Bitcoin kao oblik digitalne valute i elektroničkog plaćanja

Šimić, Ivana

LIBERTAS MEĐUNARODNO SVEUČILIŠTE

ZAGREB

IVANA ŠIMIĆ

SPECIJALISTIČKI DIPLOMSKI RAD

BITCOIN KAO OBLIK DIGITALNE VALUTE I ELEKTRONIČKOG PLAĆANJA

Zagreb, veljača 2017

LIBERTAS MEĐUNARODNO SVEUČILIŠTE

ZAGREB

SPECIJALISTIČKI DIPLOMSKI STUDIJ

MENADŽMENT FINANCIJA, BANKARSTVA I OSIGURANJA

BITCOIN KAO OBLIK DIGITALNE VALUTE I ELETRONIČKOG PLAĆANJA

KANDIDAT: **IVANA ŠIMIĆ**

MENTOR: **ZVONKO AGIČIĆ**

Zagreb, veljača 2017.

Sadržaj

Sažetak

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

Ključne riječi: Bitcoin, kriptovaluta, adresa, blok-lanac, transakcija

Abstract

Bitcoin is a digital store of value and payment system which was launched by Satoshi Nakamoto. It was announced in 2008 and released as an open-source software in 2009. The system is peer-to-peer which mean users it can make transactions directly without a need for an intermediator. Transactions are verified by network nodes and recorded in a public distributed ledger called blockchain. The ledger uses its own unit, also called bitcoin. Bitcoin is not controlled by central banks, state institutions or corporations. Bitcoin is often called the first cryptocurrency, although prior systems existed as such. Bitcoin is more correctly described as the first decentralized digital currency and it is the largest of its kind in terms of total market value.

Keywords: Bitcoin, cryptocurrency, address, blockchain, transaction

Uvod

Digitalni novac se pojavio u devedesetim godinama prošlog stoljeća u računalnim igrama, a najpoznatiji primjer je Linden Dollar iz igrice Second Life koji postoji od 2003. god. i funkcionira kao prava valuta i ima mogućnost zamjene za nedigitalne valute kao što su dolar ili euro.

Bitcoin je prvi oblik digitalnog novca koji za prijenos vrijednosti koristi kriptografske algoritme. Npr. Bitcoin adrese (engl. address) je niz od 27-34 brojeva i slova koji označava određenu količinu Bitcoina, otprilike kao broj računa u banci. Kreiraju se iz privatnog ključa[1] temeljem asimetrične kriptografije. Nadalje, sve Bitcoin transakcije uključuju digitalne potpise, što je također metoda iz područja kriptografije. Digitalne valute koje su postojale prije Bitcoina nisu koristile kriptografiju na ovaj način. Svi algoritmi koje Bitcoin mreža koristi za funkcioniranje uključuju neki oblik kriptografije te se za Bitcoin kaže da je prva kriptografska valuta ili kriptovaluta.

Nakon što je Bitcoin dobio na popularnosti pojavile su se mnoge kopije ove digitalne valute. Zajedničko svim tim kopijama je da u svojoj biti sadrže kriptografske algoritme, te stoga kopije Bitcoina također nazivamo kriptovalutama. Neke od aktivnih kriptovaluta su: Bitcoin, Ethereum, Ripple, Litecoin, Ethereum Classic i Monero.

Otac kriptografije smatra se Japanac Satoshi Nakamoto koji je početkom 2009. god. pustio u uporabu prvi puta Bitcoin. Bitcoin je bio zamišljen kao sigurna valuta, a za njegovu sigurnost bi se brinuli jedinstveni potpisi koji bi bili ugrađeni u softver kroz sistem slagalice. Na taj način bi se eliminirale banke, kartična plaćanja i različite financijske usluge. U veljači 2010. god. otvoreno je prvo Bitcoin tržište, a u travnju 2011. god. Nakamoto je prepustio kodove za programiranje jednom od svojih ljudi iz tehničke podrške i povukao se. Mnogo se nagađa o samom identitetu Nakamota, neki pretpostavljaju da je u pozadini cijele priče grupa Japanskih inženjera, drugi pak misle da je to tajna ženska vladina organizacija itd.

Kako uistinu funkcionira Bitcoin? Bitcoin je elektronski novac, ne novac pohranjen elektronski i tu je glavna razlika. Sistem generira fiksni broj Bitcoina po satu – prema prognozama zadnji Bitcoin bi trebao bit kreiran 2140. god., ako se sistem bude održao tako dugo. Dakle, cijela kompjutorska mreža i sve što se oslanja na sami softver u njegovoj konačnici se naziva blok-lanac (Block Chain).

Što je zapravo Bitcoin? Najlakše ga možemo vizualizirati kao žeton – ₿ simbol

[1] Privatni ključ neke adrese posjeduje samo osoba koja je tu adresu izračunala.

Budući da je digitalan, može se razdvojiti u najmanje djeliće Bitcoina, čak na 8 decimalnih brojeva: 0,00000001.

Kao što se i svaka druga valuta može podijeliti na manje dijelove, tako i Bitcoin možemo podijeliti kao što prikazuje Tabela 1.

Tabela 1. Podjela Bitcoina na manje dijelove

1 BTC	a bitcoin
0,01 BTC	a bitcent
0,001 BTC	an mbit
0,000 001 BTC	a ubit
0,000 000 01 BTC	a satoshi

Izvor: Understanding Bitcoin (2015)

Predmet i cilj rada

Predmet ovog rada je definicija digitalnog novca i Bitcoina kao dijela platne mreže. Digitalne valute su već dugo dio internet svijeta i poslovanja i rad se bavi pojmovima i analizom koliko je Bitcoin zastupljen kao takav. Problematika ovog rada se bavi time da li je Bitcoin kao dio virtualnog svijeta prihvatljiv za korisnika i koje su prednosti i nedostaci rukovanja istim. Budući da je još uvijek smatran fiktivnim i fizički neopipljivim, može li on zaista zamijeniti dosadašnji pojam novca. Napretkom tehnologije pojavili su se i novi načini plaćanja usluga i dobara pa stoga će se u radu pokušati približiti značenje same digitalne valute.
Cilj ovog rada je objasniti ključne pojmove vezane uz Bitcoin i njegove glavne karakteristike od kojih je najvažnija ta da njegovi korisnici mogu trgovati izravno i bez posrednika uz neznatnu proviziju na način da se eliminiraju banke, kartična plaćanja i različite financijske usluge.

Istraživačka pitanja

U ovom radu pokušat će se dati odgovori na sljedeća pitanja:

1. Koliko je realno da će digitalne valute uistinu zamijeniti standardan novac?
2. Može li Bitcoin naći svoje mjesto kao segment financijskog tržišta u smislu transfera novca?
3. Koliko su investicije u kriptovalute sigurno utočište za čuvanje vrijednosti novca?

1. Elektronički novac

Nagli razvoj interneta je pokrenuo elektroničko trgovanje. Također, doveo je i do razvoja nekih novih oblika imovine, od kojih je svakako najviše pozornosti privukao elektronički novac. Taj pojam se odnosi na sustave plaćanja u realnome i virtualnom svijetu ciji je cilj unaprijediti efikasnost postojećih sustava plaćanja i zamijeniti novčanice i kovanice u maloprodajnim transakcijama.

Elektronički novac jedan je od načina plaćanja na internetu, on je zamjena za gotovinu te samo plaćanje elektroničkim novcem podsjeća na obično plaćanje gotovinom.

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

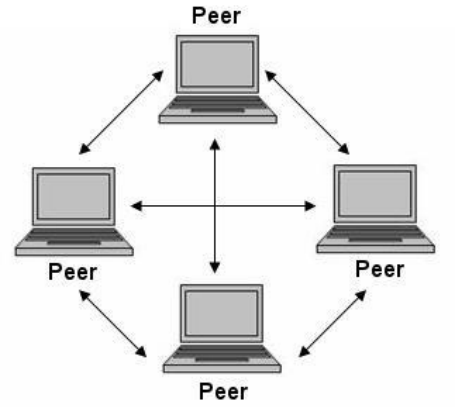
U Zakonu o elektroničkom novcu (NN, br. 139/2010.) dana je sljedeća definicija: elektronički novac jest elektronički, uključujući i magnetski, pohranjena novčana vrijednost koja je izdana nakon primitka novčanih sredstava u svrhu izvršavanja platnih transakcija u smislu zakona kojim se ureduje platni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

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

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

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

Slika 1: Peer to peer sustav



Izvor: Understanding Bitcoin (2015)

Peer to peer sustavi (skraćeno P2P) sastoje se od međusobno povezanih čvorova koji se mogu samostalno organizirati u mrežu sa svrhom dijeljenja raspoloživih resursa kao što su korisnički podatci, procesorsko vrijeme, kapacitet za pohranu podataka ili mrežna propusnost, te koji se mogu samostalno adaptirati na ispade funkcionalnosti i nepredvidive dolaske i odlaske čvorova na mreži, uz zadržavanje prihvatljive razine spojenosti i performansi bez potrebe za nadzorom, kontrolom i podrškom iz jednog središnjeg mjesta.

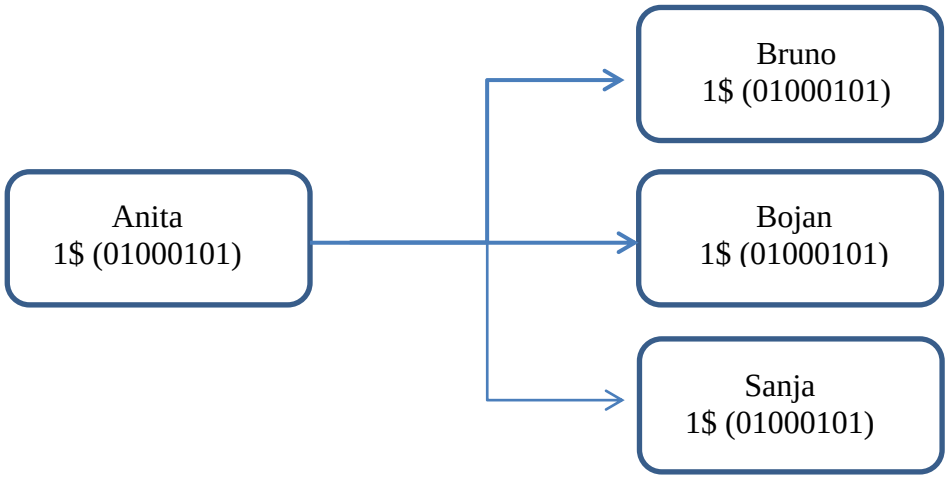
Na Slici 1. može se vidjeti prikaz jednostavnog peer to peer sustava. Uočljivo je da je komunikacija između čvorova izravna (nema poslužitelja). Također, možemo vidjeti i da je svaki čvor ravnopravan i neovisan. Jedan od najznačajnih primjera korištenja peer to peer sustava su digitalne valute, odnosno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

2. Nastajanje Bitcoina

2.1. Centralizirana baza

Najjednostavniji način kako kreirati digitalnu valutu jest prvo odrediti njenu vrijednost prema nizu brojeva nula i jedinica. Problem sa ovakvim pristupom je što je takav digitalan niz vrlo lako kopirati bez gotovo ikakvih troškova. To vodi do problema duple prodaje valute kao što je objašnjeno u Slici 2. Pretpostavimo da Anita ima digitalnu valutu koja ima binarni broj 01000101. Anita ju želi proslijediti Bruni i to će napraviti na način da će mu poslati poruku sa gore spomenutim binarnim brojem. Problem je što Anitu ništa ne sprječava da isti kod ne pošalje drugom korisniku ili njima više istovremeno, te tako Anita proda istu valutu više puta. Dolazimo do zaključka da digitalna valuta ne može sadržavati samo niz brojeva budući da je taj niz lako replicirati više puta i kao takav nema vrijednost.

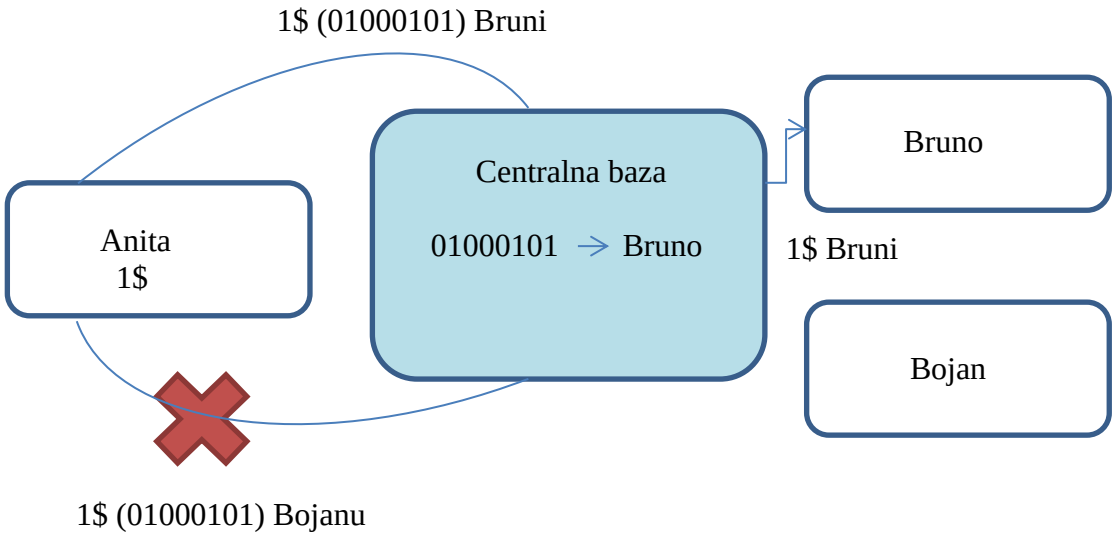
Slika 2. Problem duple potrošnje



Izvor: sistematizacija autora

Kako bi se doskočilo tom problemu kreirana je centralna baza podataka sa listom svih korisnika i njihovim digitalnim valutama koje posjeduju.

Slika 3. Centralna baza podataka



Izvor: sistematizacija autora

Anita, kako bi prodala svoju digitalnu valutu, sada mora poslati zahtjev serveru sa centralnom bazom podataka koji radi transfer valute direktno Bruni. Server sam radi nadogradnju sustava i sada ta valuta pripada Bruni. Ukoliko bi Anita pokušala prodati istu valutu ovaj put Bojanu, server bi automatski odbio jer bi prepoznao da ta valuta sa šifrom 01000101 pripada Bruni i ne bi bila autorizirana za prodaju.

Centralna baza podataka rješava problem sa duplom prodajom valute, ali uz uvjet da su svi korisnici registrirani. Tako centralna baza sadrži podatke o identitetu korisnika te njihovu financijsku povijest trgovanja sa valutama[2], ali je isto tako laka meta za hakere. Ako netko od hakera uspije doći do same baze može promijeniti vlasništvo nad bilo kojom digitalnom valutom i ukrasti ju od pravog vlasnika. Vjerovatno glavna mana baze je što i najmanji kvar na sistemu može prouzrokovati gašenje i „pad“ baze podataka, no s vremenom sistem je postao elastičniji i bolje zaštićen od napada hakera.

2.2. Adrese i transakcije

Bitcoin mreža predstavlja decentraliziranu glavnu knjigu korisnika i informacije o stanju sredstava na korisničkim računima i prepoznaje svoje korisnike pomoću kombinacije brojki i

[2] Centralna baza podataka sadrži podatke koji nisu javni i dostupni te se koriste samo u svrhe trgovanja digitalnim valutama.

slova kao npr. „14nvuksgGnjjlhs8Rno“. Ova kombinacija predstavlja adresu javno-privatnog kriptografskog ključa[3], ali privatni dio ključa je uvijek pod kontrolom njegova korisnika.

Slika 3. prikazuje kako korisnica (Anita) šalje sredstva drugom korisniku (Bruni): Anita koristi svoj privatni ključ za poruku „Želim proslijediti jedan svoj Bitcoin korisniku 1gr6U6…“ koju zaprima glavni server. Možemo primjetiti da Anita ne identificira samog korisnika već navodi samo adresu na koju šalje sredstva tako da možemo lako zaključiti da je Anita zaprimila adresu nekim drugim kanalom kao što je email itd.

Prilikom zaprimanja Anitinog zahtjeva za transakciju, pristupna točka u mreži mora verificirati:

- ispravan potpis tj. istinite korisničke podatke
- dovoljan broj sredstava koji se žele prebaciti sa korisničkog računa; ako na korisničkom računu nema dovoljno sredstava koje se žele prebaciti na drugi račun, transakcija neće biti potvrđena
- nadograditi bazu podataka sa novim stanjem oba korisnika.

Kao što smo napomenuli, Bitcoin mreža predstavlja decentraliziranu mrežu transakcija što je ujedno i glavna razlika u odnosu na npr. bankovne transakcije koje imaju centraliziranu mrežu i koje bivaju kontrolirane.

2.3. Različita značenja Bitcoina

Bitcoin je višeznačna riječ koje može značiti više toga:

- Protokol – specifikacija kako konstruirati distribucijsku mrežu podataka (blok-lanac); kako ju raščlaniti; kako transakcije trebaju biti obavljene; što se podrazumijeva pod valjanom transakcijom itd.
- Mreža podataka – mreža gdje se 2 korisnika povezuju u jednoj pristupnoj točki; korisnici izmjenjuju informacije i sredstva u pristupnoj točki i tako se kreiraju nove transakcije koje pridonose kreiranju i nadogradnji mreže podataka
- Valuta – Bitcoin se označava sa malim slovom „b“ i predstavlja jedinicu za tu valutu u cijeloj Bitcoin mreži
- Otvoreni projekt – projekt otvorenog tipa u koji se još uvode procedure; projekt je nedavno rebrandiran pod nazivom Bitcoin Core da se izbjegne eventualna zabuna oko samog značenja Bitcoina

[3] Bitcoin adrese su zapravo privatni ključevi, ali su izvedeni iz javnih ključeva.

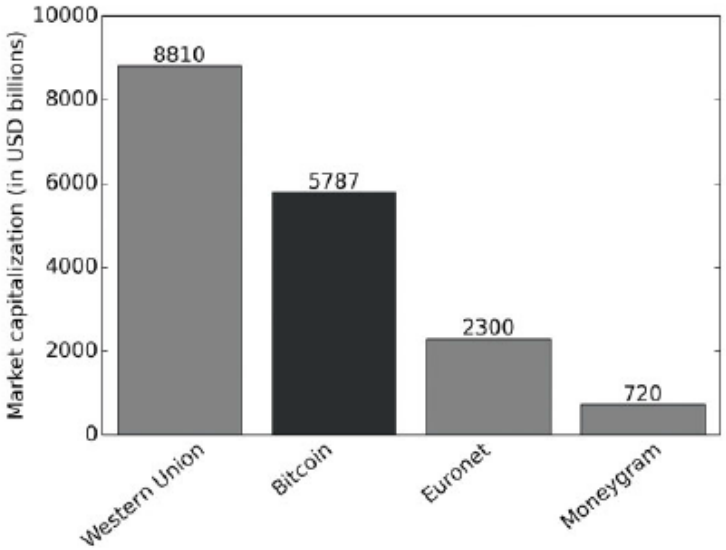
3. Uporaba Bitcoina

3.1. Transfer novca

Prosječna naknada za standardno slanje novca se kreće u rasponu 8% - 9%, dok trenutna naknada za Bitcoin plaćanje iznosi 0,01% do 0,05%. Iz toga možemo jednostavno zaključiti da Bitcoin ima prednost u odnosu na ostale načine transfera novca, ali svejedno postoji par činjenica koje ipak osporavaju ovu prednost:

- Sve pravne osobe koje se bave transmisijom novca su obavezne plaćati državne regulative te su na kraju troškovi plaćeni od strane konzumenata usluge; nove tvrtke koje bi omogućavale transfer novca samo u Bitcoinu bi se s vremenom suočile sa istim problemom
- Barijere koje otežavaju ulazak na tržište transfera novca kao što su npr. banke koje izdvajaju određene iznose vezane za troškove protiv pranja novca itd.
- Troškovi transakcija za Bitcoin su podložni rastu kako naknade za kreiranje blokova padaju u blok-lancu[4]
- Tržišta koja su tek u razvitku nemaju pristup svim tehničkim sredstvima kao ostala tržišta pa samim time im je ograničeno korištenje Bitcoina ili drugih kriptovaluta
- Slaba likvidnost bi utjecala na troškove konverzije Bitcoina u domicilnu valutu

Grafikon 1. Tržišna kapitalizacija Bitcoina



Izvor: Understanding Bitcoin (2015)

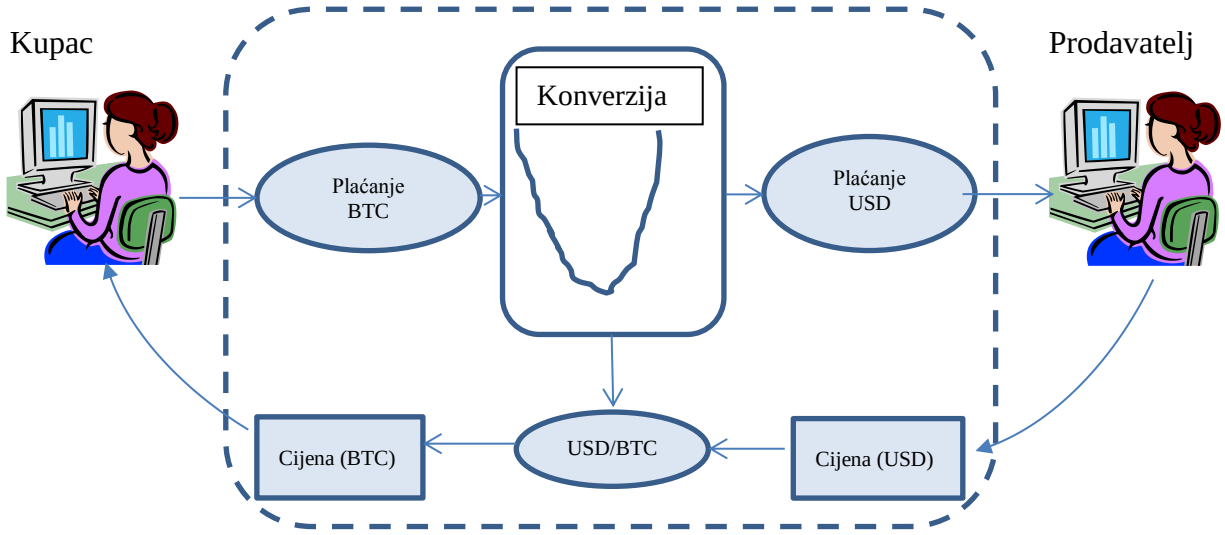
[4] Naknade su dodijeljene programerima koji „skladište“ podatke (blokove) i njihovi su vlasnici

Grafikon 1. pokazuje komparaciju tržišne kapitalizacije najvećih tvrtki za transfer novca u usporedbi sa Bitcoinom. Još uvijek je otvoreno pitanje bi li Bitcoin našao mjesto na ovoj ljestvici u odnosu na pritisak konkurencije i da li bi ta tehnologija bila održiva.

3.2. Način i obrada plaćanja

Postoje već razrađeni načini plaćanja koji omogućavaju prodavatelju određenih dobara prihvaćanje Bitcoina kao valutu.

Slika 4. Način plaćanja Bitcoina i USD



Izvor: sistematizacija autora

Slika 4. prikazuje proces razmjene između prodavatelja i kupca gdje prodavatelj navodi cijenu svoje usluge ili proizvoda u USD i ta cijena je konvertirana u odgovarajući broj Bitcoina uzimajući u obzir neki tečaj koji je isto tako prezentiran kupcu. Kupac plaća u Bitcoinima, a pri tom se odmah vrši konverzija u USD i prodavatelju dolazi novac u USD. Budući da je vrijeme same transakcije nekoliko minuta, a samim time i konverzija traje toliko, eventualna tečajna razlika je vrlo mala. Trošak transakcije iznosi oko 1%, što je znatno povoljnije nego 2% ili 3% koliko iznose standardne metode prijenosa novca kao što su kreditne kartice ili sl. Bitcoin transakcije su ipak zanemarene u odnosu na druge metode plaćanja i prilično su u nezavidnom položaju kada je riječ o konkurentnosti. Monopol kartičnih kuća, regulative Know Your Customer (KYC) i Anti-Money Laundering (AML) te klasične metode

plaćanja/financiranja itekako sprječavaju da plaćanje Bitcoinom bude zanimljivije korisnicima.

3.3. Bankomati

Bankomati za Bitcoin omogućavaju korisniku da na njemu i prodaju i kupuju Bitcoin u samo nekoliko jednostavnih koraka. Prvo se korisnik identificira i zatim bankomat provjerava identitet kao što kod običnih bankomata funkcionira za PIN-om. Tada korisnik odabire funkciju koju želi, kupnja ili prodaja, i skenira svoj QR kod koji je generiran aplikacijom za „novčanik“ na svom pametnom telefonu (ili može biti direktno isprintan na bankomatu). Većina bankomata zahtjeva da se korisnik identificira svojom osobnom iskaznicom ili vozačkom dozvolom.

Tečaj po kojem se trguje sa Bitcoinima je najčešće onaj koji je valjan za taj dan, a operateri na bankomatima uzimaju proviziju između 3% i 7%.

U Republici Hrvatskoj postoje trenutno 4 dvosmjerna bankomata (Zagreb, Split i Rijeka) za kupnju i prodaju, a isplata je moguća samo u kunama.

Slika 5. Prvi Bitcoin bankomat u Republici Hrvatskoj

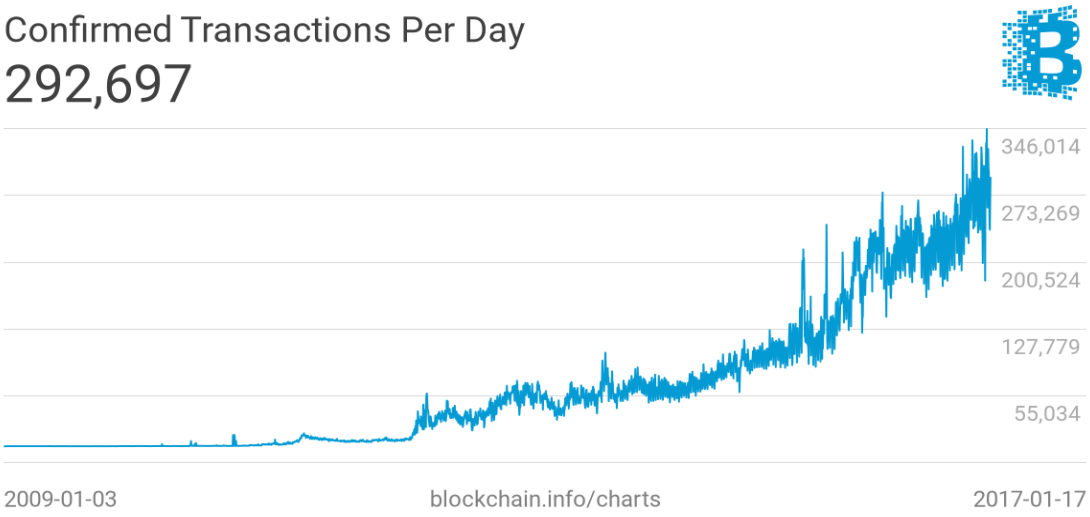
Izvor: crobitcoin.com

4. Ekonomsko značenje

4.1. Medij razmjene

Kao medij razmjene Bitcoin je prihvaćen u poslovnom svijetu, iako njegovi protivnici tvrde da on ne bi mogao nikada zamijeniti klasičan način plaćanja.

Grafikon 2. Dnevne transakcije Bitcoina



Izvor: blockchain.info

Na Grafikonu 2. je vidljiv lagan porast broja transakcija po danu, ali brojka manja od 500.000 transakcija je smatrana još uvijek niska u odnosu na ostale načine plaćanja. Većina ekonomista se slaže da Bitcoin još uvijek ima malu bazu korisnika i uvjet da postane prihvatljiv način plaćanja jest da dosegne kritičnu masu. Kritična masa je točka gdje profit novih korisnika premašuju troškove usvajanja novih tehnologija. Za neke tehnologije kao što su digitalne valute, profit novih korisnika raste, kako raste i broj ostalih korisnika koji su usvojili te tehnologije jer je puno veća mogućnost plaćanja u toj valuti. Taj pojam je već ranije poznat kao efekt umrežavanja. Kada određena tehnologija dosegne točku kritične mase i premaši ju, tada možemo reći da je ona usvojena.

Kritičari Bitcoina podsjećaju da u slučaju kada bi netko od internetskih giganata za trgovinu uveo infrastrukturu digitalnog plaćanja, to bi dovelo do hipotetskog natjecanja između Bitcoina i standardnih načina plaćanja gdje bi Bitcoin, kao relativno otvoreni projekt, se morao natjecati sa kartičnim tvrtkama koje imaju veliki financijski budžet. Kada bi rezultat tog natjecanja išao u korist jednoj od tih kuća, ekonomska teorija kaže da bi Bitcoin (ili bilo koja druga kriptovaluta) bile potisnute sa tržišta trgovanja valutama. Isto tako, kritičari naglašavaju da se Bitcoin ne bi mogao natjecati sa ostalim načinima plaćanja zbog troškova programera koji održavaju blok-lanac infrastrukturu. Naknada koju primaju programeri varira između 1% i 5% te većina tih prihoda (više od 99%) dolazi od izdavanja novih Bitcoina, samo mali dio dolazi iz troškova samih transakcija koje plaćaju korisnici. U slučaju kada bi naknade programerima bile smanjene, morale bi se pokriti iz transakcijskih troškova što bi dovelo do izjednačavanja sa današnjim plaćanjima putem kreditnih kartica (ako bi naknade programerima ostale iste).

4.2. Za i protiv

Što se tiče prednosti koje plaćanje Bitcoinom čini izdvojenim od ostalih možemo istaknuti da je takav način plaćanja dobara i usluga sigurniji od ostalih u smislu da prodavatelj nije ugrožen i relativno siguran da će određena usluga biti plaćena jer se plaćanje vrši promtno. Transakcijski troškovi su isto tako puno niži nego kod kreditnih kartica i omogućava mikro plaćanja za npr. novine i sl. Bitcoin i slične tehnologije plaćanja omogućavaju transfer bilo kakve imovine u digitalnu imovinu. Također Bitcoin radi na principu "push" plaćanja, slično kao gotovina, gdje korisnik proaktivno generira plaćanje dok npr. kreditne kartice rade na osnovi "pull" plaćanja gdje se prodavatelj autorizira (često zahtjeva upisivanje osjetljivih informacija) da povuče sredstva sa korisnikovog računa. Plaćanja Bitcoinom mogu više ili manje anonimna u odnosu na tradicionalne načine plaćanja (pod anonimnošću se misli korištenje pseudonima) i kao novi način plaćanja, neovisan o tradicionalnom financijskom sektoru, može pružiti neovisnost u slučaju financijske krize.

Nedostaci koje možemo navesti kao glavne u ovom trenutku su te što se dosta korisnika Bitcoina služi različitim posrednicima koji uživaju njihovo povjerenje zbog toga što su obeshrabreni novim tehnologijama plaćanja. Nove tehnologije su uglavnom zastupljene u tvrtkama koje se njima služe pa prema tome nema značajnijih pomaka u smanjenju troškova. Isto tako, Bitcoin je nelikvidan u odnosu na svjetske vodeće valute kada uspoređujemo EUR vs. USD ili GBP vs. USD. Tome možemo dodati da ne nudi kreditnu opciju kao kreditne

kartice gdje je to već ugrađeno kao mogućnost unaprijed, ali isto tako se radi na tome da i Bitcoin nudi takvu opciju putem web novčanika. Klasifikacijom Bitcoina kao kapitalne imovine nailazi se na problem eventualnog oporezivanja i ostalih troškova koje bi ga kao takvog snašle. Proces plaćanja traje nekoliko minuta što je vrlo nezgodno ako plaćamo digitalnom valutom u trgovačkom centru na kasi – transakcija mora biti potvrđena od strane centralnog servera, ali uvođenjem već spomenutog web novčanika tom problemu bi se moglo doskočiti. Također bi se i sama državna vlast mogla uplesti na način za izdavanjem određene kriptovalute koja bi bila u potpunosti otkupljiva za domicilnu valutu. U tom slučaju svi bi bili u mogućnosti zamijeniti digitalnu valutu za valutu države u kojoj žive ostavljajući kriptovalutu iza sebe.

4.3. Bitcoin kao ulaganje/investicija

Ulaganja Bitcoina u male start-up kompanije klasificira takva investiranja u visokorizična, rizičnija nego u ostale oblike ulaganja. Jedna od prednosti ulaganja u Bitcoin je to što je Bitcoin jednostavan za korištenje i dostupan svakome tko želi investirati, ali i to što je nekonkurentan na tržištu kao takav.

"Bitcoin start-up" je novi način plaćanja koji je povezan sa točno određenim proizvodima i u tom slučaju Bitcoin je sredstvo koje daje pristup tom sustavu plaćanja. Što više start-up tvrtki koristi takav način financiranja, to je veća vrijednost Bitcoina. Kako se tržište Bitcoina razvija, tako i njegovi korisnici mogu birati hoće li ih koristiti kao sredstvo transakcije ili špekulirati o njihovoj vrijednosti u toj start-up tvrtki. Kod novih start-up tvrtki uvijek postoji mogućnost da će vrijednost Bitcoina rasti do određenog iznosa, ali i da će pasti pa će tako i vrijednost investicije biti jednaka 0. Neki od razloga za ovu drugu mogućnost bi bili: pokušaj hakiranja, konkurentske kriptovalute (alt-coin, meta-coin…), nestanak električne energije i neumreženost.

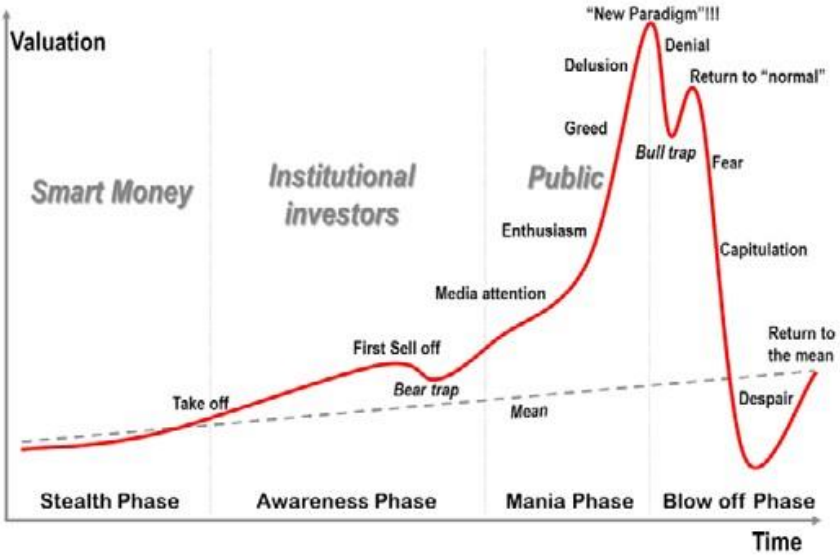
4.4. Razvoj i tehnička analiza

Značajniji razvoj Bitcoina počinje u 2011. godini kada je zabilježen prvi već porast vrijednosti na oko 30 $. U fazi uzleta najveća pozornost na Bitcoin bila je usmjerena za vrijeme ciparske financijske krize 2013. godine, kada je vrijednost jednog Bitcoina premašila 250 $. Tijekom navedenog razdoblja naglo su se povećali broj korisnika i broj transakcija te su nastale prve online mjenjačnice. Također, sve je više poduzeća počelo prihvaćati Bitcoin kao sredstvo plaćanja, a kada ga je prihvatio i jedan od najvećih kineskih internetskih giganata

došlo je do naglog rasta cijene. Potom je i u Kini otvorena prva Bitcoin mjenjačnica, koja je po ostvarenom prometu bila veća od do tada najpopularnije japanske Mt. Gox i europskog Bitstampa. U istom razdoblju u Kanadi je postavljen prvi Bitcoin bankomat. U studenom 2013. godine Bitcoin je priznat kao legitimno sredstvo plaćanja u SAD-u, što uzrokuje rast do 1.099 $. Činilo se da je Bitcoin na putu da postane globalna zamjena za valute koje su regulirale monetarne vlasti. Činilo se i da će Bitcoin kao kriptovaluta koja nije pod utjecajima institucija biti sigurno utočište za čuvanje vrijednosti novca te da neće biti podložan inflaciji. Takva očekivanja stvorila su privid da će Bitcoin u budućnosti sve više dobivati na značaju te su postala generator porasta potražnje i rasta cijene. Tome treba pridodati špekulacije dijela neiskusnih ulagača koji su, potaknuti medijskim napisima, ulaganje u Bitcoin promatrali kao dobru investicijsku priliku.

Rast je zaustavljen odlukom centralne kineske banke iz prosinca 2013. godine kojom se zabranjuje upotreba Bitcoina u svim kineskim financijskim institucijama. Kineska odluka bila je povod, odnosno okidač koji je izazvao nagli pad vrijednosti Bitcoina ali nije bila i pravi uzrok njegovog daljnjeg pada. Uzrok pada vrijednosti Bitcoina leži u tome što se kod dotadašnjeg naglog porasta cijene radilo o pojavi poznatoj kao investicijski balon.

Grafikon 3. Faze investicijskog balona



Izvor: Rodrigue (2008)

Do postizanja maksimalne cijene od 1.099 $ činilo se da se ne vidi kraj rastu vrijednosti Bitcoina. To su trenuci kad je javnost postala upoznata s velikim porastom cijene i kad se buduća vrijednost Bitcoina ekstrapolirala na temelju povijesnih podataka. To je vrijeme kad javnost, privučena pažnjom medija, kupuje Bitcoin čime mu zbog priljeva novog kapitala još više povećava vrijednost. No ubrzo nakon toga počinje pad vrijednosti koji se uz manje oscilacije trajno nastavlja. Početkom veljače 2014. godine zabranjen je rad jedne od najpoznatijih Bitcoin mjenjačnica Mt. Gox zbog navodnih tehničkih problema. Nekoliko tjedana kasnije mjenjačnica je prijavila da je upad hakera u sustav uzrokovao gubitak od 850 tisuća Bitcoina, što je tada iznosilo oko 473 milijuna $. Korisnici mjenjačnice nisu vjerovali obrazloženju te su podigli tužbu protiv mjenjačnice, koja proglašava bankrot i prestaje s radom. Zatvaranje mjenjačnice uzrokovalo je daljnji pad vrijednosti Bitcoina do razine od oko 400 $.

Promatrajući broj prodanih Bitcoina može se zaključiti da je postojala stabilna kupnja sve do prvog značajnog porasta cijene. Tada se postiže maksimum od preko 668 tisuća prodanih Bitcoina, što se može povezati s razdobljem prve velike prodaje (engl. first sell off). Na Grafikonu 3. sljedeća velika prodaja Bitcoina nastaje u vrijeme njegove visoke cijene kad institucijski investitori izlaze iz pozicija i prodaju Bitcoin. Promatrajući Grafikon 3. može se uočiti velika sličnost kretanja cijene Bitcoina s uobičajenim kretanjima kod pojave investicijskih balona, što implicira potrebu za velikim investicijskim oprezom. Sve četiri faze klasičnog investicijskog balona te svih pet ključnih momenata (prva velika prodaja, nova svjetska neregulirana valuta kao „nova paradigma“, prvi veliki pad, kratkotrajni oporavak, duboki pad) jasno se mogu prepoznati na slici cijene Bitcoina. Tehnička analiza pokazuje kako je kod pada cijene najprije probijena zona potpore na 650 $ koja je zatim postala zona otpora. Kao nova zona potpore pojavila se razina cijene od 400 $, ali i ona je uskoro probijena te je postala nova zona otpora. Najnovija zona potpore uspostavljena je sredinom siječnja 2015. na 200 $ kad se trgovalo s preko 378 tisuća Bitcoina.

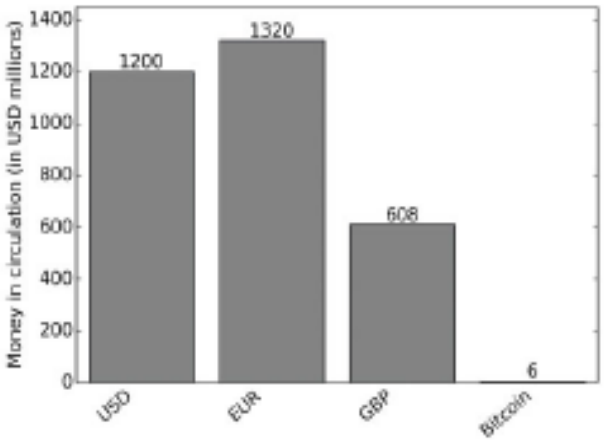
4.5. Efekt na financijsku i monetarnu politiku

Na ulazak u financijski sektor svakim danom je sve manje barijera pa tako je i Bitcoinu omogućen ulazak u tu sferu. Ulaskom Bitcoina na tržište novca mogao bi se promijeniti tempo inovacija, a financijske ustanove bile bi prisiljene mijenjati svoju infrastrukturu da bi dosegle razinu koju posjeduje "state-of-the-art" kriptografska tehnologija. Isto tako, jedan od

rizika za današnje financijske institucije je neposredovanje kod ulaganja, ako ulagač želi uložiti veća sredstva u obliku kriptografskih valuta.

Naime, pojavilo se pitanje da li je moguće zadržati obveze rezerve u obliku Bitcoina, kao što to npr. banke čine u slučaju depozita zadržavajući dio, a ostatak multipliciraju pomoću efekta multiplikatora.

Grafikon 4. Novac u optjecaju u odnosu na Bitcoin tržišnu kapitalizaciju



Izvor: Understanding Bitcoin (2015)

Monetarna baza Bitcoina je i dalje mala uspoređujući sa ostalim svjetskim valutama. Grafikon 4. prikazuje količinu novca u optjecaju za USD, EUR, GBP i BTC gdje se jasno vidi da Bitcoin ima premali utjecaj na monetarnu politiku.

Što se tiče same Kvantitativne Teorije Novca, pobornici Bitcoina tvrde da bi Bitcoin imao veliki efekt na nju i na monetarnu politiku.

Novac x Brzina Optjecaja Novca = Cijena x Transakcija

U ovom slučaju gdje bi Bitcoin utjecao na faktor brzine optjecaja novca, zbog svoje uporabe na tržištu, potreba za ulaganjima u današnjim valutama bi se smanjila. U konačnici, neki ekonomisti tvrde da Bitcoin, i generalno kriptovalute, bi mogli ojačati elastičnost ekonomije kreirajući alternativne načine plaćanja koji bi bili korisni u postojećim financijskim strukturama.

5. Kriptografija

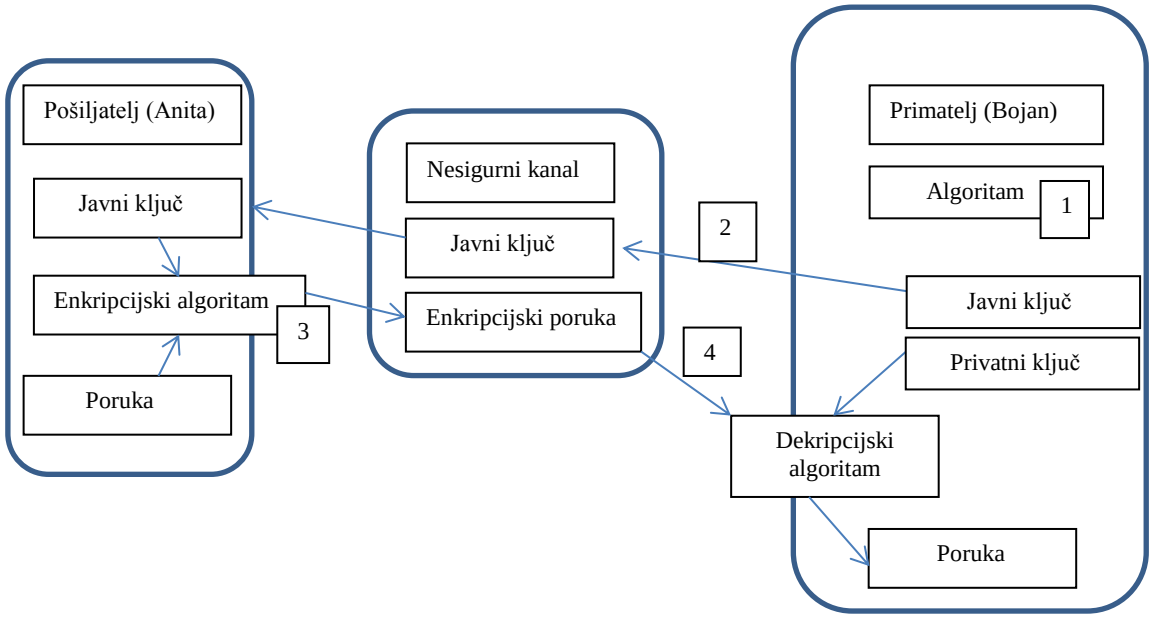
5.1. Enkripcija podataka – javni i privatni ključevi

Kriptografija javnog ključa se pojavila već 1970. god. Bitcoin ne koristi algoritme za enkripciju javnih ključeva, ali koristi nešto vrlo slično naziva digitalni potpis.

Kriptografija javnog ključa se razvila kao odgovor na slabu točku simetričke enkripcije[5] imena distribucijski ključ. Kada dvoje ljudi koristi simetričku enkripciju, moraju prije toga osigurati siguran kanal za komunikaciju, a internet ne pripada u ovom slučaju u sigurne kanale komunikacije. Prema tome, nemoguće je uspostaviti siguran način izmjene podataka tim putem i u tu svrhu je kreirana kriptografija javnog ključa. Simetrički ključ se može koristiti dvosmjerno, za zaključavanje (enkripciju) i otključavanje (dekripciju) šifriranih poruka. Jedan od ključeva, **javni ključ** se može koristiti za zaključavanje, dok drugi, **privatni ključ** se koristi za otključavanje.

Kako enkripcija javnog ključa rješava problem privatnosti? Bitno je da razumijemo da samo privatni ključ (ključ koji dešifrira poruku) mora ostati u tajnosti, a javni ključ može biti dostupan javnosti (ključ kojim zaključavamo poruku).

Slika 6. Enkripcija javnog ključa



Izvor: sistematizacija autora

[5] Klasična (simetrička) kriptografija je povezana sa enkripcijom podataka, a definira se kao dešifriranje poruke.

Slika 6. pokazuje kako enkripcija javnog ključa funkcionira u praksi. Prvo primatelj poruke (Bojan) generira par javnih i privatnih ključeva pomoću algoritama (1). Javni i privatni ključevi su tzv. par javno-privatnih ključeva i matematički su povezani. Svaki protokol koji se odnosi na javne ključeve ima i točno svoje određene algoritamske ključeve.

Primatelj (Bojan) šalje svoj javni ključ pošiljatelju (Anita) (2), ali svoj privatni ključ drži tajnim. Nakon primitka Bojanovog javnog ključa, Anita nastavlja sa procesom enkripcije koristeći Bojanov javni ključ (3) i rezultat je šifrirana poruka. Enkripcijska poruka je poslana Bojanu nesigurnim kanalom, u ovom slučaju (4). Haker koji eventualno uđe u trag komunikaciji može stopirati poruku između obje strane, ali ne može učiniti njenu dekripciju. Samo Bojan, koji ima odgovarajući par privatnih ključeva koji odgovara javnim, ima mogućnost enkripcije koristeći dekripcijske algoritme.

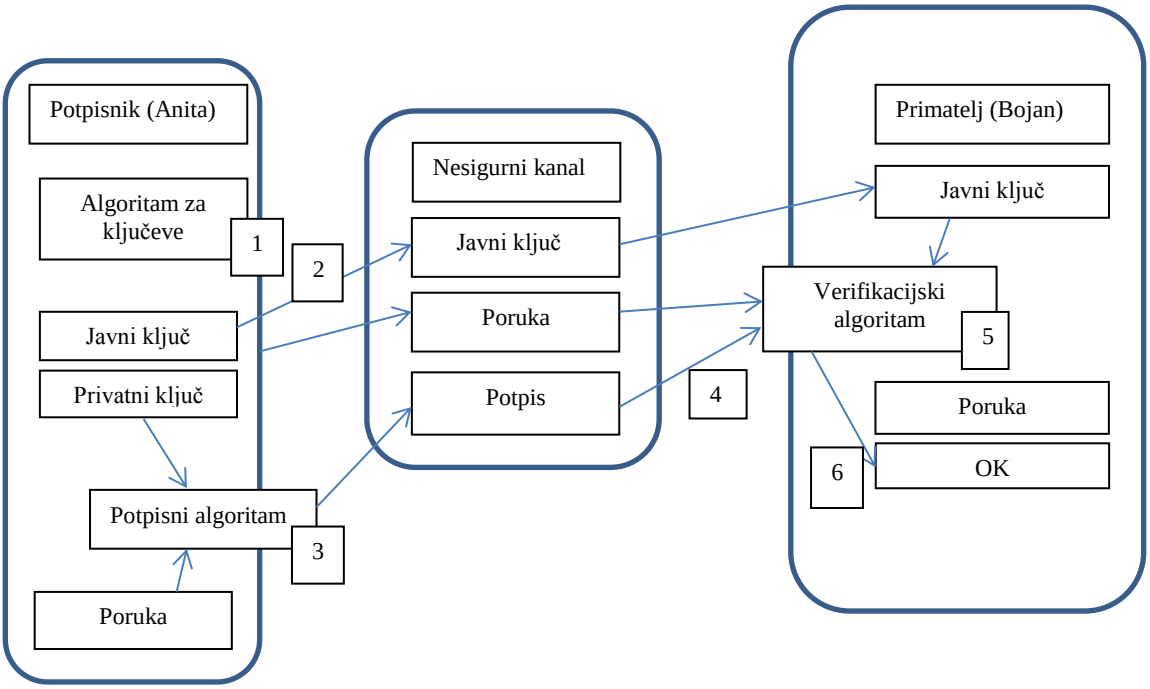
U ovoj shemi postoji problem nesigurnog kanala jer eventualni haker kontrolira komunikaciju. Haker može presresti poruku i promijeniti kod prije nego je primljena. Kako bi se to izbjeglo, postoji nekoliko načina koji se najčešće koriste kao što je npr. e-mail komunikacija te ostali kompjuterski programi (Pretty Good Privacy, Privacy Guard…) koji osiguravaju nesmetanu komunikaciju.

5.2. Digitalni potpis

Druga najpoznatija aplikacija koja se koristi u svijetu kriptografije je digitalni potpis. Cilj digitalnog potpisa je sličan ručnom potpisu, osigurati da poruka koja se prenosi od strane pošiljatelja nije mijenjana u međuvremenu i da se potpis nakon potpisivanja ne može povući natrag.

Digitalni potpisi su vrlo često korišteni u Bitcoin protokolu. Bitcoin adrese su zapravo javni ključevi koji su u korelaciji sa privatnim ključevima tj. Bitcoin adresama. Javni ključevi se mogu interpretirati kao brojevi bankovnog računa, a privatni ključevi kao potpisi koji daju pristup tim bankovnim računima.

Slika 7. Digitalni potpisi



Izvor: sistematizacija autora

Slika 7. prikazuje proces potpisivanja. Prvo, potpisnik (Anita) kreira par javno-privatnih ključeva koristeći algoritme za njihovu izradu (1). Anita šalje javni ključ putem komunikacijskog kanala (2)[6] i zatim koristi svoj privatni ključ za digitalni potpis poruke (3). Važno je da Anita zadrži privatni ključ za sebe. Kad je poruka potpisana, i poruka i potpis, su poslane primatelju (Bojan) (4). Trebamo napomenuti da poruka nije dešifrirana, samo potvrđena i tek tada Bojan provjerava potpis koristeći Anitin javni ključ. Ako verifikacija odgovara javnom ključu tada Bojan može biti siguran da ju je poslala Anita. U protivnom, može ju odbiti kao nevažeću.

Glavni oblici digitalnog potpisa koji se koriste su:

- RSA – baziran na RSA algoritmima i najčešće se koristi u praksi
- Schnorr potpis – najjednostavniji oblik potpisne sheme koji se koristi logaritmima i algoritmima eliptične krivulje
- Elgamal potpis – ne koristi se često u praksi
- DSA (Digital Signature Algorithm) – često se koristi u praksi jer je patentiran tako da se može koristiti besplatno.

[6] Komunikacijski kanal je nesiguran način komunikacije, ali Bitcoin nije meta u ovom slučaju jer je osiguran blok-lanac tehnologijom koja će biti objašnjena u nastavku.

Bitcoin u svojoj tehnologiji koristi algoritme eliptične krivulje i DSA oblik za digitalni potpis.

5.3. RSA

RSA algoritam moguće je koristiti za kriptiranje poruke i za njezino potpisivanje. Pošiljatelj poruku potpisuje pomoću vlastitog privatnog ključa, a kriptira korištenjem javnog ključa primatelja. Nakon primitka poruke primatelj dekriptiranje vrši pomoću vlastitog privatnog ključa , a provjera vjerodostojnosti potpisa provodi se uz korištenje potpisnikovog javnog ključa.

Algoritam se sastoji od sljedećih koraka:

a) stvaranje ključeva
b) potpisivanje poruke
c) kriptiranje poruke
d) dekriptiranje poruke
e) provjera vjerodostojnosti potpisa.

6. Transakcije

6.1. Kreiranje i provođenje

Bitcoin transakcije definiramo kao zapise u bazi podataka zvanoj blok-lanac u kojoj se određeni iznos Bitcoina prenosi sa jedne adrese (ili više njih) na drugu adresu (ili više njih). Važno je napomenuti da Bitcoin nije smješten i ne postoji kao takav u korisnikovom računalu. On je ulaz u bazu podataka – blok-lanac. U Bitcoin blok-lancu nisu pohranjeni računi ni iznosi, već samo transakcije.

Transakcije se sastoje od lista ulaznih (TxIn) i izlaznih (TxOut) transakcija. Transakcije su javne, transparentne i pseudoanonimne i nedvojbeno potvrđuju da je određena količina Bitcoina prenesena s jedne adrese na drugu.

Bitcoin novčanik omogućava svome vlasniku da kreira nove transakcije sa adrese koje pripadaju tom novčaniku. Obzirom da su transakcije javne, moguće ih je pratiti putem weba.

Svaka izlazna transakcija sadrži dva podatka: količinu novca i adresu primatelja. Adresa je izvedena iz javnog ključa te jedino vlasnik privatnog ključa može otključati sredstva pohranjena u izlaznu transakciju. Kako bi se otključala sredstva, vlasnik privatnog ključa mora potpisati transakciju kojom šalje sredstva na novu Bitcoin adresu.

Ulazna transakcija sadrži izvješće o prethodnoj ulaznoj transakciji i potpis koji dokazuje da primljena sredstva iz prethodne izlazne transakcije mogu trošiti. Potpis se mora napraviti pomoću privatnog ključa povezanog s javnim ključem u Bitcoin adresi. Ako se potpis ne poklapa, transakcija se smatra nevažećom i mreža ju odbacuje.

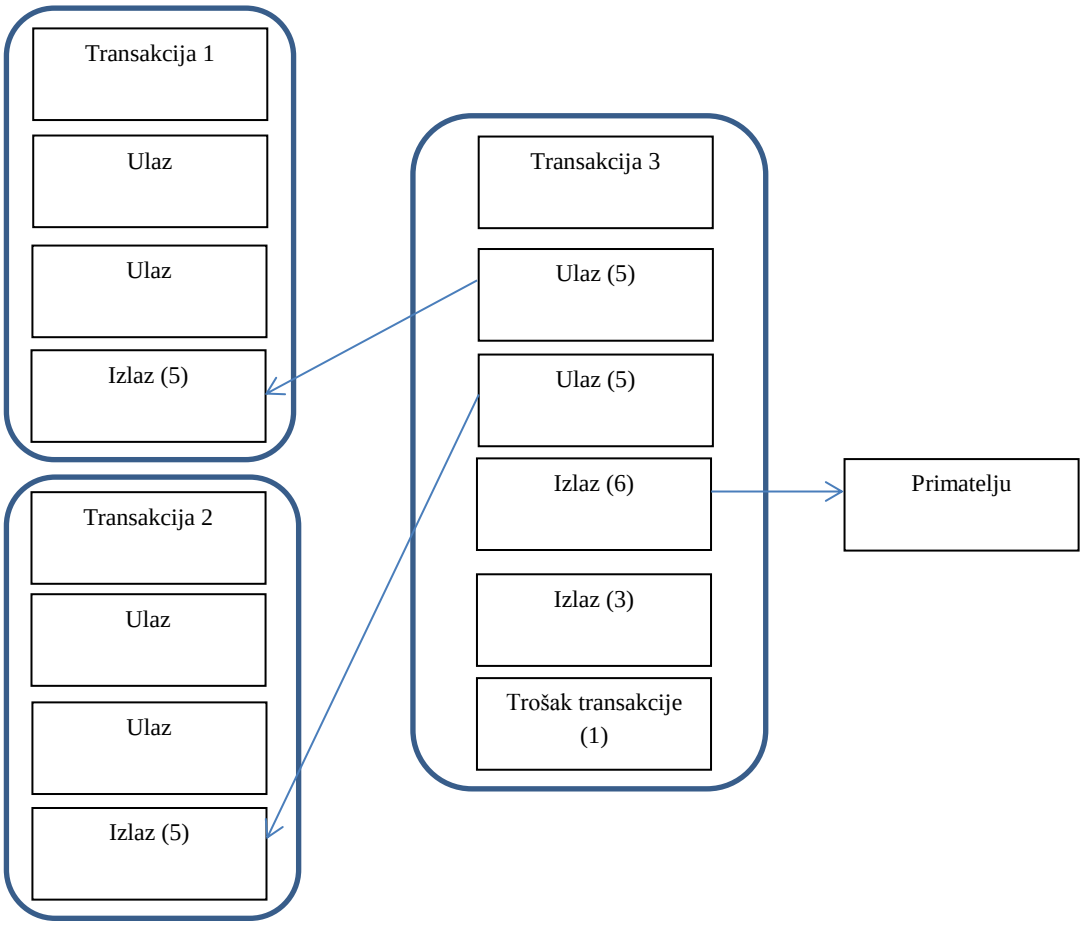
Transakcije se sastoje od nekoliko ulaznih i izlaznih transakcija, s tim da svaka mora sadržavati barem jedna ulaznu i jedna izlaznu transakciju. Njihova svrha je distribuirati sredstva među korisnicima. Ulazi transakcija odgovaraju izlazima prethodnih transakcija. Ti izlazi ne smiju biti potrošeni, inače se transakcija smatra nevažećom.

Da bi transakcija bila valjana, zbroj iznosa ulaza mora biti veći ili jednak zbroju iznosa izlaza. Razlika između ulaza i izlaza (ukoliko postoji) je naknada za transakcije. Transakcijsku naknadu skupljaju rudari koji uključuju transakcije u blokove. Izlazi u blok-lanac mogu biti potrošeni samo jednom te moraju biti potrošeni u potpunosti. Ako je iznos izlaza veći od potrošenog iznosa, transakcija stvara ostatak. Pošiljatelj transakcije moze prikupiti ovaj ostatak uključujući adresu ostatka kao dodatnu izlaznu transakciju.

Činjenica da ostatak na adresi obično kontrolira pošiljatelj transakcije, može se aktivno koristiti u algoritmima za rudarenje podataka primijenjenim na blok-lanac. Adresa s koje

potječu sredstva može se koristiti kao adresa na kojoj ce stići ostatak nakon obavljene transakcije, no ipak se preporuča generirati potpuno novu adresu za ostatak pri svakoj transakciji s ciljem povećanja privatnosti.

Slika 8. Transakcija



Izvor: sistematizacija autora

Slika 8. prikazuje primjer transakcije. U ovom primjeru, pošiljatelj želi poslati 6 milibitcoina primatelju. Međutim, pošiljatelj nema na raspolaganju nijednu izlaznu transakciju s iznosom od točno 6 millibitcoina. On kontrolira samo dvije izlazne transakcije, svaku sa po 5 millibitcoina. Stoga, on stvara transakciju grupiranjem ove dvije izlazne transakcije i šalje 6 millibitcoina primatelju. Pošiljatelj uključuje u izlaz adresu koju je ranije stvorio kako bi primao ostatak transakcije (3 millibitcoina). Jedan millibitcoin ostavlja kao naknadu za

rudare. Prije slanja transakcije u mrežu, on mora biti potpisati dvije ulazne transakcije kako bi dokazao da kontrolira adrese.

Transakcija se zatim šalje na mrežu. Prvi čvor u mreži koja prima transakcija potvrđuje da je valjana transakcija. Ako je transakcija ispravna, čvor je proslijedi drugim čvorove u mreži. Kako bi bili sigurni da je transakcija valjana, čvor mora slijediti ove korake:

- provjeriti postoje li dosadašnje promatrane izlazne transakcije te da nisu potrošene
- provjeriti je li zbroj vrijednosti ulaza veći ili jednak zbroju izlaza, odnosno provjerava da transakcija nije provela vise od dostupnih izlaza. Razlika između zbroja vrijednosti izlaza i zbroj vrijednosti ulaza smatra se naknadom za rudare sto je uključeno u coinbase transakcije
- provjeriti je li potpis za svaki ulaz valjan, odnosno da je svaki ulaz potpisan privatnim ključem s odgovajućim javnim ključem povezan s adresom.

6.2. Vrste potpisa Bitcoin transkacija

Kao što smo spomenuli, Bitcoin transakcije sastoje se od ulaza i izlaza. Ulazi sadrže reference na izlaze prethodnih transakcija koji su pod kontrolom korisnika za svaki ulaz koji omogućuju trošenje sredstava s prethodnih transakcija. Izlazi šalju vrijednosti iz trenutačne transakcije na adrese drugih korisnika.

Kada se Bitcoin transakcija potpisuje, moguće je potpisati razne kombinacije ulaza i izlaza. Postoje tri moguće vrste potpisa, tzv. sighash_all, sighash_none te sighash_single. Uz to, uz svaki od tri tipa može ići dodatni modifikator anyonecanpay.

Sighash_all je najčešća vrsta potpisa kod koje se potpisuju svi ulazi i izlazi iz transakcije. Ovaj način potpisivanja štiti cijelu transakciju od mogućih promjena.

Sighash_none je način potpisivanja transakcije koji potpisuje sve ulaze, ali niti jedan izlaz što omogućuje bilo kome da odredi kuda će se poslati Bitcoin iz transakcije.

Sighash_single je način potpisivanja gdje se potpisuje točno jedan izlaz čiji indeks odgovara ulazu specificiranom parametrom. Dakle, potpisuje se samo jedan ulaz i izlaz. Ostali se izlazi potpisuju samo djelomično (može im se promijeniti broj u nizu, engl. Sequence number). Takva transakcija omogućuje drugim korisnicima da dodaju vlastite izlaze u nju. Ovaj tip potpisa ne bi smio imati više ulaza nego izlaza, no Bitcoin protokol to ne zabranjuje.

Sighash_anyonecanpay modifikator znači da se potpisuje samo ulaz specificiran parametrom. Ostali korisnici modu dodavati ulaze po želji. To još daje tri mogućnosti potpisivanja transakcija:

- sighash_all sighash_anyonecanpay koji potpisuje sve izlaze i samo jedan ulaz; ovo omogućuje bilo kome da pridruži još ulaza u transakciju no ostali ne mogu promijeniti koliko će se Bitcoina poslati i na koju adresu
- sighash_none sighash_anyonecanpay koji potpisuje samo jedan ulaz te niti jedan od izlaza i omogućuje ostalima da dodaju ulaze i izlaze po želji, odnosno da potroše transakciju kako žele
- sighash_single sighash_anyonecanpay koji potpisuje samo jedan ulaz i izlaz i ostalima omogućuje proizvoljno dodavanje ulaza i izlaza.

7. Blok-lanac tehnologija

7.1. Hash funkcije

Blok-lanac tehnologija je nedvojbeno jedna od najvažnijih inovacija koju je uveo Bitcoin i poveznica je koja omogućava komunikaciju između dvije strane koje žele razmjenjivati digitalnu valutu, te je baza koja sadrži sve Bitcoin transkacije od njihovog samog početka i metoda koja ih drži sigurnim. Software koji koristi blok-lanac (npr. u svojstvu novčanika) ima zadaću raščlaniti blok-lanac da bi došao do važnih informacija i takve informacije su obično vrlo korisne i poželjne za bazu podataka (npr. kopije nedovršenih transakcija i sl.). Blok-lanac tehnologija je ujedno i dokaz da se transakcija dogodila, što bi značilo da je sigurna od hakerskih napada. U slučaju da se pojave prijetnje sustavu, informatičkim jezikom rečeno, potrebno bi bilo mijenjati cijelu mrežu i sve podatke koji bi se do tada zatekli u bazi.

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

Važne karakteristike hash-funkcije su sljedeće:

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

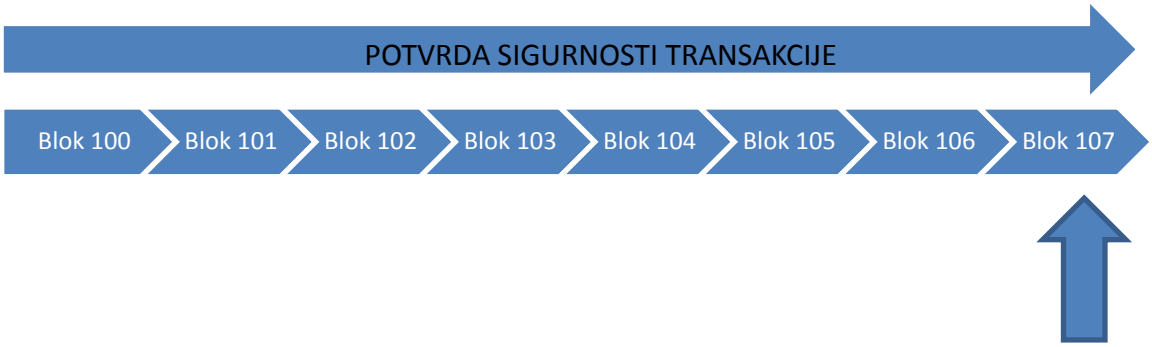
Budući da je algoritam hash-funkcije javan, njena sigurnost leži u jednosmjernosti, jer nije moguće dobiti originalni niz podataka iz same hash-vrijednosti. Najčešće korištenje hash funkcija je u osiguravanju vjerodostojnosti podataka, zaštiti datoteka od promjene, zaštiti elektroničkih financijskih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

7.2. Dupla potrošnja i ostale opasnosti

Pokušaj duple potrošnje se javlja kada se dvije različite transakcije pokušaju provesti nad istim sredstvima. Bitcoin protokol se brani od takvih pokušaja tako da odluči koja je valjana transakcija na način da prihvati onu koja je prva našla svoj put do blok-lanca. To bi značilo da Bitcoin rješava ovaj problem na decentraliziran način, bez potvrde centralnog sustava koja je transakcija valjana.

Transakcija je nadalje „osigurana“ kako god se slažu blokovi jedan na drugi u blok-lancu gdje se transakcija provodi. To se može vidjeti na Slici 9. gdje haker koji pokušava promijeniti kod u jednom od blokova mora rudariti od početka lanca pa do njegovog samog kraja. Kako se blokovi dodaju jedan na drugi, tako i netko tko pokušava promijeniti njegov kod, mora također mijenjati kod na svakom od njih, što bi u konačnici značilo vrlo kompleksan i dugotrajan posao. Jedini način na koji bi haker mogao promijeniti kodove u lancu, i time uspio hakirati ga, je kad bi to bilo izvršeno na 51% blok-lanca.

Slika 9. Osiguranje valjanosti transakcije unutar blok-lanca



Izvor: sistematizacija autora

Haker koji bi imao kontrolu nad 51% blok-lanca i uspio im promijeniti tijek transakcije bi mogao učiniti da dođe do tzv. duple potrošnje. Iako bi bilo moguće te lažne transakcije zamijeniti sa onim pravima, ne bi ih ipak bilo moguće u potpunosti promijeniti jer su one

zaštićene i drugom vrstom potpisa (ECC potpis)[7]. Ovakav tip hakiranja blok-lanaca je ujedno i jedan od najučestalijih.

Drugi tip napada tj. opasnosti je vektorski tip koji se pojavljuje kada prodavatelj pokušava primiti sredstva za nepotvrđenu transakciju provjeravajući samo neke od čvorova. Kako bi se obranio od ovog tipa opasnosti, prodavatelj bi trebao pričekati dok određena transakcija ne bude uključena u barem jedan od blokova.

[7] Ideja ECC potpisa se sastoji u tome da se pomoću originalne poruke i privatnog ključa osobe A generira digitalni potpis za osobu A. Imajući na raspolaganju poruku, digitalni potpis i javni ključ osobe A, osoba B može verificirati da je potpis autentičan.

8. Novčanici za kriptovalute

Kao što smo ranije spomenuli, Bitcoin ne postoji fizički u korisnikovom računalu, već je put ka ulazu u blok-lanac u kojem se nalaze raspoloživa sredstva za svaku pojedinu adresu. Privatni ključ koji je povezan sa adresom se koristi za potpisivanje transakcije za potrošnju sredstava sa te određene adrese. Bitcoin novčanik je, najjednostavnije rečeno, zbir privatnih ključeva. Iako Bitcoin novčanik ima analogno ime fizičkom novčaniku, oni se uvelike razlikuju:

- fizički novčanik sadrži fizički novac pa tako nema mogućost kopiranja dok se Bitcoin novčanik može kopirati i tko god ima pristup Bitcoin novčaniku ima i mogućnost potrošnje sredstava koja se u njemu nalaze
- Bitcoin novčaniku se može pristupiti preko različitih uređaja na način da se pristupanju sredstava moraju kombinirati 2 različita elektronička uređaja, a to se postiže višepotpisnim transakcijama
- moguće je kreirati Bitcoin novčanike samo za primitak sredstava, što bi značilo da se na određenu adresu mogu samo primiti sredstva, ali ih nije moguće potrošiti što je vrlo dobra opcija, ako postoji rizik od krađe.

Za svakog korisnik Bitcoin novčanika je potrebno da je upoznat sa software-om i da ima elementarna znanja o njemu:

- što je blok-lanac i kako raspolagati sredstvima u Bitcoin novčaniku
- kako generirati novu adresu za primitak novih sredstava
- što je korisničko sučelje za generiranje QR koda u kojem su sadržane adrese, transakcije itd.
- kako pratiti transakciju
- kako napraviti kopiju novčanika i kako ga obnoviti

8.1. Online i offline novčanici

Uobičajeno je da uređaj koji sadrži Bitcoin novčanik je povezan sa internetom iz razloga da bi imao mogućnost komunikacije sa Bitcoin mrežom (obavijesti o stanju računa, slanje transakcija te kontrola potvrda), to je tzv. online novčanik (ili engl. hot wallet). Kao što sa svakim uređajem koje je povezan sa internetom postoji opasnost da bude kompromitiran, tako postoji i sa online novčanikom i zato se u praksi u online novčaniku drže samo sredstva koja su potrebna za dnevne aktivnosti. Ostatak sredstava je preporučljivo držati u offline

novčaniku gdje su sadržani i privatni ključevi koji nemaju pristup internetu. Treba napomenuti da offline novčanici mogu samo potpisati transakcije izvanmrežno. Hladna pohrana se odnosi na mjesto koje možemo odabrati gdje se drže privatni ključevi koji nemaju pristup internetu. Privatni ključevi koji se drže u hladnoj pohrani se prebacuju u novčanik (online ili offline) prije potrošnje sredstava.

8.1.1. Eksterno spremanje podataka

Jedan od načina za kreiranje hladne pohrane za privatne ključeve je pohrana u vanjske uređaje kao što su USB medij ili optički disk. U trenutku kada je potreban privatni ključ, kao što je potpisivanje transakcije, privatni ključ se mora preuzeti iz eksternog medija. Važno je samo napomenuti da se mediji pohrane mogu katkada izgubiti, može im isteći vijek trajanja ili sl. Stoga je preporučljivo napraviti kopije privatnih ključeva na više mjesta.

Ako su privatni ključevi preuzeti sa online novčanika, uređaj sa online novčanikom može biti kompromitiran i datoteka sa privatnim ključevima ukradena. U tom slučaju je preporučljivo napraviti enkripciju datoteke sa privatnim ključevima koje su pohranjene u eksternim medijima.

Ukratko, prilikom korištenja eksternih uređaja za pohranu podataka, kritičan period za eventualnu krađu podataka je vrijeme kada su privatni ključevi uvezeni online klijentu za potpis transakcije. Tada je sigurnija opcija raditi na način da se privatni ključevi uvezu iz tzv. hladne pohrane u offline novčanik.

8.1.2. Papirnati novčanici

Drugi način za kreiranje hladne pohrane za privatne ključeve je njihova bilješka na komadu papira koji se treba smjestiti na sigurno. To su tzv. papirnati novčanici, iako to tehnički i nisu pravi novčanici.

U papirnatom novčaniku, javni ključevi ili Bitcoin adrese, su najčešće tiskani pored privatnih ključeva tako da papirnati novčanik može biti lako identificiran bez uvoza privatnog ključa. Privatni ključevi mogu biti prikazani kao QR kodovi čineći cijeli proces jednostavnijim, a i manja je mogućnost pogreške prilikom upisivanja podataka.

Slika 10. Papirnati novčanik sa QR kodovima

Izvor: Understanding Bitcoin (2015)

Slika 10. prikazuje papirnati novčanik generiran od bitaddress.org stranice. S lijeve strane je adresa sa QR kodom, a desna strana je privatni ključ i njegov pripadajući QR kod.

Papirnati novčanici mogu biti vrlo siguran način pohrane Bitcoina ako se poštuju pravila sigurnosti prilikom njihova generiranja. Preporučljivo je da se papirnati novčanici naprave tako da se koriste offline uređaji npr. računala povezana sa printerom i da su oba izvan dometa mreže. Kao što je bio slučaj sa eksternom pohranom, tako i ovdje privatni ključevi iz papirnatog novčanika moraju biti uvezeni u softver novčanika da bi se mogla potpisati transakcija i to u trenutku kada se sredstva misle koristiti iz razloga što je manji rizik za krađu ili neku drugu vrstu napada.

Fizički Bitcoin koji je opipljiv je novčanica ili komad papira koji sadrži privatni ključ iza cijelog mehanizma. Adresa koja je povezana sa privatnim ključevima sadrži određeni iznos Bitcoina. Kako bi se mogao raditi transfer sa sredstvima sa fizičkog Bitcoina privatni ključ mora biti uvezen u novčanik.

8.2. Web novčanici

Web novčanici su online računi koji daju eksterni davatelji usluga gdje korisnik može deponirati svoja sredstva i u isto vrijeme se brine za njihovu sigurnost. Pristup sredstvima

odnosno potpisivanje transakcija se radi putem autorizacije web novčanika. Njihova glavna prednost je lagana instalacija (samo je potrebno registrirati se kod davatelja usluga) i rukovanje sa privatnim ključevima za koje je zadužen davatelj usluga. Postoje još dodatne prednosti kao što su niski troškovi za proviziju kod transakcija ili nenaplaćivanje provizije kod korisnika koji imaju istog davatelja usluga. Web novčanici su slični online bankarstvu, stoga su i davatelji usluga skloni nazivati aplikacije Bitcoin bankama iako nisu potpuno regulirane kao bankarski sustav. Zbog sigurnosnih razloga najbolje je u web novčaniku držati sredstva potrebna za dnevne transakcije, dok ostatak sredstava bi se trebao zadržati u offline novčanicima tj. hladnoj pohrani.

Što se tiče privatnosti web novčanika, prednost je što se anonimnost korisnika može zadržati jer adrese u transakcijama i one u web novčanicima nemaju direktnu poveznicu sa korisnikom. S druge strane, ta anonimnost nije toliko velika jer davatelj usluga ima podatke o svim izvršenim transakcijama i samim time sadržava i osobne podatke korisnika.

9. Alternativne kriptovalute

Alternativne kriptovalute (engl. alt-coins) su kriptovalute koje imaju puno zajedničkih karakteristika sa Bitcoinom. Većina kriptovaluta su bazirane na Bitcoin kodu sa određenim promjenama na njima. Kako je Bitcoin pušten u optjecaj sa otvorenim kodom, dozvoljeno ga je kopirati, modificirati ga i tako pustiti novu kriptovalutu u optjecaj, što su mnogi programeri i učinili kreirajući tako nove kriptovalute.

Poput plemenite kovine, Bitcoin je ograničen resurs, što je jedan od razloga zašto mu raste cijena. Isti principi, uz rijetke izuzetke, vrijede i za njegove alternative.

Slika 11. Trenutno aktualne kriptovalute

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$12,792,143,570	$794.74	16,096,112 BTC	$303,055,000	-12.41%	
2	Ethereum	$852,512,677	$9.71	87,805,440 ETH	$24,426,500	-8.74%	
3	Ripple	$235,503,735	$0.006481	36,338,178,044 XRP *	$3,729,970	-2.07%	
4	Litecoin	$189,601,047	$3.85	49,286,454 LTC	$21,605,300	-17.41%	
5	Monero	$161,506,034	$11.80	13,683,241 XMR	$4,432,950	-12.70%	
6	Ethereum Classic	$104,582,541	$1.19	87,762,800 ETC	$3,150,810	-16.67%	

Izvor: coinmarketcap.com

9.1. Ethereum

Mreža Ethereum posebna je po tome što od prvog dana ima intenzivnu podršku i internetske zajednice i velikih kompanija poput Microsofta, a mogla bi postati budućnost interneta, jer će dokinuti potrebu za online posredništvima.

Bitcoin je još uvijek vladar digitalnog novca od kojih se jedna ipak u vrlo kratko vrijeme prometnula u ozbiljnog konkurenta što ozbiljno prijeti Bitcoinu. Valuta pod nazivom Ether, u sklopu mrežnog protokola Ethereum, puštena je u promet na ljeto 2015. godine, a već danas u

trgovanju dostiže polovicu Bitcoin volumena od pedesetak milijuna $ dnevnog prometa, izguravši time bez ikakvih poteškoća Litecoin koji je dugo držao drugo mjesto.

Mreža Ethereum bazirana je na Blockchain tehnologiji koju je osmislio autor Bitcoina, no posebna je po tome što za razliku od glavnog konkurenta od prvog dana ima intenzivnu podršku i internetske zajednice i individualnih ulagača i velikih kompanija poput Microsofta. Nadalje kroz inovativna tehnička rješenja lako izbjegava probleme koji trenutno ozbiljno prijete Bitcoinu. Protokol je osmislio mladi kanadski programer i internetski novinar ruskog podrijetla Vitalik Buterin s nepunih dvadeset godina te ga je pokrenuo u suradnji s Gavinom Woodom. U najkraćim crtama mogli bismo reći da su pokretači Ethereuma htjeli postići decentralizirano svjetsko računalo.

Naime sama valuta Ether je tek jedan od alata, a ne konačna svrha Ethereuma, dok je mreža zamišljena kao decentralizirana platforma za izvršavanje aplikacija (u Ethereumu ih nazivaju „pametnim ugovorima“). Prvenstvena namjena takvih aplikacija bilo bi reguliranje nekog poslovnog odnosa između stranaka među kojima ne postoji uzajamno povjerenje. Recimo između ponuđača i korisnika neke usluge. Trenutno se takvim posredovanjem bavi niz izrazito uspješnih internetskih kompanija poput Ubera, Kickstartera, Airbnb ili pak velikih mjenjačnica digitalnog novca. No sve bi te poslove umjesto posredničkih tvrtki koje kontroliraju proces razmjene i na tome dobro zarađuju mogle obavljati decentralizirane aplikacije, odnosno već spomenuti „pametni ugovori“. Svrha kriptovalute Ether je dvojaka – ona služi kao „gorivo“ koje se koristi pri postavljanju aplikacija u mreži, ali analogno Bitcoin protokolu i kao sredstvo za motiviranje takozvanih „rudara“ koji održavaju mrežu na životu.

Doduše, za razliku od Bitcoina čija se cijena u posljednje vrijeme razmjerno stabilizirala cijena Ethera podložna je kockarskim špekulacijama investitora pa divlja uz promjene od 80 i više posto na mjesečnoj, pa čak i tjednoj razini. Čini se da iako postoji svijest da je Ethereum još uvijek uvelike tehnološki „mačak u vreći“.

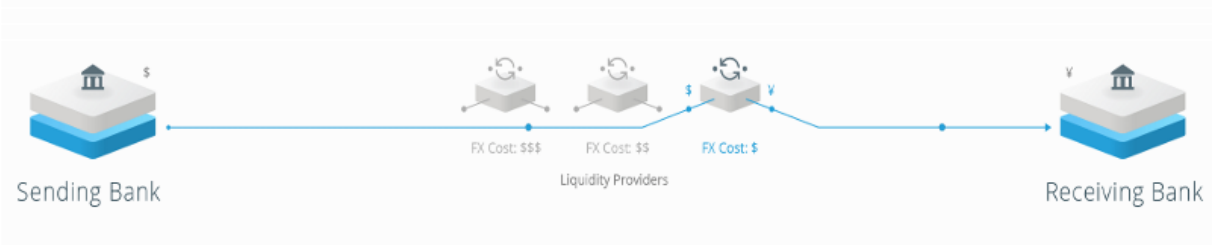
Optimizmu koji prevladava kad je u pitanju Ethereum protokol doprinose lakoća s kojom zaobilazi probleme koji muče Bitcoin. Primjerice problem premale veličine transakcijskog bloka koji sve više zagušuje Bitcoin mrežu, a oko čijeg se rješenja korisnici ne mogu dogovoriti, u Ethereumovom je protokolu u potpunosti je izbjegnut pomoću promjenjive veličine bloka, prilagodljive trenutnim potrebama mreže.

9.2. Ripple

Ripple je sistem za financijsko poravnanje u realnom vremenu (RTGS), platforma za razmjenu valuta i sistem plaćanja. Također se naziva i Ripple transakcijski protokol (RTXP), i sve to funkcionira u Ripple mreži u čijem se okviru koristi i istoimena kriptovaluta. Ripple-ov cilj je da omogući sigurne, brze i globalne transakcije bez provizije. Omogućava korištenje tokena koji se mogu mijenjati za FIAT valute, robe, usluge ili bilo što što ima određenu vrijednost. Od 2016, Ripple je treća decentralizirana kriptovaluta po tržišnoj kapitalizaciji, poslije Bitcoina i Ethereuma.

Ripple se također koristi kao platforma za transakcije između banaka, i ima nekoliko projekata u toku. Glavne kompanije i banke koje koriste Ripple platformu su UniCredit banka, NBAD, Santander Inno Ventures, CGI i još mnogi drugi. Ripple trenutno surađuje sa 12 banaka, ima 60 uspješnih integracija, 60 zemalja ima pristup Ripple mreži i 116 mjenjačnica koje funkcioniraju u okviru Ripple mreže.

Slika 12. Ripple-ov zamišljeni koncept



Izvor: digitalmoneypulse.com

Do 2014., Ripple razvojni tim je sudjelovao u nekoliko projekata, od kojih je jedan bila aplikacija za Apple mobilne telefone koja je korisnicima omogućavala da šalju novac putem mobilnih telefona, ali ta aplikacija više nije u funkciji. Još 2013. godine, protokol je bio prihvaćen od strane većeg broja financijskih institucija jer je ponudio alternativnu mogućnost za plaćanje. Ripple je tako omogućio prekogranične transakcije za privatne osobe, mala poduzeća, kompanije i banke koje se odvijaju direktno između korisnika, transparentne su i banke nisu morale plaćati uobičajene provizije koje inače vrijede za sve njihove međusobne transakcije.

Prva banka koja je prihvatila Ripple je Fidor Banka iz Munchena 2014. godine. Tržišna vrijednost Ripple-a je mala, otprilike kao i Bitcoin na svom početku - oko 0,1$. Ali

zbog ogromnog potencijala koji ima zahvaljujući suradnji sa bankama i raznim kompanijama, Ripple u budućnosti može imati znatan rast vrijednosti.

Grafikon 5. Kretanje cijene Ripple-a na svjetskom tržištu

Izvor: digitalmoneypulse.com

9.3. Litecoin

Litecoin je po mnogim stvarima vrlo sličan Bitcoinu, ali ima i nekoliko ključnih razlika. Primarne razlike su u većem broju tokena previđenih za izradu - 84 milijuna, drugačijem Algoritmu i drugačijem korisničkom sučelju.

Litecoin razvojni tim je izbacio verziju 0.8.6.1 početkom prosinca 2013. Nova verzija je omogućila višestruko smanjenje transakcijskih naknada, zajedno s drugim poboljšanjima sigurnosti i performansi, kako kod klijenata, tako i mreže.

Vrijednost Litecoin-a je počela od svega nekoliko centi na početku, da bi na vrhuncu vrijedio oko 50 $. Od tada je njegova vrijednost naglo pala i sada se uglavnom kreće između 3 i 4 $:

Grafikon 6. Kretanje cijene Litecoin-a na svjetskom tržištu

Izvor: digitalmoneypulse.com

Litecoin ima tri glavne razlike u odnosu na Bitcoin.

Prva razlika je u tome što Litecoin mreža može izvršiti obradu jednog bloka tokena na svakih 2,5 minuta, za razliku od Bitcoinove mreže, gdje je za to potrebno 10 minuta, što omogućava znatno brže transakcije. Mana u ovom slučaju je da postoji veća mogućnost da neki blokovi tokena budu „izgubljeni“, dok su dodatne prednosti veća sigurnost od raznih hakerskih napada.

Druga razlika je ta što Litecoin koristi skriptu (sekvencijalnu memorijsku funkciju) u svom algoritmu, koja zahtijeva znatno više memorije u odnosu na druge algoritme. Treća razlika je ta što će Litecoin mreža proizvesti ukupno 84 milijuna tokena, što je 4 puta više od Bitcoina.

Prvobitna uloga skripte je bila da korisnicima omogući da istovremeno izrađuju Bitcoin i Litecoin, dok je njena druga funkcija da pruži jednake mogućnosti za izradu korisnicima koji koriste različite resurse za izradu tokena.

Decentralizirana mreža slična Bitcoinovoj regulira transakcije, e-novčanike i plaćanja putem skripte.

Litecoini se trenutno mogu mijenjati za FIAT valute i druge kriptovalute preko online mjenjačnica. Za razliku od standardnih internet transakcija, gdje postoji mogućnost povrata novca u slučaju odustajanja od kupovine, kod Litecoin transakcija to nije moguće.

9.4. Monero

Monero je kriptovaluta koja se fokusira na privatnost i decentralizaciju. Za razliku od ostalih kriptovaluta koje su derivatni Bitcoina, Monero se zasniva na CryptoNote protokolu i posjeduje značajne razlike u algoritmu u odnosu na Bitcoin. Monero također uživa veliku podršku od strane online zajednice, i njegov modularna struktura je pohvaljena od Wladimira J. van der Laan-a, koji je zadužen za održavanje Bitcoina. Tržišna kapitalizacija Monera je za godinu dana narasla sa 3,7 milijuna $ na preko 170 milijuna $.

Pokrenut je kao prva branša kriptovalute zasnovane na CryptoNote-a koja se zove ByteCoin, ali sa dvije ključne razlike. Prva je ta što je smanjeno vrijeme presjeeka bloka sa 120 na 60 sekundi, i brzina izrade je smanjena za 50% Uz sve to, Monerovi programeri su pronašli i ispravili brojne greške i slabosti u algoritmu koje su vremenom ispravili i unaprijedili.

Predviđeno je da se ukupno izradi 18,4 milijuna tokena u periodu od 8 godina. Njegova početna vrijednost je, kao i kod svake druge kriptovalute bila neznatna, da bi u posljednjih nekoliko mjeseci zabilježila eksponencijalni rast.

Grafikon 7. Kretanje cijene Monera na svjetskom tržištu

Izvor: Izvor: digitalmoneypulse.com

Monero koristi CryptoNote protokol koji se zasniva na jednokratnim „prstenastim potpisima“ i tajnim adresama, što predstavlja mješavinu kombinacija koje su prošle testiranje.

Vrlo jaka privatnost korisnika je osnovna karakteristika ove kriptovalute, ali postoji mogućnost za eksternu reviziju (npr. za plaćanje poreza ili prikazivanje prihoda). Monerovi programeri trenutno rade na uvođenju C++ I2P usmjerivača u svoj kod, što znači da će korisnici moći sakriti svoje IP adrese prilikom korištenja ove kriptovalute.

S obzirom na to da je nedavno zabilježio ogroman skok vrijednosti, ostaje vidjeti je li to privremeni skok koji će se vremenom ispraviti na dolje, ili će se njegova vrijednost održati ili možda čak dodatno porasti. U svakom slučaju je preporučljivo pratiti, jer ljudi koji su izrađivali ili kupovali ovu valutu kada je vrijedila manje od 1 $ su za kratko vrijeme ostvarili veliku zaradu.

9.5. Ethereum Classic

Ethereum Classic je nastao drugom polovinom srpnja 2016., nakon što je hakiran 17. lipnja iste godine, što je prouzrokovalo pravu buru na tržištu decentraliziranih kriptovaluta. Nakon tog događaja, Ethereum je proveo određene izmjene u svom blok-lancu i cjelokupnom sustavu, što se nekim članovima nije svidjelo, tako da su se oni praktički „odvojili“ i nastavili su rad sa neizmjenjenim blok-lancem, koji se danas naziva Ethereum Classic.

24. srpnja 2016. je formirana Ethereum Classic zajednica tako što se formalno odvojila od Ethereumovih i formirala svoje komunikacijske kanale. 10. kolovoza je anonimna hakerska grupa pokušala ostavizi veliku količinu Ether tokena (oko 7,2 milijuna), što je rezultiralo zamrzavanjem tih sredstava. Rezultat toga je bila visoka nestabilnost koja je trajala nekoliko dana, sve do 15. kolovoza kada se Ethereum Classic oporavio.

Danas se vrijednost Ethereum Classic-a kreće oko dva $ za token, sa manjim ili većim varijacijama.

Grafikon 8. Kretanje cijene Ethereum Classic-a na svjetskom tržištu

Izvor: digitalmoneypulse.com

Generalno gledajući, Ethereum Classic je neizmjenjena verzija Ethereuma, tako da je naslijedio sve njegove prednosti i mane. Iako ima veliku primjenu u industriji aplikacija, ostaje vidjeti koliko će se održati na tržištu kriptovaluta.

9.6. Steem

Steem je decentralizirana društvena platforma zasnovana na blok-lancu gdje svi sudionici mogu dobiti nagrade u vidu Steem kriptovalute. Nagrade se dobivaju kada se na mreži postavljaju razne objave koje se svide drugim korisnicima, kada se dugo doprinosi mreži, potvrđuju transakcije, trguje na mjenjačnici i ako neko prvi „lajka“ neku objavu.

Tržišna vrijednost Steem-a se okvirno kreće između 1 i 2 $, a njegova najveća vrijednost je iznosila oko 4 $, ali je nakon toga pala za više od 75%. Budući da je Steem zasnovan kao društvena mreža, on i dalje ima potencijal za dalji rast vrijednosti.

Grafikon 9. Kretanje cijene Steem-a na svjetskom tržištu

Izvor: digitalmoneypulse.com

9.7. Burze i mjenjačnice

Kao i sa tradicionalnim valutama, moguće je trgovati i Bitcoinom. To nam omogućuju Bitcoin burze i mjenjačnice. Danas već postoji desetak stabilnih Bitcoin burza i mjenjačnica u kojima je moguće trgovati i mijenjati Bitcoin za altcoin i druge valute. Trgovanje kriptovalutama ima isti koncept kao i trgovanje tradicionalnim valutama poput američkog dolara, eura… Jedina je razlika što se ovdje trguje Bitcoinom i takozvanim altcoinovima kao npr. već spomenutim Ethereumom, Ripplom, Litecoinom itd.

Također postoje i hibridne Bitcoin burze/mjenjačnice u kojima je moguće napraviti depozit u tradicionalnoj valuti (USD, EUR, HRK) i konvertirati istu u Bitcoin/Litecoin/Altcoin te početi trgovati.

Najpoznatije Bitcoin burze su:

Bitcoin.de - najveća Bitcoin burza u Europi, omogućuje korisničko plaćanje i kupovinu; možemo kupiti željenu količinu Bitcoina od nekoga tko ih prodaje, dobiti njihove bankovne podatke iz Bitcoin.de i poslati iznos preko SEPA transfera. Nakon što je druga strana primila sredstva, Bitcoin.de otpušta kupljeni Bitcoin (minus tržišna naknada) za svoju uslugu.

Bitstamp.net - najeftinija burza. Prodaja se vrši pomoću SEPA transfera, obično u roku jednog dana kada će transakcija biti izvršena.

MtGox.com – najskuplja burza, imala je monopol na Bitcoin trgovinu u prošlosti. Sjedište joj je u Tokiju, trgovina se ostvaruje putem SEPA transfera za Europljane i imaju SAD bankovni račun za Amerikance.

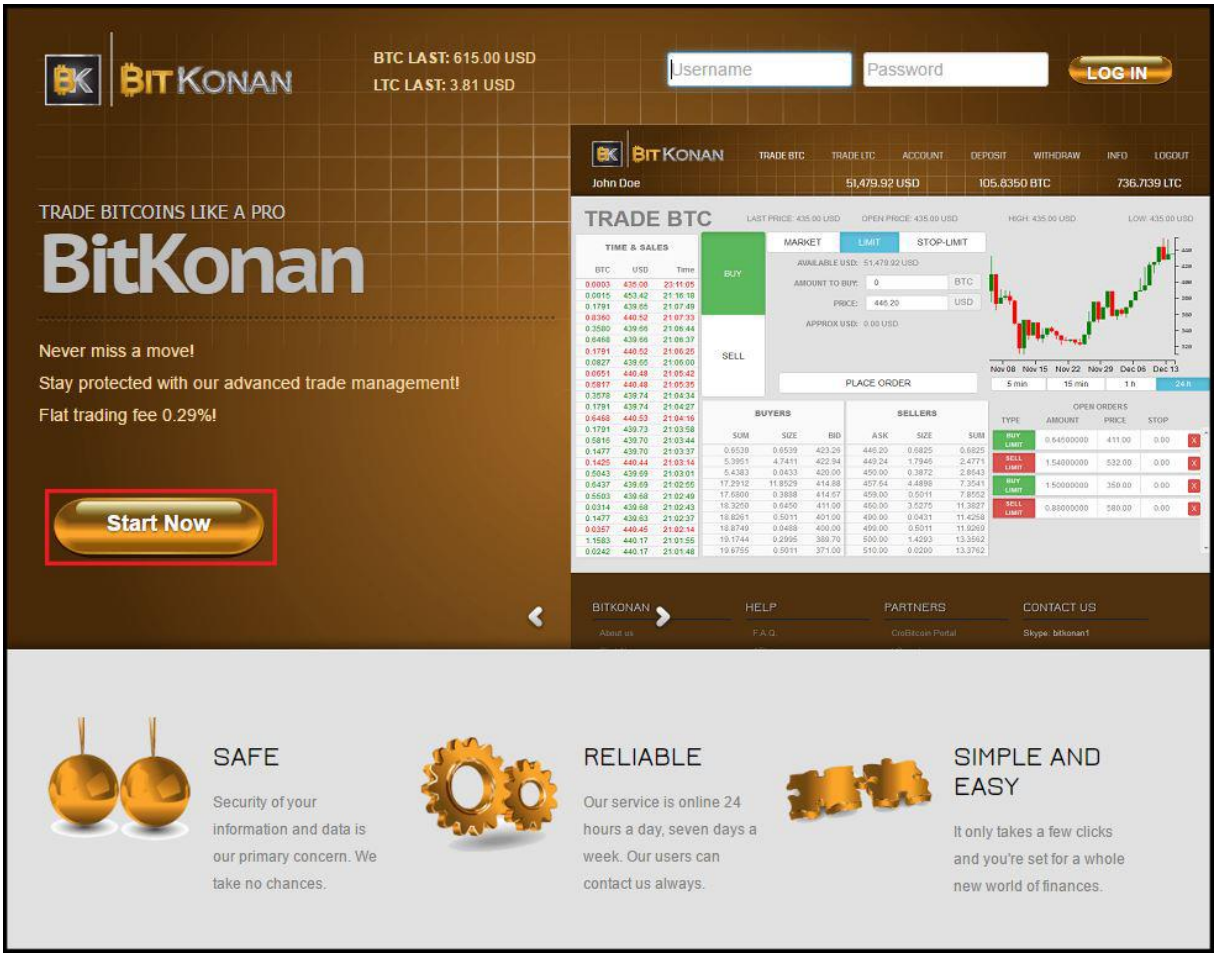
Od ostalih burzi najviše s trguje na Poloniex-u, Bittrex-u i Bitfinex-u.

U Republici Hrvatskoj postoji burza i mjenjačnica pod nazivom BitKonan čije su usluge otvorene prema inozemnom i tuzemnom tržištu.

Službena valuta je američki dolar (USD) te se sve ostale konvertiraju u istu.

Depozit Bitcoina/Litecoina se vrši besplatno te su sredstva spremna za upotrebu nakon 6 potvrda u mreži.

Slika 13. BitKonan portal



Izvor: bitkonan.com

9.8. ICO

ICO (Initial Coin Offering) je ekvivalent IPO-u (Initial Public Offering) odnosno inicijalna javna ponuda kojom korporacija na „standardnom“ tržištu kapitala po prvi puta javno emitira svoje dionice puštajući tako investitore s javnog tržišta u svoju vlasničku strukturu. Kod kompanija u „crypto“ domeni ovaj proces se naziva ICO te je postao način za dizanje kapitala i investicije u tvrtke i projekte. Kod ICO-a radi se inicijalna distribucija tokena prema potencijalnim investitorima, a kapital koji je prikupljen se alocira u daljnji razvoj, marketing, pravna pitanja i sve što zapravo definira određeni projekt. Neke od popularnih kriptovaluta koje su koristile ovaj model financiranja su Ethereum, Augur, Bitshares, NXT, Mastercoin, Factom.

Slika 14. Otvaranje inicijalne ponude za kriptovalutu

Izvor: newsbtc.com

Zaključak

Bitcoin je jedinstvena digitalna valuta koja se po svojim karakteristikama razlikuje od prethodnih digitalnih valuta i u isto vrijeme označava istoimenu organizaciju, softver i protokol koji se prvi put pojavio 2009. godine. Valuta je računalno programirana i decentralizirana, a ono što ju čini specifičnom je isključivost trećih osoba, bilo da se radi o krivotvorenju ili zlouporabi. Bitcoin ima budućnost u segmentu financijskog tržišta, a to je transfer novca. Razlog je taj što su transakcijski troškovi niski za razliku od ostalih oblika transfera novca kao što su banke, tvrtke za organiziran prijenos gotovog novca te kartičnog poslovanja. Budući da je vlasnicima Bitcoin valute omogućena anonimnost, puno je kritika da se tako stvara prostor za pranje novca, poreznih oaza i kreiranje crnog tržišta. Neke od zemalja su počele regulirati transakcije, ali je pitanje nadzora i regulacije još uvijek otvoreno.

Ako promatramo cijenu Bitcoina kroz kraći period, možemo zamijetiti da u vrlo kratkom vremenu dolazi do velikih promjena u njegovoj vrijednosti. Na dan 10. siječnja 2017. godine cijena jednog Bitcoina je iznosila 907,41 USD, dok je pet dana kasnije cijena iznosila 1.007,74 USD. Ovdje se nameće samo po sebi pitanje je li Bitcoin dobra investicijska prilika i može li biti dugoročno sredstvo čuvanja vrijednosti.

Sigurnosni algoritmi, mehanizmi i protokoli (kriptiranje, digitalni potpis itd.) koji se koriste su vrlo dobro prihvaćeni i zadovoljavaju sve zahtjeve koje postavljaju modeli elektroničkog novca, ali klasični oblici plaćanja, kakve sada poznajemo, će biti još dugo zastupljeni. Zagovornici ove digitalne valute smatraju da će kroz koje desetljeće Bitcoin u financijskim tokovima imati status klasične valute, kao što to danas ima npr. švicarski franak.

U Grafikonu 2. gdje su prikazane dnevne transakcije Bitcoina vidljiv je eksponencijalan rast korisnika, iako je broj transakcija još uvijek nizak obzirom na ostale načine plaćanja.

Prema procjenama stručnjaka, u sljedećih 15 godina Bitcoin će postati šesta valuta po zastupljenosti u deviznim rezervama država.

Iako se Bitcoin i cjelokupna kriptografska tehnologija na kojoj se zasniva doima zamršenim, sustav ima jednostavan pristup za korisnika. Za bilo kakvu transakciju dovoljan je pristup internetu, korisnički račun i novčanik gdje korisnik sa bilo koje lokacije može trgovati digitalnom valutom.

Popis literature

Knjige:

1. Franco, P., (2015), Understanding Bitcoin, West Sussex: Wiley

2. Pagliery, J., (2014), Bitcoin and the future of money, Chicago: Triumph books LLC

3. Patterson, S., (2013), Bitcoin beginner, Netherlands: Better life publishers

4. Vigna, P., Casey, M.J., (2015), The age of crypocurrency, New York: Picador

Članak Internet:

1. Rodrigue, J.P. (2015), The Geography of Transport systems, https://people.hofstra.edu/geotrans/eng/ch7en/conc7en/stages_in_a_bubble.html, pristupljeno 10.11.2016

Internet:

1. Bitcoin Croatia, Vodič, http://bitcoin-croatia.info/vodic/, pristupljeno 20.01.2017

2. Blockchain Info, Charts, https://blockchain.info/charts, pristupljeno 20.01.2017

3. Coin Market Cap, Currencies, https://coinmarketcap.com/currencies/,pristupljeno 20.01.2017

4. Digital Money Pulse, Digital Currencies, http://www.digitalmoneypulse.com/, pristupljeno 12.01.2017

5. Novi List, Znanost i tehnologija, http://www.novilist.hr/Znanost-i-tehnologija/Tehnologija/Ethereum-buducnost-interneta-ili-poligon-za-spekulante, pristupljeno 12.01.2017

Popis tablica, slika i grafikona

TABLICE

SLIKE

GRAFIKONI

Europass Životopis

Osobni podaci

Prezime / Ime	**Šimić/ Ivana**
Adresa(e)	20, Blaškovečka ulica, 10382, Sv.I.Zelina, RH
Telefonski broj(evi)	Broj mobilnog telefona: 099 3166 939
Broj(evi) faksa	
E-mail	isimic1983@gmail.com
Državljanstvo	RH
Datum rođenja	26.08.1983
Spol	

Radno iskustvo

Datumi	01.01.2005. - …
Zanimanje ili radno mjesto	Asistent u prodaji
Glavni poslovi i odgovornosti	Asistiranje u vođenju prodaje, vođenje CRM sustava
Ime i adresa poslodavca	GC Corporation (Japan)
Vrsta djelatnosti ili sektor	Medicina/stomatologija

Obrazovanje i osposobljavanje

Datumi	03-2012 – 02-2017
Naziv dodijeljene kvalifikacije	
Glavni predmeti / stečene profesionalne vještine	
Ime i vrsta organizacije pružatelja obrazovanja i osposobljavanja	Libertas međunarodno sveučilište
Datumi	10-2005 – 02-2009
Naziv dodijeljene kvalifikacije	
Glavni predmeti / stečene profesionalne vještine	
Ime i vrsta organizacije pružatelja obrazovanja i osposobljavanja	Sveučilište u Splitu

Osobne vještine i kompetencije

Materinski jezik(ci)	Hrvatski jezik

Drugi jezik(ci)	Engleski jezik – aktivno u govoru i pismu Njemački jezik – pasivno Talijanski jezik - pasivno
Računalne vještine i kompetencije	MS Office, SAP, CRM
Vozačka dozvola	B