpisivanja:

1. Osoba A zaštićuje dokument tzv. faktorom sljepoće (eng. *blinding factor*): $m_1 = \left(m r^e\right) \bmod n$.
2. Osoba A šalje dokument osobi B.
3. Osoba B potpisuje dokument i vraća ga osobi A: $m_2 = m_1^d \bmod n = \left(m r^e\right)^d \bmod n$.
4. Osoba A skida faktor sljepoće dobivši time od osobe B potpisan originalan dokument: $m_3 = \left(m_2 / r\right) \bmod n = \left[\left(m r^e\right)^d / r\right] \bmod n = \left[\left(m^d r\right) / r\right] \bmod n = m^d \bmod n$.

Vrijedi: $\left(m r^e\right)^d = m^d r^{e d} = \left(m^d r\right) \bmod n$.

Ako pri dijeljenju sa *r* ostane ostatak, treba imati na umu da je: $a \bmod n = \left(a + k n\right) \bmod n$, gdje je *k* prirodan broj.

Analogija potpuno slijepom potpisu bila bi potpisivanje na dokument koji se zajedno s indigo-papirom nalazi u omotnici. Osoba se potpisuje preko omotnice i indigo-papira na dokument, ali ne može pročitati dokument jer se on nalazi u zatvorenoj omotnici. Takvo je, međutim, potpisivanje obično rizično, pogotovo za banku koja treba potpisati elektroničku novčanicu, a ne zna u biti na koji iznos glasi ta novčanica. Zato se uvodi slijepi potpis s djelomičnim uvidom u sadržaj dokumenta. Protokol takvog potpisivanja je sljedeći:

1. Osoba A priprema *n* (npr, *n* = 100) digitalnih novčanica iste nominalne vrijednosti, ali drugačijih serijskih brojeva, te ih prikrivene faktorom sljepoće šalje banci.
2. Banka provjerava sadržaj slučajno odabranih *n - 1* novčanica zahtijevajući od osobe A da s njih ukloni faktor sljepoće.
3. Ako su sve otkrivene novčanice valjane, banka potpisuje preostalu neotkrivenu novčanicu (čiji serijski broj nije u mogućnosti vidjeti) i vraća je osobi A.

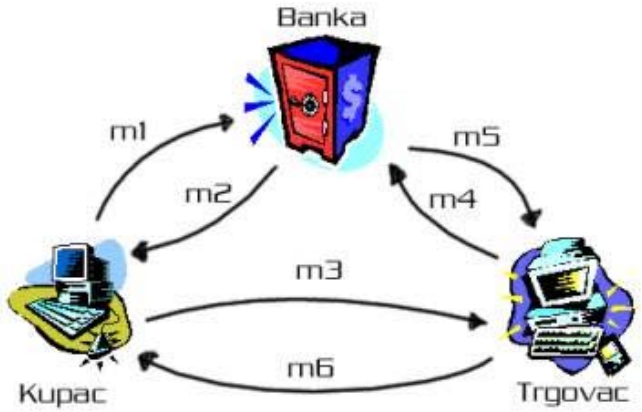
Banku se može prevariti na taj način da se pošalje *n - 1* novčanica s jednim iznosom (na primjer 10 kuna) i jedna novčanica drugog iznosa (100 kuna). Prijevara je moguća samo ako banka slučajno odabere baš tih

n - 1 novčanica na kojima piše 10 kuna i zaključi da se i kod zadnje novčanice, iznosa 100 kuna, radi o novčanici od 10 kuna. Vjerojatnost takvog događaja je 1/*n*.

5.2. Protokol bez anonimnosti

Proces plaćanja, odnosno kupovine se može podijeliti u tri faze i pratiti na slici 6:

1. Podizanje novca iz banke:
    - kupac šalje zahtjev banci za određenom količinom elektroničkog novca (m1);
    - banka oblikuje elektroničku novčanicu (sa serijskim brojem) te stavlja digitalni potpis [8];
    - banka šalje elektroničku novčanicu kupcu te umanjuje njegov račun (m2).
2. Plaćanje:
    - kupac šalje elektronički novac trgovcu (m3);
    - trgovac provjerava digitalni potpis banke na primljenoj novčanici.
3. Polaganje novca u banku
    - trgovac šalje elektroničku novčanicu banci (m4);
    - banka provjerava potpis na novčanici;
    - banka uspoređuje serijski broj novčanice s postojećima u bazi uporabljenih elektroničkih novčanica;
    - banka unosi serijski broj novčanice u bazu uporabljenih novčanica;
    - banka uvećava račun trgovca;
    - banka šalje odgovor trgovcu (m5);
    - trgovac šalje kupljenu robu kupcu (m6).



Slika 6. Dijagram protokola bez anonimnosti.
Izvor: FER

U fazi podizanja novca iz banke, banka stavlja digitalni potpis na elektroničku novčanicu te tako onemogućava krivotvorenje novčanica. Kada banka provjerava ispravnost novčanice, ona provjerava digitalni potpis i prema tome zaključuje je li novčanica krivotvorena ili ne. Kada banka oblikuje elektroničku novčanicu, stvara i serijski broj novčanice koji pohranjuje u svoju bazu. Na taj se način onemogućava višestruko korištenje iste novčanice te umnožavanje elektroničke novčanice. Banka zapisuje serijski broj kod primitka svake novčanice. Ukoliko se ista novčanica ponovno pojavi, banka ju označava nevažećom. Kod stvaranja elektroničke novčanice, banka može zapamtiti vezu između kupca i serijskog broja novčanice i time ugroziti privatnost kupca i pratiti njezino kretanje. Sustav ne jamči anonimnost te postoji mogućnost praćenja transakcija. Dakle, narušavanje privatnosti je nedostatak ovog protokola. Spomenuti nedostatak je ispravljen u protokolu s anonimnošću.

5.3. Protokol s anonimnošću

Protokol s anonimnošću osigurava anonimnost kupca pred bankom. Također, banka nije u mogućnosti pratiti kretanje novčanice kroz transakciju u sustavu plaćanja elektroničkim novcem. Spomenuto se svojstvo ostvaruje mehanizmom slijepog potpisa s djelomičnim uvidom u sadržaj dokumenta. Protokol bez anonimnosti se razlikuje od protokola s anonimnošću u prvoj fazi, kada kupac podiže novac iz banke. Prva faza protokola izgleda ovako:

Podizanje novca iz banke:

- kupac oblikuje N elektroničkih novčanica s jednakim iznosom, ali različitim serijskim brojem i kriptira ih;
- kupac šalje N kriptiranih elektroničkih novčanica banci;
- banka šalje zahtjev kupcu za ključevima za dekriptiranje N-1 slučajno odabrane elektroničke novčanice da provjeri njihov iznos;
- kupac šalje banci N-1 traženi ključ za dekriptiranje;
- banka provjerava valjanost N-1 elektroničke novčanice (iznos) i stavlja svoj digitalni potpis na preostalu novčanicu;
- banka šalje potpisanu elektroničku novčanicu kupcu i umanjuje račun kupca za tu novčanicu;

Druga i treća faza ovog protokola jednake su odgovarajućim fazama protokola bez anonimnosti. Anonimnost kupca je osigurana time što kupac sam oblikuje elektroničku novčanicu sa serijskim brojem. Banka ju prikrivenu (kriptiranu) potpisuje što znači da nije u mogućnosti pročitati taj serijski broj i kasnije dovesti u vezu novčanicu i kupca. Sve osobine elektroničke novčanice ostaju nepromijenjene u odnosu na protokol bez anonimnosti (digitalni potpis banke, serijski broj novčanice). Prava vrijednost novčanice nije poznata, no vjerojatnost prijevare je 1/N, što je vrlo mala vjerojatnost jer je N vrlo veliki broj. Međutim, i ovaj protokol ima nedostatak, nije moguće identificirati osobu koja je pokušala upotrijebiti istu novčanicu više puta ili u nekoliko transakcija. Ovaj nedostatak je ispravljen u konačnom obliku protokola.

5.4. Konačni oblik protokola plaćanja elektroničkim novcem

Konačni oblik protokola zadržava anonimnost kupca, ali samo do trenutka kada je ista elektronička novčanica korištena u više od jedne transakcije. Tada (i samo tada) je moguće otkriti identitet kupca pomoću podatka o identitetu koji se ugrađuje u elektroničku novčanicu. Protokol je podijeljen u tri faze:

1. Podizanje novca iz banke:
    a) kupac oblikuje N elektroničkih novčanica s jednakim iznosom, ali različitim serijskim brojem i kriptira ih;
    b) kupac šalje N kriptiranih elektroničkih novčanica banci;
    c) banka šalje zahtjev kupcu za ključevima za dekriptiranje N-1 slučajno odabrane elektroničke novčanice da provjeri njihov iznos;
    d) kupac šalje banci N-1 traženi ključ za dekriptiranje i N-1 podatak o identifikaciji (koristi se n nizova identifikacijskih bitova koji se stvaraju se na temelju podataka svojstvenih osobi koja sudjeluje u transakciji, odnosno za osobu koja stvara elektroničku novčanicu. Ti podaci mogu biti ime i prezime osobe, adresa elektroničke pošte, telefonski broj te ostale bitne informacije o sudioniku transakcije koje ga identificiraju);
    e) banka provjerava valjanost N-1 elektroničke novčanice (iznos i podatak o identifikaciji) i potpisuje preostalu elektroničku novčanicu;
    f) banka šalje potpisanu elektroničku novčanicu kupcu te umanjuje račun kupca;
2. Plaćanje:
    a) kupac šalje potpisanu elektroničku novčanicu trgovcu;
    b) trgovac provjerava digitalni potpis banke;
    c) trgovac šalje kupcu slučajni odabirući niz (eng. *selector string*);
    d) kupac šalje tražene podatke trgovcu;

e) trgovac provjerava valjanost podataka o identifikaciji na elektroničkoj novčanici;

3. Polaganje novca u banku:
   a) trgovac šalje potpisanu elektroničku novčanicu, identificirajući niz, podatke o identifikaciji i broj bankovnog računa banci;
   b) banka provjerava digitalni potpis uz primljenu elektroničku novčanicu;
   c) banka uspoređuje serijski broj elektroničke novčanice s onima u bazi uporabljenih novčanica;
   d) banka unosi serijski broj elektroničke novčanice, odabirući niz i podatke o identifikaciji u bazu uporabljenih elektroničkih novčanica;
   e) banka šalje odgovor trgovcu o ispravnosti elektroničke novčanice i uvećava račun trgovca;
   f) trgovac provjerava odgovor banke i šalje robu kupcu;

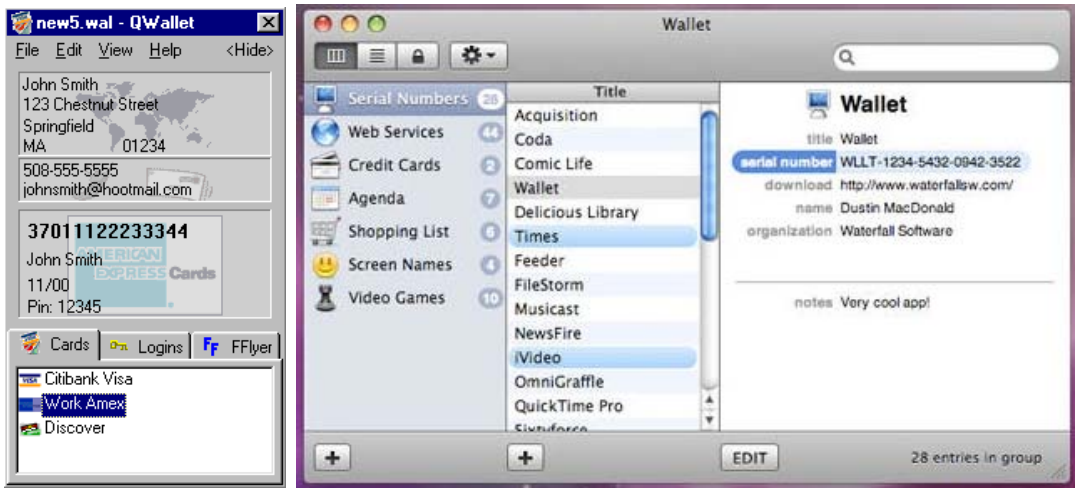
U posljednjoj točki plaćanja trgovac se uvjerava da je elektronička novčanica uistinu vlasništvo kupca koji komunicira s trgovcem. Na taj je način onemogućena krađa elektroničke novčanice što nije bio slučaj u prijašnja dva protokola.

Konačni oblik protokola plaćanja elektroničkim novcem ispunjava sve preduvjete za njegovu implementaciju. Krivotvorenje novčanice se sprječava digitalnim potpisom banke u kojoj se nalaze bankovni računi kupca i trgovca, slijepi potpis s djelomičnim uvidom u sadržaj dokumenta osigurava anonimnost kupca, višestruka potrošnja sprječava se mehanizmom dodavanja podataka o identifikaciji i integritet elektroničke novčanice osiguran je digitalnim potpisom.

5.5. Komercijalni protokoli

5.5.1. CyberCash

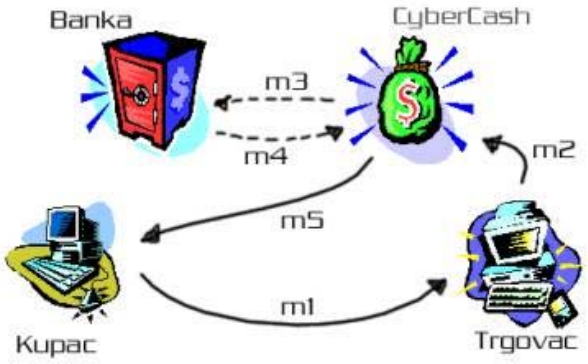
Protokol CyberCash koristi 768-bitni RSA [12] kriptografski algoritam kojim se jamči sigurnost transakcije. Kako bi kupac mogao koristiti CyberCash protokol, mora posjedovati programski paket „The Wallet“, koji je besplatan i dostupan u nekoliko inačica. Prodavač mora imati prodavački račun u tvrtci kreditnih kartica i svoju identifikaciju (eng. *terminal ID*) za primanje Internet transakcija kod njihovih postojećih banaka.



Slika 7. Primjer programskog paketa Wallet po nazivu QWallet i Wallet for Mac.

Protokol se odvija u nekoliko koraka:

1. Kupac zatraži neki proizvod ili uslugu (m1)
2. Prodavač šalje potvrdu kupcu
3. Ako kupac potvrdi kupnju, prodavač šalje podatke o transakciji CyberCash-u (m2, m3)
4. Prodavačeva banka kontaktira kompaniju kreditnih kartica kako bi provjerila da je sve u redu
5. Ako da, banka šalje odobrenje CyberCash-u (m4)
6. CyberCash obavještava kupca da je transakcija uspjela (m5).



Slika 8. CyberCash protokol.
Izvor: FER

Za obavljanje procesa potrebno je petnaest do dvadeset sekundi.

5.5.2. E-cash

E-cash je skup protokola i metoda korištenih za obavljanje financijskih transakcija preko računalnih mreža poput Interneta. Protokol se temelji na korištenju „elektroničkih kovanica“, odnosno niza znakova koji sadrži:

- podatke o vrijednosti,
- serijski broj kojeg je pružila banka koja podržava e-cash tehnologiju i
- digitalni potpis banke.

„Elektroničke kovanice“ služe kao osnovna jedinica plaćanja u transakcijama. U slučaju da ne postoji dovoljan broj manjih kovanica, kupac zahtjeva od banke da mu razmijeni jednu veću na dvije manje kovanice, od kojih jedna ima iznos isti kao račun koji treba podmiriti. Nakon obavljanja plaćanja, određeni broj digitalnih kovanica se prenosi preko Interneta, od kupca do trgovca. Krajnji rezultat je umanjivanje broja kovanica kupca za plaćeni iznos i uvećavanje broja kovanica trgovca. Kovanice se u svakom trenutku mogu pohraniti ili povući s računa, a sve transakcije se zapisuju kako bi se olakšala evidencija.

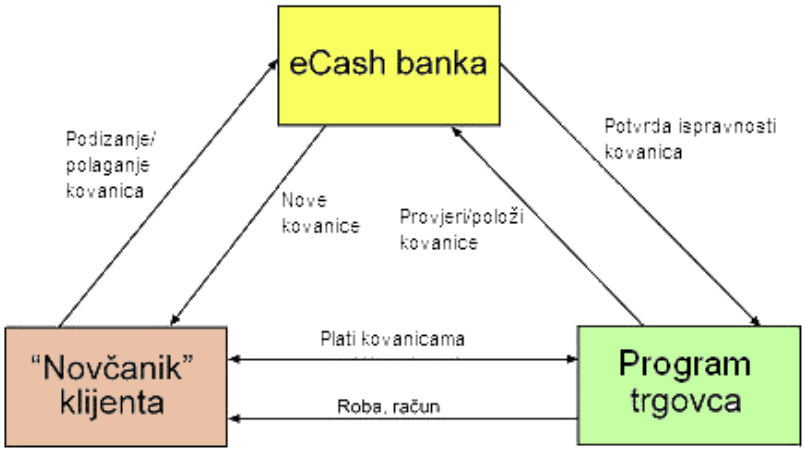
Protokol se dijeli i tri faze:

1. Podizanje novca s bankovnog računa:
   - kupac stvara slučajne brojeve za serijske brojeve *e-cash* kovanica. Na serijske se brojeve postavlja slijepi potpis. Kovanice sa slijepim potpisom šalju se *e-cash* banci;
   - banka provjerava potpis i tereti bankovni račun vlasnika potpisa;
   - banka potvrđuje kovanice i vraća ih kupcu;
   - kupac uklanja faktor sljepoće s novčića.
2. Plaćanje:
   - kupac šalje zahtjev za kupnjom trgovcu;

- trgovac šalje zahtjev natrag kupcu da upotrebom virtualnog novčanika pošalje novac;
- kupac potvrđuje transakciju i upotrebom programskog paketa (virtualnog novčanika) prebacuje točan broj kovanica.

3. Polaganje novca na račun:
   - trgovac mora provjeriti ispravnost kovanica i šalje ih banci koja ih je izdala da se uvjeri kako novac već nije bio potrošen;
   - banka provjerava serijski broj zbog višestruke uporabe. Ako su kovanice valjane, banka uništava kovanice, dodaje serijski broj u bazu podataka potrošenih kovanica i povećava trgovčev račun.

Nakon što je kovanicama utvrđena valjanost, trgovci šalju kupljenu robu ili priznanicu i financijska transakcija je završena.



Slika 9. Model e-cash sustava.

Elektroničke kovanice koje se koriste u *e-cash* sustavu jedinstvene su po tome što ih stvara kupac prije nego ih potpiše banka. Svaka kovanica ima serijski broj kojeg joj je dodijelio virtualni novčanik. Serijski brojevi su izabrani slučajno i dovoljno su veliki, pa je malo vjerojatno da će bilo tko drugi ikada stvoriti isti serijski broj. Serijski broj se potpisuje slijepim potpisom i šalje banci na potpis. Potpis na kovanici s kojeg je uklonjen faktor sljepoće je kao i svi drugi normalni digitalni potpisi. Ne postoji način na koji bi se moglo prepoznati da je kovanica potpisana upotrebom slijepog potpisa.

6. Primjeri elektroničkih novčanih sustava

Razvojem Interneta počeli su se javljati brojni prijedlozi za standarde elektroničkih plaćanja. Neki komercijalni sustavi koriste sustave kreditnih kartica, drugi čekove, treći obračunavaju kupnju preko telefonskog računa kupca. Postoji velik broj komercijalnih rješenja kao što su CyberCash, First Virtual, DigiCash, Secure Pay, Web900 i drugi.

6.1. First Virtual

First Virtual je jedan od prvih platnih sustava na Internetu, i počeo je s radom 1994. godine. Cilj tvrtke First Virtual Holdings bio je stvoriti jednostavan sustav plaćanja na Internetu. Sustav je jedinstven po tome što ne koristi enkripciju. Umjesto upotrebe brojeva kreditnih/debitnih kartica, transakcije se obavljaju uporabom posebnog osobnog identifikacijskog broja (Virtual PIN) koji je vezan uz korisnikov račun. Spomenuti identifikacijski brojevi mogu se slati preko Interneta jer, čak i kada nisu kriptirani, ne mogu se iskoristiti za zaduživanje korisnikovog računa. Račun neke osobe se nikada ne tereti dok ona, putem elektroničke pošte, ne potvrdi da prihvaća zaduženje. Sustav First Virtual se temelji na postojećim Internet protokolima, elektroničkoj pošti i MIME standardu. Elektronička se pošta koristi za komunikaciju s korisnikom i potvrđivanje zaduženja korisnikovog računa.

Elektroničko poslovanje preko sustava First Virtual može se opisati na primjeru kupca i prodavača:

- kupac posjećuje web poslužitelj koji koristi sustav First Virtual i odabire artikle koje želi kupiti. Prilikom kupnje kupac unosi svoj Virtual PIN koji se prosljeđuje trgovcu.
- prodavač putem elektroničke pošte šalje sustavu First Virtual:
    - kupčev Virtual PIN,
    - prodavačev Virtual PIN,
    - iznos i valutu,
    - opis proizvoda/usluge.
- ako je Virtual PIN kupca važeći, First Virtual obavještava prodavača da može nastaviti s transakcijom.
- kupac šalje potvrdu sustavu First Virtual elektroničkom poštom naznačujući "prihvati" (nastavlja se naplata), "odbaci" ili "prijevara" (First Virtual poslužitelj stavlja prodavačev Virtual PIN na crnu listu).

6.2. DigiCash

DigiCash je nizozemska tvrtka koju je osnovao David Chaum. Temeljeno na Chaumovom istraživanju anonimnog elektroničkog novca, DigiCash je razvio *e-cash*, sustav plaćanja sličan novcu koji pruža visoki stupanj anonimnosti i neprativosti. *E-cash* je temeljen na konceptu slijepog potpisa. Sustav *e-cash* je programski paket koji se sastoji od virtualnog novčanika i elektroničkih kovanica koji se pohranjuju na čvrstom disku korisnika.

6.3. SecurePay

SecurePay je sustav tvrtke Redi-Check koji se koristi čekovima kao platnim sredstvom. Kupac treba posjedovati račun u banci koja prima čekove u američkim dolarima. Kupac odabire artikle i upisuje svoj identifikacijski niz znakova (Secure Pay ID) i lozinku koju poznaje otprije. Ti se podaci prosljeđuje tvrtci Redi-Check. Tamo se nakon autorizacije identifikacijskih podataka izdaje ček s podacima kupca i potrošenim iznosom koji se šalje natrag poslužitelju putem normalne pošte. Poslužitelj kod ovog protokola raspolaže s novcem nakon što protekne 24 sata od kupovine.

6.4. Mikroplaćanje

Mikroplaćanja (eng. micropayments) su posebna vrsta elektroničkog novca, čija glavna osobina jest da se radi o vrlo malim novčanim iznosima (reda veličine 1 centa ili čak manje). Ovakva vrsta plaćanja potrebna je za plaćanje vrlo jeftinih sadržaja, koji se međutim moraju kupovati vrlo brzo. Tipičan primjer potrebe za

ovakvim plaćanjem je telefonska govornica. U toku telefonskog razgovora telefonska govornica mora svakih nekoliko sekundi naplatiti po vrlo mali iznos. Kako se transakcije moraju odvijati u kratkom roku, nema vremena za složene protokole i algoritme, niti za *online* vezu sa bankom. Stoga ova plaćanja moraju biti riješena kao *offline*. Na mikroplaćanja se postavlja gornja granica dozvoljenog iznos plaćanja i to je iznos reda veličine 1 USD. Zahvaljujući ovom ograničenju, potreba za sigurnosnim mehanizmima je smanjena, pa i jednostavniji sustavi zadovoljavaju namjenu.

Metoda mikroplaćanja, za razliku od sustava kreditnih kartica, koristi debitni sustav. Korisnik kupuje digitalne žetone ili mikro-novac. Korisnikov se bankovni račun tada tereti za količinu digitalnih žetona koje je kupio. Digitalni žetoni mogu se kupiti i kreditnom karticom te se mogu potrošiti na web stranicama koje podržavaju takav način plaćanja. Korisnik pri tome ne treba odavati broj svoje kreditne kartice web stranici na kojoj obavlja trgovinu.

Svaki sustav mikroplaćanja nudi različite stupnjeve enkripcije i mogućnosti certificiranja. Većina sustava koji koriste žetone traže veću količinu digitalnih žetona (na primjer 20 dolara ili više) koristeći kreditnu karticu ili bankovne transakcije. Korisnici mogu kupovati žetone kod pružatelja sadržaja, zasebnog posrednika (poput banke), tvrtke kreditnih kartica, pružatelja Internet usluga i sl.

Većina sustava mikroplaćanja sastoji se od klijentske aplikacije, poslužitelja trgovca i poslužitelja posrednika. Kada korisnik odobri isplatu, poslužitelj trgovca provjerava identitet korisnika kod poslužitelja posrednika i bilježi uplatu.

Načini prebacivanja kredita od posrednika trgovcu ovise o sustavu i veličini kompanije trgovca. To se uobičajeno obavlja prebacivanjem novca između bankovnih računa. Metode potvrđivanja uplate za prebacivanje točne količine novca između posrednika i trgovca moraju biti unaprijed dogovorene. Postoji više načina na koji posrednici mogu zaraditi, kao na primjer terećenje korisnika prilikom kupnje digitalnih žetona (npr. 100 žetona u protuvrijednosti 1$ stajalo bi 1.10$). Uobičajenija metoda je da posrednici naplaćuju proviziju trgovcima za svaku transakciju.

7. Sigurnost elektroničkog novca

7.1. Višestruko korištenje ili kopiranje novčanice

Kako bi se valjanost elektroničkog novca mogla provjeriti i dokazati koristi se metoda digitalnog potpisa. Svaka valjana novčanica nosi potpis financijske institucije koja ju je izdala. Elektronički novac sastoji se od niza bitova čije je kopiranje jednostavno. Kopija se ne razlikuje od originala pa bi krivotvorenje bilo nemoguće otkriti. Jednostavni sustavi bi dozvoljavali kopiranje elektroničkog novca i potrošnju obje kopije. Sustavi elektroničkog plaćanja moraju sprječavati dvostruku potrošnju.

Višestruko korištenje iste novčanice u nekoliko transakcija ili kopiranje iste elektroničke novčanice sprječava se upisivanjem serijskog broja korištene novčanice u bazu podataka banke. Svaki puta kada banka primi neku novčanicu, ona provjerava serijski broj u svojoj bazi podataka i zna je li novčanica već bila korištena ili nije. Ukoliko banka otkrije pokušaj prijevare, identificira osobu koja je pokušala prijevaru preko podataka o identifikaciji koje klijent šalje uz novčanicu, kao što je opisano u protokolima za plaćanje elektroničkim novcem.

Kod *online* sustava višestruka potrošnja sprječava se tako što se obvezuje trgovca da stupi u vezu s bankom tokom svake prodaje. Računalo banke održava bazu podataka potrošenog elektroničkog novca i može jednostavno javiti trgovcu ako je korišteni elektronički novac još uporabljiv. U protivnom slučaju trgovac odbija prodaju.

Kod *offline* sustava postoje dva pristupa otkrivanju dvostruke potrošnje, sklopovski i programski pristup.

Sklopovski pristup se oslanja na posebnu pametnu karticu koja sadrži čip otporan na neovlaštene promjene. U tom čipu čuva malu baza podataka o elektroničkom novcu koje je ta pametna kartica potrošila. Ako vlasnik kartice pokuša kopirati manju svotu elektroničkog novca i potrošiti ga dva puta, ugrađeni čip bi otkrio pokušaj i ne bi dozvolio transakciju. Spomenuti je čip otporan na neovlaštene promjene i vlasnik ne može obrisati bazu podataka bez trajnog oštećenja kartice.

Programski pristup uključuje oblikovanje elektroničkog novaca i kriptografskih protokola koji otkrivaju identitet osobe koja je dva puta upotrijebila novčanicu do trenutka kada elektronički novac dolazi u banku.

7.2. Krivotvorenje elektroničkih novčanica

Krivotvorenje elektroničkih novčanica nije moguće jer banka stavlja digitalni potpis na svaku novčanicu i taj potpis se ne može krivotvoriti. Potpis se obavlja tajnim ključem banke koji zna samo ona. Kada se novčanica vrati u banku, ona provjerava svoj potpis. Na taj način je osigurano da novčanicu nije nitko drugi stvorio.

7.3. Krađa elektroničke novčanice

U posljednjoj točki druge faze konačnog protokola za plaćanje elektroničkim novcem, trgovac provjerava valjanost podataka o identifikaciji na elektroničkoj novčanici. Na taj način se uvjerava da je elektronička novčanica uistinu vlasništvo kupca te je onemogućena njena krađa.

7.4. Problemi sigurnosti transakcija

Sigurnost sustava za elektroničko plaćanje ovisi o sigurnosti koju pružaju kriptografski algoritmi. Kriptografski algoritmi i protokoli pružaju visok stupanj sigurnosti i ako su ispravno primijenjeni, sigurnost ne bi trebala biti ugrožena. Međutim, i dalje postoji prostor za napredak kriptoanalize te neizbježni ljudski faktor (gubitak tajnog ključa, provala u sustav, ucjena) kojim se ta sigurnost može ugroziti.

Omogućavanje sigurnih transakcija zahtijeva stvaranje elektroničkih sustava sigurnosti. Spomenuti sustavi moraju štiti poruke koje zahtijevaju prijenos novca ili sam novac te pružati uslugu stvaranja digitalnih potpisa koji se ne mogu krivotvoriti niti poricati. Takvi sustavi moraju osiguravati:

- **privatnost** - sadržaj prenesenih poruka, činjenica da je uopće poslana, tko ju je poslao i kome je namijenjena trebaju ostati poznati samo sudionicima u komunikaciji,

- **vjerodostojnost** - sudionici u komunikaciji moraju biti u stanju jedan drugom dokazati svoj identitet,
- **autorizacija sudionika** – pravo da identificirani sudionik ima ovlasti koristiti se određenom uslugom u određenom trenutku,
- **neopozivost** (eng. *nonrepudiation*) - niti jedna strana ne može drugoj strani osporiti da je sudjelovala u komunikaciji
- **cjelovitost, integritet** - poruka mora na svoje odredište stići u nepromijenjenu obliku, odnosno primatelj poruke mora moći otkriti bilo kakvu promjenu u komunikacijskom kanalu.

Navedeni zahtjevi mogu se ispuniti primjenom raznih tehnoloških rješenja.

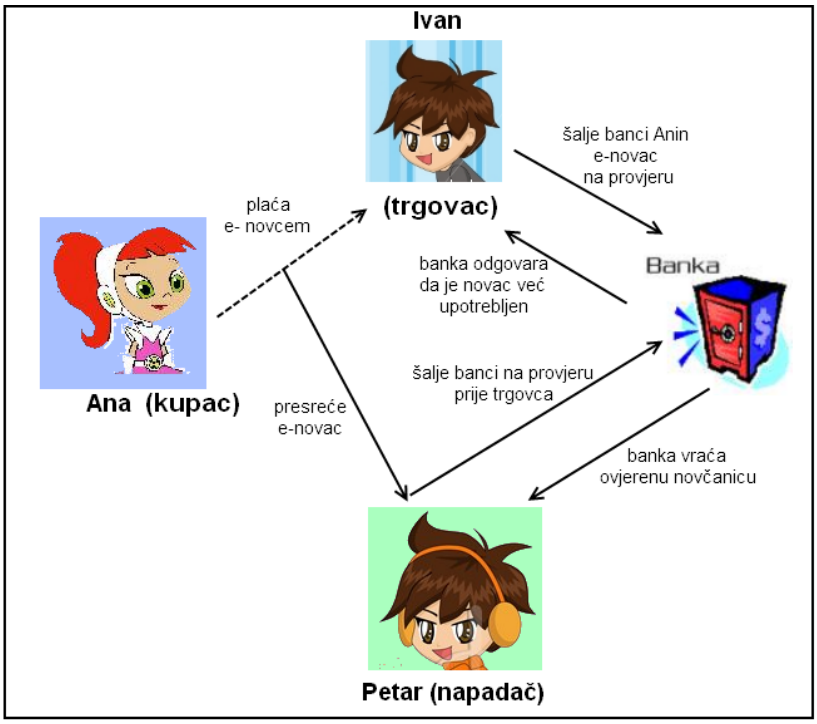
8. Moguće zlouporabe elektroničkog plaćanja

Protokoli koji se koriste pri razmjeni elektroničkog novca počivaju na sigurnosnom sustavu koji koristi više elemenata: algoritme za kriptiranje, funkcije sažetka, jednosmjerne funkcije, generatore slučajnih brojeva, lozinke itd. Svaki od ovih elemenata podložan je napadu zlonamjernog napadača. No, u praksi se pokazalo da su najčešći i najuspješniji napadi usmjereni na ljude – korisnike sustava.

Ako treća strana može prisluškivati komunikaciju između dvije strane te ju želi samo ometati, to joj je uvijek omogućeno. Dakle, umjesto poruke koja je na putu od jedne strane ka drugoj, treća strana može spomenutu poruku promijeniti i dalje ju pustiti prema cilju. Osim toga, napadač (treća strana) ju može ukloniti s njenog puta i/ili poslati novu poruku umjesto izvorne. Uz to može jednostavno izmisliti neku novu poruku i poslati je postojećem cilju iako nikakva poruka nije namijenjena tom cilju. Bar jedna od spomenutih operacija je moguća bez obzira na kriptografske metode koje se koriste u komunikaciji. Rezultat takvog napada je, ovisno o robusnosti sustava koji se napada, ometanje pravilnog funkcioniranja sustava. U pravilu, takvim ometanjem ne bi se trebala nanijeti ozbiljnija šteta, već se uglavnom usporava rad sustava koji se ometa. Na primjer, započeta transakcija se tijekom obavljanja ometa te ju je potrebno ponoviti. Problem se rješava tako da se onemogući bilo kakvo prisluškivanje od neželjene treće strane. Na Internetu je tako nešto nemoguće ostvariti zbog njegove veličine, količine protokola koji se koriste te činjenice da nisu svi komunikacijski kanali zaštićeni.

Ako treća strana pokuša napad s kopiranom porukom iz neke od prethodnih transakcija, komunikacija se odmah odbija jer se u svakoj novoj transakciji stvaraju novi simetrični ključevi te se izvorne poruke kriptiraju s tim novim ključevima. Na taj način, određena poruka kriptirana simetričnim ključem u jednoj transakciji nije jednaka poruci iz istog koraka u drugoj transakciji iako se možda kupuje identična roba kod istog trgovca.

Kod obavljanja transakcija elektroničkim novcem upotrebom protokola elektroničkog plaćanja, napadač može prisluškivati i presresti elektronički novac kojeg kupac šalje trgovcu. Napadač može poslati novčanicu banci prije nego što je to kupac stigao učiniti. Napadač će povećati iznos na svojem računu, a za kupca će se smatrati da je kriminalac jer pokušava drugi put unovčiti istu novčanicu. Ovakav se napad može spriječiti uspostavljanjem tajnog komunikacijskog kanala između kupca i trgovca tako da napadač ne može presresti novčanice niti saznati odvija li se transakcija.



Slika 10. Primjer napada s čovjekom u sredini.

Ako kupac ne zaštiti svoje računalo dovoljno dobro protiv napada preko mreže, napadač može situaciju iskoristiti za neovlašten pristup sustavu, te na taj način i direktorijima te datotekama koje se nalaze na ugroženom sustavu. Napadač može kopirati digitalne novčanice i potrošiti ih umjesto kupca. Također, može dva puta iskoristiti novčanicu. Dobra zaštita protiv takvih napada su enkripcijski programi, kao što je PGP (eng. *Pretty good privacy*), ili visoko zaštićene mreže (na primjer vatrozidom).

9. Utjecaj elektroničkog novca i njegova budućnost

Zbog povećane upotrebe elektroničkog novca u današnje vrijeme provedena su različita istraživanja o njegovom utjecaju na ekonomiju i na mogućnost upravljanja njegovim zalihama. Mnogi ekonomisti vjeruju da bi elektronički novac mogao u potpunosti zamijeniti papirnati novac, dok drugi smatraju da upotreba elektroničkog novca ipak neće biti toliko utjecajna na društvo i ekonomiju.

Većina zemalja (odnosno monetarnih unija) ima središnju monetarnu instituciju koja izdaje i povlači novac, određuje kamatne stope i obavezne rezerve banaka itd. Upravo utjecajem na količinu novca u opticaju i uvjetima davanja kredita poslovnih banaka središnja banka utječe na gospodarstvo u okviru svojih zakonskih ovlasti.

Sposobnost upravljanja zalihama novca ovisi o definiciji novca (M1). M1 trenutno uključuje gotovinski novac, putničke čekove i pologe na zahtjev. Ukoliko se upotreba M1 smanji zbog ovisnosti o elektroničkom novcu, M1 više ne bi bio dobra mjera novca u ekonomiji. Smanjena sposobnost mjerenja monetarnih agregata ograničila bi sposobnost središnje banke (eng. *central bank*) za obavljanjem operacija na otvorenom tržištu i utjecala bi na zalihu novca. Mogućnost prijevare može utjecati na središnju banku da ograniči promjene na M1 i spriječi rast elektroničkog novca. Ona može poduzeti sljedeće mjere:

- ograničiti rast i širenje elektroničkog novca kako bi spriječila zamjenu novca u središnjoj banci,
- izdavati elektronički novac i obrađivati transakcije elektroničkog novca na jednak način kao i običan novac,
- primijeniti zahtjeve za velikim rezervama digitalnog novca,
- apsorbirati višak likvidnosti koju su stvorile monetarne operacije.

Navedene bi mjere dozvolile središnjoj banci da održava nadzor monetarnih agregata, iako bi te mjere mogle više naškoditi banci nego pomoći zbog ograničenih tehnoloških poboljšanja. Odupiranje promjeni možda nije najbolji pristup, no elektronički novac bi se trebao prihvatiti postupno kako iznenadne promjene ne bi uzrokovale ekonomsku krizu.

Očekuje se da će elektronički novac u potpunosti promijeniti način međunarodne trgovine i razmjene valuta. Elektronički novac omogućuje jednostavne transakcije sredstava. Pri tome razmjena elektroničkog novca obavljala bi se u jaču valutu što bi uzrokovalo nestabilnost tečajne liste, financijskog sustava i ograničilo utjecaj monetarne politike. Kao posljedica toga, središnja banka bi morala prihvaćati strane valute i politike kako bi zadržala upravljanje domaćim monetarnim agregatima. Elektronički novac ukida granice i razlike između država i mogao bi biti preteća jedinstvene valute koju bi podupirala dobra i usluge s jedinstvenom cijenom postavljenom na aukcijskom tržištu. Smanjena sposobnost upravljanja međunarodnim razmjenama valuta smanjuje nadzor središnje banke nad zalihama novca.

Elektronički novac utječe na pričuve (eng. *reserves*). Ako se zahtjevi pričuve prebace na bilance elektroničkog novca, nema promjene jer se pretpostavlja da će se novac u prometu smanjiti jednako kao što će bilanca elektroničkog novca rasti. Međutim, to pretpostavlja da se zahtjevi pričuve mogu postaviti na sve bilance elektroničkog novca. Kada su privatne institucije odgovorne za pametne kartice i mrežni novac, to nije slučaj. Ako središnja banka odluči poduzeti ispravljačke akcije, ona može ograničiti inflacijski efekt povećanja novca. To ne bi trebao biti problem ako su promjene spore i mjerljive te omogućuju središnjoj banci da im se prilagodi. Ako je ova pretpostavka pretjerano optimistična u smislu sposobnosti središnje banke da se može prilagoditi, središnja banka bi mogla izgubiti nadzor nad inflacijom, što bi moglo rezultirati povećanom upotrebom privatno izdanog elektroničkog novca.

Jedan od utjecajnijih efekata koje bi elektronički novac mogao imati je onaj na dohodak od PDV-a. Novac od PDV-a koristi se za upravljanje središnjom bankom i njegov bi gubitak mogao uzrokovati financijske poteškoće. Ovaj se novac također koristi za pružanje novčanih sredstava državnom proračunskom manjku i drugim državnim programima te bi gubitak dohotka od PDV-a mogao ozbiljno naštetiti državi. Spomenuti gubitak se može spriječiti ako se bilance elektroničkog novca tretiraju slično kao sredstva po viđenju i povećavanjem zahtjeva pričuve. Dakle, povećanje elektroničkog novca će:

- ograničiti sposobnost upravljanja zalihama novcem središnje banke,
- smanjiti dohodak od PDV-a,
- smanjiti pričuve,
- smanjiti nadzor nad međunarodnim prometom novca i

- promijeniti multiplikator novca.

Korištenje digitalnog novca zahtijeva donošenje zakona koji rješavaju četiri ključna problema:

1. poziciju elektroničkog novca u postojećem monetarnom sustavu,
2. poziciju elektroničkog novca u poreznom sustavu,
3. formalnopravnu valjanost digitalnog potpisa te
4. sprječavanje kriminalnih radnji.

Utjecaj elektroničkog novca je ovisan i ograničen na porast upotrebe elektroničkog novca. Mnogi stručnjaci smatraju da elektronički novac ipak neće zamijeniti papirnati novac zbog manjka sigurnosti i troškova stvaranja odgovarajućih programskih rješenja.

Budućnost elektroničkog novca je ovisna o njegovom rastu, nadzoru i tehnološkom napretku kojim bi se povećala njegova sigurnost.

10. Zaključak

Elektronički novac je danas još uvijek nepoznanica kojom se ljudi ne koriste previše. Zastupljenost sustava elektroničkog plaćanja je u današnje vrijeme još uvijek mala. Razlozi tome nisu nemogućnost ostvarenja sustava elektroničkog plaćanja koji će osigurati maksimalan stupanj sigurnosti, već nepovjerenje banaka i ljudi u takve sustave.

Sve brži razvoj tehnologije i umreženost mogli bi ubrzati probijanje sustava elektroničkog plaćanja, koji bi u konačnici mogli zamijeniti papirnati novac. Međutim, razvoj sustava elektroničkog plaćanja ne ovisi samo o napretku u računarskim znanostima. Kako bi došlo do značajnijih pomaka treba izgraditi zakonski okvir koji bi ulio sudionicima sigurnost i omogućio brže širenje sustava elektroničkog plaćanja. Osim toga, potrebno je imati na umu svjetsku ekonomiju i pažljivo osmisliti metode prijelaza na elektronički novac (ukoliko bi on u budućnosti u potpunosti zamijenio običan novac).

Sigurnosni algoritmi, mehanizmi i protokoli (kriptiranje, digitalni potpis itd.) koji se koriste su dobro prihvaćeni i zadovoljavaju sve zahtjeve koje postavljaju modeli elektroničkog novca. Postoji nekoliko modela elektroničkog plaćanja, *online* i *offline* plaćanja, s identifikacijom i anonimni, za velika, mala i mikro plaćanja, notacijski i simbolički sustavi, centralizirani i raspodijeljeni. Uporaba elektroničkog novca u praksi, u usporedbi s klasičnim oblicima plaćanja na Internetu (kreditne kartice), je zanemariva. Postoji nekoliko implementacija elektroničkog novca koji su u upotrebi, međutim koriste samo mali dio mogućnosti koje elektronički novac pruža i nisu globalno rašireni.

Iako je koncept elektroničkog novca vrlo dobro definiran, kao i protokoli i sustavi koji ga podržavaju, klasični oblici plaćanja će još dugo biti znatno zastupljeniji.

11. Reference

[1] Electronic money, http://en.wikipedia.org/wiki/Electronic_money, kolovoz 2010.

[2] Ripple Project, http://ripple-project.org/, srpanj 2009.

[3] DigiCash, http://www.digicashinc.com/index.php, rujan 2010.

[4] J. Simon, E.Starbuck Gerson, „Online shopping options offer credit card safety“, http://www.creditcards.com/credit-card-news/credit-card-fraud-and-online-shopping-1282.php, listopad 2009.

[5] Robert Šipek, Elektronički novac, prosinac 2002.

[6] Luka Baranović, Protokoli plaćanja elektroničkim novcem, 2001.

[7] Nino Zeljko, Protokoli plaćanja elektroničkim novcem, 2002.

[8] Digitalni potpis, http://www.cert.hr/documents.php?id=275, veljača 2007.

[9] Kriptoanaliza, http://www.cert.hr/documents.php?id=392, rujan 2009.

[10] Blind signature, http://en.wikipedia.org/wiki/Blind_signature, svibanj 2010.

[11] S. M. Sullivan, Electronic Money and Its Impact on Central Banking and Monetary Policy, rujan 2010.

[12] Napad na RSA, http://www.cert.hr/documents.php?id=26, travanj 2003.

[13] S. Androutsellis-Theotokis, D. Spinellis, “A survey of peer-to-peer content distribution technologies“, ACM Computing Surveys, prosinac 2004.