EKONOMSKA PERSPEKTIVA KRIPTOVALUTA I BLOCKCHAIN TEHNOLOGIJE

Tadinac, Marin

Undergraduate thesis / Završni rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, Faculty of economics Split / Sveučilište u Splitu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:124:315408

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

REFST - Repository of Economics faculty in Split

SVEUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

Marin Tadinac

EKONOMSKA PERSPEKTIVA KRIPTOVALUTA I BLOCKCHAIN TEHNOLOGIJE

Završni rad

Mentor:

doc.dr.sc. Vinko Muštra

Student:

Marin Tadinac

Split, lipanj, 2018.

SAŽETAK

Kroz razvoj čovječanstva novac se pojavljivao u različitim oblicima, točnije nekad davno novac nije ni postojao nego su ljudi koristili različite predmete i proizvode koji su imali vrijednost na temelju koje se moglo trgovati. Nakon principa trampe došlo je zlatno doba gdje je novac zamjenjivalo zlato. Nakon perioda zlatnog standarda uslijedio je period tiskanja novca koji je prisutan i u sadašnjici no možda ne i u budućnosti. Pojavom digitalnog novca smanjuje se fizičko tiskanje novca jer je sada moguće trgovati novim načinom. Razvijanjem tehnologije te pojavom modernog doba korištenje kartica kao sredstvo plaćanja postalo je svakodnevnica. Problem se pojavio u tome što je digitalni novac pod vodstvom banke koja ima centralizirani sustav, a prisutna je i kontrola države. Zbog centraliziranog sustava i kontrole države nad novcem nastale su kriptovalute.

Predmet ovog rada predstavlja mogućnost upotrebe kriptovaluta i ekonomskih učinaka istih na primjeru Bitcoina, a cilj je rada je utvrditi prikazati uporabu kriptovaluta, sigurnost takvih transakcija, oporezivanje i mogućnosti daljnjeg korištenja kriptovaluta. Lanac blokova odnosno eng. *blockchain* je baza podataka za spremanje podataka, informacija i dokumenata. Pomoću Blockchain tehnologije omogućena je distribucija digitalne informacije među svim čvorovima koji sudjeluju u sustavu. U Bitcoin sustavu ne postoji središnja banka koja izdaje novac te čuva i obrađuje transakcije, niti postoji jedinstveni vlasnik Bitcoin mreže. Ključna razlika Bitcoina u odnosu na centralizirane sustave proizlazi iz činjenice da svaki korisnik ima uvid u vlastite transakcije kao i transakcije ostalih sudionika.

Ključne riječi: **Blockchain**, **struktura podataka**, **digitalna informacija**, **kriptovaluta**, **Bitcoin**.

SUMMARY

Through the development of humanity, money appeared in various forms, more precisely, back in time money had never existed, but people used different objects and products that had the value on which they could trade. After the tattered principle came the golden age where money replaced the gold. After the gold standard period, there was a period of money printing that is present in the present and perhaps not in the future. Digital cash is reduced by physical printing because it is now possible to trade in a new way. By developing technology and the emergence of modern times, using cards as a means of payment has become everyday. The problem has arisen in the fact that digital money is under the leadership of a bank that has a centralized system and there is also control of the state. Because of the centralized system and state control over money, cryptovalutes were created.

The subject of this paper is the possibility of using cryptovalue and its economic effects on the Bitcoin example, and the aim of the paper is to establish the use of cryptovalue, the security of such transactions, the taxation and the possibility of further use of the cryptovalue. Block chain ie eng. blockchain is a database for storing data, information and documents. Blockchain technology enabled the distribution of digital information across all nodes participating in the system. There is no central bank in the bitcoin system that issues money and keeps and processes transactions, nor does it have a unique owner of the bitcoin network. The key difference between bitcoins and centralized systems derives from the fact that every user has an insight into their own transactions as well as the transactions of other participants.

Keywords: **Blockchain**, **data structure**, **digital information**, **cryptovalue**, **Bitcoin**.

SADRŽAJ:

1. UVOD 5

1.1. Predmet istraživanja 5

1.2. Cilj istraživanja 5

1.3. Metode istraživanja 5

1.4. Struktura rada 5

2. TEORIJSKI ASPEKTI BLOCKCHAIN TEHNOLOGIJE KRIPTOVALUTA 6

2.1. Struktura bloka 8

2.2. Zaglavlje bloka 8

2.3. Binarno hash stablo 9

2.4. Anonimnost digitalnih valuta baziranih na Blockchain sustavu 10

2.5. Elektronički oblici novca 10

2.6. Pojmovno određenje kriptovaluta 13

2.7. Odnos virtualnih valutnih shema i elektroničkog novca 13

2.8. Ekonomske značajke kriptovaluta 17

2.9. Pregled tržišta kriptovaluta 18

3. BITCOIN KAO NAJPOZNATIJA KRIPTOVALUTA 21

3.1. Pojmovno određenje Bitcoina 21

3.2. Nastanak i povijest bitcoina 22

3.3. Kriptografski mehanizmi Bitcoina 23

3.4. Kriptografija javnog ključa 24

3.5. Hash-funkcija 26

3.6. Digitalni potpis 27

3.7. Oporezivanje bitcoina 28

3.8. Oporezivanje bitcoin transakcija neizravnim porezima 29

3.9. Analiza bitcoina na globalnom financijskom tržištu 30

3.9.1. Razvoj i tehnička analiza 30

3.9.2. Investicijski potencijal bitcoina 34

3.9.3. Utjecaj kriptovaluta na financijske tokove 35

4. ZAKLJUČAK 38

LITERATURA 40

1. UVOD

1.1. Predmet istraživanja

Postojeća struktura financijskih tržišta je suboptimalna, posebice promatrajući mogućnost postojećeg tehnološkog znanja. Navedeno se posebice reflektira kroz nedovoljno korištenje tehnologije lanca blokova (eng. *blockchain*), što pak zaziva mnoge promjene koje je potrebno sagledati iz različitih perspektiva. Budući da donose radikalne inovacije kriptovalute karakterizira izrazita nestabilnost: mnoge nastaju, no mnoge i nestaju.

1.2. Cilj istraživanja

Cilj je ovog rada analizirati ekonomske perspektive blockchain tehnologije i kriptovaluta te prikazati ekonomski značaj kriptovaluta, uz posebni osvrt na najpopularniju – Bitcoin.

1.3. Metode istraživanja

U ovom radu su korišteni izvori podataka iz raznih stručnih knjiga, časopisa vezanih za ovu temu, također korištena je i literatura sa Interneta koja najviše doprinosi u izradi ovog rada zbog najveće baze podataka i značajnih informacija vezanih za predmet istraživanja.

Pri izradi rada korištene su sljedeće metode: metoda analize i sinteze, metoda indukcije i dedukcije, metoda deskripcije i kompilacije te metode slučaja.

1.4. Struktura rada

Rad je podijeljen u četiri poglavlja. U uvodnom se dijelu uvode teorijske osnove obrađene tematike, izvori te metode koje su korištene za prikupljanje podataka i struktura rada. Drugi dio rada donosi teorijski pregled blockchain tehnologije te ekonomske značajke kriptovaluta i njihova usporedba s tradicionalnim novcem, dok se u trećem poglavlju opisuje Bitcoin kao najpoznatiju kriptovalutu, nastanak i povijest, kriptografske mehanizme i međuovisnost blockchain i Bitcoin-a. U zaključnom, četvrtom poglavlju, donosi se pregled pojmova obrađenih u radu, te zaključni rezultat cjelokupnog rada.

2. TEORIJSKI ASPEKTI BLOCKCHAIN TEHNOLOGIJE KRIPTOVALUTA

Blockchain ili, drugim riječima, lanac blokova je distribuirana struktura podataka, odnosno lista digitalnih informacija podijeljenih među svim čvorovima koji su sudionici u sustavu. Pomoću Blockchain tehnologije omogućena je distribucija digitalne informacije među svim čvorovima koji sudjeluju u sustavu. Na taj način svaki čvor održava vlastitu kopiju svake relevantne informacije, pa nema potrebe za središnjim autoritetom čija bi uloga bila kontrolirati informacije. Nadalje, kontrola je distribuirana pomoću mehanizama za validaciju zbog čega je svaki čvor siguran da je informacija zapisana na „Blockchain-u“ točna (Šijanović Pavlović, Bolanča i Pavlović, 2018:112).

U današnje, suvremeno doba informatizacije, informacije su od presudne važnosti. Ipak, s obzirom na sveprisutnost informacija i mehanizme njihova dijeljenja, porasla je i količina povjerljivih, osjetljivih, informacija, a metoda njihove razmjene nije se uvelike promijenila još od 90-ih godina prošlog stoljeća.

Povjerljivu skupinu informacija je potrebno zaštiti zbog čega se od sustava za pohranu zahtijevaju sljedeće odlike (Šijanović Pavlović, Bolanča i Pavlović, 2018:112):

1) Informacije se kreću kroz sigurnu mrežu.
2) Informacije se ne smiju modificirati tijekom ni nakon zapisivanja.
3) Pravo korištenja digitalnih ili materijalnih dobara vezanih za informaciju pripada samo ovlaštenom korisniku.
4) Brzina dijeljenja informacija mora biti što veća.
5) Pregled informacija jednostavno se izvršava od strane svakog zainteresiranog korisnika.

„Blockchain“ omogućava maksimalnu zaštitu integriteta zapisa uporabom kriptografskih metoda pa su zapisi distribuirani, svaki čvor u sustavu posjeduje ekvivalentne podatke, zahvaljujući algoritmima pomoću kojih se postiže konsenzus, poput eng. *proof-of-work, proof-of-stake, delegated-proof-of-stake, proof-of-authority, proof-of-importance, proof-of-capacity, proof-of-activity, proof-of-stake-anonymous* algoritama. Kao dodatna prednost ističe se nemogućnost naknadnog mijenjanja ili ometanja zapisa.

Blockchain je sastavljen od blokova međusobno povezanih u lanac u kojem svaki blok sadrži niz zapisa, a blokovi su međusobno povezani algoritmom koji koristi kriptografsku „hash“ funkciju.

Uloga je eng. *hash* funkcije vršiti transformaciju poruke proizvoljne dužine, u izraz čija je dužina fiksna. Svaka je hash funkcije opisana određenim skupom osobina od kojih su pojedine obvezne za sve hash funkcije, dok su druge izborne te kao takve ovisne o konkretnoj primjeni. Govoreći o obveznim osobinama, hash funkcija uvijek mora biti jednosmjerna, drugim riječima, za određenu je izlaznu vrijednost hash funkcije teško, u praksi gotovo i nemoguće, pronaći odgovarajuću ulaznu poruku. Nadalje, očekuje se da hash funkcija posjeduje osobinu „kolizijske otpornosti”, odnosno da je teško pronaći dva različita ulaza koji imaju isti izlaz (Šijanović Pavlović, Bolanča i Pavlović, 2018:112). Vezu između blokova u lancu nije moguće krivotvoriti, osim ako je riječ o iznimnoj količini resursa kojima napadač raspolaže. Do sada je svaka zainteresirana strana u postupku održavala lokalne baze podataka s različitim informacijama.

Neovisno o tome radi li se o centraliziranoj ustanovi kao što je banka ili pak o pojedinoj organizaciji u sustavu poslovanja, informacije se dijele među strankama isključivo u slučaju opravdane potrebe. Integritet podataka sadržanih u lokalnim bazama štiti se na najvišoj razini, no napadi na digitalne podatke sve su češći i sa sve dalekosežnijim posljedicama. Naime, posljedice napada na izoliranu lokalnu bazu podataka mogu imati katastrofalne razmjere. U takvim je situacijama moguće rekreirati bazu iz backupa pri čemu ipak dolazi do gubitka dijela informacija, a nepotpunost podataka potencijalno znači i značajne financijske gubitke. U slučaju kasnijeg otkrivanja napada postoji opasnost i da podaci neće biti konzistentni s podacima partnera u poslovanju. Navedeno će narušiti uzajamno povjerenje, a otklanjanje problema uzrokovanih napadom dugotrajan je i težak proces.

Blockchain tehnologija pruža mogućnost toga da podaci postanu korisni ne samo jednoj organizaciji, nego svim partnerima u mreži. S druge strane, podacima se, kao i ostalim procesima između partnera, kontrolirano upravlja uz visoku razinu sigurnosti i povjerenja. Neke od osnovnih značajki Blockchaina su (Šijanović Pavlović, Bolanča i Pavlović, 2018:113):

1) Uobičajeno je da je sustav koji koristi Blockchain izgrađen prema modelu ravnopravnih partnera (eng. *peer-to-peer*).
2) Sustav je u potpunosti decentraliziran, nije potreban središnji autoritet.

3) Svaki novi zapis je u gotovo realnom vremenu distribuiran između mnoštva čvorova.
4) U svrhu identifikacije sudionika u sustavu, potvrde identiteta, dokazivanja autentičnosti i u nekim slučajevima iskorištavanja prava za čitanje/pisanje koristi se kriptografija.
5) Čvorovi sustava mogu dodavati podatke u Blockchain.
6) Čvorovi sustava mogu čitati podatke iz Blockchaina.
7) Blockchain ima razvijen mehanizam koji onemogućuje promjenu nad podacima koji su jednom upisani u Blockchain ili u najmanju ruku omogućuje lako otkrivanje
8) promjena na podacima.

2.1. Struktura bloka

Blockchain, kako proizlazi već iz samog naziva, sadržan je od blokova koji predstavljaju strukturu podataka u kojoj su zapisane digitalne informacije koje se dijele putem blockchaina. Jedan se blok sastoji od zaglavlja u kojem su upisani metapodaci te liste digitalnih informacija varijabilne dužine.

Tablica 1. Struktura bloka

Veličina	Naziv	Opis
4 bajta	Veličina bloka	Veličina bloka u bajtovima
80 bajtova	Zaglavlje bloka	Meta-podaci o bloku
1-9 bajtova	Brojač zapisa	Koliko zapisa sadrži blok
Varijabilno	Zapisi	Zapisi pohranjeni u bloku

2.2. Zaglavlje bloka

Zaglavlje svakog bloka sastoji se od 80 bajtova podataka koji služe kao dodatne tehničke informacije o bloku i povezivanju blokova u lanac. Struktura zaglavlja bloka prikazana je u Tablici 2.

Tablica 2. Struktura zaglavlja bloka

Veličina	Naziv	Opis
4 bajta	Verzija	Verzija protokola u vrijeme nastajanja bloka (Specifično za Bitcoin)
32 bajta	Hash prethodnog bloka	Referenca na prethodni blok u lancu koji još nazivamo roditelj bloka
32 bajta	Korijen binarnog hash stabla	Kriptografski hash koji sadrži informacije o svim zapisima u bloku
4 bajta	Vremenska oznaka	Vrijeme kada je blok kreiran i uključen u blockchain
4 bajta	Težinska oznaka	Težina algoritma čije je rješenje potrebno za uključivanje bloka u blockchain
4 bajta	Nonce	Broj pomoću kojeg je riješen algoritam za uključivanje bloka u blockchain

S ciljem postizanja vremenske uštede čvor može sadržavati zasebnu bazu podataka u kojoj su spremljeni hash-evi blokova. Vremenska oznaka predstavlja vrijeme kada je blok dodan u lanac. Polja težinska oznaka i nonce su meta-podaci koji se koriste prilikom dodavanja bloka u lanac. Korijen binarnog hash stabla predstavlja informaciju dobivenu od svih zapisa u bloku.

2.3. Binarno hash stablo

Svaki blok u zaglavlju sadrži polje pod nazivom korijen binarnog hash stabla pomoću kojeg je omogućen sažeti prikaz svih zapisa u bloku, ali i jednostavna provjera integriteta velikog skupa podataka. Binarno stablo je konačan skup podataka istog tipa koje zovemo čvorovi.

Blockchain predstavlja zajedničku bazu podataka koja eliminira ulogu trećih strana u transakcijskim procesima i dijeljenju informacija na više načina. Tehnologija, zalihe, ugovori, plaćanja i ostali podaci dijele se izravno među stranaka pomoću šifriranih veza. Primjerice,

robne razmjene s Blockchainom u mogućnosti su podržati trgovanje naftom i plinom izravno između stranaka na bilo kojoj lokaciji u svijetu.

2.4. Anonimnost digitalnih valuta baziranih na Blockchain sustavu

Blockchain je, s teorijskog aspekta, potpuno automatiziran sustav s mogućnošću pružanja potpune anonimnosti korisnicima. Ipak, s obzirom na uvjete koji prevladavaju u današnjem suvremenom okruženju, u ponekim je situacijama teško jamčiti potpunu anonimnost preko razine koju to dozvoljava aktualno pravno okruženje, a isto se u punom opsegu odnosi i na kriptovalute.

Iako samo tehničko rješenje omogućava praktično potpunu anonimnost transakcija, isto se oslanja na postojeću telekomunikacijsku strukturu koju je u određenoj mjeri kontrolirana od strane vlasti. U kombinaciji s transparentnošću sustava, ova činjenica stvara određene indirektne načine na koje anonimnost potencijalno može biti narušena.

Analitička obrada kompletnog dnevnika transakcija (Blockchain-a) omogućuje povezivanje i grupiranje pojedinih transakcija prema postavljenim parametrima, poput adrese pošiljatelja, adrese primatelja, vremena transakcije, iznosa, a u pojedinim slučajevima i IP adrese pošiljatelja. Kombinacijom ovih podataka, moguće je dobiti kronologiju događanja za svaku pojedinu adresu, uključujući i povezanost (preko transakcija) s drugim adresama sustava. Bitno je naglasiti kako su aktualna daljnja nastojanja unaprjeđenja anonimnosti sustava kombinacijom transakcija, primjerice eng. *CoinJoin*, *CoinShuffle* (Selij, 2015). Krajnji i potpun rezultat navedenoga je potpuna transparentnost sustava do razine vlasništva adrese, jer su za svaku poznati svi podaci, ali nije moguće izravno povezati adrese s njihovim vlasnicima (Doguet, 2012:1119).

2.5. Elektronički oblici novca

Elektronički oblici novca pojavili su se 60-ih godina prošlog stoljeća u Sjedinjenim Američkim Državama, predstavljanjem EFT POS – a (eng. *Electronic Funds Transfer at Point Of Sale*) sustav koji je uveo elektroničko plaćanje među bankama, a u narednom su se razdoblju sve se europske banke povezuju EFT sustavima (Buterin, Ribarić, Savić, 2015:146)

Govoreći o elektroničkom novcu, istim se smatra novac koji postoji isključivo unutar bankarskog sustava i čiji se promet ostvaruje računalnim sustavima i uporabom računalnih mreža, internetom i digitalnim sustavima za pohranu podataka – kreditnim karticama.

Digitalnom se pak valutom smatra onaj oblik elektroničkog novca koji djeluje kao alternativna valuta te ju je moguće prenositi među pojedincima bez posredstva tradicionalnog bankarskog sustava.

Digitalni odnosno elektronički novac jedan je od načina odvijanja elektroničkog plaćanja, a javlja se i širi posljedično s razvojem interneta te radi potrebe iskorištavanja mogućnosti računalnih mreža. Povećanjem broja elektroničkih transakcija povećava se ukupan promet računalnih mreža, čime se izravno utječe na zadovoljstvo potrošača te se pojednostavljenjem odvijanja transakcija smanjuju njihovi troškovi. U ovom je kontekstu bitno naglasiti kako su troškovi internetskih transakcija znatno niži od onih nastalih obavljanjem transakcija u bankarskim poslovnicama.

Iz navedenoga se zaključuje kako je razvoj digitalnog ili elektroničkog novca snažno uvjetovan zadržavanjem svih prednosti tradicionalnog, papirnatog, novca uklanjajući istovremeno sve eventualne nedostatke. Najveće su prednosti papirnatog novca:

- univerzalna prihvaćenost,
- anonimnost kupca,
- jednostavna verifikacija,
- nema potrebe za otvaranjem bankovnog transakcijskog računa
- nije potrebna poslovna sposobnost
- laka prenosivost.

Ključni su nedostaci papirnog novca (Buterin, Ribarić, Savić, 2015:146):

- mogućnost krivotvorenja,
- nepraktičnost transporta velikih količina,
- visoki troškovi distribucije i proizvodnje,
- ograničen broj nominacija,
- postojanje više valuta.

U realnim okolnostima gotovo pa je nemoguće zadržati sve prednosti, a ukloniti sve nedostatke papirnatog novca odnosno tzv. gotovine. Temeljna je razlika između elektroničkog i papirnatog novca, ta što elektronička verzija nije prenosiva. Drugim riječima, papirnata novčanica primljena u nekoj od prethodnih transakcija ponovno je uporabljiva i u daljnjim transakcijama. Novčanica je dakle lako prenosiva i traje više od jedne transakcije, što bi bilo iznimno korisno i za digitalne novčanice, prije svega jer se u tom slučaju digitalna novčanica

ne bi trebala pohranjivati u banku što bi smanjilo broj interakcija s bankom a samim time i troškove sustava.

U elektroničkom novčanom sustavu korisnik novčanice bi trebao svakoj novčanici, odnosno svakom skupu bitovnih podataka, dodati podatke o vlastitoj identifikaciji, zbog čega bi se količina bitovnih podataka pohranjenih u virtualnoj novčanici sa svakom transakcijom koja je pomoću nje obavljena povećavala. Zbog navedenoga bi broj mogućih transakcija takvim novčanicama bio ograničen maksimalnom veličinom novčanice, a jasno je da je to popriličan nedostatak i ujedno i razlog zbog čega još uvijek nisu razvijeni prenosivi sustavi elektroničkog novca i zbog čega, barem još uvije, svaka elektronička novčanica ima rok trajanja od jedne transakcije.

Elektronički novac, baš kao i papirnati, jamči anonimnost osobe koja pomoću istoga obavlja transakciju zbog čega ga nije moguće pratiti. Drugim riječima, osoba koja prima elektroničku novčanicu ne može ući u trag identitetu osobe koja ju je upotrijebila. Elektronički oblici novca, odnosno obavljanje financijskih transakcija razmjenom informacija elektroničkim putem temelj su elektroničkog poslovanja. Protok elektroničke informacije između dviju strana koje komuniciraju internetom omogućuje nesmetano promatranje, ali otvara opcije eventualnih zlouporaba od treće strane. S ciljem minimaliziranja ovakvih neželjenih situacija, koristi se zaštita kriptiranjem kao i provjera autentičnosti sudionika u transakciji.

Kriptografska se zaštita odnosi prije svega na razne kriptografske algoritme i mehanizme te dodatno razvijene protokole više razine pomoću kojih se osigurava zaštita elektroničke informacije, kao i privatnost subjekata koji obavljaju transakcije. Jasno je kako elektroničke valute moraju udovoljavati kriterijima koji se odnose na zaštitu privatnosti sudionika, koji su sve striktniji. Nadalje, elektroničke valute moraju zadovoljiti kriterije sigurnosti, brzine i pouzdanosti, kao i osigurati neposrednu naplatu i obradu resursa, kao i upravljanje rizicima (Buterin, Ribarić, Savić, 2015:148).

Uzevši u obzir da su elektroničke valute i dalje u fazi razvoja, no i da su općeprihvaćene od strane korisnika, niti jedna od trenutno dostupnih valuta ne udovoljava svim uvjetima, prije svega zato što još uvijek ne postoji nikakva usvojena standardizacija.

Za elektroničke valute koje su neovisne o bankarskom sustavu brzina provedbe transakcije ovisi o vremenu potrebnom da bi se ista odobrila, a isto u aktualnim uvjetima poslovanja iznosi nekolicinu sekundi. Ovakav je pristup moguć samo u realizaciji usluga bez potpore

reverzibilnih transakcija, koje u slučaju pogreške, neovlaštenog korištenja ili nepouzdanih dobavljača transfera nije moguće poništiti. Navedeno kao posljedicu ima minimaliziranje rizika plaćanja a ujedno i povećava vjerojatnost realizacije ugovora prije roka. Dakle, kriptovaluta je digitalno sredstvo razmjene, digitalni ekvivalent novcu, čija je temeljna karakteristika nepostojanje centralne institucije koja ih izdaje odnosno koja njima upravlja (Buterin, Ribarić, Savić, 2015:148).

Kriptovalute se generiraju procesom rudarenja ili razmjenom roba ili usluga. Održavanje stabilnosti kriptovaluta postiže se uporabom različitih unutarnjih mehanizama ugrađenih u njihov protokol. Kriptovaluta se razmjenjuje za stvarne valute na burzama prema tečaju ovisnom o odnosu ponude i potražnje. Danas je na tržištu prisutno preko 650 kriptovaluta, među kojima se po važnosti i značaju izdvaja bitcoin.

2.6. Pojmovno određenje kriptovaluta

Kriptovalute (eng. *cryptocurrencies*), virtualne valute (eng. *Virtual currencies*), virtualni novac (eng. *Virtual money*), digitalni novac (eng. *Digital money*), digitalne valute (eng. *Digital currencies*) sinonimi su kojima se nazivaju valute bazirane na blockchain sustavu.

Europska centralna banka usvojila je naziv eng. *Virtual currency schemes*, iz kojega se naslućuje kako je riječ o sustavu nekolicine komponenti, od kojih se kao ključna i specifična, izdvaja informacijski sustav na kojem se postojanje valute i temelji, odnosno bez čijeg prisustva valuta ne bi mogla funkcionirati (Ecb.europa.eu, 2012).

2.7. Odnos virtualnih valutnih shema i elektroničkog novca

Osnovne sličnosti i razlike između decentraliziranih virtualnih valutnih shema i elektroničkog novca su sljedeće (Plassaras, 2013:377):

1) Format, pojavnost novca: valuta se u oba slučaja pojavljuje u digitalnom obliku, a postoji i opcija prijenosa vrijednosti virtualnih valutnih shema na druge medije, primjerice tisak na papir, no isto ne treba miješati s tiskom klasičnih novčanica. Funkcija je takvog medija predstavljati materijalan nositelj vrijednosti skupa znakova koji je svojevrstan ključ potreban za trošenje novca. Poznavanje ključa izjednačeno je s posjedovanjem vrijednosti.

2) Obračunska jedinica: obračunska jedinica kod elektroničkog novca klasična valuta, primjerice USD, EUR, GBP, HR. Virtualne valutne sheme obračunavaju se u vlastitim obračunskim jedinicama (Bitcoin, Litecoin, Ethereum …)
3) Stjecanje valute: Elektronički novac stječe se preuzimanjem izravno od izdavača, bilo u digitalnom, bilo u stvarnom obliku, koji se zajednički prate na računu korisnika, ili uplatama na račun ili u naravi po različitim osnovama. Virtualne valutne sheme stječu se kupovinom ili trgovinom unutar virtualne zajednice korisnika.
4) Pravna reguliranost: elektronički je novac u potpunosti podložan regulativi klasičnih valuta, koju provode nacionalne institucije država (nacionalne banke i vlast). S druge strane, virtualne valutne sheme nisu centralizirano upravljane, a u velikom broju slučajeva nisu niti pravno regulirane, drugim riječima, u njihovoj regulaciji sudjeluje svaki zainteresirani korisnik. Osnovni regulator sustava je konsenzus većine korisnika proveden korištenjem određenih tehničkih sustava.
5) Izdavač: ovlašteni izdavač elektroničkog novca je legalno uspostavljena institucija a kod virtualnih valutnih shema izdavač je privatno poduzeće, pojedinac ili udruga.
6) Ponuda novca: ponuda elektroničkog novca posljedica je ponude i potražnje bazne ili klasične valute. Ponuda je regulirana od strane izdavatelja i ujedno služi kao fiskalni regulator ekonomije izdavatelja. Puštanje u opticaj ili povlačenje novca iz opticaja podložno je strogoj kontroli i regulativi. Nadalje, kod virtualnih valutnih shema ponuda je najčešće fiksna ili slijedi neki unaprijed predvidivi algoritam. Moguća je i opcija kod koje izdavatelj regulira ponudu, ali takva rješenja nisu šire prihvaćena zato što poništavaju osnovnu prednost sustava, decentraliziranost.
7) Mogućnost otkupa sredstava: elektronički novac kao ekstenzija legalnog sredstva plaćanja podrazumijeva neograničenu mogućnost otkupa od strane izdavača. Tečaj je u najvećoj mjeri rezultat tržišta klasičnih valuta i u većini slučajeva je relativno stabilan. Kod virtualnih valutnih shema nema garancija otkupa sredstava jer se kao obračunska jedinica koristi sama virtualna valuta (Mishkin i Eakins, 2005:44-51). Ovdje su glavni regulatori tečaja tržište i potražnja. Volatilnost je vrlo velika i vrijednost valute nije garantirana. Drugim riječima, opcija otkupa i prihvaćenost valute izravno utječu na njenu tržišnu vrijednost.
8) Nadzor i kontrola: kod elektroničkih inačica klasičnih valuta nadzor i kontrola provode se na jednak način kao i za klasični novac, od strane legalnih institucija. U ovom je slučaju pravni okvir egzistentan i potkrijepljen velikim obujmom sudske

prakse. S druge strane, virtualne valutne sheme slabo su pravno regulirane i brojne zemlje se i dalje nisu u dovoljnoj mjeri izjasnile u pogledu njihova statusa. Tako se iste smatraju vrijednosnicama, a ne novcem u pravnom smislu.

9) Sigurnost i rizik: elektronička inačica tradicionalnih valuta donosi novu, tehničku komponentu sustava, a samim time i nov faktor rizika. U praksi je riječ o operativnom riziku koji ne predstavlja prepreku za uporabu – prednosti sustava nadmašuju njegove nedostatke. Kod virtualnih valutnih shema, osim operativnog rizika, postoje značajni pravni i ekonomski rizici, koje korisnici u potpunosti preuzimaju. Ti rizici uvelike utječu na vrijednost valute, što znači na tečaj i likvidnost te su od mnogo većeg značaja od tehničkih i operativnih rizika.

Kriptovalute su u posljednje vrijeme prilično aktualna tema, no osim tehnološkog napretka i inventivnog dizajna prve kriptovalute – Bitcoina, mnogima je primarni motiv isključivo bila brza i velika zarada. Navedeno ne iznenađuje, osobito ako se uzme u obzir da je dana 1.1. 2016. Bitcoin imao cijenu od 434 US dolara, već 1. 1. 2017. bio je na 998 USD, a 31. 12. 2017. koštao je 12.755 USD. Skok s cijene s 1.000 na 12.000 u jednogodišnjem razdoblju pokazao se snažnim magnetom za špekulante te je par mjeseci potom Bitcoin došao na 18.000, da bi se nedugo potom njegova cijena prepolovila. Silovite i intenzivne oscilacije nanose štetu Bitcoinu kao valuti koja aspirira dugoročno opstati i zahvatiti najširi krug korisnika jer korisnici ne žele posjedovati valutu koja snažno aprecira, već ju tezaurira za budućnost. Nadalje, malo je onih koji žele posjedovati valutu koja snažno deprecira, već je se želi što prije riješiti. Opisana snažna volatilnost nije iznenađujuća s obzirom na to da su kriptovalute zasnovane na ideji financijskog sustava bez institucija, što isključuje i središnje banke čija je osnovna funkcija očuvati stabilnost vrijednosti novca.

Bitno je naglasiti kako je kriptovaluta u potpunosti čija se uporaba temelji na povjerenju zasnovanom na kriptografiji. Svaki je financijski sustav utemeljen na povjerenju no kod Bitcoina se povjerenje ne stječe po sili zakona, regulativom niti službenim dekretima, a također ne izvire niti iz povijesti institucija, stručnosti i vrlina čelnih osoba, kulturno-povijesnog nasljeđa, količine zlatnih (i ostalih robnih) rezervi i sličnog, nego se isključivo zasniva na povjerenju u matematiku, odnosno kriptografiju.

Dalje, iako se kriptovalute nominalno nazivaju valutama i unatoč tomu što pretendiraju preuzeti funkcije novca, trenutno kriptovalute ne ispunjavaju niti jednu funkciju novca. Stavimo li novac u kontekst općeprihvaćenog sredstva razmjene, mjerilo vrijednosti i

spremište vrijednosti kroz vrijeme, nedvojbeno se zaključuje kako kriptovalute nisu općeprihvaćene, samo anegdotalno služe kao mjerilo vrijednosti jer je mogućnost kupnje roba odnosno usluga u bitcoinima iznimka, a zbog snažne volatilnosti prouzrokovane nepostojanjem središnje institucije koja bi održavala stabilnost njegove vrijednosti, ne preporučuju se kao sredstvo konzervacije vrijednosti kroz dulje vrijeme.

Govoreći o kapacitetima, bitno je naglasiti kako je Bitcoin mreža snažnim širenjem prerasla vlastite kapacitete. Standardni platni sustavi procesuiraju po 2.000 transakcija po sekundi (s kapacitetom za preko 20.000), a Bitcoin može samo sedam. Zbog interesa pojedinih skupina još uvijek nije moguće postići konsenzus većine oko izmjene elemenata Bitcoin sustava koji bi omogućili bržu provedbu većeg broja transakcija, te zbog toga nastaju brojne druge kriptovalute koje u inerciji Bitcoin Core (Legacy) mreže vide prostor za vlastiti razvoj.

Slijedom navedenoga, opravdano se postavlja pitanje je li svjetskoj ekonomiji potrebno stotine ili tisuću kriptovaluta. Naposljetku, potrošnja energije i emisija štetnih plinova uslijed potrošnje energije je enormna čemu u prilog ide činjenica kako Bitcoin mreža troši energije koliko i država u rangu Grčke ili Izraela (DigiEconomist, 2018).

Oporezivanje kriptovaluta još je jedna kontroverza, a u kontekstu Republike Hrvatske se navodi kako je hrvatski sustav poreza na dohodak/dobit dostatno opremljen za akomodaciju problematike oporezivanja transakcija bitcoinom i da nije potrebno donositi posebna pravila (Čičin-Šain, 2017:687).

Promatrano u vremenskom razdoblju od dvije godine, većina je kriptovaluta ostvarila značajan porast cijene u promatranom razdoblju, a kod pojedinih je kriptovaluta taj rast poprimio značajke ekstrema, a najveći raspon od minimuma do maksimuma imale su NEO (234.162,00 %) i Ether (148.455,00 %).

Bitno je naglasiti da, kada se dnevne cijene promatraju na relativnoj razini, kao postotak promjene u odnosu na prethodni dan, za kriptovalute je značajan 4 do 40 puta veći raspon cijena u usporedbi s klasičnim financijskim instrumentima. Bez obzira što je koeficijent varijacija (kao omjer standardne devijacije u odnosu na aritmetičku sredinu) veći kod klasičnih financijskih instrumenata, to je prije svega zbog toga što je njihov prosječni dnevni prinos u promatranom razdoblju bio blizak nuli dok su kriptovalute u prosjeku rasle (primjerice Bitcoin u prosjeku 0,5% dnevno, što je na godišnjoj razini preko 500%). U isto je

vrijeme volatilnost kriptovaluta bila od 2 do 40 puta veća nego volatilnost uobičajenih financijskih instrumenata.

Dnevne promjene cijena kriptovaluta u najvećem broju slučajeva nisu korelirane s dnevnim promjenama cijena klasične financijske imovine. Izuzetak su korelacija Bitcoin Casha i indeksa S&P1200 te korelacija NEO i nafte, no iako su statistički signifikantne mogu se smatrati više kao slučajne, nasumične iznimke nego kao smisleni pokazatelji. Najveća negativna korelacija (-0,75) je kod indeksa Global Dow u odnosu na cijenu zlata, a najvišu pozitivnu (0,59) iskazuju dionički indeksi međusobno.

Prosječne unutardnevne oscilacije (aritmetička sredina razlika najviše i najniže dnevne cijene) u razdoblju od 1. 1. 2016. do 17. 1. 2018. iznosila je za Bitcoin 4,80%, za Ether 9,47%, a za Ripple 8,33% pri čemu je u istom razdoblju najlikvidniji i najveći svjetski burzovno trgovani fond SPDR S&P500 (ETF SPY) imao oko deset puta manje unutardnevne oscilacije (0,74%), što dodatno opisuje volatilnost kriptovaluta.

Rezultati financijske analize pokazuju iznimno visoku promjenjivost cijena kriptovaluta u odnosu na klasične financijske imovine. Također, cijene kriptovaluta nisu značajnije povezane s kretanjima na standardnim financijskim tržištima, što pak otvara nove mogućnosti za diverzifikaciju rizika pri konstrukciji portfelja. Zbog navedenoga se kriptovalute mogu promatrati kao nova investicijska klasa: distancirana od uobičajenih financijskih tržišta, no iznimno volatilna s potencijalom visokih prinosa, ali i gubitaka. Navedeno je razlog zbog čega se manjim investitorima, koji nisu u mogućnosti podnijeti totalne gubitke, ne savjetuje ulagati u kriptovalute.

Najizravnija prilika kriptovaluta manifestira se u vidu online plaćanja. Danas su najpopularniji oblici plaćanja online kreditne kartice, koje se nisu znatno unaprijedile u posljednjih 20 godina te su podložne prijevarama. Drugi popularan način je Paypal, no pati od sličnih problema (Meisser, 2013).

2.8. Ekonomske značajke kriptovaluta

Velika transparentnost kriptovaluta je jedan od najbitnijih razloga zašto digitalne valute pridonose razvoju društva. Upotreba kriptovaluta je anonimna, ali sve se transakcije pohranjuju u otvorenoj knjizi (*blockchain*). To znači da su podaci vidljivi svima u bilo kojem trenutku, i u tome se ističe transparentiji bankarski sustav. Pri kupnji kriptovaluta nije bitno

gdje se kupci nalaze iz razloga što je sve omogućeno preko mobitela kojeg danas svi koriste. Bitne prednosti implikacije kriptovaluta: „U svijetu gdje e-trgovina bilježi rast, uniformna odnosno jednoobrazna valuta bi omogućila poslovno kruženje u kojem ne postoji rizik izlaganja valutnog tečaja. Smanjenje transakcijskog vremena bi omogućilo povećanu efikasnost trgovine uz smanjenje konverzijskih troškova trenutka društvu kao takvom. Dodatno, micanje mogućnosti da se stvara dodatna valuta pruža nadu migaciji potencijalnih rizika inflacije, ali i može generirati upite vezano za državno saniranje deficita te likvidnosti financijskih tržišta“ (Waltzer, 2014).

Postoji niz načina na koji se mogu koristiti kriptovalute. Većina ljudi koji koriste digitalne valute, koriste ih u svrhu investiranja, tako da prate tržišne fluktuacije kriptovaluta te kupuju ili prodaju iste. Neki korisnici ih koriste za kupnju ulaznica u svrhu raznih događaja, kockanje na internetu, u svrhu transfera novca i sličnih situacija. Mnogi ne favoriziraju kriptovalute iz razloga što olakšava crnoj ekonomiji lakše obavljanje transakcija putem interneta zbog transparentnosti. Kao i kod svake nove tehnologije, postoje oni koji iskorištavaju naivnost i neiskustvo druge strane, varanjem i krađom njihovog zarađenog novca. To se svakako pokazalo kao slučaj s digitalnim valutama pa je važno biti svjestan sigurnosnih rizika. Bitne mane u međunarodnom poslovanju: „Volatilnost kriptovalute predstavlja problem jer u tom slučaju same kompanije se neće upuštati u poslove koristeći digitalne valute, uzimajući u obzir da bi to pridonjelo nepredvidivosti i nesigurnosti tekućih poslova. Pošto nema središnjeg regulatornog tijela koje bi nadgledalo transakcije, a i samu narav kriptovaluta, konkretno B*itcoina* jer je limitiran iznosom i ne može se standardnim monetarnim mehanizmima dovoditi pod kontrolu u slučaju devijacija, nije teško pretpostaviti otklon ka korištenju“ (Meisser, 2013: 6).

2.9. Pregled tržišta kriptovaluta

Kako je već spomenuto, danas na tržištu egzistira preko 650, a prema nekim autorima čak i preko 700 aktivnih, a računajući i one ugašene broj značajno prelazi 1000 (Koblitz, Menezes, 2016:9).

Situacija na tržištu je takva da je i dalje prisutan trend porasta i broja valuta i tržišne kapitalizacije, pri čemu se potrebno osvrnuti na činjenicu kako veći dio valuta radi iznimno male kapitalizacije nema ekonomski značaj. Najbolji pokazatelji popularnosti kriptovaluta su tržišna kapitalizacija i dnevni promet. Prema tržišnoj kapitalizaciji pokazatelji su sljedeći:

- preko 10000 mil. USD vrijedi 1 digitalna valuta
- preko 1000 mil. USD vrijede 2 digitalne valute
- preko 100 mil. USD vrijedi 9 digitalnih valuta
- preko 10 mil. USD vrijede 42 digitalne valute
- preko 1 mil. USD vrijedi više od 100 digitalnih valuta

Ukupna kapitalizacija prvih 100 valuta iznosi više od 25 milijardi $. Usporedbe radi, prije pet godina je samo 34 valute vrijedilo preko 1 mil. $ (Gandal i Halaburda, 2014:8). Aktualnim trendom, ukupna kapitalizacija se svake godine gotovo utrostruči.

Od svih aktualnih valuta, njih 605 ima zabilježenu bilo kakvu tržišnu kapitalizaciju, no bitno je naglasiti kako popis nije potpun jer valute nastaju gotovo na dnevnoj bazi no one najkvalitetnije bivaju predmetom trgovine na tržištu i prisutne na web stranici coinmarketcap.com, dok su druge izostavljene uslijed premale likvidnosti. Ipak, postojanje velikog broja irelevantnih kriptovaluta ne umanjuje činjenicu da važnost tzv. altcoin valuta raste u smislu alternativnih investicijskih opcija (Elendner i sur., 2016).

Alternativne varijacije kriptovaluta pojavljuju se pod nazivom Altcoins, a također su bazirane na blockchain tehnologiji. Drugim riječima, riječ je o alternativnim verzija bitcoina, što objašnjava porijeklo naziva (Mayo, 2012). Prema načinu implementacije, dvije su vrste kriptovaluta. Tako su valute kao Bitcoin, Litecoin, Peercoin, Dogecoin i slične bazirane na implementaciji vlastite blockchain arhitekture, dok primjerice Augur, MadeSafeCoin, Golem, DigixDAO, StorjcoinX koriste platforme treće strane. Implementacija vlastite blockchain tehnologije složen je i zahtjevan proces, čiji je preduvjet izvrsno tehničko znanje za stvaranje, pa čak i samo za kloniranje postojeće blockchain tehnologije. Kreiranje digitalne valute na bazi postojeće tehničke osnove je, s druge strane jednostavniji proces koji ne traži veliku tehničku stručnost. U tom je slučaju riječ o principu korištenja tehničkih usluga dostupnih najčešće kao internetski servis (Mayo, 2012).

Na tržištu u posljednjih 2 godine puno je projekata kojima se želi unaprijediti sustav kriptovaluta. Više od 800 ih je propalo i danas ih više nema. To nam daje naznake kakvo je tržište danas i eng. *dot-com bubble* 2000. godine. Nove kriptovalute koje se stvaraju kroz proces koji se naziva eng. *Initial Coin Offering (ICO)* u kojem startup emitira novac koji investitori mogu kupiti. Ljudi danas često kupuju u ICO jer su tu digitalne valute jeftine i omogućuju potencijalnu zaradu u budućnosti. Tokom 2017. godine tvrtke su putem ICO-a prikupile 3,8 milijardi američkih dolara, a u 2018. godini 11,8 milijardi dolara. Danas su na

stotine tih projekata mrtvi zbog prevara među kojima je najpoznatiji Bitconnect. Mnogi su stvarali nove procese iz šale ili proizvod nikad nije materijaliziran. Kriptovalute su pod velikim pritiskom, ali svi koji trguju njima vjeruju da će regulatori pokazati više razumijevanja za njih te da bi to moglo obnoviti tržište. Arthur Hayes, izvršni direktor kriptovalutne mjenjačnice BitMEX, rekao je kako bi Bitcoin do kraja 2018. godine mogao ojačati na više od 50.000 američkih dolara.

3. BITCOIN KAO NAJPOZNATIJA KRIPTOVALUTA

3.1. Pojmovno određenje Bitcoina

Bitcoin je digitalna, decentralizirana, pseudonimna valuta, neovisna o državnim odlukama i odlukama drugih pravnih osoba i čija je vrijednost neovisna o vrijednosti zlata i drugih roba. Bitcoin valuta se oslanja na ravnopravnu računalnu mrežu, a integritet održava pomoću kriptografije (Gervais, 2014:1).

Prvi spomen ove najveće i najpoznatije kriptovalute zabilježen je 2008. godine u članku naslovljenom *Bitcoin - A Peer-to-Peer Electronic Cash System* kojim je predstavljen način funkcioniranja Bitcoina (Buterin, Ribarić, Savić, 2015:145).

Bitno je naglasiti kako je pojam bitcoina skovan od engleskih riječi *bit* – mjerna jedinica količine informacija i eng. *coin* – kovanica (Kalinić i Visković, 2014:281). Nadalje, najmanja jedinica Bitcona je Satoši, a jedan Bitcoin sadrži 100 milijuna Satošija. Prema dizajnu cijelog sustava, ukupna količina svih Bitcoina ne prelazi 21 milijun, odnosno 2100 milijardi Satošija. Ukupna količina Bitcoina u optjecaju se povećava planirano i očekivano, temeljem programskog koda, do postizanja maksimalne količine u 2140. godini (Woo, Gordon i Iarlov, 2013:2).

Nedugo nakon objave članka, 2009. godine, objavljen je i software kada isti ulazi u uporabu. Autor članka i softwarea Bitcoina široj se javnosti predstavio pseudonimom Satoshi Nakamoto, no pravi identitet osobe autora članka i utemeljitelja ove virtualne valute do danas nije otkriveno. Naravno, zabilježena su mnoga nastojanja otkrivanja njegova pravog identiteta, a do sada je poznato samo da je Nakamotov internetski račun povezan s Japanom, dok mu je e-mail adresa preko koje je pristupio vlastitom profilu registrirana preko besplatnog e-mail registriranog u Njemačkoj. Nerijetko se navodi kako je u kreaciji bitcoina sudjelovalo više osoba ili čak organizacija, jer je to posao ogromna opsega za samo jednu osobu.

Valuta je dosegla iznimnu popularnost prvoj polovini 2013. godine, kada je zbog krize ciparskih banaka mnoštvo ljudi povuklo štednju iz tih banaka te je dio tog novca bio uložen u kupnju Bitcoina, prije svega jer Bitcoini nisu vezani uz tečaj neke druge valute. Njihova se cijena određuje slobodno na tržištu putem ponude i potražnje (Mayo, 2012).

Pojmovi koji su u vezi s Bitcoinom su rudarenje odnosno pojam rudara. Bitcoine je moguće steći ili derivativnim putem – kupoprodajnim ugovorom, ugovorom o zamjeni,

nasljeđivanjem itd., ili originalnim putem, specifičnim za virtualne valute, a to je rudarenje. Rudarenje je, najopćenitije rečeno, postupak provjere svake transakcije Bitcoina na način da se rješavaju komplicirani algoritmi u zamjenu za novostvorene Bitcoine. Rudar (eng. *miner*) jest osoba koja na takav originaran način stekne vlasništvo nad novonastalim bitcoinom (Čičin-Šain, 2016:656).

Bitcoin je složen sustav, a njegova implementacija uključuje kombinaciju kriptografije, distribuiranih algoritama i usuglašenog ponašanja zajednice korisnika. Štoviše, najnoviji razvoj događaja ukazuje na okolnost da Bitcoinove operacije mogu uključivati rizike čija priroda i udio su širokom puku potpuno nerazumljivi (Badev, Chen, 2014:2).

U prvim godinama korištenja, Bitcoin nije imao veliku vrijednost, a aktivnosti su bile slabe i najčešće su se svodile na razmjenu Bitcoina među pojedincima entuzijastima. Smatra se da je prvu kupovinu ovom kriptovalutom izvršio kompjutorski programer 2010. godine koji je za pizzu vrijednu 25 dolara platio 10.000 bitcoina, čija je današnja vrijednost oko 2,2 milijuna dolara (Buterin, Ribarić, Savić, 2015:149).

3.2. Nastanak i povijest bitcoina

Sustav na kojem je utemeljen Bitcoin naziva se eng. *Peer-to-Peer*, a njegova je temeljna odlika ta da se temelji na složenim kriptografskim algoritmima.

Peer-to-peer (eng.) označava mrežu u kojoj nema središnjeg autoriteta koji izdaje novi novac ili prati transakcije. Zadacima u takvoj mreži upravljaju kolektivno čvorovi mreže. Ključne su prednosti takvog sustava pojednostavljen prijenos novca preko interneta, bez posrednika, pri čemu treća strana ne može spriječiti niti na bilo koji način upravljati korisnikovim transakcijama.

Sam izraz eng. *Peer-to-peer* engleskog je porijekla a u prijevodu znači „isti sa istim“ ili „svaki sa svakim,“ u tehnologiji računalnih mreža podrazumijeva koncept umrežavanja računala bez poslužitelja, u kojem je svako računalo inteligentna radna stanica, koja pronalazi druga računala putem emitiranja paketa podataka/poruka, i izravno s njima komunicira, bez da je nužna autorizacija na nekom centralnom poslužitelju (Bandara, Dilum i Jayasumana, 2013).

U bitcoin sustavu ne postoji središnja banka koja izdaje novac te čuva i obrađuje transakcije, niti postoji jedinstveni vlasnik bitcoin mreže. Ključna razlika bitcoina u odnosu na centralizirane sustave proizlazi iz činjenice da svaki korisnik ima uvid u vlastite transakcije

kao i transakcije ostalih sudionika. Svaka transakcija sadrži digitalni potpis korisnika koji ju je započeo. Digitalni potpis se generira iz kombinacije transakcijske poruke i privatnog ključa korisnika. Potpis je u svakoj poruci različit, zbog čega je krivotvorenje i zlouporaba neizvediva bez originalnog privatnog ključa. Svaki korisnik posjeduje i javni ključ koji je u matematičkoj relaciji s privatnim ključem (Buterin, Ribarić, Savić, 2015:149).

Bitcoin se temelji na raspodijeljenom sustavu koji se sastoje od međusobno povezanih čvorova, tj. poslužitelja koji imaju mogućnost samostalno se organizirati u mrežne topologije kako bi podijelili raspoložive resurse, primjerice korisničke podatke, procesno vrijeme, kapaciteta za pohranu podataka ili mrežne propusnosti. Oni se mogu samostalno adaptirati na ispade funkcionalnosti i nepredvidive dolaske i odlaske čvorova na mreži, uz zadržavanje prihvatljivog stupnja performansi bez potrebe za nadzorom, kontrolom i podrškom iz jednog središnjeg mjesta (Buterin, Ribarić, Savić, 2015:149).

Slijedom navedenoga, moguće je identificirati ključne osobine partnerskog načina rada (Buterin, Ribarić, Savić, 2015:149):

- ravnopravnost čvorova,
- izravna komunikacija među čvorovima,
- samostalno prikupljanje informacija o dostupnosti drugih čvorova,
- pojedinačni čvorovi imaju u svom lokalnom sustavu za pohranu na raspolaganju samo dio podataka, odnosno podskup ukupnih podataka dostupnih na mreži.

Zagovornici Bitcoina promoviraju stav da isti predstavlja pravedan novac koji će u narednom razdoblju ukinuti bankarski monopol te koji će pružiti mogućnost brzog i jednostavnog plaćanja pod pseudonimom. Ipak, velik broj zagovornika kriptovaluta općenito u potrazi je za načinom kako iskoristiti novonastalu „zlatnu groznicu“ i ostvarili zaradu. Tako se iz dana u dan povećava broj onih koji se bave prijevarama u sustavu, počevši od krađe tuđih računala za izradu Bitcoina pa do obične krađe virtualnih novčanika.

3.3. Kriptografski mehanizmi Bitcoina

Kriptografija, kao znanstvena disciplina čiji je predmet interesa analiza i iznalaženje metoda pomoću kojih je moguće poslati poruku u obliku u kojem ju nitko osim primatelja neće moći pročitati, ima pred sobom temeljni zadatak – omogućiti dvjema osobama komuniciranje preko nesigurnog komunikacijskog kanala tako da treća osoba, koja može nadzirati komunikacijski

kanal, ne može razumjeti njihove poruke. Poruka koju pošiljatelj želi poslati primatelju naziva se otvoreni tekst. Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni ključ, a postupak se naziva šifriranje, a rezultat šifriranja šifrirat. Nakon šifriranja, pošiljatelj pošalje šifrirat preko nekog komunikacijskog kanala. Treća osoba prisluškujući može doznati sadržaj šifrirata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primatelj koji zna ključ kojim je šifrirana poruka može dešifrirati šifrat i odrediti otvoreni tekst. Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. U najširem je smislu riječ o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Navedene dvije funkcije preslikavaju osnovne elemente otvorenog teksta u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene skupine funkcija, ovisno o karakteristikama i specifičnostima ključa. Skup svih mogućih vrijednosti ključeva zove se prostor ključeva, a kriptosustav je sastavljen od kriptografskog algoritma te svih mogućih otvorenih tekstova, šifrata i ključeva.

Formalna definicija kriptosustava je sljedeća:

Definicija 1. Kriptosustav je uređena petorka (P, C, K, E, D) za koju vrijedi:

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

Nadalje, dvije su vrste kriptosustava - kriptosustavi s tajnim ključem (simetrični) i kriptosustavi s javnim ključem (asimetrični). U ovom je radu fokus na kriptosustave s javnim ključem, s obzirom da takvi imaju važnu ulogu u funkcioniranju Bitcoina.

3.4. Kriptografija javnog ključa

Kriptosustav s javnim ključem sadržan je od dva skupa funkcija, funkcija za šifriranje eK i funkcija za dešifriranje dK, gdje K prolazi skupom svih mogućih korisnika, čije se osobine sljedeće: za svaki K je dK inverz od eK, za svaki K je eK javan, ali je dK poznat samo osobi K te za svaki K je eK osobna jednosmjerna funkcija, funkcija kojoj je teško izračunati inverz

bez poznavanja nekog dodatnog podatka. Ključ eK se zove javni ključ, a dK se zove tajni ključ.

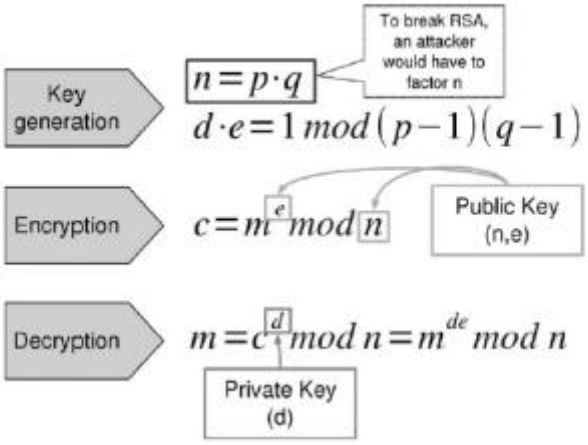
Začeci kriptografije javnog ključa pripisuju se matematičarima imena Diffie i Hellman, i koji su predložili korištenje dva različita, matematički povezana ključa. Javni ključ je objavljen i svima dostupan, a služi za šifriranje poruke namijenjene osobi – vlasniku javnog ključa. Dešifriranje poruke obavlja se korištenjem tajnog ključa poznatog samo primatelju poruke. Razmjena ključeva nije potrebna prije komunikacije, a tajni ključ nije moguće izračunati iz javnog ključa niti dešifrirati poruku pomoću javnog ključa. Asimetričnost je postignuta korištenjem asimetričnih matematičkih algoritama, primjerice faktorizacije velikih brojeva. Jednostavno i brzo se mogu pomnožiti dva velika prosta broja, ali tako dobiveni broj nije moguće jednostavno ponovno faktorizirati bez poznavanja jednog od faktora. Jedan od faktora bi mogao predstavljati upravo tajni ključ osobe čiji je umnožak javni ključ.

Navedenim konceptom postignute su sljedeće prednosti:

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

Algoritmi asimetrične kriptografije su mnogobrojni no pojedini su vrlo uspješni dok su drugi izašli iz uporabe jer su kriptoanalitičari otkrili njihove propuste. Jedan od najpoznatijih i najkorištenijih algoritama kriptografije javnog ključa jest RSA kriptosustav koji je dobio ime po prvim slovima prezimena njegovih autora: Rona Rivesta, Adija Shamira i Leonarda Adlemana. RSA je utemeljen na problemu umnoška velikih prostih brojeva i složenosti faktorizacije rezultata.

Slika 3. Shema šifriranja u RSA kriptosustavu



3.5. Hash-funkcija

U suvremenoj kriptografiji jednostrana hash funkcija od velike je praktične primjene, a u suradnji s ostalim kriptografskim alatima, ista se koristi kako bi se utvrdila vjerodostojnost podataka i njihovog porijekla. Učinkovita funkcija koja preslikava niz proizvoljne duljine u binarni niz fiksne duljine naziva se jednostrana hash-funkcija. Binarni niz fiksne duljine se zove hash-vrijednost (engl. *hash-value*) i uobičajeno je duljine 128 ili 160 bitova.

Temeljne karakteristike hash-funkcije su jednosmjernost zbog čega je gotovo nemoguće doći do originalne poruke. Svaki par poruka treba se preslikati u različite hash-vrijednosti, čak i ako se poruke razlikuju za samo jedan bit. U stvarnosti, postoje parovi poruka koje rezultiraju istom hash-vrijednošću, ali vjerojatnost mora biti mala da će taj par biti sastavljen od smislenih podataka, primjerice teksta. 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 obraduje. Najčešće duljine hash-vrijednosti su 128 i 160 bita. S obzirom da je algoritam hash-funkcije javan, njena sigurnost utemeljena je 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 zlonamjernih manipulacija. U kombinaciji s asimetričnim kriptografskim algoritmima, hash-vrijednost se koristi i za osiguravanje porijekla informacije preko sustava digitalnih potpisa.

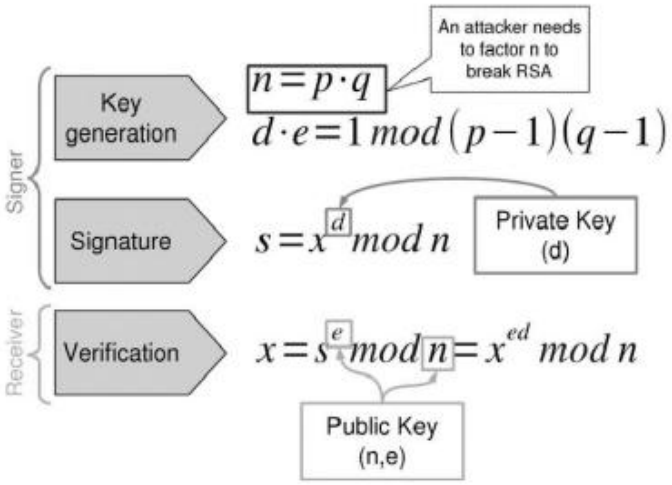
3.6. Digitalni potpis

Koncept digitalnog potpisa postao je izvediv zahvaljujući pojavi asimetrične kriptografije. Kao i kod uobičajenog parafa izvedenog rukom, postoji samo jedna osoba koja je sposobna staviti potpis na neki dokument, no mnogo drugih osoba je sposobna pročitati taj potpis.

Digitalni potpis je baziran na konceptu para ključeva. Analogno stvarnom svijetu, postoji jedan ključ koji je poznat osobi koja potpisuje dokument u vidu tajnog ključa. U tom smislu, kada osoba potpiše dokument vlastitim tajnim ključem, garancija je da su ti potpisani podaci izričito i jedinstveno povezani s tom osobom. Kako bi se potpis mogao identificirati ili verificirati, osoba distribuira svoj javni ključ. Podaci koje je moguće potpisati mogu biti bilo koji digitalni sadržaji neovisni o podatkovnoj veličini, jer se za ulaz u funkciju digitalnog potpisivanja uzima fiksna veličina i operacija kriptografske hash-funkcije.

Samo potpisivanje svedeno je na to da potpisnik pomoću hash-funkcije dobiva iz dokumenta podatak fiksne duljine, a potom primjenjuje enkripciju na dobiveni podatak, koristeći tajni ključ. U slučaju da se želi provjeriti taj potpis, pomoću hash-funkcije se iz dokumenta dobiva podatak fiksne duljine nakon čega se ta vrijednost razmatra zajedno s dobivenim potpisom na koji se primjenjuje javni ključ potpisnika. Kada se te dvije vrijednosti poklapaju, potpis je ispravan.

Slika 4. Shema digitalnog potpisa u RSA kriptosustavu



Slika 3. prikazuje proces potpisivanja u RSA kriptosustavu. Vidljivo je da se kriptosustav sastoji od tri dijela - generiranja ključa, potpisivanje i verifikacija. Generiranje ključa se odvija na isti način kao i kod šifriranja u RSA. Potpisivanje se izvodi tako da se poruka zapiše u obliku $s = x\ d \bmod n$, gdje je x originalni tekst, a d privatni ključ. Verifikacija je završena kada s e usporedimo s originalnom porukom x. Ako je $x = s\ e = x\ e{\cdot}d = x \bmod n$, potpis je točan.

RSA koristi se u praksi s ključevima od 1024 ili 2048 bita. Slika 4. prikazuje primjer od 2048-bitni RSA ključ, a suvremeni računalni procesori imaju 32-bitni ili 64-bitni.

3.7. Oporezivanje bitcoina

Kriptovalute se razvijaju iz dana u dan te im tako popularnost raste, što dovodi do pojave poreza na kriptovalute. U Hrvatskoj dana 14. srpnja 2017. godine donešen je zakon na temu oporezivanja kriptovaluta. Sav profit koji ostvari fizička ili pravna osoba mora prijaviti te platiti porez. Pod pojmom profita se smatra sav novac u kunama koji je primljen na račun na temelju poslovanja putem burze ili mjenjačnice.

U SAD-u kriptovalute se smatraju kao kapitalno dobro, te smatraju kako kriptovalute zadovoljavaju sve tri funkcije novca, te samim time kriptovalutu smatraju konvertibilnom valutom. Australija se razlikuje od SAD-a po tome što oni smatraju da su kriptovalute sredstvo razmjene, a ne strana valuta. Singapur smatra kako virtualni novac ne može biti vrijednosni papir niti zakonito sredstvo plaćanja da bi ga oni regulirali, no zato će regulirati burze i mjenjačnice na kojima se svakodnevno izvršavaju transakcije kriptovaluta. U tim transakcijama Singapur navodi kako žele spriječiti nelegalne radnje kao što su pranje novca. U Europi se smatra kako elektronički novac odnosno kriptovalute ne mogu biti zakonito sredstvo plaćanja jer nisu centralizirane. Mnogi tvrde da to nije financijski instrument te da ne mogu biti novčano sredstvo. Nitko se ne može odlučiti što će biti kriptovalute u ekonomskom i financijskom smislu, ali svakako većina država ih smatra više dobrom nego novčanim sredstvom.

Međunarodna organizacija Financial Action Task Force (FATF) u svojem izvješću navodi kako virtualnim novcem smatra digitalnu reprezentaciju određene vrijednosti pomoću koje je moguće digitalno trgovati te koja zadovoljava navedene funkcije:

- sredstvo je razmjene (*medium of exchange*),
- jedinica je za mjeru vrijednosti (*unit of account*) te
- služi za pohranjivanje vrijednosti (*a store of value*), ali nije službeno sredstvo plaćanja niti u jednoj državi.

Virtualni je novac potrebno razlikovati od realnog (tzv. fiat) novca koji postoji u obliku kovanica i novčanica, koji cirkulira državnom ekonomijom te koji je prihvaćen kao sredstvo razmjene u zemlji koja ga izdaje.

Virtualni se novac razlikuje i od elektroničko novac jer je potonji samo digitalna reprezentacija fiat valute koja služi elektroničkom prijenosu vrijednosti izražene u fiat valuti. Digitalna valuta označava digitalnu reprezentaciju virtualne valute ili prave, fiat valute. Trenutačno najpoznatiji predstavnik takvih valuta jest upravo valuta Bitcoin.

Prilikom određivanja sustava oporezivanja prometa te dobiti od Bitcoina jedno od temeljnih pitanja je pitanje kvalifikacije Bitcoina, odnosno definiranje što je točno po svojoj prirodi Bitcoin (Lambooij, 2014:138-144).

Ovakvo određenje Bitcoina relevantno je i za pitanje oporezivanja izravnim porezima (porez na dohodak odnosno porez na dobit), ali jednako tako i neizravnim porezima kao što je porez na dodatnu vrijednost. Različite države svijeta na to pitanje dale su različite odgovore. Dva se modela mogu posebno izdvojiti – koncept Bitcoina kao novca te koncept Bitcoina kao dobra. U skladu s navedenim se izdvajaju različiti modeli oporezivanja (Čičin-Šain, 2016:661).

3.8. Oporezivanje bitcoin transakcija neizravnim porezima

Oporezivanje bitcoin transakcija neizravnim porezima izvan Europske unije u velikoj se mjeri razlikuje od njihova oporezivanja tim porezima unutar Europske unije.

Poreznopravna regulacija izvan Europske unije

Kvalifikacija Bitcoina osobito je važna kada je riječ o oporezivanju neizravnim porezima. Najveći broj zemalja koje imaju nekakvu vrstu općeg poreza na promet plaćanja novcem izuzeta su od oporezivanja tim porezom. Iz navedenoga proizlazi kako je činidba, čiji je sadržaj davanje novca kao protunaknade za kupljeno dobro ili pruženu uslugu, oslobođena od

terećenja općim porezom na promet. Navedeno se oslobođenje u pravilu odnosi samo na transakcije s valutama koje su zakonsko sredstvo plaćanja.

Nacionalna pravna regulativa izražena prije svega Zakonom o porezu na dodanu vrijednost predviđa isto takvo oslobođenje. S druge strane, brojne su zemlje zauzele stav kako je plaćanje Bitcoinom zapravo sklapanje ugovora o razmjeni (eng. *barter*), što za sobom povlači oporezivanje obiju transakcija porezom na dodanu vrijednost. Tako su, primjerice, u Australiji obveznici australskog poreza na dodanu vrijednost (eng. *goods-and-services tax*, GST) sve do 30. lipnja 2017. godine morali plaćati australski porez na dodanu vrijednost ako prodaju virtualne valute te su bili obvezni platiti taj porez ako prime Bitcoine kao oblik plaćanja, što je bila posljedica činjenice da se Bitcoin nije smatrao valutom. Ako je isporuka dobara, odnosno pružanje usluga, bilo oporeziva transakcija, tada se GST plaćen na primljene bitcoine mogao koristiti kao ulazni GST te odbiti od GST-a po izlaznim računima.

Iz navedenoga je jasno vidljivo kako su Bitcoin transakcije u Australiji bile podložne dvostrukom oporezivanju tamošnjim porezom na dodanu vrijednost, odnosno GST-om. Time je način trgovanje bitcoinima na australskom tržištu bilo znatno oslabljen, a takva politika polučila je kritike u australskom društvu start-up trgovačkih društava, zbog čega je australska vlada ukinula oporezivanja kupnje bitcoina GST-om od 1. srpnja 2017. godine kao jednu od mjera za pozicioniranje Australije kao globalnog centra za financijsku tehnologiju.

Digitalne se valute od 1. srpnja u Australiji, za potrebe primjene GST-a, tretiraju poput pravog novca (eng. *allowing digital currencies to be treated just like money for GST purposes*) (Čičin-Šain, 2016:656).

3.9. Analiza bitcoina na globalnom financijskom tržištu

3.9.1. Razvoj i tehnička analiza

Značajniji razvoj Bitcoina evidentiran je, kako je ranije i navedeno, 2011. godine, kada je zabilježen prvi veći porast vrijednosti na oko 30 američkih dolara. U tom je razdoblju velika količina pozornosti bila usmjerena na ciparsku financijsku krizu 2013. godine, kada je vrijednost jednog bitcoina premašila 250 dolara.

Tijekom ciparske financijske krize naglo se povećava broj korisnika, kao i broj transakcija te nastaju prve online mjenjačnice a sve više poduzeća počinje prihvaćati Bitcoin kao sredstvo plaćanja. Kada je Bitcoin prihvatio jedan od kineskih internetskih giganta, Bitcoinu cijena naglo raste.

U navedenom se razdoblju naglo povećava broj korisnika i broj transakcija te nastaju prve online mjenjačnice. Nadalje, 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. Nedugo nakon toga u Kini se otvara prva Bitcoin mjenjačnica, koja je po ostvarenom prometu bila veća od do tada najpopularnije japanske Mt. Gox i europskog Bitstampa. U istom se razdoblju u Kanadi postavlja prvi bitcoin bankomat.

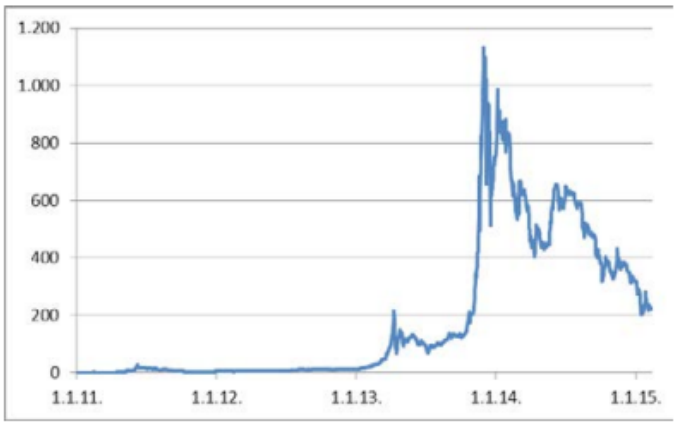
U studenom 2013. godine Bitcoin je priznat kao legitimno sredstvo plaćanja u Sjedinjenim Američkim Državama, što uzrokuje rast do 1.099 dolara. Razvoj je događaja upućivao na to da će Bitcoin postati globalna zamjena za valute regulirane od strane monetarnih vlasti.

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. Navedena su očekivanja rezultirala prividnom situacijom u kojoj je vrijedio stav kako će Bitcoin u budućnosti sve više dobivati na značaju, a ista su postala generator porasta potražnje i rasta cijene. Ovome je potrebno pridodati i špekulativna nadanja dijela neiskusnih ulagača koji su, potaknuti medijskim napisima, ulaganje u Bitcoin protumačili kao izuzetnu investicijsku priliku (Buterin, Ribarić, Savić, 2015:151).

Rast je zaustavljen odlukom Centralne kineske banke u prosincu 2013. godine kojom se zabranjuje upotreba Bitcoina u svim kineskim financijskim institucijama. Kineska odluka bila je povod, odnosno okidač zbog koje je došlo do naglog pada vrijednosti Bitcoina, no ne i uzrok daljnjeg pada vrijednosti Biotcoina.

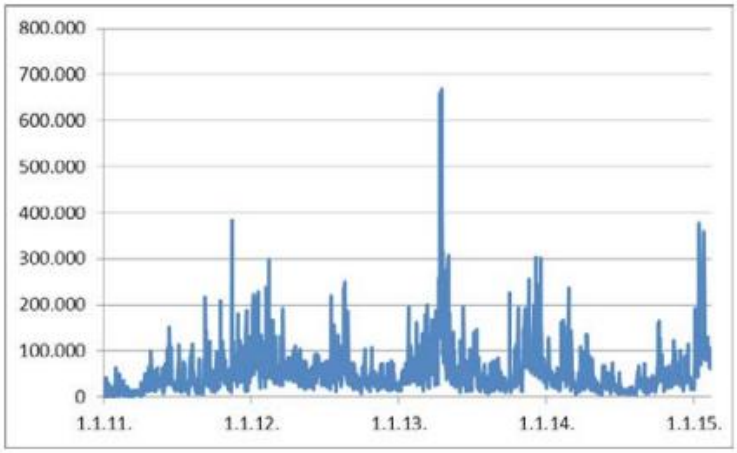
Pad vrijednosti uzrokovalo je to što se kod dotadašnjeg naglog porasta cijene bila riječ o pojavi poznatoj kao investicijski balon. Ilustracija 5. prikazuje kretanje ponderirane cijene bitcoina, a Ilustracija 6 kretanje volumena trgovine bitcoinom. Ilustracija 7 prikazuje faze nastanka investicijskih balona (Buterin, Ribarić, Savić, 2015:152).

Ilustracija 5. Kretanje cijene bitcoina od 1. 1. 2011. do 11. 2. 2015. godine (u $)



Izvor: https://www.quandl.com/BAVERAGE/USD-USD-BITCOIN-Weighted-Price

Ilustracija 6. Volumen trgovanih bitcoina od 1. 1. 2011. do 11. 2. 2015. godine



Izvor: https://www.quandl.com/BAVERAGE/USD-USD-BITCOIN-Weighted-Price

Ilustracija 7. Faze investicijskog balona

Izvor: Rodrigue (2008)

Do dosezanja maksimalne cijene od 1.099 dolara nije bilo moguće zamisliti da će se rast vrijednosti Bitcoina zaustaviti, a osobito ne pasti. U najprosperitetnijem razdoblju javnost se upoznala s velikim porastom cijena kao i s tim kad se buduća vrijednost Bitcoina ekstrapolirala temeljem povijesnih podataka. U to doba javnost, pod utjecajem medijske i sveopće društvene euforije, kupuje Bitcoin povećavajući mu na taj način, zbog priljeva novog kapitala, još više vrijednost.

Ipak, nedugo nakon toga dolazi do pada vrijednosti koji je, uz manje oscilacije, i dalje aktualan. Početkom veljače 2014. godine zabranjen je rad jedne od najpoznatijih bitcoin mjenjačnica Mt. Gox zbog navodnih tehničkih problema, a nakon nekoliko tjedana u mjenjačnici priznaju kako su doživjeli upad hakera u sustav zbog čega su izgubili 850 tisuća Bitcoina, što je tada iznosilo oko 473 milijuna američkih dolara. 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 dolara (Buterin, Ribarić, Savić, 2015:153).

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 (eng. *first sell off*). Sljedeća velika prodaja Bitcoina zabilježena je u vrijeme njegove visoke cijene kad institucijski investitori izlaze iz pozicija i prodaju Bitcoin.

Uočava se velika podudarnost kretanja cijena Bitcoina s uobičajenim kretanjima u slučaju pojava 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 prepoznaju na primjeru Bitcoina.

Tehnička analiza pokazuje kako je kod pada cijene najprije probijena zona potpore na 650 dolara koja je zatim postala zona otpora. Kao nova zona potpore pojavila se razina cijene od 400 dolara, ali i ta je cijena uskoro probijena te je postala nova zona otpora. Najnovija zona potpore uspostavljena je sredinom siječnja 2015. na 200 dolara kad se trgovalo s preko 378 tisuća Bitcoina (Buterin, Ribarić, Savić, 2015:153-154).

3.9.2. Investicijski potencijal Bitcoina

Uzevši u obzir da je Bitcoin utemeljen na decentraliziranom sustavu u kojem nema središnjeg autoriteta pa se sustav prilagođava određenim algoritmima i ni na koji način ne odražava stanje gospodarstva pojedine zemlje.

Izostanak regulatornog sustava i anonimnost karakteristike su koje Bitcoin čine pogodnim za financiranje različitog spektra kriminalnih aktivnosti, uključujući pranje novca i financiranje terorizma, trgovanje drogom i oružjem ili plaćanje dječje pornografije. Krajem 2014. godine objavljeno je da će Rusija zabraniti korištenje virtualnog novca i uvesti kazne za njegovo korištenje.

Daljnje slabosti se odnose na ranjivost računalnih sustava, zbog čega je i prethodno spomenuta, najveća Bitcoin mjenjačnica Mt. Gox bankrotirala. Tada su klijenti mjenjačnice izgubili 750.000, dok je sama mjenjačnica izgubila 100.000 bitcoina. Bez obzira na to što je kasnije 200.000 Bitcoina pronađeno u digitalnom novčaniku starijeg formata, indikativna je sama činjenica da je tako velike iznose moguće gubiti i pronalaziti.

Jedna od vodećih kompanija za rudarenje Bitcoina, američka Cointerra, u siječnju 2015. godine proglasila je stečaj kojeg mnogi znalci dovode u vezu s dugovima nastalim zbog velikog pada cijene Bitcoina na tržištu. Takvi događaji, u kombinaciji s padom cijene, negativno utječu na daljnje kretanje cijena jer uzrokuju smanjenje potražnje za Bitcoinom kao ulaganjem.

S vremenom se pokazalo kako je glavni uzrok velike volatilnosti Bitcoina taj što je cijena ovisna isključivo o odnosu ponude i potražnje, što se ne odnosi na druge valute. Na taj način, jedna od temeljnih prednosti Bitcoina postaje jedno od najvećih ograničenja očuvanja njegove tržišne vrijednosti.

Nadalje, s obzirom da je riječ o sustavu složenih matematičkih algoritama i mehanizama, takav je sustav u potpunosti razumljiv samo dijelu javnosti s visokim stupnjem informatičkog obrazovanja i pismenosti. Oni slabije informatički obrazovani u opasnosti su učiniti pogrešku zbog koje mogu čak i ostati bez svojih sredstava. Najčešće zabilježene pogreške korisnika odnose se na gubitak podataka i informacija o ključevima, mogućnost neovlaštenog upada u sustav i krađa ključeva kao i nenamjerno odavanje informacija o ključevima. Za razliku od nacionalnih valuta, bitcoin nema čvrsto uporište i nije reguliran monetarnim politikama. Suvremena tržišta su promjenjiva što može rezultirati afirmacijom nove kriptovalute, a što bi u konačnici moglo dovesti do prestanka potražnje za bitcoinom i time ga učiniti gotovo bezvrijednim (Buterin, Ribarić, Savić, 2015:154-155).

3.9.3. Utjecaj kriptovaluta na financijske tokove

Trend rasta vrijednosti Bitcoina pokazatelj je porasta broja onih koji kupovinu ove kriptovalute smatraju dobrom investicijom. Bitcoin postaje najprofitabilnija investicija onima koji su skloni većem riziku. Očekuje se da će širenje mogućnosti uporabe Bitcoina utjecati na sve veću potražnju, kako za Bitcoinom, tako i za ostalim kriptovalutama.

U doba kad su se tek pojavile, kriptovalute su uzrokovale pomutnju u svijetu financija. Javio se strah da će zamijeniti klasične valute, institucije su strahovale radi potencijalnog gubitka moći i kontrole nad novcem, zbog čega je dio javnosti burno reagirao na sam spomen kriptovaluta.

Bankarski sektor se također osjetio ugroženim jer su se stvorile mogućnosti jednostavnog i brzog prijenosa novca bez provizija posrednika. Nadalje, kriptovalute su uvijek raspoložive svojim korisnicima, za razliku od klasičnog novca.

Ugledne i moćne financijske institucije, prije svega velike bankarske grupacije, jednom godišnje ostvaruju vrlo visoke prihode temeljem provizija na različite bankarske transakcije. S druge strane, u slučaju kriptovaluta transakcije se trenutačno realiziraju bez ikakve provizije, što ugrožava interes banaka, kao i imetak njihovih vlasnika. Jasno je kako će banke

upotrijebiti svako moguće „oružje“ kako bi spriječile opstanak kriptovaluta. Druga opcija im je da svoje poslovanje prilagode tehnologijama na kojima funkcioniraju kriptovalute i prihvate njihovo postojanje.

Rapidni razvoj tehnologije sve je učinio globalnim i dostupnim pa tako i držanje koraka s promjenama zahtjeva prilagođavanje ponude potražnji. Kriptovalute se počinju prihvaćati, a blockchain tehnologija nalazi svoju primjenu u unaprjeđenju poslovanja banaka, prije svega u dijelu međunarodnih plaćanja, ali i u drugim poduzećima, primjerice u automobilskoj industriji u kojoj blockchain tehnologija unaprjeđuje operativne poslove.

Osim navedenoga, blockchain tehnologija nalazi svoju primjenu u brojnim područjima. Prepoznat je potencijal upotrebe blockchain tehnologija u različitim oblastima. Pored upotrebe u bankarstvu i financijskoj oblasti, zamijećene su mogućnosti koje isti pruža u zaštiti od cyber napada i terorizma, a Vlada Sjedinjenih Američkih Država trenutno eksperimentira s ovom tehnologijom s namjerom korištenja iste za vojne potrebe.

Rusija je uvela edukaciju vlastitih eksperata blockchain tehnologije kako bi u dogledno vrijeme navedenu tehnologiju počela upotrebljavati za potrebe državnih organa. U razvijenim zemljama poput Sjedinjenih Američkih Država, Kanade, Velike Britanije i Njemačke Bitcoin je legaliziran.

U začecima je plaćanje Bitcoinom bilo moguće samo *online* no vremenom se proširuju mogućnosti pa je danas moguće ovom kriptovalutom podmiriti račun u hotelu, restoranu, prodavaonicama koje priznaju i prihvaćaju Bitcoin kao sredstvo plaćanja.

Prva banka Bitcoin-a otvorena je početkom 2017. godine u Beču, a u Hong Kongu postoje prodavaonice Bitcoin-a. Prvi bankomat za Bitcoin je instaliran 2013. godine u Vancouveru. U Australiji od 01. srpnja 2017. godine Bitcoin dobiva tretman novca i ukida se dvostruko oporezivanje te više kupovina ove valute neće biti predmet oporezivanja,tj. plaćanja PDV-a (Young, 2017).

Japan je od travnja 2017. godine legalizirao digitalne valute kao sredstvo plaćanja i najavljuje mogućnost stvaranja regulatornog okvira za oročavanje depozita u bitcoin-u kod mjenjačnica za bitcoin.17 Japanska agencija za financijske usluge (FSA) je objavila da je u kolovozu 2017. godine primila prijave za registraciju 50 bitcoin mjenjačnica. Poljska je krajem 2016. godine zvanično priznala izdavanje, kupovinu i prodaju kriptovaluta kao zvaničnu aktivnost, ali nije prihvatila da kriptovalute budu sredstvo plaćanja.18 Rusija je najavila da će u 2018.

godini definirati status kriptovaluta, a predstavnici određenih bankarskih grupacija u Rusiji traže da se legalizira promet kriptovalutama, s tim što se potiče da prodaja kriptovaluta ne bude javna, nego da bude dopuštena samo kvalificiranim investitorima (Reiff, 2017).

Velika potražnja za bitcoin-om utjecala je na to da se u Indiji razmatraju opcije legaliziranja kriptovaluta. Švicarska je, s druge strane, u pojedinim kantonima odobrila mogućnost da se od siječnja 2018. godine Bitcoin koristi za plaćanje poreza. Iz Kine pristižu informacije o zabrani Bitcoin-a, no i dalje je nejasno radi li se o djelomičnoj zabrani ili potpunoj, s obzirom da je Kina poznata kao zemlja koja kontinuirano zabranjuje nove tehnologije. Znalci u ovom području smatraju da i ako Kina zabrani trgovinu i upotrebu Bitcoin-a u državi, zbog činjenice da se radi o trgovini virtualnom valutom, Kina takvim potezom neće spriječiti veliki odljev kapitala svojih građana u investicije za kupovinu Bitcoin-a.

Ono što izdvaja bitcoin od klasičnih valuta sklonih bankarskim špekulacijama je okolnost da ova Bitcoin funkcionira na definiranom matematičkom principu, u kojem nema utjecaja moćnika i špekulacija baziranih na koristi pojedine financijske institucije.

Jesi li kriptovalute netransparentne i anonimne u usporedbi s bankarskim transakcijama? S jedne strane postoje transakcije u virtualnim valutama zasnovanim na matematičkim algoritmima, dok s druge strane imamo valute tiskane na papirnatom obliku i koje su kontrolirane od strane centralne banke.

4. ZAKLJUČAK

Blockchain tehnologija se razvila za potrebe digitalne valute Bitcoin, no kasnije su njegov potencijal prepoznale brojne industrije, prije svega financijski sektor. Bitcoin je korištenjem blockchaina i kriptografskih funkcija postigao sigurne transakcije digitalnog novca bez središnjeg autoriteta (banke). U kontekstu Bitcoina, bitchain zauzima ulogu glavne knjige u koju je zapisana svaka transakcija ikad izvršena u Bitcoin sustavu.

Kriptoekonomija donose više sfera mogućih promjena. Najjednostavnija i najuža je ona unutar koje kriptovalute predstavljaju „samo“ novu vrstu imovine, digitalne u svojoj srži, s mogućnošću zauzimanja pojedinih niša koje trenutno popunjavaju fiat-valute (npr. sredstvo plaćanja na internetu). Najšira je ona u kojoj kriptoekonomija nudi ekonomsko-političku rekonfiguraciju cijeloga sustava i redistribuciju moći u društvu.

Pojava koja se najčešće pojavljuje u kontekstu kriptovaluta je što iste imaju decentralizirani sustav kreiranja novih jedinica koji nije pod kontrolom niti jedne institucije, za razliku od centraliziranih sustava kreiranja novih jedinica koji se danas koriste i koji su pod kontrolom centralne banke. Često se navodi kako kriptovalute imaju prevelik rizik kao što je, između ostaloga, rizik za njene korisnike, rizik regulacije i mnogi drugi. S druge strane, neki od rizika s kojima se centralne banke susreću ne postoje u sustavu kriptovaluta, a riječ je o kreditnom riziku i riziku likvidnosti, no s druge strane postoji operativni rizik koji je puno veći nego kod banka, uz još pojedine rizike koji su puno izraženiji kod kriptovaluta. Kao jedan od većih problema tehničke prirode ističe se mogućnosti hakerskih napada, koji su se već događali zbog kojih je mnogo korisnika kriptovaluta ostalo bez svoje imovine. Od ostalih se problema ističu velike fluktuacije u vrijednostima virtualnih valuta, povezanost s kriminalnim radnjama, nemogućnost povrata u slučaju prevare ili krađe, potreba konstantnog praćenja razvoja tehnologije virtualnih valuta, nelicenciranih posrednika u trgovini kriptovalutama, a licenci nema jer kriptovalute nisu pod upravom države. Bitcoin, najveća i najpoznatija kriptovaluta, prvi se put spominje 2008. godine u članku *Bitcoin - A Peer-to-Peer Electronic Cash System* kojim je predstavljen način funkcioniranja Bitcoina. Nedugo nakon objave članka, 2009. godine, objavljen je i software kada isti ulazi u uporabu. Autor članka i softwarea Bitcoina široj se javnosti predstavio pseudonimom Satoshi Nakamoto, no pravi identitet osobe autora članka i utemeljitelja ove virtualne valute do danas nije otkriveno. Značajniji razvoj Bitcoina događa se 2011. godine, kada je zabilježen prvi veći porast vrijednosti na oko 30 američkih dolara. U tom je razdoblju velika količina pozornosti bila usmjerena na ciparsku financijsku

krizu 2013. godine, kada je vrijednost jednog bitcoina premašila 250 dolara. Tijekom ciparske financijske krize naglo se povećava broj korisnika, kao i broj transakcija te nastaju prve online mjenjačnice a sve više poduzeća počinje prihvaćati Bitcoin kao sredstvo plaćanja. Kada je Bitcoin prihvatio jedan od kineskih internetskih giganta, Bitcoinu cijena naglo raste. Valuta je dosegla iznimnu popularnost prvoj polovini 2013. godine, upravo zbog krize ciparskih banaka kada je mnoštvo ljudi povuklo štednju iz tih banaka te je dio tog novca bio uložen u kupnju Bitcoina, prije svega jer Bitcoini nisu vezani uz tečaj neke druge valute. Ipak, nedugo nakon toga dolazi do pada vrijednosti koji je, uz manje oscilacije, i dalje aktualan.

LITERATURA

- **Knjige i časopisi**

1. Badev, A., Chen, M. (2014) Bitcoin: Technical background and data analysis, Finance and Economics Discussion Series, Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C.
2. Buterin, D., Ribarić, E., Savić, S. (2015) Bitcoin – nova globalna valuta, investicijska prilika ili nešto treće, Zbornik Veleučilišta u Rijeci, Vol. 3., Rijeka.
3. DigiEconomist. (2018). Bitcoin energy consumption. Dostupno na: https://digiconomist.net/bitcoin-energy-consumption (24.8.2018.)
4. Doguet, J. (2012) The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System, La. Law Rev., sv. 73, izd. 4.
5. Gandal, N., Halaburda, H. (2014) Competition in the Cryptocurrency Market, Bank Can. Work. Pap., sv. No. 33.
6. Gervais, A. i sur. (2014) Is Bitcoin a decentralized currency? Dostupno na: https://eprint.iacr.org/2013/829.pdf. (20.8.2018.)
7. Kalinić, H., Visković J. (2014) Relevantnost virtualnih valuta za nositelje monetarne politike - studija slučaja Bitcoin, Financije nakon krize - Forenzika, etika i održivost, Ekonomski fakultet Sveučilišta u Splitu, Split.
8. Koblitz, N., Menezes, A. J. (2016) Cryptocash, cryptocurrencies, and cryptocontracts, Des. Codes Cryptogr., sv. 78, izd. 1.
9. Mayo, H. (2012) Investments - an Introduction: 10th edition, Cengage Learning
10. Mishkin, F. S., Eakins, G. S. (2005) Financijske institucije i tržišta, MATE, Zagreb
11. Plassaras, Nicholas A. (2013) Regulating digital currencies: bringing Bitcoin within the reach of IMF, Chic. J. Int. Law, sv. 14.
12. Šijanović Pavlović, S., Bolanča, A., Pavlović,, D. (2018) Internet of Things“ i „Blockchain“ kao alati razvoja fleksigurnog energetskog sektora, Nafta i Plin, Vol. 38., No. 153.
13. Woo, D., Gordon, I., Iarlov, V.(2013) Bitcoin: a first assessment, FX and Rates - Global.

- **Online izvori**

1. Čičin-Šain, N. (2017) Oporezivanje bitcoina, Zbornik Pravnog fakulteta Sveučilišta u Zagrebu, Br. 67.
2. Ecb.europa.eu (2012) Virtual currency schemes. Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (20.8.2018.)
3. Elendner, H. i sur. (2016) The Cross-Section of Crypto-Currencies as Financial Assets: An Overview. Dostupno na: https://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2016-038.pdf (20.8.2018.)
4. Meisser, L. (2013) Bitcoin - A Promise of Freedom, Next Generation Finance.
5. Reiff, N. (2017) Japan Finally Recognizes Bitcoin After Long Battle. Dostupno na: http://www.investopedia.com/news/japan-finally-recognizes-bitcoin-after-long-battle/ (20.8.2018.)
6. Selij, J. (2015) CoinShuffle anonymity in the Block chain. Dostupno na: http://rp.delaat.net/2014-2015/p77/report.pdf (20.8.2018.)
7. Young, J. (2017) Australia Will Recognize Bitcoin as Money and Protect Bitcoin Businesses, No Taxes. Dostupno na: https://cointelegraph.com/news/australia-will-recognizebitcoin-as-money-and-protect-bitcoin-businesses-no-taxes (20.8.2018.)

POPIS ILUSTRACIJA

Tablica 1. Struktura bloka 8
Tablica 2. Struktura zaglavlja bloka 9
Slika 3. Shema šifriranja u RSA kriptosustavu 25
Slika 4. Shema digitalnog potpisa u RSA kriptosustavu 27
Ilustracija 5. Kretanje cijene bitcoina od 1. 1. 2011. do 11. 2. 2015. godine (u $) 32
Ilustracija 6. Volumen trgovanih bitcoina od 1. 1. 2011. do 11. 2. 2015. godine 32
Ilustracija 7. Faze investicijskog balona 33