UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Franc Dolenc

DIGITALNE DENARNE VALUTE KOT PLAČILNO SREDSTVO

DIPLOMSKO DELO

VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

Ljubljana, 2014

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Franc Dolenc

DIGITALNE DENARNE VALUTE KOT PLAČILNO SREDSTVO

DIPLOMSKO DELO

VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

Mentor: doc. dr. Dejan Lavbič

Ljubljana, 2014

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani **Franc Dolenc**,

z vpisno številko **63080419**,

sem avtor diplomskega dela z naslovom:

Digitalne denarne valute kot plačilno sredstvo.

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno, pod mentorstvom doc. dr. Dejana Lavbiča,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 22. aprila 2014 Podpis avtorja:

Iskreno se zahvaljujem svojim staršem in bratu za podporo skozi vsa leta študija, pomoč in obilo potrpljenja v času izdelave diplomskega dela. Zahvala za usmerjanje in strokovne nasvete gre posebej mentorju doc. dr. Dejanu Lavbiču ter nenazadnje tudi lektorici prof. Karmen Škrk za dragoceni čas.

KAZALO

SEZNAM SLIK

SEZNAM TABEL

SEZNAM UPORABLJENIH KRATIC

AML (ang. Anti-Money Laundering) je oznaka regulacij za preprečevanje pranja denarja.

API (ang. Application Programming Interface) je aplikacijski programski vmesnik, ki določa nabor funkcij ali rutin za opravljanje specifične naloge, lahko pa tudi deluje v interakciji z drugo programsko opremo.

ASIC (ang. Application-Specific Integrated Circuit) je integrirano vezje z matriko čipov, na katerih so lahko vključeni še mikroprocesor, različni tipi pomnilnikov in nekatere druge komponente računalniškega sistema.

CA (ang. Certificate Authority) je certifikatna agencija, ki izdaja digitalna potrdila, potrebna za dostop do nekaterih spletnih aplikacij, kjer se zahteva identifikacija s potrdili te agencije.

DDoS (ang. Distributed Denial-of-Service) je napad, pri katerem se navadno cilja visokoprofilne spletne strani. Te med napadom vire porabljajo za reševanje visokega števila distribuiranih zahtevkov, zato pogostokrat postanejo neodzivne ali povsem nedostopne.

DGC (ang. Digital Gold Currency) je oblika elektronskega denarja, katerega vrednost je določena z unčami zlata.

DNS (ang. Domain Name Server) je sistem za pretvarjanje naslovov IP v nazive domen in obratno.

DRM (ang. Digital Rights Management) je programska oprema za nadzor digitalne vsebine po nakupu, katere namen je omejevanje kopiranja.

DSA (ang. Digital Signature Algorithm) je standard, ki se uporablja za generiranje in verifikacijo digitalnih podpisov.

EFT (ang. Electronic Funds Transfer) je sistem za elektronski prenos denarnih sredstev med različnimi računi.

FinCEN (ang. Financial Crimes Enforcement Network) je agencija za preprečevanje pranja denarja in drugih finančnih kaznivih dejanj.

FPGA (ang. Field-Programmable Gate Array) je posebno integrirano vezje, sestavljeno iz večjega števila logičnih vrat in delovnega pomnilnika. Po izdelavi ga je možno naknadno konfigurirati, v osnovi pa je namenjeno predvsem zahtevnim izračunom.

GDCA (ang. Global Digital Currency Association) je združenje neodvisnih samoregulativnih menjalnic, katerega del so operaterji spletnih valut, trgovci in končni uporabniki.

HTTP (ang. Hypertext Transfer Protocol) je aplikacijski protokol za prenos informacij.

HTTPS (ang. Hypertext Transfer Protocol Secure) je različica protokola HTTP, ki dodatno uporablja protokola SSL in TLS.

HYIP (ang. High-Yield Investment Program) je oblika Ponzijeve sheme, pri kateri se za investicije v neresnične investicijske programe zagotavlja visok dobiček.

IP (ang. Internet Protocol) je osnovni komunikacijski protokol, ki določa strukturo paketov, s katerimi so podatki enkapsulirani. Hkrati določa tudi metode naslavljanja, s katerimi je mogoče za vsako podatkovno enoto (datagram) določiti informacijo o izvoru in destinaciji.

IRBA (ang. International Ripple Business Association) je združenje podjetnikov, ki vodijo storitev, povezano z omrežjem Ripple.

JSON (ang. JavaScript Object Notation) je odprt standard, ki določa format za hranjenje in izmenjavo objektov s pari atributov – vrednosti med strežnikom in spletno aplikacijo.

OTC (ang. Over-The-Counter) je oznaka za izvenborzno trgovanje, kjer se posli sklepajo ločeno od organiziranega trga.

PGP (ang. Pretty Good Privacy) je program za izvajanje kriptiranja in avtentikacije. Najpogosteje se uporablja pri podpisovanju ali pa kriptiranju elektronskih sporočil, datotek in diskovnih particij.

PHP (ang. Hypertext Preprocessor) je programski jezik, ki se izvaja na strežniški strani.

PIN (ang. Personal identification numbers) je numerično geslo, ki se uporablja za avtentikacijo uporabnika sistemu.

PKI (ang. Public key infrastructure) ali infrastruktura javnega ključa je sistem, ki ga sestavljajo certifikatne agencije, agencije za verifikacijo udeležencev v komunikaciji, imenikov za hranjenje certifikatov in sistema za njihovo upravljanje.

POS (ang. Point-Of-Sale) je terminal, na katerem se za kupljeno blago ali storitev opravi plačilo oziroma zaključi transakcija.

POW (ang. Proof-of-Work) je sistem, pri katerem se podatki producirajo z visoko stopnjo težavnosti, s čimer se zadosti vnaprej podanim zahtevam, in so obenem enostavno preverljivi.

P2P (ang. Peer-to-Peer) je tip distribuirane omrežne arhitekture, v kateri si vsi sodelujoči med seboj lahko neposredno izmenjujejo podatke, brez potrebe po centralnem strežniku, saj ima vsak sam hkrati vlogo strežnika in odjemalca.

RMT (ang. Real Money Trade) je praksa, pri kateri se za nakup digitalnih dobrin in storitev uporablja realen denar.

RPC (ang. Remote Procedure Call) je medprocesna komunikacija, s katero lahko računalniški program izvaja procedure na drugem računalniku.

RSA (poimenovan po avtorjih R. Rivest, A. Shamir, L. Adleman) je eden prvih praktičnih kriptosistemov, pri katerem se za enkripcijo uporabljajo pari javno-zasebnih ključev, katerih dolžine običajno znašajo od 1024 do 4096 bitov.

SQL (ang. Structured Query Language) je programski jezik za upravljanje podatkov, shranjenih v sistemih relacijskih podatkovnih baz.

SSL (ang. Secure Sockets Layer) je asimetrični kriptografski protokol, predhodnik protokola TLS (ang. Transport Layer Security), ki se uporablja za zagotavljanje varne komunikacije v internetu.

TOS (ang. Terms of Service) je izjava, s katero uporabnik potrdi strinjanje pri uporabi določene storitve.

URL (ang. Uniform Resource Locator) je naslov spletnih strani.

XML (ang. Extensible Markup Language) je označevalni jezik, s katerim so določena pravila za enkodiranje dokumentov v človeško in strojno berljivem formatu, zato je s tega vidika podoben formatu JSON.

POVZETEK

Diplomska naloga podaja širši pregled nad področjem virtualnih in digitalnih valut kot alternativnim načinom plačevanja. Z realno uporabo poskušamo odgovoriti na vprašanje, ali so takšni sistemi primerni za splošno integracijo v obstoječih rešitvah. V začetnih poglavjih pojasnimo pomembnost vpeljave kriptografije v spletno komunikacijo in delovanje zgoščevalnih funkcij. Sledi opredelitev večjih vlog zunanjih sistemov, povezanih z digitalnimi valutami, medtem ko kriptovalute in zasnovo transakcij opišemo v sledečih poglavjih. Možnosti plačevanja v praksi pokažemo na zasnovani spletni trgovini, razviti v programskih jezikih PHP in JavaScript. Ugotovimo, da je povezovanje s plačilnimi procesorji preko aplikacijskih programskih vmesnikov povsem izvedljivo, vendar neprimerno za poljubno rešitev zaradi deflacije in nestabilnosti kriptovalute. Sledi zaključek, da so v nasprotju s sistemi alternativnih valut pri trenutni stopnji razvoja ustaljene metode plačevanja še vedno zanesljivejše.

Ključne besede: digitalne valute, kriptovalute, protokoli, transakcije, aplikacijski programski vmesniki.

ABSTRACT

The purpose of the diploma thesis is to describe the alternative way of payment by using virtual and digital currencies. We try to find out, whether these systems are appropriate for general integration in existing solutions. Firstly, we explain the importance of introducing cryptography in online communication and the operating of hash functions. Next, there are definitions of all significant roles of external systems connected to digital currencies, followed by the description of crypto currencies and the design of transaction. The possibilities of payment are shown in the online store designed in programming languages PHP and JavaScript. We ascertain that networking with payment processors via applicative programming interfaces is completely feasible, but inappropriate for random solutions due to the instability and deflation of the crypto currency. The conclusion indicates that the regular methods of payment are still more reliable than the alternative ones at the moment.

Key words: digital currencies, cryptocurrencies, protocols, transactions, application programming interfaces.

1 UVOD

Prenosi denarnih sredstev, ki v bančnih sistemih sedaj že desetletja potekajo elektronsko, se s svojo uporabnostjo in z enostavnim rokovanjem zadnja leta vse hitreje selijo med vsakdanje uporabnike. K temu so veliko prispevali naraščanje zmogljivosti in obenem padanje cen delovnih računalnikov skupaj z napredovanjem komunikacijskih tehnologij, ki bistveno znižujejo stroške globalne povezljivosti. Nove smernice podaja nastanek digitalnih valut, ki se iz povsem ločenih virtualnih okolij selijo na svetovni splet in pri tem prinašajo podoben preskok v dojemanju vrednosti, kot ga je pred časom elektronski denar. Oblikovanje novih denarnih sistemov v zadnjem času prinaša kopico alternativ, s katerimi se lahko nadomeščajo ustaljeni načini plačevanja, ki se postopoma nagibajo k širjenju omrežja, v celoti osnovanega na arhitekturi P2P. Digitalne valute, ki so z nami že dlje časa, so nov obseg dobile s prihodom kriptovalut in prelaganjem njihovega upravljanja med uporabnike.

Kljub dejstvu, da gre pri tem za relativno zgodnje korake in bo prave rezultate pokazala šele prihodnost, nas je zanimalo predvsem, kakšne so prednosti kriptovalut pred tradicionalnimi načini plačevanja. Da je informacijo o denarju, ki je zgolj predstavitev neke vrednosti, mogoče posredovati v elektronski obliki brez dejanskih premikov, je dlje časa kazal čedalje višji delež elektronskega denarja v obtoku. Od tu do alternativnih valut je v teoriji le majhen korak in tako smo sedaj priča pojavu vse številčnejših sistemov, ki posnemajo realne valute. Uporabniki si lastijo digitalne denarnice, distribuiranje novih enot poteka sorazmerno s težavnostjo računskih problemov, stroški procesiranja so povezani s taksami, s katerimi se vzdržuje omrežje, eno zadnjih vprašanj pa ostaja oblikovanje enotne regulacije. Vendar pa pri vsem poseben vpogled nudijo šele aplikacijski programski vmesniki, ki omogočajo integracijo plačevanja v obstoječe trgovske rešitve z uporabo lastne storitve ali vpeljavo zunanjih ponudnikov. Zato nas v okviru diplomske naloge, poleg bistvenih novosti ali nadgradenj že uporabljenih sistemov, vodi vprašanje, do kakšne mere je mogoča implementacija lastne rešitve, s katero bi pokazali prednosti in pomanjkljivosti takšnega sistema v primerjavi z elektronskim. Ustaljeni plačilni procesorji, kakršen je npr. splošno razširjeni PayPal, že omogočajo relativno visoko stopnjo varnosti in hitre izvedbe transakcij, zaradi česar se morda zdi, da prostora za izboljšave ni veliko. S končnim rezultatom bi tako radi pokazali, da je alternativen sistem za plačevanje vsaj enako učinkovit in zanesljiv, obenem pa zaradi decentralizirane in odprte narave dostopen vsakomur. Zagotovo ena večjih posebnost takšnega sistema pa je končno tudi ohranjanje anonimnosti, saj identiteto udeležencev med trgovanjem določajo zgoščene vrednosti, ki se uporabljajo za naslove.

V naslednjem poglavju diplomskega dela podajamo krajši pregled razvoja od prvih elektronskih sistemov plačevanja do ključnih lastnosti digitalnih valut, ki so jih do neke mere podedovale od zasnove trga realnega denarja. Na tem mestu predstavimo še splošne elemente v kriptografiji in sestav z javnim ključem, ki so osnovni pogoj za delovanje vsake kriptovalute. Sledi opredelitev pomembnih vlog zunanjih sistemov v procesu uporabe digitalnih valut in pregled vzporednic, ki jih lahko izpeljemo iz uporabe virtualnih valut v ločenih okoljih. V tretjem poglavju razdelamo poglavitne razlike med vrstami digitalnih valut, opišemo vzrok za nastanek kriptovalut in konceptov, ki jih uporabljajo. Predstavimo pomen digitalnih denarnic, delovanje transakcij in vlogo javno dostopne glavne knjige v obliki decentralizirane podatkovne baze. Pojasnimo tudi, kako se izvaja distribuiranje denarnih enot, in navedemo primerjavo strojne opreme po učinkovitosti reševanja zahtevanih matematičnih problemov. V četrtem poglavju določimo načine plačevanja in procesiranja plačil ob nakupu digitalne vsebine z aplikacijskim programskim vmesnikom. Opredelimo postopek konfiguracije drugih gradnikov sistema, potrebnih ob celotni implementaciji in ovire, nastale pri realizaciji končne rešitve. Na koncu izdelamo še primerjavo lastnega sistema s podobnimi ter oceno odstopanja od zastavljenega cilja.

2 DIGITALNE VALUTE

2.1 OPREDELITEV DIGITALNE VALUTE

Denar v elektronski obliki pogosto označujemo z izrazi, ki so kljub podobnosti med seboj pomensko zelo različni. Za pojmom »valuta« poleg denarne enote stojita tudi denarni sistem in denar v fizični obliki, kadar razlikujemo med navadnim oziroma elektronskim denarjem [1]. Doba elektronskega denarja se je namreč pričela z letom 1960, ko je bil v ZDA predstavljen sistem EFT, ki je odpravil potrebo po uporabi papirnatih čekov, saj so vsa sredstva med bankami potekala elektronsko [2]. Desetletje pozneje so bile vse bančne podružnice v Evropi med seboj že povezane z vpeljavo strežnikov, sistem EFT pa je danes prisoten pri vseh denarnih transakcijah, povezanih z uporabo kreditnih kartic, bančnih avtomatov in terminalov POS.

Elektronski denar je denar, ki obstaja izključno znotraj bančnih računalniških sistemov in se z uporabo računalniških omrežij, interneta ter sistemov za digitalno hrambo podatkov, kakršne so plačilne kartice, izmenjuje elektronsko. Digitalna valuta je ena izmed oblik elektronskega denarja, ki deluje kot alternativna valuta in je med posamezniki prenosljiva brez potrebe po uporabi tradicionalnega bančnega sistema za izmenjavo [3].

2.2 LASTNOSTI DIGITALNIH VALUT

Podobno, kot je elektronski denar moral izpolnjevati vsaj zahteve po varnosti, hitrosti in zanesljivosti, bi morale vse digitalne valute vključevati:

- takojšnji obračun oziroma obdelavo sredstev,
- obvladljivost plačilnih tveganj,
- varnost transakcij.

Trenutno nobena izmed digitalnih valut v uporabi še ne zadostuje vsem zahtevam, saj je v praksi izvedb mnogo, manjkajo pa skupni standardi.

2.2.1 Obdelava sredstev

Dandanes je za izvedbo posamezne denarne transakcije zaradi predhodne obdelave sredstev običajno potrebnih od nekaj ur do več dni, še posebej če se vloge v veliki meri rešujejo ročno ali pa so odvisne od vnaprej določenega obratovalnega časa.

Obračunana sredstva označujejo stanje na računu, ki je pripravljeno na dvig ali uporabo v nadaljnjih transakcijah [4]. Do tega trenutka se štejejo kot čakajoča in se z njimi ne da razpolagati. Posebej pri mednarodnih bančnih prenosih je tako navadno prisotnih več faktorjev, ki vplivajo na dolžino trajanja določenih transakcij. Sem lahko štejemo vrsto storitev, ki se uporabljajo za prenos, hitrost odobritve dviga ali prenosa sredstev in števila vmesnih držav ter finančnih ustanov.

Ker digitalne valute delujejo neodvisno od bančnih sistemov, je hitrost izvajanja pogojena s časom, potrebnim za potrditev transakcije, ki v odvisnosti od vrste valute trenutno znaša nekaj sekund. Tak pristop pa je trenutno mogoč samo pri realizaciji storitve brez podpore reverzibilnih transakcij, s čimer v primeru napak, neavtorizirane uporabe ali nezanesljivega prodajalca prenosov ni mogoče razveljaviti [5]. Takšna rešitev med drugim prinaša tudi manjše tveganje pri plačilih, saj se s krajšanjem časa za obdelavo transakcij veča verjetnost, da se pogodba ali sporazum poravna pred rokom.

2.2.2 Plačilna tveganja

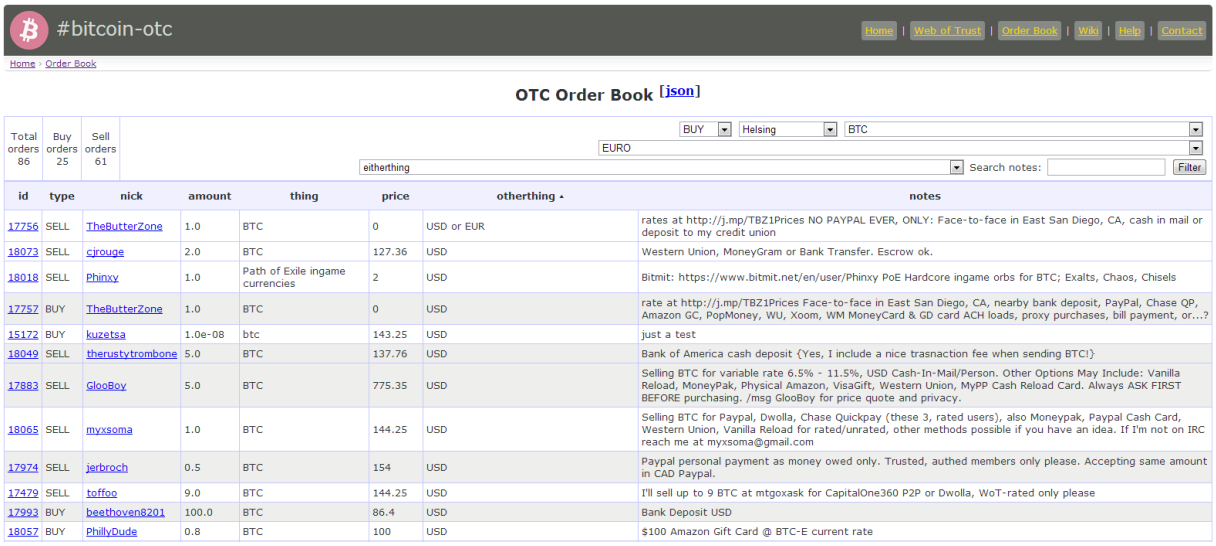
Nevarnost nepopolne poravnave obveznosti pri sklepanju posla, ki je prisotna že od nastanka denarja, predstavlja tveganje, ki se mu pri trgovanju ni mogoče v celoti izogniti in tudi ni dokončno odpravljivo. Eden od vzrokov tiči v tem, da izpolnjevanje dela obveznosti na eni strani ne poteka istočasno kot na drugi, zaradi česar je običajno najprej potrebno vzpostaviti zaupanje ali skleniti pogodbo. Včasih pa tudi to ni dovolj, saj lahko na potek mednarodnega poslovanja vplivajo zunanje razmere. Ker se torej tveganja ne da povsem izključiti, se uporablja več pristopov, ki lahko tveganje bistveno zmanjšajo ali v primeru neplačila njegove posledice vsaj omilijo [6]. Številna podjetja namreč uporabljajo različne metode, ki predvidevajo ocenjevanje stopnje tveganja, s katerim se soočijo, in se nato predhodno zavarujejo za primer oškodovanja.

Ko govorimo o digitalnih valutah, ki še niso prešle iz vloge eksperimenta v čisto polnopravno alternativo dejanskega denarja, je stanje nekoliko drugačno. Teoretično so omenjeno ranljivost prav tako podedovale, saj predstavljajo elektronski medij, katerega vrednost se izraža z drugimi valutami in se med drugim uporablja pri izmenjavi za fizične dobrine. Obseg uporabe je tako odvisen predvsem od posameznikov in trgovcev, ki so pripravljeni zaupati v takšen sistem, saj so ravno slednji tisti, ki lahko na prvi pogled največ izgubijo [7].

Kljub temu pa se v praksi že pojavljajo rešitve, ki lahko tveganja in z njimi povezane možnosti oškodovanja katere od sodelujočih strani zmanjšajo.

Trgovanje OTC je rešitev, značilna za trg vrednostnih papirjev manjših podjetij, ki so brez ustreznih kriterijev za uvrstitev na borzo, zato se posli sklepajo neposredno med strankami in jih borza ne beleži [8].

Podobno izpeljanko tega trga v obliki omrežja OTC (Slika 1) uporabljajo nekatere digitalne valute, katerih uporabniki se na podlagi preteklih poslovanj med seboj ocenjujejo, s čimer se vodita zgodovina trgovanja in evidenca slovesa posameznih udeležencev.



#bitcoin-otc

Home | Web of Trust | Order Book | Wiki | Help | Contact

Home › Order Book

OTC Order Book [json]

Total orders 86 | Buy orders 25 | Sell orders 61

BUY | Helsing | BTC | EURO | eitherthing | Search notes: | Filter

id	type	nick	amount	thing	price	otherthing ▲	notes
17756	SELL	TheButterZone	1.0	BTC	0	USD or EUR	rates at http://j.mp/TBZ1Prices NO PAYPAL EVER, ONLY: Face-to-face in East San Diego, CA, cash in mail or deposit to my credit union
18073	SELL	cjrouge	2.0	BTC	127.36	USD	Western Union, MoneyGram or Bank Transfer. Escrow ok.
18018	SELL	Phinxy	1.0	Path of Exile ingame currencies	2	USD	Bitmit: https://www.bitmit.net/en/user/Phinxy PoE Hardcore ingame orbs for BTC; Exalts, Chaos, Chisels
17757	BUY	TheButterZone	1.0	BTC	0	USD	rate at http://j.mp/TBZ1Prices Face-to-face in East San Diego, CA, nearby bank deposit, PayPal, Chase QP, Amazon GC, PopMoney, WU, Xoom, WM MoneyCard & GD card ACH loads, proxy purchases, bill payment, or...?
15172	BUY	kuzetsa	1.0e-08	btc	143.25	USD	just a test
18049	SELL	therustytrombone	5.0	BTC	137.76	USD	Bank of America cash deposit {Yes, I include a nice trasnaction fee when sending BTC!}
17883	SELL	GlooBoy	5.0	BTC	775.35	USD	Selling BTC for variable rate 6.5% - 11.5%, USD Cash-In-Mail/Person. Other Options May Include: Vanilla Reload, MoneyPak, Physical Amazon, VisaGift, Western Union, MyPP Cash Reload Card. Always ASK FIRST BEFORE purchasing. /msg GlooBoy for price quote and privacy.
18065	SELL	myxsoma	1.0	BTC	144.25	USD	Selling BTC for Paypal, Dwolla, Chase Quickpay (these 3, rated users), also Moneypak, Paypal Cash Card, Western Union, Vanilla Reload for rated/unrated, other methods possible if you have an idea. If I'm not on IRC reach me at myxsoma@gmail.com
17974	SELL	jerbroch	0.5	BTC	154	USD	Paypal personal payment as money owed only. Trusted, authed members only please. Accepting same amount in CAD Paypal.
17479	SELL	toffoo	9.0	BTC	144.25	USD	I'll sell up to 9 BTC at mtgoxask for CapitalOne360 P2P or Dwolla, WoT-rated only please
17993	BUY	beethoven8201	100.0	BTC	86.4	USD	Bank Deposit USD
18057	BUY	PhillyDude	0.8	BTC	100	USD	$100 Amazon Gift Card @ BTC-E current rate

Slika 1: Različica OTC digitalne valute Bitcoin, postavljene na mreži zaupanja (Povzeto po [9]).

Sistem ni stoodstotno zanesljiv, lahko pa nam je v spodbudo, da se pred pričetkom izvajanja nakupa ali prodaje pozanimamo o kredibilnosti soudeleženca.

2.2.3 Varnost transakcij

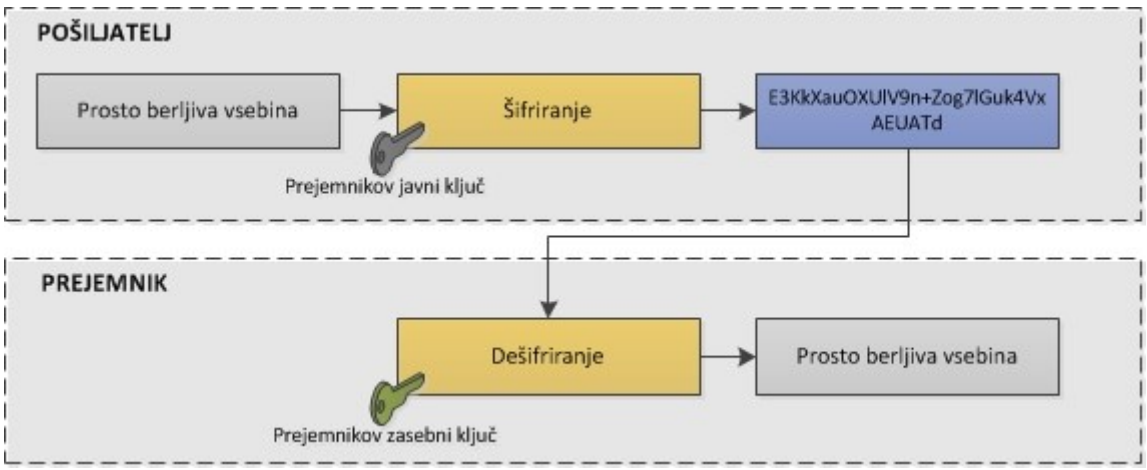
Pretok informacij skozi računalniško omrežje, ki ga v osnovi sestavlja veliko število med seboj povezanih vozlišč oziroma vseh aktivnih naprav, zmožnih pošiljanja, sprejemanja ali posredovanja podatkov, je zaradi svoje oblike v veliki meri ranljiv na prestrezanje in napade.
Te lahko razvrstimo v dve kategoriji, ki se glede na način poseganja v vsebino sporočil ločijo na pasivne in aktivne [10]. Prvi namreč podatkov ne spreminjajo in ne puščajo sledi. Ker gre predvsem za prisluškovanje in spremljanje prometa, jih je včasih zelo težko odkriti. Pri aktivnih napadih prihaja do neposrednega dodajanja ali odvzemanja delov sporočila, s čimer se največkrat želi napadalec prejemniku predstaviti kot nekdo drug.

Vpeljava kriptografije na praktično vsa področja komunikacij tako pomaga pri varovanju občutljivih podatkov, do katerih smejo dostopati le pooblaščeni. Transakcije so varne le, če se vse informacije predhodno kriptirajo, kar pomeni, da se ne prenašajo več v prosto berljivi obliki, ampak se s tako imenovanim procesom šifriranja pretvorijo v prikrite. Za izvajanje takšnega postopka sta potrebna dva bistvena gradnika, in sicer algoritem, po katerem se šifrira, in geslo oziroma ključ, ki dovoljuje uporabo obratnega procesa, torej dešifriranja.

Pri prvem, simetričnem, so tako ključa kot šifri prikrivanja in razkrivanja enaki. Šifra, za katero se predpostavlja, da je vnaprej znana, pa spreminja informacije glede na ključ, saj dajejo različni ključi različne rezultate, ne glede na to, ali gre za enako šifro [11]. Ker igrajo v takšnem postopku pomembnejšo vlogo ravno ključi, za katere rečemo, da so zasebni in ne smejo biti javno znani, je stopnja varnosti običajno odvisna ravno od njihove bitne dolžine.
Simetrični ključi so trenutno ranljivi na uporabo grobe sile, kjer napadalec prikrita sporočila razbija s preizkušanjem vseh možnih ključev. To pomeni, da je za vsak ključ dolžine n potrebno pregledati 2^n kombinacij.

Zaradi tega današnji algoritmi uporabljajo ključe dolžine večkratnika 32 bitov, ki za posamezen izračun zahtevajo bistveno višjo računsko moč in čas. Za primer vzemimo simetrična algoritma, kot sta AES, ki omogoča 128-, 192- in 256-bitne dolžine ključev, ali pa Blowfish, s podporo do 448-bitnih ključev, pri katerih hitro opazimo, da je omenjeni napad zaradi eksponentnega naraščanja zahtevnosti vse manj učinkovit [12].

Sestav z javnim ključem (Slika 2) v nasprotju s simetričnim uporablja različna postopka in ključa, zato ga označujemo kot asimetričnega. Ker se postopka šifriranja in dešifriranja razlikujeta, posledično uporabljamo dva neenaka ključa, kjer javnega uporabljamo za šifriranje, zasebnega pa za dešifriranje.

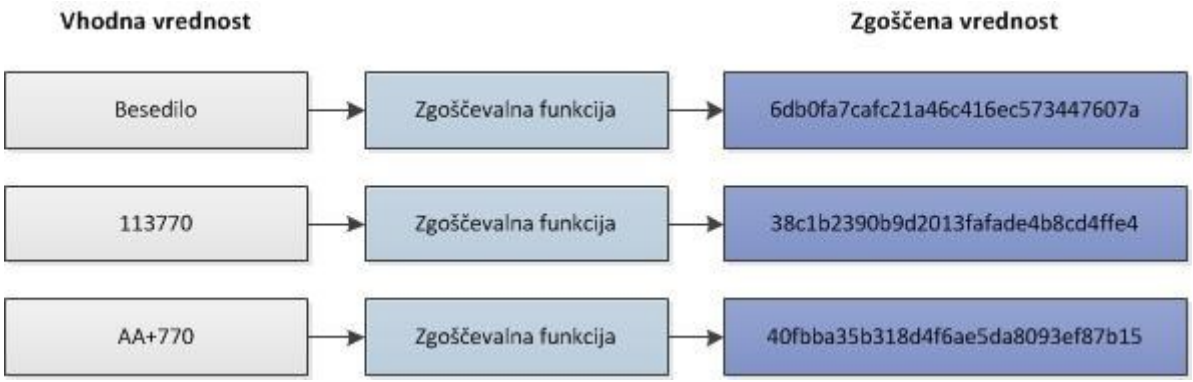


Slika 2: Koncept delovanja sestava z javnim ključem (Povzeto po [13]).

Za delovanje takšnega sistema mora biti računsko neizvedljivo, da bi samo na podlagi poznavanja javnega ključa lahko izračunali tudi zasebnega, zato je prvega mogoče objaviti, medtem ko se ključ za dešifriranje hrani v zasebnosti. Uporaba sistema javnih ključev eliminira tudi potrebo po začetnem koraku, s katerim se najprej varno izmenjajo eden ali več zasebnih ključev med pošiljateljem in prejemnikom, kot se to izvaja pri simetričnih sistemih.

Enaka logika se uporablja pri zagotavljanju integritete pošiljatelja sporočila, le da je vrstni red uporabe ključev obraten. Digitalni podpis, ki služi kot potrdilo, da ima pošiljatelj v lasti svoj zasebni ključ in s tem zelo verjetno tudi javni ključ prejemnika, zagotavlja, da med pošiljanjem šifriranega sporočila ne pride do kakršnekoli spremembe vsebine [14].

Da lahko pošiljatelj podpiše dokument, ga mora najprej zgostiti, zato se v ta namen uporablja posebna zgoščevalna funkcija (Slika 3), ki iz slednjega izračuna unikaten zapis, prav tako na podlagi zasebnega ključa. Izračunana vrednost oziroma pridobljeni zapis tako predstavlja digitalni podpis, s katerim se pošlje pripadajoči dokument. Ker zgoščena vrednost ni reverzibilna, mora prejemnik za prejeti dokument z enako funkcijo izračunati novo zgoščeno vrednost. Če se ta ujema s spremljajočim digitalnim podpisom, pomeni, da je sporočilo pristno, saj bi v nasprotnem primeru dobili drugačen rezultat.



Slika 3: Primer delovanja zgoščevalne funkcije MD5 s 128 bitnimi zgoščenimi vrednostmi (Povzeto po [15]).

Če uporabnik do spletne strani dostopa brez uporabe digitalnega podpisovanja, na začetni strani poleg prikazane vsebine prejme tudi javni ključ, ki služi kriptiranju podatkov v smeri od uporabnika do strežnika. Ker se za enkripcijo uporablja javni ključ, pomeni, da lahko kriptirane podatke prebere le strežnik z zasebnim ključem. Pri takšni uporabi pa obstaja nevarnost, da že na začetku, ko uporabnik v brskalnik vpiše naslov ciljne spletne strani, komunikacijo prestreže napadalec in zahtevo preusmeri na svojo spletno stran, ki se predstavlja za pristno. Tudi takšna stran lahko pošlje ponarejeni javni ključ uporabniku, s katerim ta kriptirane podatke nevede pošilja napadalcu.

Zato se pri vsakdanji uporabi zahteva tudi vključevanje digitalnih podpisov, ki jih hrani in izdaja CA, kakršne so pri nas Halcom CA, Pošta Slovenije, SIGEN-CA in druge, ter za vsak javni ključ določa posameznega uporabnika [16]. Ko tako uporabnik vstopi na spletno stran, skupaj z javnim ključem prejme še digitalni podpis ključa in vrsto dodatnih informacij, ki jih za infrastrukturo PKI določa certifikat X509. Brskalnik, s katerim uporabnik dostopa do spletne strani, mora imeti predhodno nameščen javni ključ CA, s katerim lahko preveri pristnost omenjenega podpisa.

Nekateri algoritmi, kakršen je RSA, se uporabljajo za kriptiranje in tudi ustvarjanje digitalnih podpisov, drugi, kot na primer algoritem DSA (ang. Digital Signature Algorithm), ki se uporablja samo za kreiranje digitalnih podpisov, pa so bolj specifični [17].

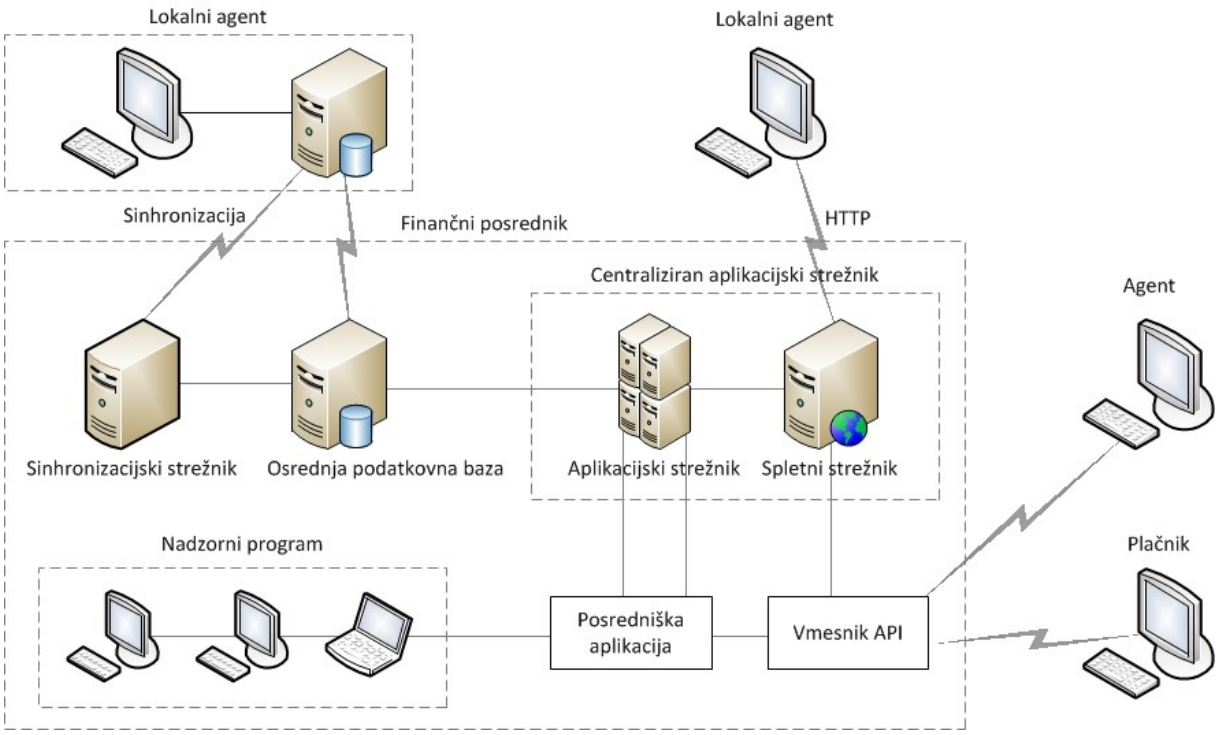
2.3 POMEMBNE VLOGE V PROCESU UPORABE DIGITALNIH VALUT

2.3.1 Finančni posredniki

Zahteve po varnem in globalnem prenašanju denarnih sredstev, ki so nastale s prihodom elektronskega denarja, danes v obliki plačljivih storitev izpolnjujejo podjetja in drugi poslovni subjekti. Te je lokalna vlada za to pooblastila in jih posledično tudi regulira ter obenem zagotavlja, da njihovo izvajanje ustreza zakonodaji. Kot finančni posrednik (ang. Money Transmitter) je določen vsakdo, ki zadostuje enemu od pogojev:

- opravlja storitev, pri kateri sprejema določeno valuto ali denarna sredstva, denominirana v kateri od valut,
- prenaša valuto in denarna sredstva oziroma njihovo vrednost v kakršnikoli obliki,
- je kakorkoli vključen v storitev prenašanja denarnih sredstev (Slika 4).

Po funkciji se finančni posredniki delijo na spletno povezljive in lokalne. Prvi za uporabo zahtevajo članstvo, saj je vsakemu uporabniku dodeljen ločen račun, povezan z vsaj enim bančnim računom [18]. Glede na vrsto storitev jih lahko kategoriziramo na dve podskupini, pri čemer nekateri striktno opravljajo zgolj vlogo posrednikov, drugi pa po funkcionalnosti delujejo kot alternative bankam.



Slika 4: Ena izmed možnih postavitev omrežja finančnega posrednika z agenti v vlogi terminalov POS (Povzeto po [19]).

Lokalni posredniki ne zahtevajo registriranih uporabnikov, saj sprejemajo le gotovino in gotovinske čeke, storitev pa običajno opravljajo podružnice za menjavo valut.

Med najbolj razširjene finančne posrednike sodijo tudi podjetja American Express, Western Union in PayPal, ki je na primer za svoje delovanje v ZDA moralo pridobiti licenco za vsako državo posebej, medtem ko v Evropi od leta 2007 dalje kot regulirana bančna ustanova opravlja tudi bančne storitve [20, 21]. Finančni posredniki so prav tako postali ponudniki digitalnih valut, katerih zgodnji predstavniki pa sprva za svoje delovanje niso imeli licence MSB (ang. Money Service Business).

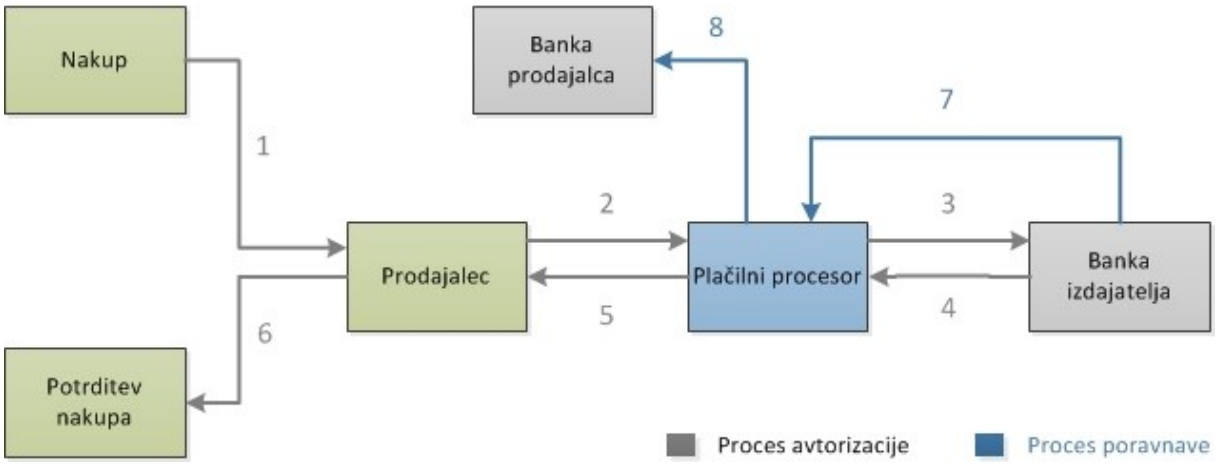
Določbe, ki so se nanašale na digitalne valute, so bile namreč v tem času relativno dvoumne, definicija finančnega posrednika, kot jo je z novo revizijo določala agencija FinCEN, pa je bila izdana julija leta 2011 in je zajemala vsak sistem, ki je kakorkoli vključeval sprejemanje valut, denarnih sredstev ali druge oblike vrednosti, ki se je izmenjavala med dvema osebama. Smernice, ki bi jih lahko uporabljali pri regulacijah digitalnih valut, so sledile z marcem leta 2013 [22]. S tem naj bi bili vsi finančni posredniki, z izjemo nekaterih, registrirani pri agenciji FinCEN, vendar je za razliko od centraliziranih sistemov izvajanje regulacij in nadzora nad finančnimi transakcijami v primeru decentraliziranih digitalnih valut zaradi oblike denarnega sistema v veliki meri še nedorečeno.

2.3.2 Plačilni procesorji

Vloga plačilnega procesorja je v nekaterih pogledih podobna funkcijam finančnega posrednika, zato v tej vlogi najdemo tudi nekatera prej omenjena podjetja. Neodvisni plačilni procesorji so praviloma registrirane in licencirane nebančne entitete, ki procesiranje finančnih transakcij nudijo strankam, običajno trgovcem, brez potrebe po neposrednem vzpostavljanju računa za spletno poslovanje na banki [23].

Plačilni procesorji, kakršni so PayPal, Amazon in Dwolla [24], so tipični primeri posrednikov med kupčevo in prodajalčevo banko, medtem ko se med digitalnimi valutami največkrat omenjajo sistemi Coinbase, BitPay ter evropski sistem BIPS (ang. Bitcoin Internet Payment System) [25].

Banke, ki sprejemajo neodvisne plačilne procesorje, so same zadolžene in odgovorne za implementacijo efektivnega programa AML, s čimer se izvaja nadzor za preprečevanje pranja denarja. Takšne okoliščine pridejo posebej do izraza med uporabo digitalnih valut, ko je ravno tako potrebno zagotoviti varnost transakcij. To pa je zaradi pomanjkanja informacij o transakcijah, ki se med ponudniki digitalnih valut in menjalnicami izvajajo zunaj običajnih bančnih sistemov, težko izvedljivo, četudi bi želeli uporabiti že obstoječe regulacije [26]. Pri današnji arhitekturi plačevanja s kreditnimi karticami (Slika 5) so področja delovanja in odgovornosti porazdeljeni med vse člene, zaradi česar je morebitne tehnične težave veliko laže reševati.



Slika 5: Poenostavljena ponazoritev vloge plačilnega procesorja pri spletnem plačevanju s kreditno kartico (Povzeto po [27]).

Sodobni plačilni procesorji so s prodajalcem pogostokrat povezani preko terminala POS oziroma storitve SaaS (ang. Software-as-a-Service), ki jih predvsem za restavracije ponujajo neodvisni razvijalci. Da bi integracija plačevanja z digitalnimi valutami lahko postala ena od opcij uporabe nekaterih prodajalcev, kaže napoved podjetja SoftTouch LLC, ki je oktobra leta 2013 za produkte SoftTouch POS napovedalo podporo kriptovaluti Bitcoin [28].

2.3.3 Menjalnice digitalnih valut

Ena od prednosti v procesu izmenjave, ki jo imajo današnje realne valute, je dojemanje njihove nominalne vrednosti, ki s potrošnikovega vidika sama po sebi predstavlja kupno moč. Za večino digitalnih valut, ki delujejo brez specifičnega kritja, kot so drage kovine, pa se vrednost odraža v odvisnosti od realnih valut.

Menjalnice digitalnih valut (v nadaljevanju menjalnice) oziroma menjalnice DCE (ang. Digital Currency Exchangers) so za proces izmenjave prav tako bistvene, saj je le preko njih možno nakazovanje digitalnih valut na plačilne procesorje. Vlogo vmesnega člena igrajo tudi pri prenosih iz enega plačilnega procesorja na drugega, ko neposreden prenos na bančni račun ni možen.

Izbira ustrezne menjalnice je običajno relativno trivialna naloga, saj nekateri ponudniki skupaj s svojo digitalno valuto nudijo tudi lastno storitev, s katero sta mogoča nakup ali zamenjava. Zaradi tveganj, ki izhajajo predvsem iz regulacij, pa določeni ponudniki digitalnih valut svojih menjalnic ne uporabljajo [29].

Tveganja, povezana z uporabo menjalnic digitalnih valut, ki so jim uporabniki pogosto izpostavljeni, zajemajo z menjalnicami povezane storitve, pri katerih se napadalci poslužujejo spletnega ribarjenja (phishing[1]) in napadov DDoS. Japonska menjalnica Mt. Gox, ki je med kriptovalutami do leta 2014 veljala za največjo, je bila na primer tarča obeh pristopov. Za preprečevanje neavtoriziranih dostopov do uporabniških računov je v ta namen sicer običajno določena dvostopenjska avtentikacija, ki poleg gesla ob prijavi zahteva še dodatno informacijo. To si lahko lasti le pristni uporabnik, zato gre pri tem največkrat za osebne dokumente ali pa pametne kartice.

[1] Napad, s katerim poskuša napadalec pridobiti uporabniška imena in gesla s pomočjo spletnih povezav v elektronski pošti ali lažne spletne strani.

Vendar pa dvostopenjska avtentikacija ni nujno privzeto vključena, temveč jo mora ponekod aktivirati uporabnik. Da je dodaten nivo zaščite priporočljiv, se je pokazalo aprila leta 2013, ko je lažna spletna klepetalnica, povezana z menjalnico Mt. Gox, ob obisku uporabnikov na njihov računalnik namestila applet (manjša aplikacija, ki se običajno izvaja v sklopu večjega programa), ki je sprožil zahtevek za samodejni prenos digitalne valute Bitcoin. Ker transakcije niso reverzibilne, sredstev, prenesenih iz uporabniških digitalnih denarnic na napadalčev račun, ni bilo mogoče povrniti [30].

Podoben primer spletnega ribarjenja se je odvil junija istega leta, le da je pri tem do lažne strani z domeno mtpox.com, ki se je predstavljala za uradno, že omenjeno menjalnico, vodil iskalni rezultat v spletnem iskalniku Yahoo. Tako iskalnika Bing kot Yahoo omogočata plačljivo sponzoriranje in oglase, ki se pojavljajo med prvimi iskalnimi zadetki, zato je pri tem nemalokrat težko ločiti med plačljivimi in iskanimi rezultati. Ob vnašanju uporabniškega imena in gesla v prijavno formo podatki niso bili posredovani naprej, saj stran ni bila v celoti funkcionalna [31].

Dober pokazatelj, ali je obiskana stran, ki podpira tehnologijo SSL, pristna, je spletni naslov ali naslov URL. Iz tega je hitro razvidna tudi domena, ki v primeru lažne spletne strani ne more biti enaka domeni pristne, torej se od nje razlikuje.

Napad DDoS, ki se je prav tako odvil aprila istega leta, za razliko od drugih napadov te vrste ni ciljal neposredno na strežniško infrastrukturo, temveč na aplikacije, ki jih je spletna stran Mt. Gox uporabljala za procesiranje in kriptiranje transakcij uporabnikov. V takšnem primeru se napad izvaja nad aplikacijsko plastjo modela OSI (ang. Open Systems Interconnection), ki se sicer uporablja kot konceptualni model za grupiranje med seboj podobnih komunikacijskih funkcij v posamezne logične plasti. Vsaka plast je zadolžena za izvajanje specifičnih funkcij in služi plasti nad seboj, komunikacija med dvema instancama posamezne plasti v omrežju lahko poteka samo horizontalno.

Aplikacije, ki uporabljajo komunikacijska protokola HTTP in HTTPS, predstavljajo ozko grlo, saj ob nenadnem pritoku velike količine podatkov izvajanje ne dohaja zahtevkov. V omenjenem primeru je pasovna širina napada dosegala 77 gigabitov na sekundo, kar je bistveno presegalo zmogljivosti tedanje strojne opreme [32].

2.4 ZAKAJ VIRTUALNI DENAR NI DIGITALNA VALUTA

Pri obeh oblikah gre sicer za elektronski medij izmenjave, vendar se virtualna valuta od digitalne loči predvsem po tem, da je omejena na uporabo znotraj socialnih omrežij in spletnih iger z lastno ekonomijo. V nekaterih primerih, kot je to dokazala digitalna valuta Ven, pa se iz virtualnega denarja lahko razvije nova valuta, ki deluje izven takšnih okvirjev.

S pojmom »virtualna ekonomija« označujemo ekonomijo, ki obstaja v realnočasovnem virtualnem oziroma sintetičnem svetu, v katerega je lahko hkrati vključenih več tisoč med seboj sodelujočih uporabnikov, predstavljenih s tako imenovanimi avatarji[2]. In čeravno se ti za prijavo največkrat odločijo zaradi želje po sprostitvi, zabavi ali preizkušanju podjetniških sposobnosti, jih je veliko, ki v tem vidijo predvsem možnost zaslužka. Narava virtualne ekonomije se namreč kljub nekaterim razlikam zgleduje po dejanski. To pomeni, da si igralci v posamezni igri lahko ekskluzivno lastijo nepremičnine in druge predmete, ki se štejejo za dobrine, s katerimi lahko trgujejo.

Blago v virtualni ekonomiji je konceptualno enako običajnim dobrinam, katerih produkcija lahko vključuje visoke mejne stroške, ki so med drugim lahko posledica naravne redkosti nekaterih dobrin. Ker je virtualne predmete v principu mogoče podvajati brez vsakršnih stroškov, se z vpeljavo umetnih omejitev in ustvarjanjem napora pri njihovem pridobivanju zagotovi ohranjanje vrednosti in unikatnost.

V praksi je jasna meja med virtualno in pravo ekonomijo večkrat zabrisana. Za primer vzemimo digitalno glasbo ali filme, ki tudi vključujejo pristope za umetno ohranjanje vrednosti. Tu se čedalje pogosteje pojavlja tehnologija DRM, ki jo nekateri proizvajalci, izdajatelji in posamezniki uporabljajo za preprečevanje neomejenega dostopanja do vsebine, kopiranja, pretvarjanje v druge formate in nameščanja na ostale naprave [33, str. 6–7].

2.4.1 Primer delovanja virtualne ekonomije znotraj digitalnih storitev

Za jasnejši vpogled v način uporabe virtualnih valut in trgovanja si bomo pogledali dva v osnovi podobna primera, ki pa med drugim uporabljata vsak svojo obliko ekonomije, pri čemer se bomo omejili zgolj na prikaz uporabe interne valute in zasnove trga.

[2] Avatar je grafična ali abstraktna predstavitev uporabnika, ki je lahko tridimenzionalne oblike, kot je to značilno za virtualne svetove, lahko pa tudi dvodimenzionalne, kot na primer ikone uporabnikov internetnih forumov.

Prvi primer je realnočasovna vesoljska simulacija Eve Online tipa MMORPG (ang. Massively Multiplayer Online Role-Playing Game), postavljena v znanstvenofantastično okolje, v katerem igralci raziskujejo zvezdne sisteme, se bojujejo, trgujejo in gradijo vesoljske ladje. Igra, ki jo je leta 2003 izdalo islandsko podjetje CCP in uporablja naročniški model, vsebuje eno kompleksnejših izvedb virtualne ekonomije. Valuta, ki jo igra uporablja je ISK (ang. Interstellar Kredits), kar je tudi akronim za dejansko islandsko krono po standardu valutnih oznak ISO 4217. Kupuje in prodaja se lahko vse od enot PLEX (naročniško obdobje 30 dni v igri) do surovin, tehnologij in plovil. Celotna vrednost proizvedenih dobrin mesečno je bila aprila leta 2013 ocenjena na 135 bilijonov ISK (od skupno 650 bilijonov ISK, kot jih je bilo maja istega leta v obtoku [34]) ali skoraj 3,9 milijona evrov, potem ko je število naročnikov februarja preseglo mejo 500 000 [35].

Da so številne masovne spletne igre dandanes relativno kompleksne, se kaže v vse pogostejšem zaposlovanju pravih ekonomistov v podjetjih, ki potrebujejo pomoč pri uravnavanju in nadzoru virtualnih svetov. To se je zgodilo tudi v podjetju CCP leta 2007, ko je po večletnem sodelovanju zaposlilo ekonomista dr. Eyjólfura Guðmundssona, katerega glavna naloga je spremljanje vseh ekonomskih aktivnosti v omenjeni igri.

Kljub relativno visoki meri delovanja po principu prostega trga ali politike nevmešavanja, v kateri izmenjava blaga in storitev med ljudmi poteka brez posredovanja tretje strani, je včasih le potreben poseg. Vsaj enkrat se je namreč izkazalo, da se v sistemu zaradi povečanih cen enot PLEX formira potencialni ekonomski mehurček, ki je sicer nevaren pojav v pravi ekonomiji in se običajno pokaže šele po nenadnem padcu cen na trgu.

V podobno smer gre drugi primer večigralskega peskovnika, prav tako leta 2003 izdana spletna igra Second Life podjetja Linden Lab, kjer uporabniki, kot že ime namiguje, soustvarjajo skupen virtualni svet, v katerem se družijo in komunicirajo z uporabo svojih avatarjev. Ekonomija v igri sloni na valuti Linden Dollar (L$), s katero se lahko trguje pri večini navideznih dobrin. Naročniki tedensko avtomatsko prejemajo tako imenovano štipendijo v določenem znesku L$, vsakih nadaljnjih 45 dni pa še dodaten bonus.
Virtualna valuta se lahko kupi na uradni strani podjetja, od zunanjih dobaviteljev ali neposredno od igralcev, pri čemer jo je možno nazaj izmenjati za realno.

Predvsem ta opcija se bistveno razlikuje od večine drugih virtualnih svetov, saj politika interne valute dovoljuje ustvarjanje dejanskega dobička. Uporabniki lahko dolarje L$ služijo podobno, kot bi denar služili v pravem svetu, torej s preprodajo virtualnih nepremičnin, razvijanjem zemljišč, vodenjem trgovin in prodajo virtualnih. Kot kaže praksa, po kateri se jih v sistem od uradno 36 milijonov uporabnikov, registriranih do junija 2013, dnevno prijavi povprečno 55 000, jih od tega le nekaj sto ustvarja dobiček v vrednosti nad 3000 evrov [36].

S tega stališča nam virtualni svetovi nudijo vpogled v sistem brez regulacijskih domen in hkrati trg, ki ga vodijo ter oblikujejo igralci sami, zato lahko nanje gledamo kot na svojevrsten eksperiment, za katerega vemo, da v pravem svetu v taki obliki ne bi mogel obstajati.

2.4.2 Segmenti virtualne ekonomije

Vse bistvene aktivnosti virtualne ekonomije v današnji obliki lahko kategoriziramo v enega izmed dveh segmentov:

- nudenje storitev za spletne igre,
- uporabniško produkcijo virtualnih dobrin.

Z naraščanjem popularnosti spletnih iger in številom igralcev, ki se jim redno posvečajo, se širi tudi velikost trga po principu povpraševanja in ponudbe.

Kot lahko v realnem svetu potrošniške dobrine predstavljajo vrednost socialnega statusa, se v večigralskih svetovih, kjer igralci med seboj tekmujejo, sodelujejo in primerjajo, podoben status dosega s številnimi aktivnostmi. Sistematično in največkrat ponavljajoče se izvajanje podobnih ali enakih nalog, s katerimi bi si igralec na primer prislužil neko virtualno dobrino, pa lahko zahteva zelo veliko vloženega časa in napora. Namesto tega se nekateri raje odločijo za njen odkup od nekoga, ki si jo že lasti ali pa »najamejo« drugega igralca, ki v zameno za plačilo igrajo v imenu lastnika. Trgovanje v obeh primerih vključuje uporabo realnega denarja in ne virtualnih valut [33, str. 9–12].

Izmenjevanje virtualnih dobrin za realen denar je sčasoma vodilo v nastanek sekundarnega trga. Večina založnikov takšne oblike trgovanja ne podpira, zato se nakupi in prodaje odvijajo na neodvisnih trgih. Kot nakazuje trend, se velikost trga RMT po vrednosti povečuje eksponentno. Leta 2001 je prva študija te vrste [33, str. 5–6], ki jo je izvedel ekonomist Edward Castronova, pokazala, da je sekundarni trg vreden 5 milijonov dolarjev, vendar je rezultat temeljil na številu izvedenih transakcij izključno na strani eBay.

Leta 2004 je tržna platforma IGE vrednost globalnega trga ocenila na 880 milijonov dolarjev, čeravno jasen opis metode ni bil javno izdan. Do leta 2009 je vrednost trga RMT po predhodnih ocenah že presegala 3 milijarde dolarjev (Tabela 1).

Država/Regija	**Število igralcev** (v milijonih dolarjev)	**Delež igralcev, ki uporabljajo sekundarni trg**	**Letna potrošnja na sekundarnem trgu** (v milijonih dolarjev)	**Velikost sekundarnega trga** (v milijonih dolarjev)
Koreja	7	0,24	369	620
Evropa, Severna Amerika, Japonska	30	0,22	369	578
Kitajska	69	0,25	87,50	1510
Države v razvoju	15	0,24	87,50	315
Globalni trg	**121**			**3023**

Tabela 1: Velikost globalnega sekundarnega trga virtualnih svetov (Povzeto po [33, str. 15–18]).

V obeh primerih digitalnih storitev je razvidna uporabniška produkcija virtualnih dobrin, ki se kot aktivnost na področju informacijsko-komunikacijskih tehnologij še ni dokončno izoblikovala in bi v prihodnosti lahko igrala bistveno večjo vlogo.

V zadnjih letih se predvideva možnost hitro dostopnih podjetniških priložnosti, povezanih s produkcijo izdelkov in storitev za nove spletne trge, ki bi bili postavljeni v virtualne svetove. Stranke in neodvisne proizvajalce bi združevali tako imenovani dvostranski trgi ali omrežja, na katerih si dve ločeni uporabniški skupini medsebojno ponujata spletne storitve. Interese ločenih skupin na dvostranskem trgu ponazarja naslednji primer: potrošniki si želijo, da bi njihovo kreditno kartico sprejemalo kar največ trgovcev, medtem ko ti težijo k temu, da bi čim več potrošnikov pri nakupih kot plačilno sredstvo uporabljalo kreditne kartice [37]. Omenjene ekonomske platforme so v uporabi že danes in jih najdemo tudi pri večjih organizacijah, kakršne so Facebook, Google, eBay in Skype.

2.4.3 Vpeljava regulacij

Potrošnikove pravice pri digitalnih storitvah, regulacija elektronskih plačilnih storitev in takse virtualnih transakcij so vprašanja, ki v sklopu virtualne ekonomije še niso bila dokončno razrešena. Zagotovo največji izziv pa predstavlja poslovni model produkcije in prodaje virtualnih dobrin za realen denar, za katerega še ni določeno, ali bi smel biti legalen ali ne.

Trgovanje RMT z digitalnimi produkti in virtualnimi valutami po eni strani sicer predstavlja socialno dobrino, ki prinaša prednost tistim z manj časa in več denarnimi sredstvi, po drugi strani pa v virtualno ekonomijo prinaša številne negativne učinke:

- pravičnost do drugih sodelujočih znotraj virtualnega sveta ne deluje takrat, ko lahko posamezniki pravila poenostavljajo z uporabo denarnih sredstev;
- hierarhija dosežkov se zaradi preskakovanja truda in časa podira, virtualni predmeti za skupnost uporabnikov izgubijo vrednost;
- sekundarni trgi niso odporni na nastanek kriminala – kot na vsakem trgu, kjer je dobrine mogoče preprodati, so tudi na tem področju nekatere virtualne dobrine zelo iskane, zaradi česar prihaja do vdorov v zasebne uporabniške račune in številnih tatvin.

Ali bo spletna storitev podpirala delovanje sekundarnega trga, je tako trenutno predvsem domena založnikov. Velika večina jih temu striktno nasprotuje z vpeljavo pogojev uporabe oziroma pogojev TOS (v nadaljevanju pogoji TOS), namenjenih predvsem za spletne strani in ponudnike spletnih storitev, ki hranijo potrošnikove zasebne podatke. Pogoji TOS, ki jih storitve vključujejo, se med seboj razlikujejo, vendar so kljub temu pravno zavezujoči. Poleg tega je predvsem v industriji lastniške programske opreme vpeljana tudi licenčna pogodba za končne uporabnike oziroma EULA (ang. End-User License Agreements).

Nekatere oblike se po namenu približajo prej omenjeni tehnologiji DRM, v splošnem pa se z njo določajo pogoji uporabe, uporabniku običajno vidni med nameščanjem programske opreme. Kot kaže praksa, je takšna orodja relativno enostavno zaobiti, saj lahko posameznik strinjanje potrdi z enim klikom, kršitelje pa je pozneje veliko teže odkriti [33, str. 18–19].

3 VRSTE DIGITALNIH VALUT

Obstoječe digitalne valute lahko po funkcionalnosti razvrstimo v več kategorij. Kriptovalute so digitalne valute, ki slonijo na kriptografiji [38], določene digitalne valute pa se med seboj razlikujejo tudi po vpeljavi kritja. Posebna vrsta so digitalne zlate valute (v nadaljevanju valute DGC), katerih vrednost se odraža z dragimi kovinami in ne zgolj z realnimi valutami [39]. V naslednjih podpoglavjih so predstavljene glavne značilnosti posameznih kategorij.

3.1 DIGITALNE ZLATE VALUTE

So vrsta elektronskega denarja, ki je podprt z zlatom, katerega posamezno enoto največkrat predstavlja gram ali unča. Za razliko od klasičnega denarja valute DGC distribuirajo podjetja, ki uporabnikom nudijo privaten sistem za medsebojno plačevanje z enotami, predstavljenimi z zlatimi palicami [40]. Te so namreč primerne za nadaljnjo obdelavo, poleg tega pa je njihova vrednost določena s čistočo zlitine in maso, zato je gram ene valute DGC praviloma vedno enak gramu katerekoli druge.

Drage kovine, kakršne so zlato, srebro, platina in paladij, imajo po standardu ISO 4217 tako kot druge valute svoje mednarodne valutne oznake. V nasprotju s sistemom delnih rezerv bank valuta DGC teoretično zagotavlja stoodstotno pokritost denarnih sredstev stranke, depoziti pa so varni pred vplivi inflacije, devalvacije in drugimi ekonomskimi tveganji. Kupec takšne valute torej dejansko kupi ustrezen delež zlata, shranjenega v trezorju na določeni lokaciji, vrednost razpoložljivih sredstev na računu pa se vsakodnevno posodablja v razmerju s trenutno vrednostjo dragih kovin.

3.1.1 Prednosti in slabosti valut DGC

Zasnova sistema je podobna vlogi delničarjev, katerih deleži predstavljajo določen odstotek lastništva, saj se s transakcijami menjujejo le oznake lastništev dragih kovin in ne fizično kovine same. Ideja o poenostavljenem trgovanju z valuto, ki jo na primer krije zlato ali srebro, pa je v realnosti že zgodaj naletela na vsaj enega izmed štirih osnovnih izzivov:

a) Upravljanje in politična tveganja

Ker so ponudniki valut DGC zasebna podjetja in ne običajne bančne ustanove, delujejo predvsem v okviru lastnih regulacij in so prav tako vključeni v združenje GDCA. V primeru upravljanja so tveganja odvisna od institucije, ki stoji za distribuiranjem valute DGC. Več dejstev je pokazalo, da takšna podjetja ne prinašajo pravih investicij niti ne razpolagajo z zlatom.

Predvsem v obdobju med letoma 1999 in 2004 je več ponudnikov, kakršna sta tedaj bolj znana OS-Gold in INTGold, propadlo zaradi zavajanj s fiktivnimi visoko donosnimi investicijami oziroma shemami HYIP brez kakršnegakoli kritja ali pa kraj osebnih sredstev iz računov uporabnikov.

Politična tveganja so v tem primeru vrsta tveganja, s katerimi se soočajo investitorji, ki jih doleti finančna izguba, in podjetja, katerih izguba delovne sile, strateškega ali finančnega položaja je lahko rezultat makroekonomske in socialne politike, lahko pa tudi politične nestabilnosti. Podjetja, katerih dejavnost je propadla med letoma 2007 in 2008, so e-Bullion, obtoženo izvajanja nelicenciranih denarnih transakcij in vpletenosti v druga kriminalna dejanja, e-gold Ltd., ki je bilo osumljeno pranja denarja, in 1mdc, podprto z valuto e-gold. Insolventnost podjetja 1mdc je nastala zaradi odsotnosti kritja, ki je prej slonelo na rezervah valute e-gold [41].

b) Varnost podatkov

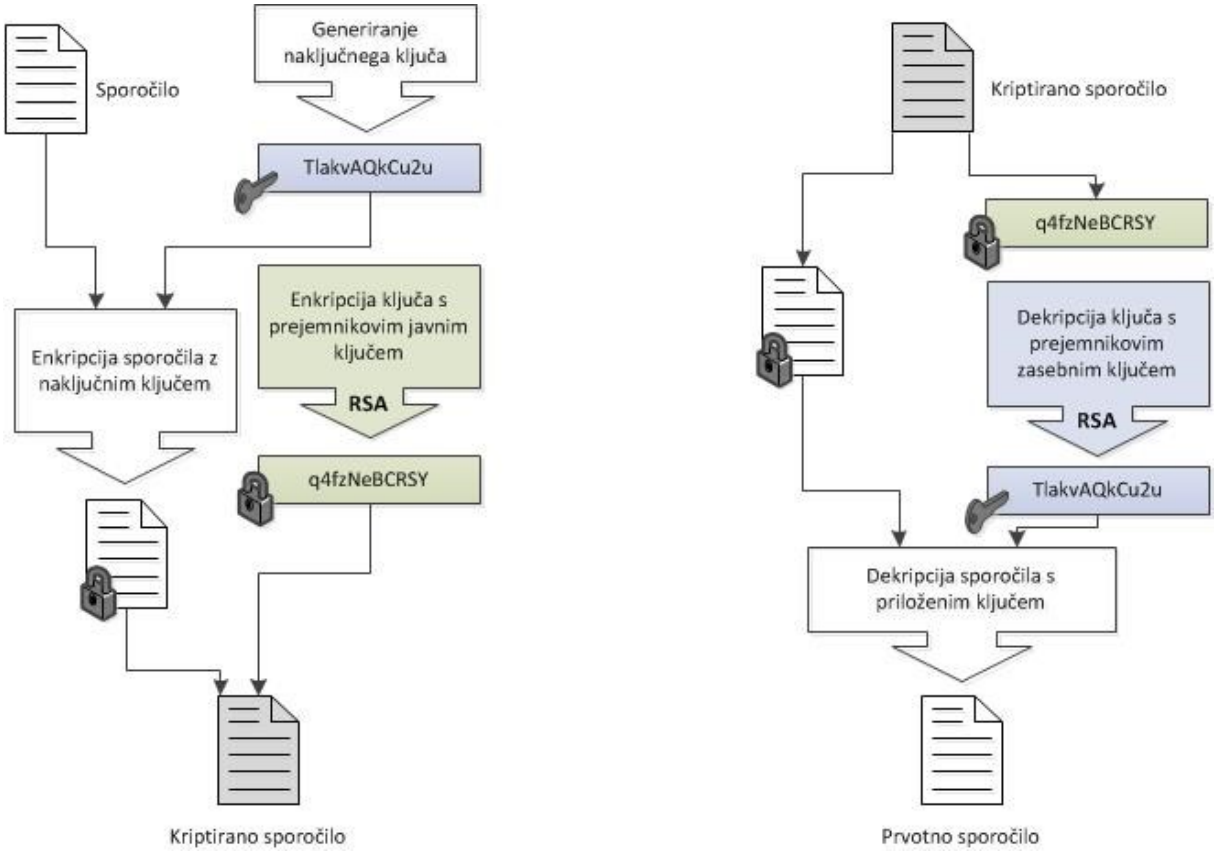
Hranjenje in prenašanje informacij o uporabniških računih kljub odprtim možnostim za napad na sistem DGC pogostokrat predstavlja večjo nevarnost za povprečen uporabnikov računalnik, saj je večina napadov usmerjenih ravno nanj. Najpogostejša primera sta:

- uporaba zlonamerne elektronske pošte, ki vsebuje škodljivo programsko opremo, katere namen je pridobitev zaupnih informacij žrtve ali pa v obliki trojanskega konja celo dovoljuje pridobitev dostopa do računalnika in omogoča tatvino osebnih podatkov. Večkrat pa je v sporočilu samo povezava do druge spletne strani, ki je v domeni napadalca. Neželeno elektronsko pošto običajno filtrirata že ponudnika elektronske pošte in spletnih storitev, vendar se lahko bolj sofisticirana in kompleksnejša sporočila kljub temu znajdejo v nabiralniku,
- ribarjenje na spletu, ki se odvija na dva načina: pri prvem prevarant s pomočjo elektronske pošte pošlje sporočilo, ki daje vtis, da prihaja z verodostojnega naslova in od prejemnika zahteva posredovanje zaupnih podatkov, druga oblika napada pa poteka preko spletnega mesta, do katerega povezava v prejetem sporočilu napoti prejemnika in je po uporabniškem vmesniku delno ali v celoti podobno uradni spletni strani. Namen takšnega napada je pridobivanje zasebnih podatkov, ki se uporabljajo ob prijavah. V določenih izjemah je že iz naslova URL jasno razvidno, da gre za prevaro, saj ta ne uporablja protokola SSL.

Ena izmed rešitev, ki jo ponujajo nekateri sistemi DGC, je uporaba varnostnih žetonov Cryptocard, pri katerih se za vsako prijavo generira drugačno geslo. Žetoni so lahko v obliki fizičnega avtentikatorja, ključa USB, pametne kartice ali pa namenske programske opreme, ki jo uporabnik namesti na osebni računalnik oziroma mobilno napravo.

Na podlagi uporabnikove PIN-kode se generira enkratno varnostno geslo, ki ga uporabnik vnese skupaj s svojim dostopnim geslom, nekatere rešitve pa dodatno omogočajo tudi ponastavljanje vrednosti PIN-kode [42].

Za efektivnejšo metodo se je izkazal standard OpenPGP, ki se je razvil iz leta 1991 nastalega programa PGP [43]. Enkripcija je kombinacija zgoščevanja, kompresije podatkov in tako simetrične kot tudi asimetrične kriptografije. Sporočila se kriptirajo z generiranim ključem (Slika 6), ki se ga nato, z uporabo algoritma RSA in prejemnikovega javnega ključa, kriptiranega pošlje skupaj s skritim sporočilom.



Slika 6: Prikaz postopka enkripcije in dekripcije z metodo PGP (Povzeto po [44]).

Posamezen javni ključ je podobno kot pri infrastrukturi PKI povezan z določenim uporabniškim imenom ali naslovom elektronske pošte, vendar za razliko od centraliziranega sistema, kjer avtentikacijo zagotavlja certifikatna agencija, ta model uporablja tako imenovano mrežo zaupanja, ki jo sestavljajo vsi uporabniki.

c) Tveganja pri izmenjavi

Ker se tečaji zamenjave med valutami lahko spreminjajo in si torej vse valute med seboj po vrednosti niso enake, se posledično razlikujejo tudi vrednosti valut DGC v odvisnosti do nacionalne valute. Uporabnik iz ene države lahko pri izmenjavi fiksne količine zlata in s tem valute DGC za realno valuto prejme določen znesek, ki pri drugem uporabniku za isto količino zlata najverjetneje znaša bistveno manj ali pa več. Tveganja pri izmenjavi so podobna tistim, na katere imetnik računa naleti v primeru, da si lasti depozit v tuji valuti. Poleg tega se s časom in tržnimi razmerami spreminja tudi kupna moč dragih kovin, ki med inflacijo praviloma znaša več, takrat je mogoče kupiti več dobrin in storitev.

V naslednjem poglavju bomo primerjali dve valuti DGC, ki sta svoj čas veljali za bolj razširjeni, vendar se je po propadu na trg znova postavila le prva.

3.1.2 Primerjava valut e-gold in Liberty Reserve

K snovanju nove digitalne valute in s tem podjetja e-gold Ltd., ustanovljenega leta 1996, je pripomoglo prepričanje enega od ustanoviteljev, da je zlato superiorno navadnemu papirnatemu denarju. Posebnost podjetja in relativno visoko zaupanje v storitev je bilo razvidno že leta 2002, ko je uporabniška skupnost presegala milijon uporabniških računov [45]. S tem se je pokazalo, da alternativni finančni sistemi, kljub neodvisnem delovanju od običajnih bančnih sistemov lahko delujejo, saj so jih številni uporabniki pripravljeni uporabljati.

Storitev e-gold je bila prvi uspešni spletni plačilni sistem, ki je izoblikoval številne tehnike spletnega trgovanja z vpeljavo izvajanja plačil preko kriptiranih povezav SSL, in prvi ponudnik tega tipa, ki je izdal lasten aplikacijski programski vmesnik (v nadaljevanju vmesnik API), s katerim so druge spletne trgovine lahko postavljale svoje storitve, ki uporabljajo transakcijski sistem e-gold. Za enega redkih uspešnih primerov se je izkazal sistem plačevanja z mikrotransakcijami v vrednosti ene desettisočinke grama zlata, saj so transakcije v vrednosti pod 1 dolarjem v realnosti predvsem zaradi višine nastalih stroškov večinoma nepraktične.

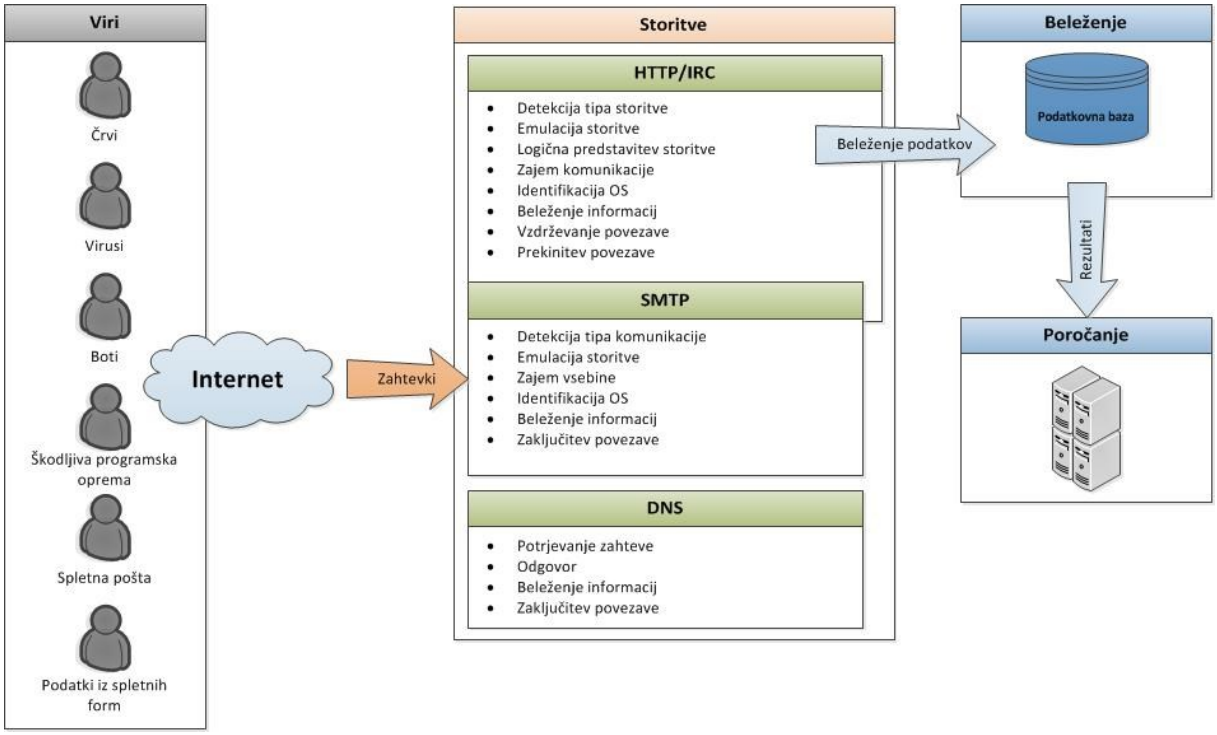
V propad podjetja so vodile kriminalne aktivnosti in spletni napadi na uporabniške račune, ki so izkoriščali varnostne luknje v operacijskem sistemu in spletnih brskalnikih. Napad z ribarjenjem na spletu, ki se je odvil leta 2001 in je ciljal uporabnike storitve e-gold, pa je bil prvi te vrste, usmerjen na finančno institucijo. Zaradi hitrosti izvajanja transakcij so valute DGC večkrat pritegnile čedalje bolj razširjena kriminalna združenja, ki so sisteme z nizkimi stroški takojšnjega obračuna sredstev lahko izkoriščala za pranje denarja [46].

Podjetje je bilo poleg preiskav kaznivih dejanj obtoženo opravljanja finančnih storitev brez licence in je z delovanjem prenehalo leta 2009, vlada ZDA je pri tem zasegla zlato v vrednosti 90 milijonov ameriških dolarjev. V sodelovanju z vodstvom podjetja se je po tem pričel postopek vračanja sredstev z računov kvalificiranim uporabnikom. Storitev e-gold je bila skupaj z dodanimi varnostnimi prijemi ponovno zagnana leta 2011.

Najboljša varnostna zaščita je ozaveščanje uporabnikov o potencialnih ranljivostih, zato je pred prijavno formo navedena povezava do daljšega seznama varnostnih priporočil, ki pomagajo zmanjšati verjetnost kraje osebnih podatkov in napada na račun. Na razpolago je namensko opcijsko orodje Account Sentinel, s katerim se lahko omejujejo možnosti povezave na spletno mesto. Če se naslov IP ne ujema, je uporabnik preko spletne pošte obveščen o morebitni spremembi in pri tem prejme enkratno PIN-kodo.

Podoben konec je dočakalo tudi podjetje Liberty Reserve, ustanovljeno na Kostariki, kjer je dejavnosti kot privatni sistem za izmenjavo valut pričelo z letom 2001. Za odprtje uporabniškega računa niso bila potrebna dokazila o istovetnosti, zadoščali so ime, rojstni datum in elektronski naslov. Na račun je bilo mogoče denar polagati z uporabo kreditnih kartic, z bančnimi nakazili in s poštnimi nakaznicami. Zaradi svoje anonimnosti je bila stran priljubljena točka za organiziran kriminal tako že od samega začetka [47]. Storitev je bila zaradi suma pranja denarja v preiskavo vključena od leta 2011, dve leti pozneje, maja 2013, pa je bila dejavnost ukinjena in domena zasežena. Na dan zaprtja je imelo podjetje registriranih več kot milijon uporabnikov, količina zlata v uporabi ni bila razkrita. Pred uradnim sporočilom javnosti je veljalo prepričanje, da je vzrok za nedostopnost strani napad DDoS, vendar se je dan zatem izkazalo, da je bilo izvajanje storitve preusmerjeno na strežnike fundacije Shadowserver. Slednja namreč zbira in proučuje informacije o škodljivi programski opremi, elektronskih prevarah ter spletnih napadih (Slika 7).

Prijem je tedaj uporabljal dva ponora, na katera so strežniki DNS pod domeno Libertyreserve.com preusmerjali promet. Pojem »ponor« označuje cilj, kamor se preusmerja škodljiv spletni promet, kjer ga je zajetega nato mogoče proučevati in analizirati.



Slika 7: Postopek zajemanja prometa iz različnih virov, kot ga izvaja fundacija Shadowserver (Povzeto po [48]).

Uporaba ponorov se zato običajno namenja prevzemanju nadzora nad omrežji botnet oziroma zbirko računalnikov, povezanih z internetom, ki določeno nalogo izvajajo porazdeljeno. Botnet je sistem, ki se uporablja za nelegalne namene in sestoji iz računalnikov, ki so največkrat asimilirani brez uporabnikovega vedenja, saj se nameščena škodljiva programska oprema izvaja v ozadju. S takšnimi omrežji se lahko izvaja tudi napade DDoS, v posamezno mrežo pa je v danes lahko povezanih več deset tisoč računalnikov.

3.2 NAVADNE DIGITALNE VALUTE

Tako kot valute DGC so tudi navadne digitalne valute praviloma centralizirane in za razliko od kriptovalut med postopkom kreiranja in upravljanja ne uporabljajo kriptografije, kar sicer ne pomeni, da enkripcijskih tehnik ne podpirajo nikjer. Med seboj se razlikujejo v načinu in obsegu implementacije kriptografije. Nekatere digitalne valute se označujejo tudi kot kriptovalute, čeprav s tehničnega vidika temu nazivu ne ustrezajo.

3.2.1 Prednosti in slabosti digitalnih valut

Ob primerjavi realnih in digitalnih valut se hitro pokaže, da med razlike ne spada zgolj dejstvo, da gre pri zadnjih za digitalno predstavitev, temveč tudi vse bolj raznolike pristope funkcionalnosti in načina uporabe. Pomembni vprašanji, ki nastajata ob distribuiranju in uporabi posamezne digitalne valute, sta tudi največkrat spregledani:

a) S čim je izražena vrednost digitalne valute?

Večina današnjih digitalnih valut kot kritje uporablja realne valute, s katerimi si pravzaprav deli vsaj eno izmed pomembnejših skupnih lastnosti, in sicer dejstvo, da kot plačilno sredstvo samo po sebi nima nobene višje vrednosti [49, 50]. Sodobne svetovne valute se od leta 1971 dalje, ko je bila neposredna konvertibilnost v zlato ukinjena, označujejo kot valute fiat, za katere je značilno, da:

- jih vlada priznava kot zakonito plačilno sredstvo,
- njihova vrednost ne izhaja iz nobenega izbranega standarda,
- njihova nominalna vrednost presega vrednost materiala posamezne enote.

Pristop, ki se pri distribuiranju digitalne valute v obtok, vsaj v začetni fazi pridobivanja uporabniške skupnosti, pogostokrat uporablja, je razdeljevanje določene količine valute med vse registrirane uporabnike. Denar v splošnem predstavlja medij, ki hrani določeno vrednost. Ta izhaja iz človeškega napora, zato je zanj potrebno delati. Pri tem se poraja dvom, zakaj bi nekdo, ki je sicer pripravljen uporabljati posamezno digitalno valuto, prodajal fizične dobrine ali storitve vsem tistim, ki so jo na začetku pridobili brezplačno. Trenutne kriptovalute to vprašanje zaenkrat rešujejo s postopkom rudarjenja (ang. mining), kar pravzaprav pomeni, da so za distribuiranje potrebni čas, elektrika in strojna oprema, ki v tem primeru predstavljajo delo.

b) Ali je ponudnik digitalne valute pristen?

Novi ponudniki digitalnih valut in z njimi povezanih storitev na trgu nastajajo iz leta v leto, vendar so za vsaj deloma delujoč produkt potrebna leta razvoja in dopolnjevanja, pri čemer se rezultati največkrat pokažejo šele po 3 letih ali več. Pri tem se vedno pojavlja skrb o pristnosti ponudnika, saj obstaja realna možnost, da gre pri določenih digitalnih valutah za sheme HYIP, ki so sicer pogostejše pri ponudnikih valut DGC, ali pa dolgoročne naložbe investitorjev.

Valuto, kakršna je Ripple (XRP), bremenijo obtožbe o načinu distribuiranja, saj je od skupno 100 milijard enot XRP, ki so bile predhodno ustvarjene, javnosti namenjena polovica, medtem ko si 20 milijard enot XRP lastijo ustanovitelji, 30 milijard pa razvijalci podjetja Ripple Labs (prej imenovan OpenCoin). Do maja leta 2013 je po ocenah v obtoku zgolj 500 milijonov enot XRP, medtem ko kriterij, po katerem distribuiranje poteka, še ni znan [51].

3.2.2 Valuta Ripple

Pojem poleg valute označuje tudi protokol za monetarni oziroma plačilni sistem, znotraj katerega lahko uporabniki pošiljajo, prejemajo in plačujejo z digitalnimi ter realnimi valutami. Podjetje Ripple Labs, ki je nudenje storitve pričelo z letom 2012, potem ko je prvotna implementacija nastala že leta 2004, se z nadaljnjim razvojem nagiba k postopnemu preoblikovanju omrežja v decentralizirano [52], tipa P2P, kjer transakcije XRP procesirajo vsi računalniki s protokolom Ripple.

Današnji običajni plačilni sistem je infrastruktura, katere namen je prenos denarne vrednosti z ene strani na drugo, s čimer se obojestransko razrešijo vsakršne obveznosti. Sistem povezuje bančne račune in zagotavlja denarno izmenjavo z uporabo bančnih depozitov. Ker depoziti na bankah pravzaprav predstavljajo dolg do komitentov, se pri tem zahteva velika mera zaupanja v takšno institucijo.

Podobno zasnovo je povzel Ripple, saj kot plačilni sistem deluje predvsem na principu dolga, kjer so uporabniki med seboj dolžniki z nazivom IOU (ang. I Owe You), s transakcijami pa se med plačnikom in prejemnikom prenašajo razmerja vrste dolgov, zato delovanje temelji na verigi zaupanja. Interna valuta XRP, ki se uporablja za registracijo uporabniškega računa oziroma digitalne denarnice (ang. Ripple Wallet) in plačevanje taks pri izvajanju transakcij, hkrati izključuje potrebo po uporabi neodvisnih menjalnic. Naslov, seznam zaupanja, ponudbe zamenjave, stanje na računu in pretekle transakcije vsakega uporabnika se hranijo v distribuirani podatkovni bazi, digitalni ustreznici glavne knjige (ang. Ledger). Porazdeljeno potrjevanje veljavnosti transakcij, kar predstavlja pogoj pri hitrosti njihovega izvrševanja, se dosega s konsenzom ali skupnim soglasjem, ki se praviloma izvaja do vsakih 5 sekund [53].

S posodabljanjem podatkovne baze nastaja veriga zapisov, zato je vsaka novonastala sprememba podatkovne baze, označena s sekvenčno vrednostjo, povezana s prejšnjimi stanji.

Kljub relativno hitrim spremembam razvoja storitve Ripple v vnaprej predvideno smer pa se še vedno razvijata oba vidika:

a) Plačilni sistem Ripple

Veriga zaupanja je za vsakega novega uporabnika sprva zahtevala predhodno število poznanstev, kar je pomenilo, da je vsakdo moral imeti vsaj enega znanca, ki je storitev že uporabljal. Pogoj je bil z novejšo različico odstranjen, zaradi česar je pošiljanje denarnih sredstev mogoče že z zamenjavo v interno valuto XRP.

Zamenjava realne ali druge digitalne valute v interno, depoziti, prenosi in dvigi se izvajajo z uporabo prehodov (ang. Gateways). V praksi lahko vlogo prehoda prevzame vsaka oseba ali organizacija, ki uporabnikom nudi možnost prenosa denarnih sredstev v omrežje in izven omrežja Ripple. V tem pogledu je delovanje prehoda podobno delovanju finančnih posrednikov, le da vsi uporabljajo distribuirano podatkovno bazo [54]. Prehodov je več, nekateri podpirajo tudi menjave med valutami, uporabnik jih sam izbere poljubno mnogo, pri čemer naj bi najbolj zaupanja vredni bili tisti, ki so del združenja IRBA [55]. Na ta način se hkrati razrešuje problem zaupanja, saj za prenos denarnih sredstev skozi omrežje uporabnik ne potrebuje večjega števila poznanstev. Pri tem ostaja vprašanje, ali lahko vsi prehodi zares opravljajo svojo funkcionalnost brez možnosti neizplačevanja posojil, saj mehanizma, ki bi to preprečeval, sistem še nima.

b) Digitalna valuta Ripple

Ker je Ripple v prvi vrsti plačilni sistem, je glavni namen interne valute XRP zagotavljanje varnosti. Zato je razpolaganje z začetno vsoto valute XRP pogoj za aktivacijo digitalne denarnice, do katere uporabnik dostopa z uporabo spletnega brskalnika, prav tako pa se s plačevanjem taks izvajanja transakcij zmanjšuje tveganje, da bi se omrežje preplavilo z večjim številom zahtevkov. Vsaka transakcija se lahko hrani ali v binarnem formatu ali pa v formatu JSON, ki določa obliko izmenjave podatkov med strežnikom in spletno aplikacijo. Binarni format se uporablja za zgoščevanje, digitalno podpisovanje in potrjevanje posamezne transakcije, medtem ko se format JSON uporablja predvsem pri prikazovanju vsebine v berljivi obliki (Slika 8) ter posredovanju.


```
{"Account":"r9p4kJL6LRvBEbUrL7yM9XyZ22VzM7FLhs","Fee":"10","Flags":0,"OfferSequence":89425,"Sequence":89446,"SigningPubKey":"03C92B297236AFB9DB2DDA37B5CD0E0FF213C7073DD99F05551DC02EDC1957BB3B","TransactionType":"OfferCancel","TxnSignature":"3046022100C5795CE17438EAB4880F6D878B701106753699ACA5DB8375B6B8FBDDB387FBD2022100C131711E024F63FA9DE42BD8495081E687121F59F42E43904F0610F21300ECA2","date":436369230,"hash":"5739A20AF3F94FC357E84F1BA55F3E071042BA0B07B821EA291D27965C337CA1"}
```


Slika 8: Zapis transakcije Ripple v formatu JSON (Povzeto po [56]).

V splošnem se tudi formati transakcij med seboj razlikujejo, saj ni nujno, da so hkrati določeni vsi atributi. Seznam na strani za razvijalce jih namreč določa 9 (Tabela 2).

Naziv atributa	Tip	Vključevanje	Krajši opis
Account	Account	Obvezno	Račun, ki izvaja transakcijo
Fee	Amount	Obvezno	Vrednost takse transakcije
Flags	UInt32	Opcijsko	Določa dodatne opcije transakcije
Sequence	UInt32	Obvezno	Sekvenčna vrednost transakcije
PreviousTxnID	Hash256	Opcijsko	ID predhodne transakcije (še ni implementirano)
SigningPubKey	Public Key	Obvezno	Javni ključ, uporabljen pri digitalnem podpisu transakcije
SourceTag	UInt32	Opcijsko	Omogoča identifikacijo transakcije
TransactionType	UInt16	Obvezno	Določa tip transakcije
TxnSignature	VariableLength	Opcijsko	Digitalni podpis transakcije

Tabela 2: Atributi osnovnega formata transakcije Ripple (Povzeto po [57]).

S tega vidika je valuta XRP v veliki meri zanesljiva in je, po zagotovilih podjetja, varna pred inflacijo, saj skupno število ustvarjenih enot ne bo nikoli preseglo 100 milijard. Vsak uporabnik lahko torej valuto XRP kupi pri kateri od neodvisnih prehodov s seznama, kakršnega upravlja združenje IRBA, ali pa jo pridobi brezplačno med distribuiranjem, ki je del katere od promocij [58]. Vendar je dolgoročni učinek ravno nasproten, saj je deflacijska narava valute posledica uničevanja enot XRP znotraj omrežja potem, ko se transakcija zaključi. Število uničenih enot XRP ustreza številu enot, ki so bile vplačane v sklopu posamezne takse [59]. Kljub relativno majhni vrednosti taks je torej del količine valute v obtoku časovno omejen in bi se brez posegov po več letih uporabe popolnoma izrabil.

3.3 KRIPTOVALUTE

Kot kriptovaluta se določa vsaka digitalna valuta, ki je decentralizirana in katere implementacija za potrjevanje transakcij uporablja kriptografijo, kar posledično prinaša tudi relativno visoko stopnjo varnosti [60]. Uporabo kriptovalut se zato največkrat primerja s protikulturnim gibanjem, kjer je upravljanje valute prestavljeno iz institucij k posameznikom. Za prvo povsem funkcionalno in široko razširjeno kriptovaluto velja Bitcoin, vendar pa sama ideja o takšni obliki digitalne valute obstaja že vsaj od leta 1990 dalje [61].

3.3.1 Nastanek prve kriptovalute

Sistem Bitcoin, ki je bil vzpostavljen z letom 2009, je kot novo digitalno valuto opisoval leto prej izdan dokument *The Cryptography Mailing List* [62] z definicijami pomembnih lastnosti sistema:

- za delovanje niso potrebni posredniki, ki zahtevajo zaupanje ali izvajajo distribuiranje,
- udeleženci so lahko anonimni,
- nove enote kriptovalute Bitcoin (BTC) se kreirajo in verificirajo z uporabo sistema POW,
- sistem POW poleg kreiranja razrešuje tudi problem dvojnega plačevanja (ang. double spending) znotraj omrežja P2P.

Kdo natanko je ustanovitelj Bitcoina, ni dokončno znano, saj se je javnosti predstavljal le s psevdonimom »Satoshi Nakamoto« [63].

Številni mehanizmi, ki jih je pozneje implementiral Bitcoin, so prej opisovali nekateri predlogi, v posameznih primerih pa so bili tudi delno ali povsem realizirani. David Chaum, ustanovitelj podjetja DigiCash, ki je leta 1993 postavilo lasten elektronski denarni sistem ecash, je problem dvojnega plačevanja predstavil že zelo zgodaj in je pri tem razvil protokol, s katerim je ranljivost mogoče zaznati in preprečiti. Digitalne valute so v osnovi namreč dovzetne za različna podvajanja, saj je posamezno enoto mogoče poljubno razmnoževati in tako z njo za isto dobrino plačati večkrat. V ta namen se je posebej izvajal nadzor nad transakcijami, ki pa je bil, za razliko od Bitcoinove distribuirane digitalne glavne knjige, povsem centraliziran [64].

Drugi pomembnejši protokol, ki ga Bitcoin prav tako uporablja, je bil v sklopu osnutka o njegovem predhodniku B-money izdan leta 1998 in je predvideval sistem POW. Leta 1997 je bila namreč predlagana osnovna izvedba, in sicer kot simetrična funkcija hashcash, ki jo kot metodo za omejevanje neželene elektronske pošte ter napadov DDoS implementirajo ponudniki elektronske pošte in številni filtrirni sistemi, medtem ko svojo izpeljanko Bitcoin uporablja pri postopku rudarjenja za potrjevanje kreiranih enot BTC [65].

3.3.2 Vzpon sorodnih sistemov

Letu 2009 je sledil prihod množice alternativ, ki sta jim v veliki meri skupni arhitektura omrežja P2P in distribuiranje denarnih enot s pomočjo rudarjenja. Predvsem ta dejavnost zaradi relativno nizke stopnje zahtevnosti omogoča, da se lahko na začetku izoblikuje osnovna uporabniška skupnost. Istočasno pa številni primeri [66] kažejo tudi, da vsaka predstavljena kriptovaluta ni nujno pristna niti se na trgu ne bo obdržala dlje časa.

Med večje kriptovalute poleg omenjene trenutno sodijo Namecoin, Litecoin, Dogecoin in Peercoin (v nadaljevanju PPCoin) [67]. Razlik med njimi je več (Tabela 3), kažejo pa se že pri implementaciji zgoščevalnih funkcij, kjer poleg kvadratne funkcije hashcash-SHA256 (v nadaljevanju funkcija SHA256d) najdemo še funkcijo scrypt. Slednja je namenjena izračunavanju zgoščenih zapisov [68], ki se v sklopu sistema POW uporabljajo pri preverjanju iskane rešitve, s katero se kreirajo nove enote.

Kriptovaluta	**Končno število enot v obtoku** (v milijonih)	**Generiranje novega bloka** (vsakih *n* minut)	**Višanje zahtevnosti iskanja rešitve** (vsakih *n* blokov)	**Zgoščevalna funkcija**	**Leto vzpostavitve sistema**
Bitcoin	21	10	2016	SHA256d	Januar, 2009
Namecoin	21	10	2016	SHA256d	April, 2011
Litecoin	84	2,5	2016	scrypt	Oktober, 2011
Dogecoin	99 000+	1	240	scrypt	December, 2013
PPCoin	neznano	10	1	SHA-256	Avgust, 2012

Tabela 3: Pregled ključnih razlik med večjimi kriptovalutami (Povzeto po [69]).

S tehničnega vidika sta si s seznama najbolj podobni prvi kriptovaluti, vendar gre sistem Namecoin še dlje. V tej fazi poleg vloge sistema za plačevanje zavzema tudi funkcionalnost decentraliziranega sistema DNS, za katerega se arhitektura omrežja P2P uporablja tudi kot osnova. Na ta način je mogoče neodvisno od posrednikov za nakup vrhnjih internetnih domen TLD (ang. Top-Level Domain), kakršna je ICANN, te kupiti in urejati posamezno za bistveno manjše plačilo [70].

3.3.3 Distribuiranje denarnih enot

Postopek rudarjenja, pri katerem se kreirajo nove enote kriptovalute, je v osnovi matematični problem vnaprej znane težavnosti, za katerega namenski program, nameščen na računalniku uporabnika, išče zadostno rešitev. Težavnost se sproti avtomatično regulira, tako da je število globalnih rešitev ob nekem času konstantno.

Najdena rešitev se znotraj omrežja verificira z zadostnim številom potrditev (ang. Confirmations) in skupaj z drugimi informacijami (Tabela 4) zapakira ter shrani v zapis, imenovan »blok«.

Polje	Velikost	Krajši opis
Magic no	4 biti	Magično število oziroma fiksna vrednost 0xD9B4BEF9
Blocksize	4 biti	Število bitov v bloku
Blockheader	80 bitov	Glavo bloka sestavlja 6 elementov
Transaction counter	Od 1 do 9 bitov	Pozitivno število spremenljivke
Transactions	<Transaction counter> - Transactions	Seznam transakcij

Tabela 4: Struktura bloka kriptovalute Bitcoin (Povzeto po [71]).

Vsak blok predstavlja transakcije, ki so se izvedle nazadnje in še niso bile shranjene v katerem od prejšnjih blokov, s čimer se hrani stanje, kakršno je bilo, tik preden je bil generiran, in skupaj z drugimi sestavlja verigo blokov vse do izvornega (ang. Genesis block).

Vsi uporabniki, ki izvajajo rudarjenje, prejmejo za novo generirani blok delež nagrade, kar dejansko predstavlja nove enote posamezne kriptovalute. Sprva je število kreiranih enot kriptovalut Bitcoin (BTC), Namecoin (NMC) in Litecoin (LTC) na blok v celotnem omrežju znašalo 50, vendar se ta vrednost približno vsake 4 leta razpolovi [72, 73]. Kriptovaluta Dogecoin (Doge) za nagrajevanje uporablja vnaprej fiksirano stopnjo, ki se vsakič določi za nadaljnjih 100 000 blokov, medtem ko PPCoin (PPC) poleg sistema POW podpira še koncept POS (ang. Proof-Of-Stake), s katerim se določa odstotek nagrade [74].

Posamezni enoti BTC in NMC sta deljivi vse do 8 decimalnih mest, kar je tudi najmanjša vrednost, ki jo trenutno podpirajo transakcije, čeprav je protokol zasnovan tako, da lahko po potrebi v prihodnosti podpira še manjše denominacije. Ker novi bloki nastajajo tudi ob trgovanju, pomeni, da bodo generirani še potem, ko novih enot ne bo mogoče več kreirati oziroma bo dosežena zgornja meja.

Postopek rudarjenja je bil na samem začetku relativno nezahteven in tudi donosen, predvsem zato ker je bilo uporabnikov malo, zastavljen problem pa je lahko reševal vsakdo z lastnim računalnikom, saj so procesorske zmogljivosti tedaj temu še zadoščale. Kljub dejstvu, da so praktično vsi sodobni centralni procesorji (CPU) večjedrni in večnitni, pa so se z naraščanjem težavnosti s stališča porabe časa in energije izkazali za neučinkovite. Pričele so jih zamenjevati grafične kartice (GPU), saj so zaradi arhitekture, ki omogoča paralelno izvajanje večjega števila ukazov, zmožne v enakem obdobju sočasno izvesti večje količine matematičnih operacij. Spodnji primer (Tabela 5) prikazuje zmogljivost strojne opreme pri generiranju zgoščenih zapisov v milijonih na sekundo.

Strojna oprema	Proizvajalec	Model	Št. jeder/niti	Poraba (Watt)	Frekvenca jedra	mHash/s
CPU	Intel	Core i7-3930k	6/12	190	4.625 GHz	66.6
CPU/APU[3]	AMD	A8.3850	4	100	2.9 GHz	60
		HD 6550D (integrirana)	400 SP[4]		600 MHz	60
GPU	Nvidia	Asus GTX 680 2GB	1536 CUDA cores	221	1280 MHz	127.3
GPU	AMD	Radeon HD 7970 3GB	2048 SP	214	1290 MHz	825
ASIC	Bitminer	Avalon Clone	320 ASIC	650	282 MHz	85000

Tabela 5: Primerjava zmogljivosti strojne opreme pri rudarjenju enot BTC (Povzeto po [75]).

Pri tem višje število grafičnih jeder ne nujno ustreza višji zmogljivosti, saj je ta odvisna predvsem od zasnove arhitekture, ki se kaže v tem, da so trenutne grafične kartice podjetja Nvidia s platformo CUDA primernejše za splošnonamensko programiranje in znanstvene aplikacije, medtem ko se grafične kartice podjetja ATI veliko bolje izkažejo v kriptografiji.

Kljub temu se pri rudarjenju izbira ne omejuje samo na strojno opremo masovne proizvodnje, temveč tudi posebne naprave, ki so namenjene zgolj določeni nalogi. Pri tem se največkrat uporabljajo:

- moduli FPGA, ki so po zmogljivosti v rudarjenju primerljivi z grafičnimi karticami,
- integrirana vezja ASIC v obliki čipov SoC (ang. System-on-Chip). Za razliko od modulov FPGA so vezja ASIC že spočetka prilagojena vrsti uporabe in zato tudi cenovno predstavljajo višji strošek. Naprave, namenjene rudarjenju, običajno vsebujejo vsaj nekaj deset čipov ASIC, v zgornji tabeli naveden Bitminer Avalon Clone jih vsebuje 320, kjer je vsak posamezen v teoriji zmožen generirati 280 milijonov zgoščenih zapisov na sekundo.

Današnja težavnostna stopnja rudarjenja pri kriptovalutah, kakršna je Bitcoin, ne dopušča veliko možnosti, da bi postopek lahko izvajali neodvisno, zato se uporabniki povezujejo v posebne skupine (ang. pools), kjer pri generiranju blokov sodelujejo tako, da prispevajo računsko moč lastne strojne opreme in si posledično, glede na delež prispevka strojnih zmogljivosti, nagrado tudi razdelijo [76].

[3] APU (Accelerated Processing Unit) so centralni procesorji z dodatno funkcionalnostjo, ki razširja osnovne računske zmogljivosti, največkrat v obliki integrirane GPU na istem čipu.
[4] SP (Stream Processors) ter CUDA (Compute Unified Device Architecture) sta izraza podjetij AMD in Nvidia, s katerima se označujejo jedra grafičnih kartic, ki se po arhitekturi razlikujejo od običajnih procesorskih.

Večjo priložnost tako prinašajo določene kriptovalute, kot sta Namecoin in Litecoin, saj zaradi manj razširjene podpore namenskim vezjem ter možnosti vzporednega izvajanja postopka rudarjenja z Bitcoinom dajejo možnost tudi uporabnikom brez zahtevnejše strojne opreme [77]. To je posledica izbire zgoščevalnih funkcij, kjer je SHA256d bistveno primernejša za višjo stopnjo paralelnosti, medtem ko funkcija scrypt izrablja večje količine procesorskega pomnilnika, zato se običajno ne izvaja v več instancah. Hkrati pa ta vidik ponovno postavlja vprašanje o smiselnosti produkcije in uporabe večjega števila integriranih vezij ASIC, saj je tedaj postopek izdelave dražji od primerljivih aritmetično logičnih enot, ki jih za operacije s celimi števili uporabljajo centralni procesorji [78].

3.3.4 Namen sistema POW

Ker je veljavnost generiranega bloka pogojena z zgoščeno vrednostjo vhodnega podatka, ki mora biti manjši ali enak podanemu cilju oziroma 256-bitni vrednosti [79, 80], je bila za to potrebna posebna funkcija, ki bi bila hkrati učinkovito preverljiva in simetrična. Funkcija SHA256d, ki jo uporabljata Bitcoin in Namecoin, je zahtevnejša izvedba podobne funkcije SHA1 in tako kot scrypt tudi ta istočasno rešuje problem izračuna dveh enakih rešitev. Za podano 256-bitno vrednost, ki si jo omrežje deli pri postopku rudarjenja, je pomembno zagotoviti različne začetne točke, saj bi v nasprotnem primeru več različnih rešitev pomenilo sprejetje prve in zavrnitev vseh ostalih kljub enaki količini dela.

Operacijo zgoščevanja v splošnem ponazarja zapis H(s, x, c), kjer je spremenljivka s vhodni podatek oziroma niz, c pa števec, ki se iterativno povečuje. Vsakemu uporabniku oziroma skupini je tako za reševanje dodeljena naključna začetna točka (spremenljivka x), podana na osnovi enkratnega naslova in za katero je obenem statistično neizvedljivo, da bi si delila katerakoli dva uporabnika.

Doseganje zastavljenega časovnega intervala, ob katerem se generirajo novi bloki, prinaša sprememba v osnovni formuli [81], po kateri stopnjo težavnosti označuje število s plavajočo vejico (spremenljivka k) in ne več celo število. Zato je podani cilj (niz dolžine n) zapisan kot težavnost $2^{(n-k)}$, delo pa primerjava izračunane zgoščene vrednosti ob vsaki iteraciji s ciljem, definiranim kot

$$\boldsymbol{H(s,x,c) < 2^{(n-k)}} \tag{3.1}$$

Uporaba sistema POW poleg tega razrešuje še problem dvojnega plačevanja. Ker gre za omrežje arhitekture P2P, se informacije o vsaki transakciji posredujejo vsem ali vsaj zadostnemu številu vozlišč, zaradi česar se vsakokrat povečana veriga blokov oziroma del nje vzdržuje globalno. Pri tem veljavnost transakcije, ki naj se doda v verigo, zahteva vključen blok, ki je bil dejansko generiran med postopkom rudarjenja in vključuje sistem POW. Vezava blokov v verigo onemogoča poljubne spremembe, zato se v takšnem primeru vsi nadaljnji bloki razveljavijo in znova izračunajo [82]. Kompleksnost oziroma dolžina verige obenem preprečuje sprejetje vzporednih vej, ki nastanejo, kadar se istočasno pojavita dve veljavni različici, saj se vedno sprejme samo tista, ki je najdaljša.

4 IMPLEMENTACIJA PLAČEVANJA S KRIPTOVALUTO BITCOIN

V nadaljevanju so navedeni nekateri vidiki uporabe kriptovalute v praksi, predvsem s stališča procesiranja plačil pri kupovanju digitalne vsebine. Implementacija omogoča realizacijo dveh rešitev, kar je pravzaprav rezultat izbire med stopnjama avtomatizacije procesiranja nakupov in plačil.

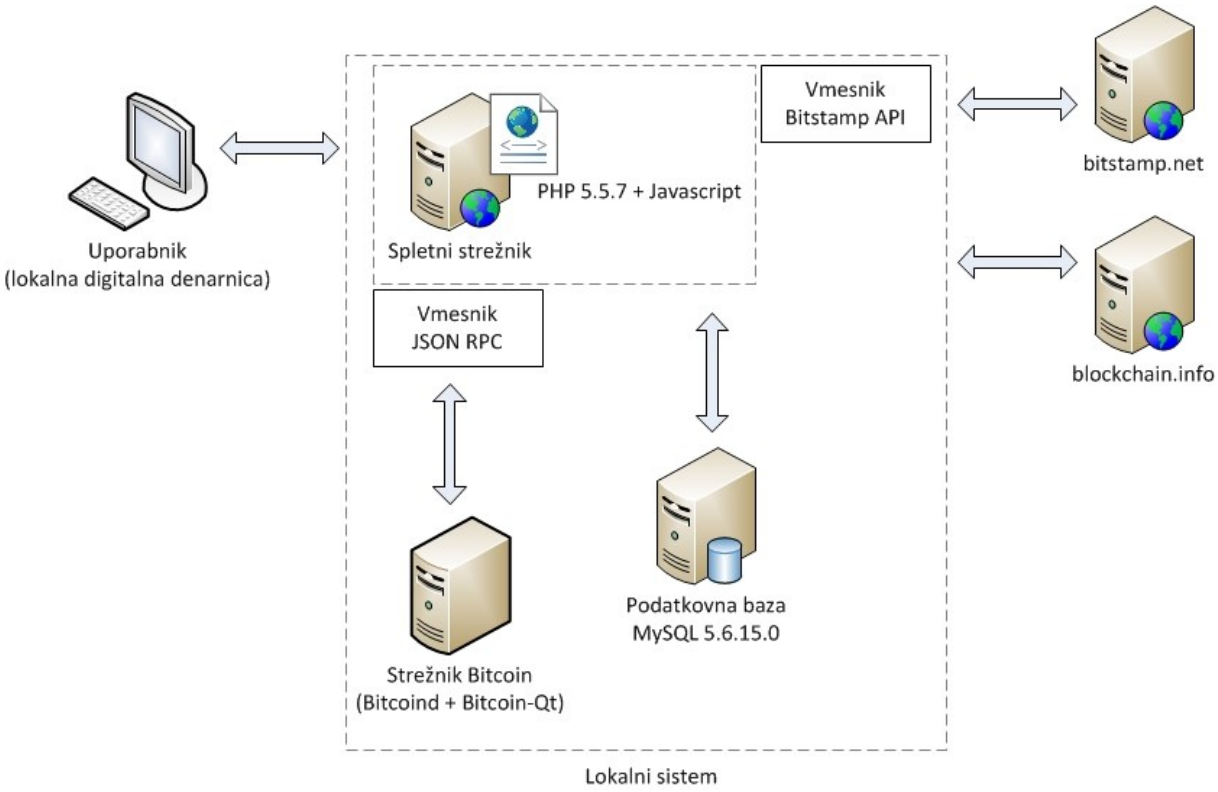
4.1 NAČINI PLAČEVANJA

Za prikaz delovanja nakupa digitalne vsebine je bila postavljena osnovna spletna trgovina, ki obiskovalcem nudi možnost nakupa digitalnih slik s kriptovaluto Bitcoin, pri čemer nakup lahko opravijo samostojno ali pa se z registracijo odločijo za samodejno izvedbo nakupa.
Pristop, opisan v tem poglavju, uporablja lasten sistem za generiranje naslovov za plačevanje in informacije javno dostopne podatkovne baze preteklih transakcij ponudnika Blockchain [83]. Pri programiranju storitve je bil izbran programski jezik PHP, s katerim je realiziran večji del spletne trgovine, posredovanje informacij med stranmi (POST) in zunanje poizvedbe pa opravlja jezik JavaScript.

4.1.1 Samostojna izvedba

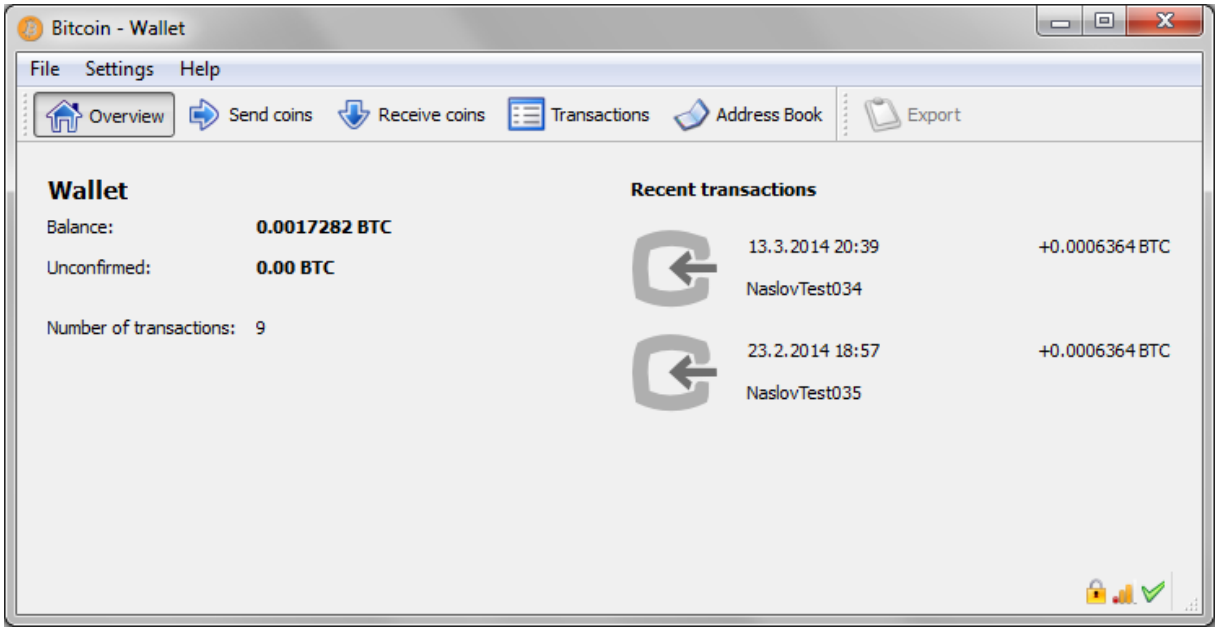
Sistem z neodvisno rešitvijo za procesiranje nakupov v vsakem primeru zahteva postavitev lastnega strežnika, ki za prejeta naročila sam generira ciljne naslove in po potrebi opravlja verifikacije. Privzeto je z začetnim zasebnim ključem vnaprej generiranih 100 nerabljenih naslovov, ki se vračajo ob klicih pred nakupom, zato je ob doseženi meji potrebno izračunati nov ključ, s katerim se generira novih 100 razpoložljivih naslovov za plačila. Odjemalec in hkrati digitalna denarnica Bitcoin-Qt, ki se uporablja v strežniške namene, ta korak izpolni samodejno, vendar je pri tem potrebno geslo, s katerim je digitalna denarnica kriptirana.

Trenutna arhitektura predstavlja postavitev sistema na isti platformi (Slika 9), zato se tudi izvajanje klicev RPC lahko izvaja lokalno, brez potrebe po dejanskem oddaljenem povezovanju.



Slika 9: Diagram z osnovnimi komponentami arhitekture realizirane rešitve.

Z uporabniškega vidika se nov in enkraten naslov za plačilo generira pred potrditvijo nakupa. Klici se izvajajo z uporabo vmesnika JSON RPC, s katerim se strežnik PHP lahko povezuje s strežnikom Bitcoin oziroma programom Bitcoin Daemon (ang. Bitcoind), odjemalcem brez programskega vmesnika, ki ga nekatere digitalne denarnice, v tem primeru tudi uporabljena Bitcoin-Qt (Slika 10), že privzeto podpirajo [84].



Slika 10: Vmesnik odjemalca oziroma digitalne denarnice Bitcoin-Qt.

Izbrani odjemalec je od verzije 0.5 dalje združen z odjemalcem Bitcoin Daemon. Ob namestitvi je pred uporabo potreben prenos celotne verige blokov velikost nad 12 GB, zaradi česar je praktična uporaba omogočena šele po več urah. Takrat dobi računalnik tudi funkcijo vozlišča omrežja Bitcoin, vendar za razliko od nekaterih odjemalcev, kakršen je MultiBit, ne podpira več denarnic znotraj enega vmesnika.

Tako imenovani »lahki« odjemalci, med katere štejemo MultiBit in Electrum, za delovanje ne potrebujejo celotne kopije verige blokov, saj informacijo o posamezni opravljeni transakciji v obliki glave bloka prejmejo od drugih strežnikov.

4.1.2 Vpeljava zunanjega plačilnega procesorja

Glavna prednost pri izbiri načina za avtomatizacijo plačila je preskok uporabe digitalne denarnice in ročnega kopiranja generiranega naslova v polje za plačilo znotraj lastnega odjemalca. Tak princip zahteva uporabo ustreznega vmesnika API, kakršnega med drugimi nudijo tudi ponudniki Coinbase, Blockchain in Bitstamp [85] za razvoj spletnih storitev, ki razširjajo seznam že podprtih ali pa se usmerjajo izključno na sprejemanje specifične valute.

Po neuspešnem poskusu povezave lastne storitve z vmesnikom API ponudnika Mt. Gox je bila implementirana alternativa. Izvajanje klicev tako opravlja razred *BitStampAPI* [86], znotraj katerega so definirane osnovne metode vmesnika API ponudnika Bitstamp. Za praktično delo se uporabljata predvsem funkciji *balance()* in *withdrawalBitcoin()*, s katerima strežnik PHP preverja uporabnikovo stanje in izvaja samodejni prenos sredstev BTC ob vplačilu.

Razred zahteva predhodno namestitev orodja in knjižnice cURL [87], ki v sklopu omenjenega razreda opravlja pošiljanje in prejemanje podatkov glede na podani naslov URL ter obenem podpira večje število internetnih protokolov. Za naš primer je pomemben predvsem protokol HTTPS, saj se poizvedbe opravljajo na strani, do katere poteka kriptirana povezava. To tudi pomeni, da se pri posebnih ukazih uporablja avtentikacija, zaradi česar je potrebna vključitev certifikatov, kot jih določa certifikatna agencija CAcert.org, do katerih pot navedemo v vrstici, preden podamo naslov URL:

```
curl_setopt ($curl, CURLOPT_CAINFO, "C:\cacert.pem");
```

Naslov strani in ustrezen ukaz, ki vrača rezultate poizvedb storitve Bitstamp, nato podamo s klicem funkcije:

```
curl_setopt($curl, CURLOPT_URL, 'https://www.bitstamp.net/api/'<ukaz>'/');
```

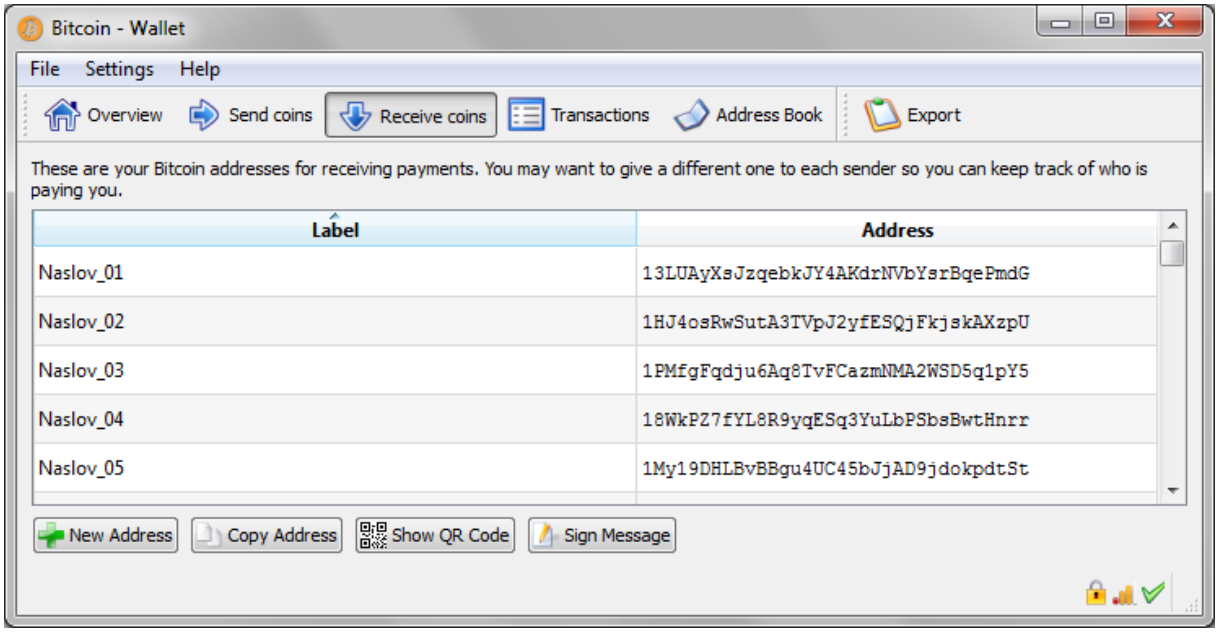
4.2 KONFIGURACIJA STREŽNIKA BITCOIN

Algoritem ECDSA (ang. Elliptic Curve Digital Signature Algorithm), ki ga Bitcoin uporablja za izračun zasebnega ključa, iz katerega lahko generiramo nove naslova, določa 160-bitno dolžino javnega ključa [88]. V praksi to pomeni, da se lahko pri implementaciji plačevanja poslužujemo enkratne uporabe posameznega naslova, na katerega lahko stranka nakaže sredstva. Tak pristop je običajno tudi ustaljen pri večini spletnih trgovcev, ki podpirajo plačevanje z omenjeno valuto, zato se za vsak nakup posebej samo enkrat lahko uporabi določen naslov, s čimer se zmanjšuje tako imenovana stopnja sledi (ang. Taint) za transakcijami.

Zagon odjemalca Bitcoin-Qt v strežniškem načinu zahteva konfiguracijo datoteke *bitcoin.conf*, ki med številnimi opcijami določa predvsem naslednje:

- spremenljivki za strežniški način *server=1* in *daemon=1*,
- uporabniško ime in geslo za povezovanje s klici RPC *rpcuser* ter *rpcpassword*,
- dovoljene vhodne naslove IP v vrstici *rpcallowip*,
- vrata, na katerih se strežnik oglaša z vrstico *rpcport*, katere privzeta vrednost je 8332.

Odjemalec v strežniškem načinu se po uporabniškem vmesniku od običajnega odjemalca ne loči, kljub temu pa je mogoče spremljat rezultate (Slika 11), ki jih vračajo klici razreda *jsonRPCClient*.



Slika 11: Seznam generiranih naslovov po klicih RPC.

Nov naslov najprej generiramo v skripti PHP s podanim konstruktorjem, kjer podamo vrednosti atributov za dostop, kot smo jih navedli v datoteki *bitcoin.conf*:

```
$bitcoin = new jsonRPCClient("http://up_ime:geslo@naslov_ip:vrata/");
```

Nov naslov s pripadajočo oznako (Label) pa generiramo s klicem funkcije:

```
$newAddress = $bitcoin->getnewaddress($label);
```

Nadaljnje preverjanje, ali je bil zahtevan znesek za podani naslov vplačan, je tudi bistveno enostavnejše, saj je začetni znesek za vsak generiran naslov enak 0,00000000 BTC.

4.3 POSTAVITEV LOKALNE PODATKOVNE BAZE

Uporaba lokalne podatkovne baze je poleg hranjenja seznama digitalnih slik, njihovih informacij, kjer so definirane tudi kategorije in cene glede na resolucijo, pomembna tudi za registracijo uporabnikov in zapisovanje odprtih ter zaključenih transakcij.

Vse zahtevane tabele so bile kreirane z orodjem MySQL Workbench 6.0 CE in nato shranjene v lokalno podatkovno bazo MySQL, od koder je ustvarjene tabele po potrebi mogoče naknadno izvažati.

Pred povezovanjem spletne storitve z bazo se definirajo atributi za povezovanje, ki so bili določeni ob kreiranju modela MySQL. Vsak model namreč lahko vsebuje več podatkovnih baz (ang. Schemata), izmenično pa se lahko povezuje z več modeli, ki jih določajo nastavljene povezave (ang. Connections). Poleg uporabniškega imena in gesla za povezovanje privzete vrednosti določajo še metodo povezovanja (TCP/IP), naslov IP strežnika (ang. Hostname) in vrata ter ustrezno podatkovno bazo, nad katero se izvajajo poizvedbe.

Z razredom *DBConnection* so določeni konstruktor za vzpostavljanje povezave, funkcija *RunQuery()* za izvajanje poizvedb SQL in destruktor za prekinjanje povezave, ki se uporablja opcijsko, saj se ta po opravljeni poizvedbi prekine sama. Spodnja razpredelnica (Tabela 6) podaja seznam tabel, ki jih uporablja spletna trgovina:

Naziv tabele	**Stolpci**	**Podatkovni tip**
tabelaslike	IDSlike	int(11), PK, AI
	NazivSlike	varchar(45)
	AvtorSlike	varchar(45)
	DatumIzdaje	date
	VelikostMB	decimal(5,3)
tabelaoznakekategorije (tabela z nazivi kategorij)	IDOznake	int(11), PK
	NazivKategorije	varchar(45)
tabelaslikekategorije (tabela s kazalci kategorij za posamezno sliko)	IDSlikeKategorije	int(11), PK, AI
	IDSlike	int(11)
	KategorijaSlike	int(11)
tabeladimenzijecene (cene glede na izbrano resolucijo)	IDDimenzijeCene	int(11), PK
	Dimenzije	varchar(45)
	CenaBTC	decimal(10,8)
tabelareguporabnikov (tabela z informacijami registriranih uporabnikov)	IDUporabnika	int(11), PK, AI
	UporabniskoIme	varchar(45)
	Email	varchar(255)
	Geslo	char(64)
	IDKlienta	int(11)
	APIKey	varchar(45)
	Podpis	varchar(90)
tabelatransakcij (tabela z informacijami o odprtih in zaključenih nakupih)	IDTransakcije	int(11), PK, AI
	IDArtikla	varchar(45)
	NazivSlike	varchar(45)
	DimenzijeSlike	varchar(45)
	CenaBTC	decimal(10,8)
	VplacanoBTC	decimal(10,8)
	NaslovZaPlacilo	varchar(45)
	DatumIzvrsbe	datetime
	KljucInfo	char(32)
	TransakcijaZakljucena	varchar(45)

Tabela 6: Seznam uporabljenih tabel in podatkovnih tipov.

Z oznakama PK (ang. Primary Key) in AI (ang. Auto Increment) se označujejo stolpci, katerih vrednosti določajo primarne ključe oziroma enolične oznake posameznih zapisov v tabeli in kjer se številčenje zapisov povečuje avtomatsko. Podatkovna tipa *int* ter *varchar* določata največje število bajtov za zapise, ki hranijo celoštevilske (ang. Integer) ali pa alfanumerične vrednosti. Stolpci tipa *decimal(10,8)* se uporabljajo za decimalne vrednosti zneskov BTC, ki trenutno zavzemajo 8 decimalnih mest, kar je tudi najmanjša podprta vrednost, ki se lahko pošilja.

4.4 DODELITEV CENOVNIH POSTAVK IN OBDELAVA VPLAČILA

4.4.1 Menjalni tečaj

Začetna predpostavka o cenah digitalnih slik je, da se te ne razlikujejo glede na podan artikel, temveč jih določa zgolj izbrana resolucija. Vendar pa z uporabnikovega vidika ta ni posebej informativna, zato je priporočljivo dodati menjalni tečaj, iz katerega se lahko razberejo vrednosti v kateri od domačih valut. Menjalni tečaj na strani, ki vrednosti posodablja glede na rezultate, prebrane iz zunanjih virov, kot so Bitstamp, BTC-E, LocalBitcoins, Coinbase, je realiziran s skripto PHP, kjer se poizvedbe opravljajo iterativno za vsak naslov URL posebej. Tako lahko nad prvim virom opravimo klic:

```
$source = file_get_contents('https://www.bitstamp.net/api/ticker/');
$bitstamp = json_decode($source);
```

Poizvedba vrne objekt, ki v določenem časovnem obdobju glede na razmerje med povpraševanjem in ponudbo na primer znaša do približno 640 dolarjev za 1 enoto BTC:

```
stdClass Object
(
   [high] => 639.88
   [last] => 634.95
   [timestamp] => 1394991555
   [bid] => 632.02
   [vwap] => 634.43
   [volume] => 3297.77009925
   [low] => 629.02
   [ask] => 634.95
)
```

Natačnejše menjalno razmerje dobimo s povprečjem najvišje (ang. High) in najnižje (ang. Low) vrednosti 1 enote BTC v dolarjih.

Menjalni tečaj je tako predstavljen s povprečjem rezultatov poizvedb iz vseh štirih virov, s čimer dobimo relativno ustaljeno trenutno menjalno razmerje v dolarjih, medtem ko je na koncu potrebna še ena poizvedba, ki s strani *http://www.xe.com/datafeed/samples/sample-xml-usd.xml* vrača menjalno razmerje iz dolarjev v evre.

4.4.2 POSTOPEK OBDELAVE VPLAČILA

Preverjanje, ali je bil znesek nakazan na podani naslov, je iterativno opravilo, ki se vnaprej določenih 40 minut izvaja v časovnem intervalu 15 sekund. Način, pri katerem se skripta, ki na naslovu blockchain.info preverja status plačila, ne izvaja po nepotrebnem ves čas, je pomemben iz dveh razlogov:

- generirani naslovi BTC so s prvo uporabo še nepreverjeni, zato jih mora, preden se lahko uporabijo za plačilo, potrditi omrežje Bitcoin. Posledica tega koraka je daljša obdelava plačil, ki v primerjavi s potrjenimi naslovi namesto nekaj sekund znaša do 30 minut[5] za manjše zneske;
- preverjanje je bistveno bolj smiselno izvajati potem, ko uporabnik potrdi vplačilo, tudi če tega dejansko izvede nekoliko pozneje.

Da bi bil celoten čas nakupa čim krajši, se za uspešen zaključek vplačila zahteva le ena potrditev omrežja, saj bi v nasprotnem primeru priporočljivih 6 k temu pridalo skoraj celo uro glede na to, da se trenutno vsaka nadaljnja potrditev izvede približno vsakih 10 minut [89]. V tem primeru se atribut, ki označuje 1 zahtevano potrditev, doda na konec poizvedbe:

```
$.getJSON("https://blockchain.info/q/getreceivedbyaddress/" + addressBTC + "/1",
function(data){});
```

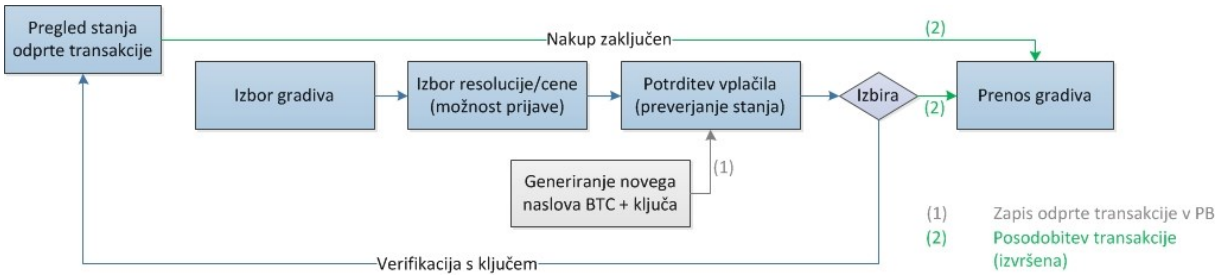
Funkcija iz posredovanega naslova URL vrne znesek za generirani naslov, vendar je tedaj vrednost celoštevilska, zato jo je pred primerjavo s ceno artikla potrebno pretvoriti v decimalno.

Če poizvedbo izvedemo nad naslovom BTC *1BN5H2M3VLo5AGaCpkNhXoHa1ZcvSuQ5L6*, bo vrnjena vrednost predstavljena s številom 63640. Ker lahko trenutno najmanjši podprt znesek v trgovanju vsebuje 8 decimalnih mest, naša vrednost pa jih zavzema 5, moramo številu z leve dodati tri ničle. Tedaj dobimo novo število 00063640, ki ga pretvorimo v decimalni zapis in šele nato lahko vrednost 0,00063640 primerjamo s cenovno postavko.

[5] Čas obdelave vplačil je naveden za obdobje do marca leta 2014 in se v prihodnje lahko spremeni.

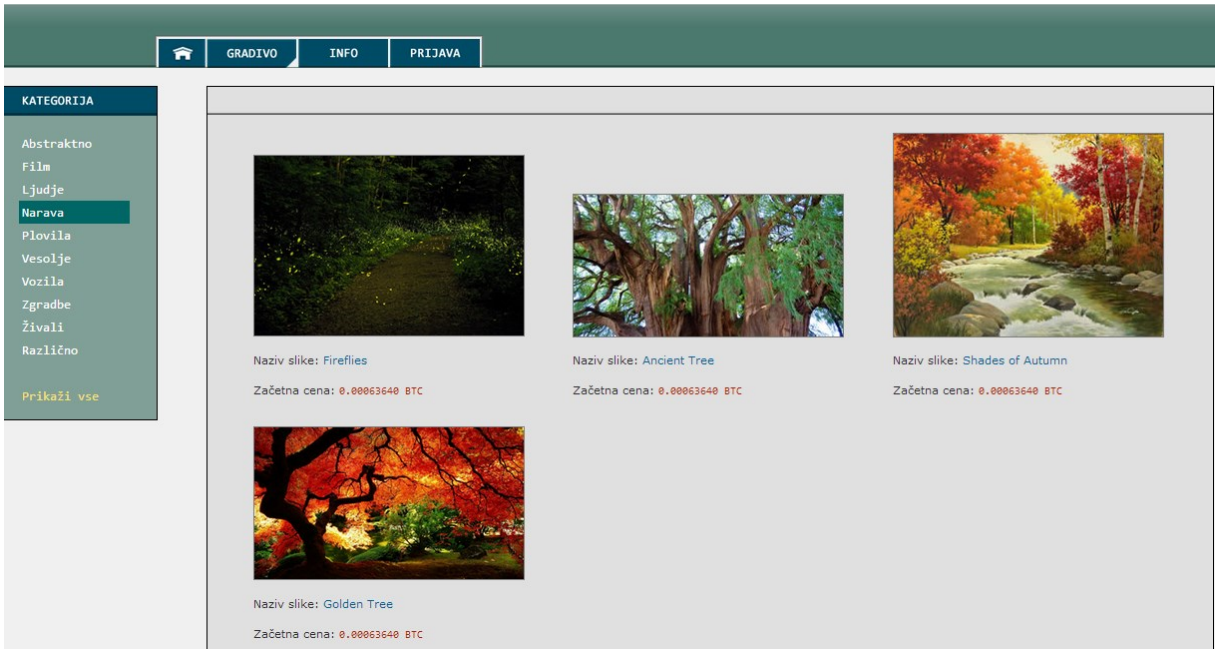
4.5 PREGLED TOKA IZVAJANJA NAKUPA

V tem koraku opisana implementirana različica plačevanja z valuto Bitcoin na spletni trgovini predvideva anonimne uporabnike, kar pomeni, da se lahko nakup opravi brez potrebe po registraciji. Tak korak je sicer smiseln takrat, ko so pred uporabo storitve zahtevani nekateri osebni podatki obiskovalca, vendar je prvotni cilj te rešitve (Slika 12) prikaz delovanja decentralizirane valute, katere ena od lastnosti je višja stopnja zasebnosti od nekaterih alternativnih načinov plačevanja.



Slika 12: Diagram s koraki poteka nakupa in plačila.

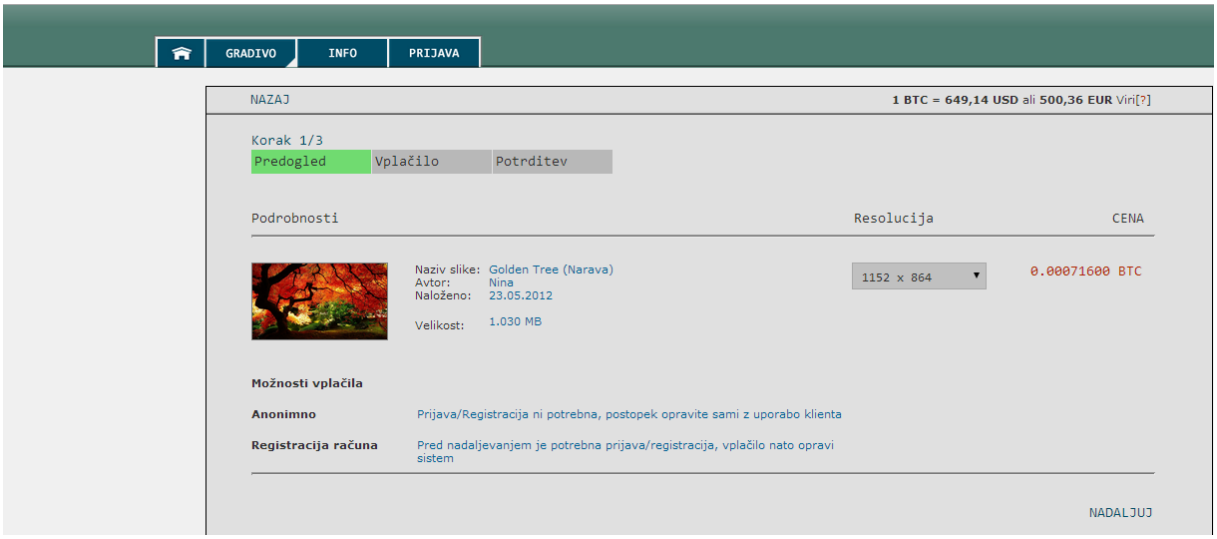
Na spodnji sliki (Slika 13) je za implementirano rešitev podan vpogled v zavihek s slikovnim gradivom, kjer si uporabnik izbere digitalno sliko za nakup.



Slika 13: Izbira slikovnega gradiva na spletni strani pred nakupom.

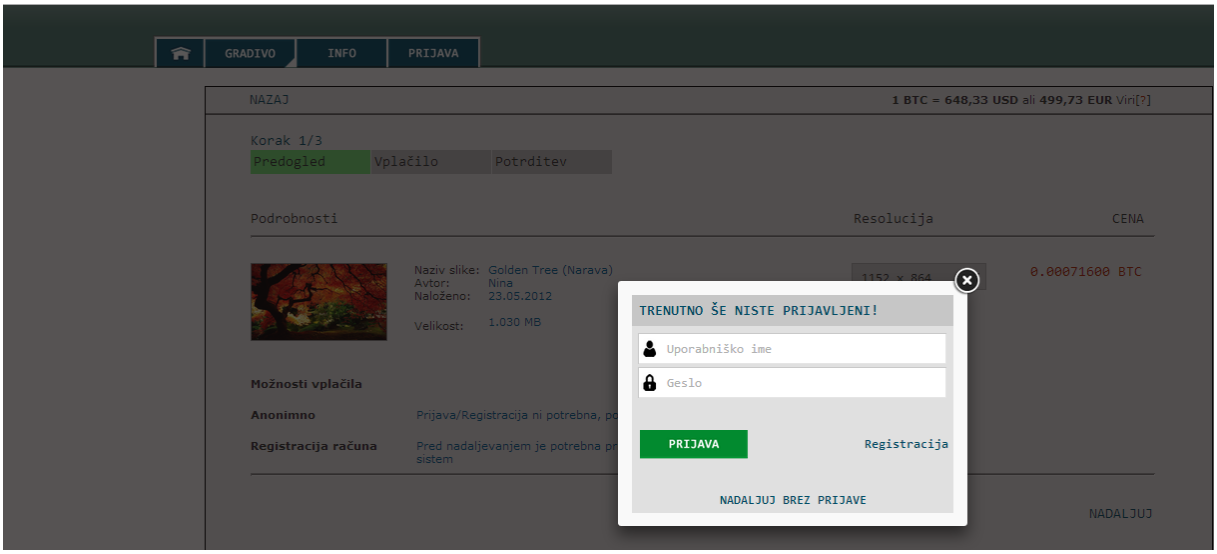
Hiter pregled nad digitalnim gradivom pokaže, da je na začetku cenovna postavka za vse artikle enaka. V naslednjem koraku (Slika 14) se ob izbrani resoluciji izpiše cena, ki jo z uporabo tehnike AJAX vrne poizvedba SQL:

SELECT CenaBTC FROM tabeladimenzijecene WHERE IDDimenzijeCene=$res;



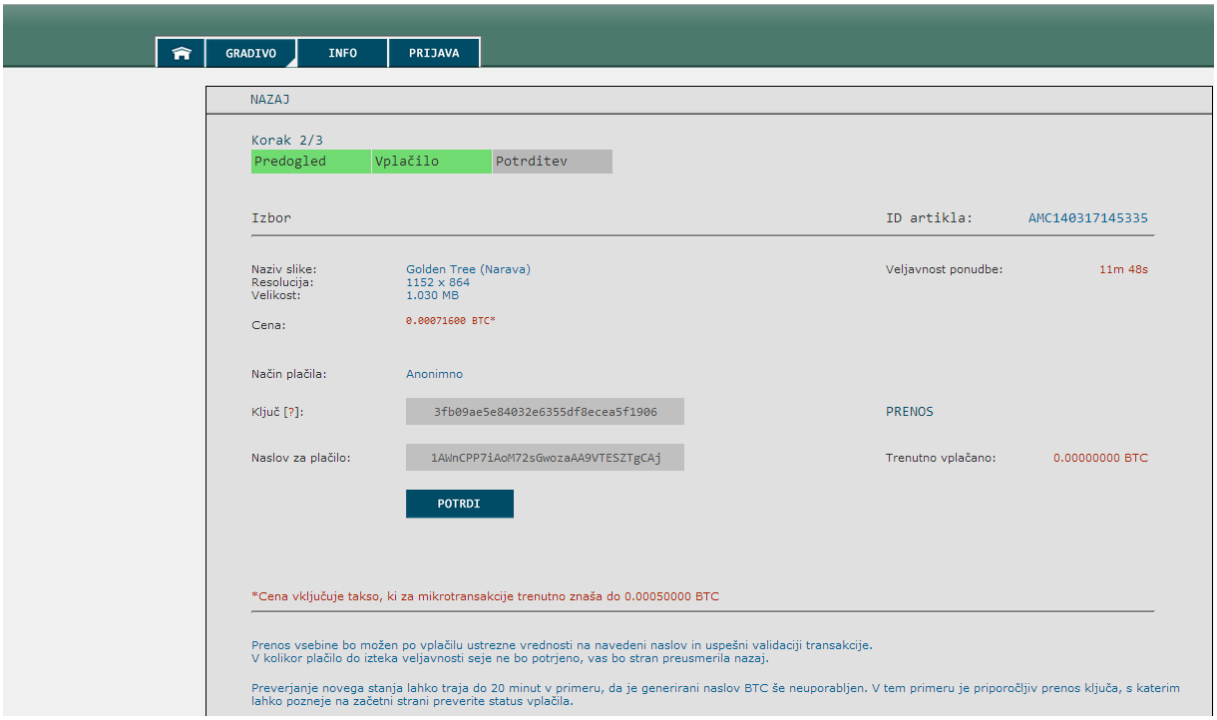
Slika 14: Obrazec za izbiro resolucije pred nadaljevanjem na stran za vplačilo.

Na tem mestu je pred nadaljevanjem še mogoča prijava oziroma registracija (Slika 15), s čimer se ob preusmeritvi prikaže obrazec za avtomatiziran (ang. Bitstamp API) način plačila.



Slika 15: Okence s formo za prijavo/registracijo pred posredovanjem na stran za vplačilo.

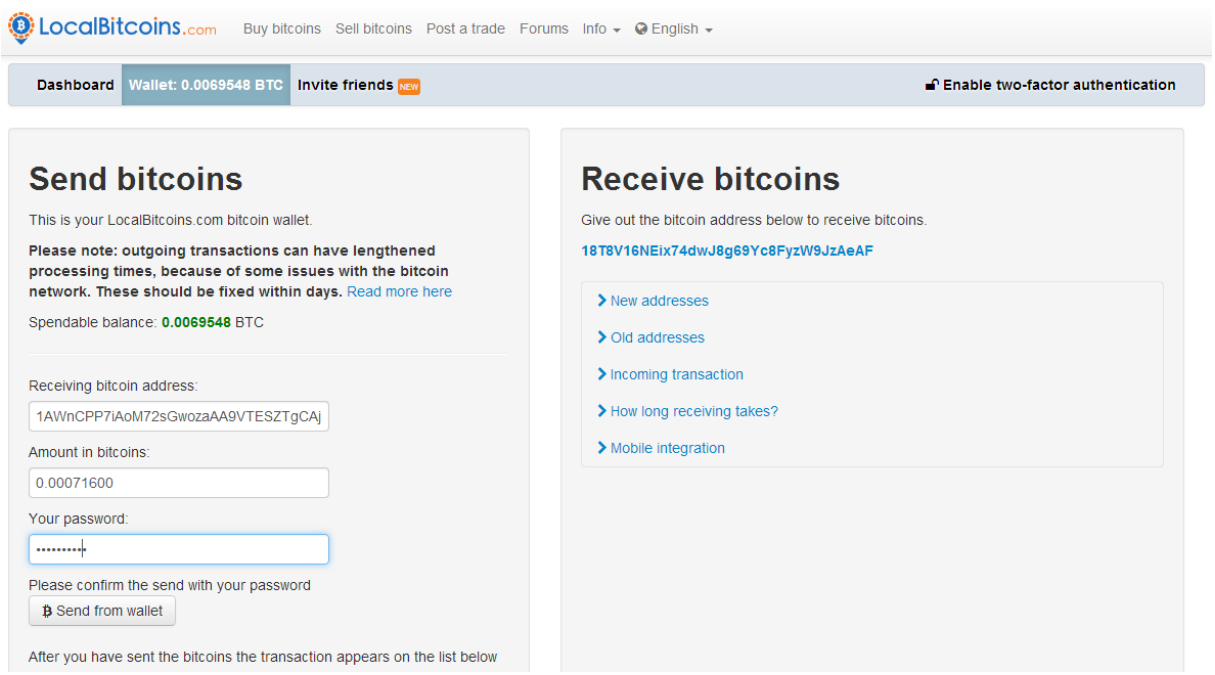
Ob izbiri opcije *NADALJUJ*, ki omogoča tudi nadaljevanje brez prijave, se za neprijavljenega uporabnika prikaže možnost za prijavo oziroma registracijo, saj sta obe opciji zaradi preverjanja statusa uporabnika na naslednji strani onemogočeni. Ta princip hkrati preprečuje, da bi se novi naslovi BTC generirali po nepotrebnem (Slika 16).



Slika 16: Obrazec z generiranim naslovom BTC za plačilo.

Na tem koraku se skupaj z generiranim naslovom BTC generira časovno omejena ponudba, za katero uporabnik opravi vplačilo. Vrstni red vplačila in potrditve ni pomemben, priporočljivo pa je, da se potrjevanje izvede po nakazilu sredstev na generiran naslov, saj se šele potem veljavnost ponudbe pavzira, skripta pa prične z iterativnim preverjanjem zneska.

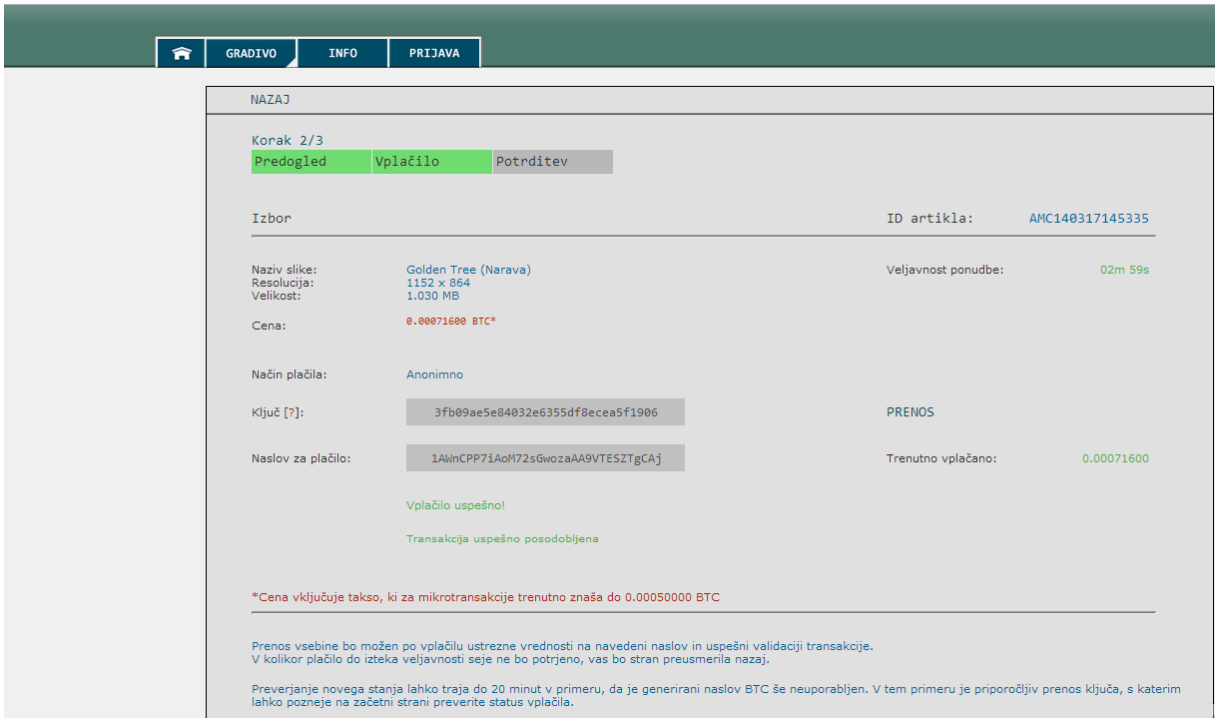
Podan primer prikazuje vplačilo, opravljeno šele po potrditvi, medtem, ko je bil znesek nakazan iz lokalne digitalne denarnice storitve LocalBitcoins (Slika 17).



Slika 17: Plačilo zneska z uporabo storitve LocalBitcoins.

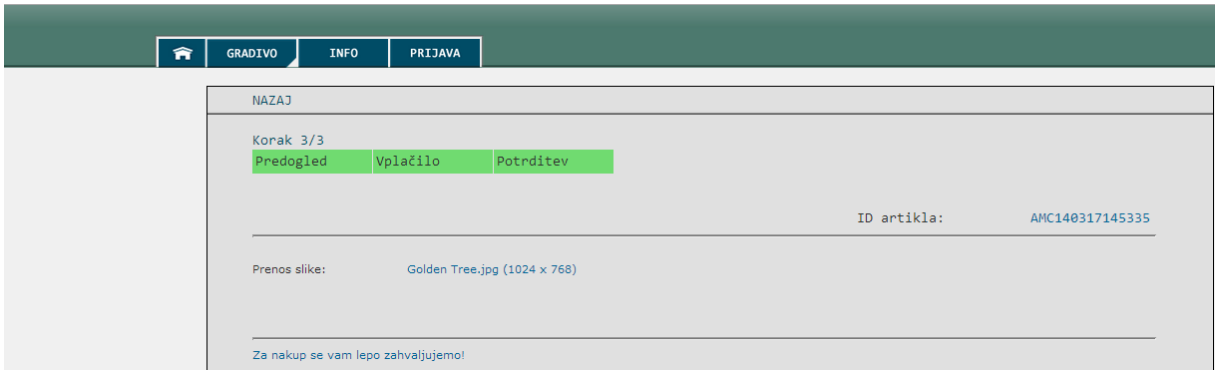
Omenjena alternativa, ki za kakršenkoli dvig sredstev z računa ne odšteje takse neposredno od same vrednosti, kot je to običajno z uporabo nameščenih odjemalcev, temveč se ta nato odšteje od novega stanja na računu, dopušča prenos natančnih zneskov, zato pri zapisih v podatkovno bazo ne prihaja do razlik med ceno artikla in vplačanim zneskom. Ne glede na vrsto digitalne denarnice je pri preverjanju potrebno od ciljne vrednosti odšteti variabilno takso, ki lahko ponekod znaša od 0,00010000 BTC do 0,00050000 BTC [90].

Če uporabnik po potrditvi, ki hkrati še zabeleži odprto transakcijo, ostane na isti strani, se skripta, ki se izvaja v ozadju, ne prekine. Tedaj je sporočilo o zaključenem nakupu (Slika 18) mogoče razbrati tik pred preusmeritvijo na zadnjo stran za prenos vsebine.



Slika 18: Obvestilo po uspešno zaključenem nakupu.

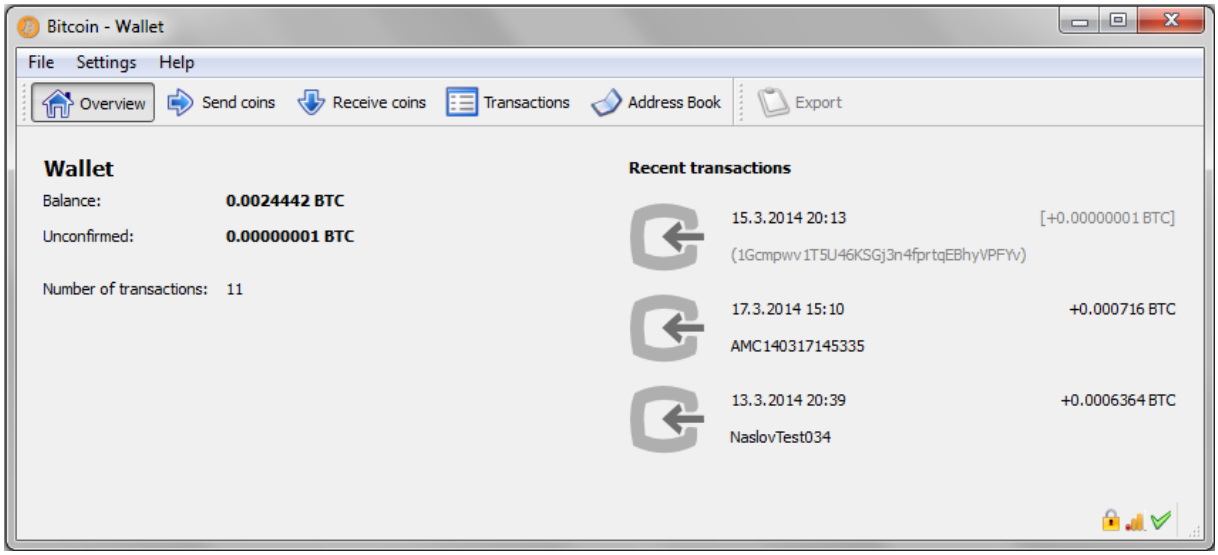
Prikazani tok nakupa predvideva, da uporabnik pred zaključkom nakupa ne zapušča strani, če se znesek na generirani naslov prenese v nekaj minutah. V nasprotnem primeru je mogoč prenos ključa, s katerim se preverjanje stanja in zaključitev nakupa opravita pozneje na začetni strani. Ko je nakup uspešno zaključen, se na zadnji strani (Slika 19) lahko opravi še enkraten prenos kupljene vsebine.



Slika 19: Zadnja stran z opcijo za prenos kupljene vsebine.

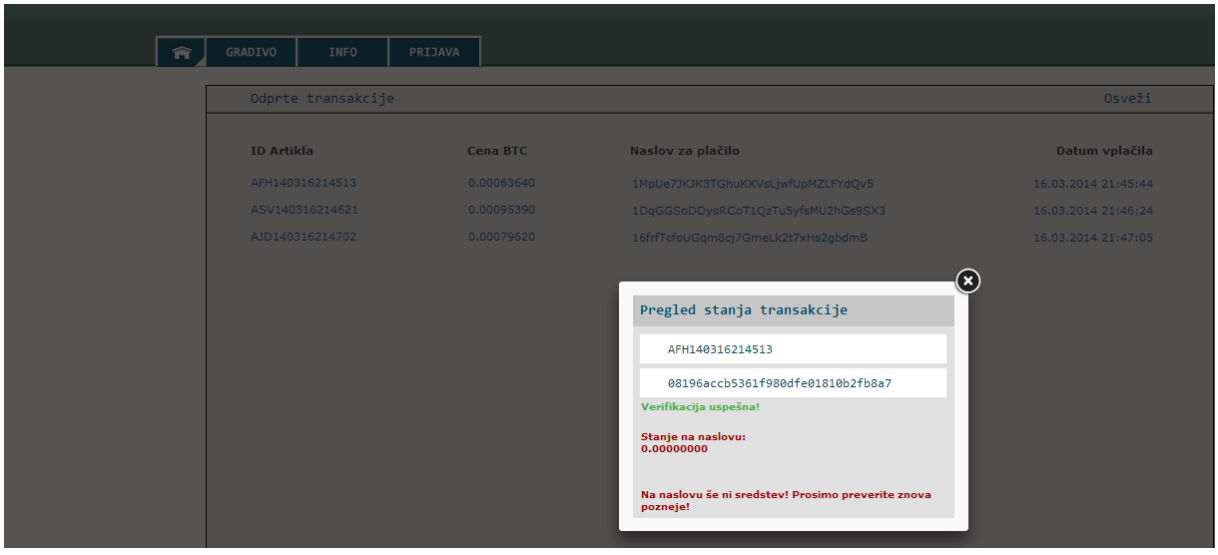
Enolični niz, ki opredeljuje spremenljivko *IDArtikla*, se uporablja za identifikacijo posamezne transakcije in obenem označuje generirani naslov v odjemalcu Bitcoin-Qt, s katerim lahko te povezujemo.

Čeprav so nakazana sredstva na naslovu dejansko razpoložljiva čez približno eno uro, je obvestilo mogoče prebrati takoj po zaključku. Na spodnji sliki (Slika 20) je transakcija identificirana z nizom *AMC140317145335*, ki je hkrati oznaka novo generiranega naslova.



Slika 20: Oznaka generiranega naslova v odjemalcu Bitcoin-Qt določa oznako transakcije.

Druga alternativa (Slika 21) nudi pregled statusa nakupa na začetni strani, potem ko ob vplačilu zapustimo stran z generiranim naslovom. Tedaj je vpogled v katerokoli od odprtih transakcij mogoče opraviti neodvisno od časovnih omejitev, potrebna je le verifikacija s podanim ključem.



Slika 21: Primer preverjanja stanja za neizvršeno transakcijo.

Način izvajanja preverjanja stanja na naslovu za posamezno transakcijo se na tem mestu od prejšnjega nekoliko razlikuje. Postopek ni več iterativen, temveč se ob vsakem preverjanju izvede samo enkrat, saj naj bi, glede na predpostavko, da se ta korak navadno izvaja šele nekoliko pozneje, tak princip zadostoval.

4.6 NAJPOGOSTEJŠE OVIRE PRI REALIZACIJI KONČNE REŠITVE

V tem poglavju so zapisani nekateri problemi, ki so se pojavili med razvijanjem omenjene rešitve in pri tem pod luč postavljajo vprašanje, kako bi določene vidike razdelali pri podobni storitvi v dejanski vsakdanji rabi.

4.6.1 Povezovanje z odjemalcem Bitcoin-Qt

Implementirana spletna trgovina uporablja postavitev, pri kateri se strežnika PHP in Bitcoin nahajata na isti platformi, zato s tega stališča težava ni tako izrazita, kljub temu pa se ta pojavi pri ločeni konfiguraciji. Odjemalec RPC sicer podpira oddaljene klice, vendar je zaradi zasnove strežnika Bitcoin, ki privzeto podpira samo lokalne klice RPC (http://localhost:8332/), potrebna nastavitev:

- strežniškega certifikata *server.cert* in zasebnega ključa *server.pem*,
- dovoljenih naslovov IP, ki se lahko povezujejo; te v dokumentu *bitcoin.conf* definiramo z atributom *rpcallowip=<naslov IP>,*
- povezave SSL v istem dokumentu z atributom *rpcssl=1*.

4.6.2 Zanesljivost vmesnikov API

Prednosti pri vpeljavi zunanjih ponudnikov digitalnih denarnic, ki med drugim omogočajo avtomatiziran prenos sredstev iz računa (ang. Withdrawal) na druge naslove BTC z uporabo klicev API, sta pri večkratni uporabi hitrost in enostavnost. Vendar pa je v trenutni fazi predvsem zaradi nenadnih sprememb v funkcionalnosti sistema, pomanjkljive oziroma povsem odsotne dokumentacije in nezanesljive podpore storitev v takšni obliki velikokrat neprimerna za vključevanje v lastne trgovske rešitve. Eden od zadnjih primerov je storitev Mt. Gox, ki je pred propadom februarja leta 2014 prav tako omogočala vključitev lastnega vmesnika API v obstoječe trgovske rešitve, s katerimi so lahko registrirani uporabniki nakup opravili hipoma.

Drugi problem je postopek registracije pri katerem od takšnih ponudnikov, kjer se v sklopu programa AML zahteva verifikacija računa. Za polno delovanje storitve je namreč potrebno posredovanje kopij osebnih dokumentov, zato se kljub dejstvu, da gre pri tem za odgovor na izkoriščanje nove digitalne valute za pranje denarja, pojavlja vprašanje, ali je anonimnost pri uporabi kriptovalute Bitcoin vedno zagotovljena.

4.6.3 Določanje taks pri transakcijah

Vrednost taks, ki se glede na posredovani znesek zaračunajo zaradi hitrejše obdelave v omrežju, je, kot je bilo omenjeno, z uporabniškega vidika vnaprej neznana, kar je predvsem posledica načina zalaganja sredstev znotraj digitalne denarnice. Transakcija se brez potrebe po plačilu taks lahko izvede takrat, ko:

- njena velikost ne presega 1000 bajtov,
- je znesek za nakazilo večji od 0,01000000 BTC,
- je njena prioriteta višja od meje 57 600 000.

Ker so v našem primeru cene manjše od 0,01000000 BTC in število potrebnih potrditev po vplačilu ni večje od 1, pomeni, da niti zadnji pogoj ni izpolnjen:

$$prioriteta = \frac{vsota}{velikost\ v\ bajtih}, vsota = znesek\ \times število\ potrditev \qquad (4.1)$$

Spremenljivka *vsota* označuje vsoto vseh zmnožkov (*znesek* × *število potrditev*), ki jih prištevamo skladno s številom vhodnih zapisov (ang. input) izbrane transakcije. Vsak vhodni zapis podaja vrednost zneska, ki je bil uporabljen v predhodnih transakcijah, zato ima ena transakcija lahko več vhodnih zapisov [91].

Razpoložljiva sredstva v digitalni denarnici so torej skupek ločenih transakcij, ki se uporabljajo tudi več kot enkrat, zaradi česar sta njihova velikost ob vplačilu in stopnja takse nepoznani.

4.7 KRAJŠA PRIMERJAVA PLAČEVANJA S STORITVIJO PAYPAL

Med primerjavo sistemov, kakršna sta Bitstamp in Bitpay, ki uporabljata integrirano plačevanje s kriptovaluto Bitcoin, s storitvijo, kot je PayPal, se ključne razlike kažejo predvsem pri zgradbi sistema plačevanja in stopnji zahtevanih osebnih podatkov.

PayPal, regulirana finančna institucija, je v prvi vrsti posrednik med kupčevo in prodajalčevo banko. To pomeni, da je zaradi povezanosti uporabniških računov z bančnimi lahko za katerikoli nakup možno preveriti naročniške podatke, medtem ko je z uporabo javnih ključev znotraj omrežja Bitcoin za isto storitev potreben le ustrezen odjemalec, ki ne razkriva identitete uporabnika. Omenjena sistema privzeto podpirata tudi lastne spletne denarnice, kar je pričakovano, glede na dejstvo, da sta eni izmed glavnih funkcionalnosti obeh storitev možnost zalaganja računa z denarnimi sredstvi in nakazovanje na druge naslove. Iz teh ter prenesenih sredstev je praviloma relativno zahtevno razbrati, za koga gre, še posebej, če se za posamezen nakup uporabi enkraten naslov, katerega odstotek sledi bo v tem primeru enak za vse [92].

Vendar pa postaja tudi pri takšnih plačilnih procesorjih, ki za polno funkcionalnost storitve, ne glede na to, ali gre za običajnega uporabnika ali za trgovca, čedalje bolj ustaljena zahteva po verifikaciji registriranega računa. Sistema Bistamp in Bitpay je z lastnimi rešitvami kljub temu mogoče integrirati delno ali v celoti.

4.7.1 Registracija storitve

Podobnosti se kažejo pri nakupih digitalnih vsebin, kjer so si procedure tako za Bistamp in Bitpay kot PayPal zelo podobne. Večina ponudnikov ob implementaciji vmesnika API za predhodno registrirane uporabnike pri ustreznem plačilnem procesorju nudi izvedbo plačila šele po prijavi, kar je časovno primerljivo s hitrostjo postopka avtentikacije in procesiranja naročil pri PayPalu. S stališča opravljanja večjih naročil pa je ravno slednji zanesljivejši. Bitcoin je v trenutni fazi bistveno bolj naklonjen trgovcem, še posebej storitev Bitpay, saj za uporabnika ni nobenega zagotovila, da bo plačan produkt tudi dobil. Ker ni nobenega posrednika, to pomeni, da lahko vsak član P2P omrežja sam postavi lastno storitev, povsem neodvisno od drugih posrednikov.

Večje razlike se predhodno kažejo tudi pri registraciji storitve. PayPal za trgovce, kjer prodaja poteka mednarodno, trenutno zahteva 3,9-odstotno takso za vsako transakcijo ter fiksno takso za vsako prejeto valuto [93]. Nasprotno pa se določajo takse pri uporabi kriptovalute Bitcoin, kjer se v grobem uporabljata dva principa.

Takse pri plačilnih procesorjih za osnovni račun trenutno znašajo običajno 1 odstotek ter do 0,00050000 BTC na posamezno transakcijo, pri čemer se ta lahko odšteje od preostalih razpoložljivih sredstev na računu. Pri nekaterih plačilnih procesorjih, kot je Bitstamp, taks pri nakazilih sredstev še ni, vendar se to v prihodnje lahko spremeni. Primeri zato kažejo, da enotnega standarda na tem področju zaenkrat ni, medtem ko se takse pri uporabi lokalnih digitalnih denarnic odštevajo sproti za vsako transakcijo, zato je pri natančnih zneskih potreben predhoden izračun [94, 95].

4.7.2 Klici storitev API

Tudi druge rešitve, ki se v tej fazi uporabljajo ob implementaciji vmesnikov API sistemov Bitstamp in Bitpay, sicer še niso dokončno razvite, vendar se pristop od vmesnika za PayPal med drugim loči po uporabi poverilnic za oddaljene klice. V prvem primeru zadostuje že generiran ključ API (ang. API Key), s katerim se lastnik računa, če uporablja plačilni procesor, avtenticira na strežniku. V nasprotnem primeru pa vsak klic vsebuje uporabniško ime, geslo in podpis ter drugačen sestav vrednosti vnosnih polj.

Širši je tudi nabor podprtih formatov za klice in poleg protokola SOAP (ang. Simple Object Access Protocol) podpira še JSON in NVP (ang. Name-Value Pairs). Prvi za posamezen klic zahteva formatiranje podatkov z jezikom XML [96].

5 SKLEPNE UGOTOVITVE

Ob implementaciji plačevanja v praksi je jasno, da so digitalne valute po več letih nastanka še vedno v fazi razvoja in testiranja. Tveganje nastane ob vpeljavi zunanjega ponudnika, saj ni zagotovila, da storitev ne bo že ob naslednji uporabi dostopna uporabnikom. Spletna storitev, ki bi primarno podpirala samo eno digitalno valuto, zato ni najboljša možnost. Drugo varnostno vprašanje postavljajo digitalne denarnice. Praksa kaže, da so zanesljivejše lokalne, nameščene na lastnem računalniku, saj so tarča napadov tudi ob dvostopenjski avtentikaciji najpogosteje spletne različice digitalnih denarnic. Kljub pomanjkljivostim se največje prednosti kažejo pri hitrosti procesiranja transakcij v omrežju in stopnji zahtevnosti pri uporabi. Razlike v primerjavi z danes splošno sprejetimi storitvami, kot so plačila SEPA, ostajajo velike, poleg tega pa je celoten proces mogoče spremljati večino časa brez potrebe po razkrivanju zasebnih informacij.

V okviru diplomskega dela nam, z izjemo uporabe obstoječih vmesnikov API za delo s strežnikom Bitcoin in storitvijo Bitstamp za registrirane uporabnike, povsem izdelana samostojna spletna rešitev vključno z lokalno podatkovno bazo kaže, da je osnovna postavitev alternativnega sistema za plačevanje relativno nezapletena. Najtežji del implementacije je bilo povezovanje s katerim izmed razmeroma zanesljivih storitev, v tem primeru s sistemom Bitstamp, ki bi omogočal avtomatizacijo plačevanja. Kljub temu tudi ta princip ni najbolj praktičen, saj uporaba zaradi daljšega postopka zahtevane verifikacije računa ni takojšnja.
Pomemben rezultat prikazane rešitve je dejstvo, da je trgovanje z nekaterimi storitvami mogoče opravljati tudi v praksi, še posebej kadar gre za storitve v digitalni obliki. Trenutno najprimernejša uporaba digitalnih valut se kaže pri razširjanju obstoječe ponudbe, in sicer predvsem za produkte ali storitve nižjega cenovnega ranga, kjer je tveganje manjše.

Kako se bodo digitalne valute razvijale naprej, ni moč napovedati z gotovostjo. Spremembe, ki jih prinašajo, so dobrodošle in njihova pot zagotovo ne bo tako dolga, kot je bila od nastanka prvega bankovca pred skoraj tisoč leti.

LITERATURA

[1] J. A. Dorn, *The Future of Money in the Information Age*, Massachussetts: Cato Institute, 1997, str. 3–6.

[2] (2014) Eletronic Data Interchange and Electronic Funds Transfer. Dostopno na: http://www.referenceforbusiness.com/management/De-Ele/Electronic-Data-Interchange-and-Electronic-Funds-Transfer.html

[3] J. A. Dorn, *The Future of Money in the Information Age*, Massachussetts: Cato Institute, 1997, str. 16–20.

[4] R. R. Bliss, R. Steigerwald, "Derivatives clearing and settlement: a comparison of central counterparties and alternative structures", *Economic Perspectives*, št. Q, zv. IV, str. 22-23, 2006.

[5] (2014) Money and Currency in the 21st Century. Dostopno na: http://www.apfn.org/Mind_Control/money/21st_century.htm

[6] (2014) Risks in Payment and Securities Settlement. Dostopno na: http://www.nationalbanken.dk/C1256BE9004F6416/(sysPrintViewDefault)/Payment_Systems_in_Denmark_publ/$file/kap05.html

[7] (2014) The Paradox of Cryptocurrencies. Dostopno na: http://www.forexminute.com/litecoin/the-paradox-of-cryptocurrencies-24875

[8] D. Duffie, N. Gârleanu, L. H. Pedersen, "Over-the-Counter Markets", *Econometrica*, št. 6, zv. 73, str. 1815–1847, 2005.

[9] (2014) OTC Order Book. Dostopno na: http://bitcoin-otc.com/vieworderbook.php

[10] (2014) Network Security Types of Attack. Dostopno na: http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

[11] (2014) Enkripcija podatkov. Dostopno na: http://www1.fov.uni-mb.si/Studentske_strani/seminarske/enkripcija%20podatkov/enkripcija.htm

[12] (2014) Symmetric-Key Algorithm. Dostopno na: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Symmetric-key_algorithm.html

[13] (2014) Guide to a Successful Encryption Project. Dostopno na: http://www.mcpressonline.com/security/ibm-i-os400-i5os/your-guide-to-a-successful-encryption-project.html

[14] (2014) Asymmetric-Key Cryptography. Dostopno na: http://www.cs.cornell.edu/courses/cs5430/2011sp/TL04.asymmetric.html#sec-12

[15] (2014) About MD5 Cryptographic Hash Function. Dostopno na: http://md5-hash-online.waraxe.us/

[16] (2014) Elektronsko podpisovanje v spletnih storitvah in namenskih programih. Dostopno na: http://www.ajpes.si/ostale_vsebine/elektronsko_podpisovanje

[17] (2014) Digital Signature Algorithm. Dostopno na: https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Digital_Signature_Algorithm.html

[18] (2014) Registration of Money Transmitting Business. Dostopno na: http://www.law.cornell.edu/uscode/text/31/5330

[19] (2014) Transmitter Architecture. Dostopno na: http://transmittersystem.com/architecture.htm

[20] (2014) Money Transmitter Licensing. Dostopno na: http://moneytransmitterlicense.blogspot.com/2010/01/money-transmitter-license-information.html

[21] (2014) PayPal, History. Dostopno na: https://www.paypal-media.com/history

[22] (2013) Digital Currency Providers and Regulators. Dostopno na: http://www.hunton.com/files/Publication/a511980b-751f-4148-bf78-204507d4c654/Presentation/PublicationAttachment/9ca3d7fa-5705-4779-942b-2bc03b2c94d8/Uncertainty_Looms_for_Digital_Currency_Providers_and_Regulators.pdf

[23] R. P. DeGennaro, *Principles of Financial Management*, San Diego: Cognella, 2011, str. 173–174.

[24] (2014) 10 Excellent Online Payment Systems. Dostopno na: http://sixrevisions.com/tools/online-payment-systems/

[25] (2014) A New Challenger in the Bitcoin Merchant Processing Race. Dostopno na: http://themonetaryfuture.blogspot.com/2013/03/a-new-challenger-in-bitcoin-merchant.html

[26] (2014) Money Laundering in Digital Currencies. Dostopno na: http://www.justice.gov/archive/ndic/pubs28/28675/intro.htm

[27] (2014) How Payment Processing Works. Dostopno na: http://www.cybersource.com/developers/learn/getting_started/how_payment_processing_works/

[28] (2014) SoftTouch POS Integrates Bitcoin Virtual Currency Payment Processing. Dostopno na: http://www.digitaljournal.com/pr/1531781

[29] M. Herpel, "2011 Observations on the Digital Currency Industry", *DGCmagazine*, št. januar 2011, str. 5–9, 2011.

[30] (2014) Java Applet Attack Wipes Out Bitcoin Accounts On Mt. Gox. Dostopno na: http://techcrunch.com/2013/04/11/mt-gox-cross-site-scripting-attack-wipes-out-bitcoin-accounts/

[31] (2014) MtGox Phishing Campaign. Dostopno na: http://krebsonsecurity.com/2013/06/mtgox-phishing-campaign-hits-bing-yahoo/

[32] (2014) DDoS attacks on Mt. Gox. Dostopno na: http://arstechnica.com/security/2013/04/potent-ddos-attacks-on-mt-gox-delays-rollout-of-new-virtual-currency/

[33] Dr. M. Ernkvist, Dr. V. Lehdonvirta, *Knowledge map of the virtual economy*, Washington: World Bank, 2011.

[34] (2014) The Invisible Hand of EVE Online. Dostopno na: http://www.rockpapershotgun.com/2013/05/03/eve-fanfest-2013-the-invisible-hand-of-eve-online/#more-151831

[35] (2014) Eve Subscribers. Dostopno na: http://www.rockpapershotgun.com/2013/02/28/after-ten-years-eve-stands-at-500k-subscribers/

[36] (2014) My Virtual Life. Dostopno na: http://www.businessweek.com/stories/2006-04-30/my-virtual-life

[37] M. Rysman, " The Economics of Two-Sided Markets", The Journal of Economic Perspectives, št. 3, zv. 23, str. 125–143, 2009.

[38] W. J. Luther, *Cryptocurrencies, Network Effects and Switching Costs*, Virginia: Mercatus Center, 2013, str. 3–4.

[39] (2014) Digital Gold Currency. Dostopno na: http://www.resourceinvestor.com/2010/04/22/digital-gold-currency-dgc-long-wave-innovation-ft

[40] C. J. Wells, *Digital Currency Systems: Emerging B2B e-Commerce Alternative During Monetary Crisis in the United States*, Colorado: Aspen University, 2011, str. 2–6.

[41] S. J. Hughes, S. T. Middlebrook, B. W. Peterson, "Developments in the Law Concerning Stored-Value Cards and Other Electronic Payments Products ", *The Business Lawyer*, št. 1, zv. 63, str. 237–269, 2007.

[42] (2014) Multi-Factor Authentication (MFA). Dostopno na: http://www.safenet-inc.com/products/data-protection/multi-factor-authentication/?tabnum=2

[43] (2014) About OpenPGP. Dostopno na: http://www.openpgp.org/about_openpgp/

[44] (2014) Network Security. Dostopno na: http://www.cs.ru.nl/~ths/a3/html/h8/h8.html

[45] (2014) eGold. Dostopno na: http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html

[46] (2014) The Improbable Rise and Fall of E-Gold. Dostopno na: http://www.wired.com/threatlevel/2009/06/e-gold/

[47] (2014) Digital Currency Exchange Money Laundering Scheme. Dostopno na: http://rt.com/usa/money-currency-reserve-liberty-903/

[48] (2014) Sinkholes. Dostopno na: https://www.shadowserver.org/wiki/pmwiki.php/Stats/Sinkholes

[49] J. A. Ritter, "The Transition From Barter to Fiat Money", *American Economic Review*, št. marec 1995, str. 1–4, 1995.

[50] M. McLeay, A. Radia, R. Thomas, "Money in The Modern Economy: An Introduction", *Bank of England*, št. marec 2014, str. 6, 2014.

[51] (2014) Ripple. Dostopno na: http://www.thebitcointrader.com/2013/05/ripple-is-now-tsunami.html

[52] (2014) P2P. Dostopno na: http://www.techterms.com/definition/p2p

[53] (2014) How Ripple Works. Dostopno na: https://ripple.com/how-ripple-works/

[54] (2014) Gateway Integration Manual. Dostopno na: https://ripple.com/wiki/Gateway_Integration_Manual

[55] (2014) Gateways and Exchanges. Dostopno na: http://ripplefederation.org/business-listings

[56] (2014) Ripple Ledger. Dostopno na: https://ripple.com/devs/

[57] (2014) Ripple Transaction Format. Dostopno na: https://ripple.com/wiki/Transaction_Format

[58] (2014) Guide to Getting XRP and Activating Ripple Account. Dostopno na: https://ripple.com/guide-to-getting-xrp-and-activating-your-ripple-account/

[59] (2014) Introducing Ripple. Dostopno na: http://bitcoinmagazine.com/3506/introducing-ripple/

[60] J. Davidson, M. Naveed, *The Digital Coin Revolution – Cryptocurrency*, Massachusetts: JD-Biz Corp, 2014, pogl. 1.

[61] (2014) What is Cryptocurrency. Dostopno na: https://upbit.org/en/what-is-it/

[62] (2014) Bitcoin P2P e-cash paper. Dostopno na: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

[63] (2014) Satoshi Nakamoto. Dostopno na: https://en.bitcoin.it/wiki/Satoshi_Nakamoto

[64] (2014) Detecting Double Spending. Dostopno na: http://finney.org/~hal/chcash2.html

[65] (2014) B-money Proposal. Dostopno na: https://en.bitcoin.it/wiki/B-money_Proposal

[66] (2014) Bitcoin Alternatives. Dostopno na: http://electronician.hubpages.com/hub/Bitcoin-Alternatives-The-Best-Cryptocurrencies-to-Invest-In-for-2014

[67] (2014) Alternative Cryptocurrencies. Dostopno na: https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies

[68] (2014) Block Hashing Algorithm. Dostopno na: https://litecoin.info/Block_hashing_algorithm

[69] (2014) Currencies. Dostopno na: https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies#Namecoin_.28NMC.29

[70] (2014) Namecoins and .bit Domains. Dostopno na: http://www.coindesk.com/what-are-namecoins-and-bit-domains/

[71] (2014) Bitcoin Block. Dostopno na: https://en.bitcoin.it/wiki/Block

[72] (2014) Sending Payments. Dostopno na: https://en.bitcoin.it/wiki/Introduction#Sending_payments

[73] (2014) Litecoin. Dostopno na: https://litecoin.info/Litecoin

[74] (2014) Proof of Stake. Dostopno na: https://en.bitcoin.it/wiki/Proof_of_Stake

[75] (2014) Mining Hardware Comparison. Dostopno na: https://en.bitcoin.it/wiki/Mining_hardware_comparison

[76] (2014) Mining. Dostopno na: https://en.bitcoin.it/wiki/Mining

[77] (2014) Mining Litecoin and other Altcoins. Dostopno na: http://www.coindesk.com/information/how-to-mine-litecoin/

[78] (2014) Comparison Between Litecoin and Bitcoin. Dostopno na: https://litecoin.info/Comparison_between_Litecoin_and_Bitcoin

[79] (2014) Bitcoin Target. Dostopno na: https://en.bitcoin.it/wiki/Target

[80] (2014) Litecoin Target. Dostopno na: https://litecoin.info/Target

[81] (2014) Hashcash. Dostopno na: https://en.bitcoin.it/wiki/Hashcash

[82] (2014) Preventing double-spending. Dostopno na: https://en.bitcoin.it/wiki/Introduction#Sending_payments

[83] (2014) Zgodovina transakcij. Dostopno na: https://blockchain.info/sl

[84] (2014) Bitcoind. Dostopno na: https://en.bitcoin.it/wiki/Bitcoind

[85] (2014) Coinbase API. Dostopno na: http://www.thebitcoinchannel.com/archives/tag/api

[86] (2014) Bitstamp PHP API. Dostopno na: https://github.com/conejoninja/bitstamp-php-api/blob/master/BitStampAPI.php

[87] (2014) cURL. Dostopno na: http://curl.haxx.se/

[88] (2014) Technical Background of Version 1 Bitcoin Addresses. Dostopno na: https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

[89] (2014) Confirmation. Dostopno na: https://en.bitcoin.it/wiki/Confirmation

[90] (2014) Bitcoin Fees. Dostopno na: http://bitcoinfees.com/

[91] (2014) Bitcoin Protocol Specification. Dostopno na: https://en.bitcoin.it/wiki/Protocol_specification

[92] (2014) Comparison of Online Payment Methods. Dostopno na: https://blockchain.info/sl/wallet/paypal-vs-bitcoin

[93] (2014) PayPal Fees. Dostopno na: https://www.paypal.com/webapps/mpp/paypal-fees

[94] (2014) Transaction Fee. Dostopno na: https://multibit.org/en/help/v0.5/help_whatIsTheTransactionFee.html

[95] (2014) BitPay Features and Pricing. Dostopno na: https://bitpay.com/pricing

[96] (2014) PayPal Classic APIs. Dostopno na: https://developer.paypal.com/docs/classic/api/gs_PayPalAPIs/#requestType