

POTENCIJALI I OGRANIČENJA PRIVATNIH DIGITALNIH VALUTA POTENTIALS AND LIMITS OF PRIVATE DIGITAL CURRENCIES

Apstrakt: Monetarni sistem prožima ukupno funkcionisanje ekonomije. Novac je pre društvena nego državna tvorevina. Danas koristimo nacionalne valute kojima je pravno obezbeđen status jedinog zakonskog sredstva plaćanja i prometa, a sve do skoro smo ih koristili u toj ulozi isključivo. Na krilima uverenja jednog uvaženog ekonomiste da isključivo pravo na emitovanje novca i regulisanje monetarnih tokova od strane države nije proizvelo ništa bolji novac od onoga koji bi drugačije postojao da svega toga nema izniču nove privatne digitalne valute predvođene svojim najprominentnijim članom – bitkoinom. U radu se izlažu prva zaokružena ekonomska vizija privatne valute, nastanak i obeležja digitalnih valuta, tehnologija plaćanja i validacija platnih transakcija u sistemu digitalnih valuta, kao i ocena njihovih dosadašnjih postignuća. Digitalne valute mogu biti dostojni izazivači nacionalnih valuta samo ako su sposobne da obavljaju tri ekonomske funkcije novca. One predstavljaju zadivljujuće tehničko i idejno postignuće, ali nije do kraja jasno da li su one novi novac, novo zlato ili nova finansijska investicija, jer inkorporiraju ponešto od svega toga, što ih i čini jedinstvenima. U radu se predlaže da se u daljem razmatranju i proučavanjima krajnjih dometa digitalnih valuta napravi distinkcija između relativnog položaja tri grupe valuta, zvaničnih valuta razvijenih zemalja, zvaničnih valuta manje razvijenih zemalja i digitalnih valuta. Nisu sve zvanične valute iste i neće sve biti u podjednakom stepenu podložne upornim atacima digitalnih valuta. Dizajn digitalnih valuta nije savršen i on pati od mana koje se mogu ispostaviti kao fatalne u nekom trenutku. Pored toga, one nailaze na snažan odijum zvaničnih institucija. Dati čvrsto predviđanje kako će izgledati njihova budućnost je nemoguće, ali predvideti budućnost bez njih u njoj bi sigurno bila kardinalna greška.

Ključne reči: digitalna valuta, bitkoin, blokčein, monetarna ekonomija

Abstract: The monetary system pervades the overall functioning of the economy. Money is social rather than government creation. Today, we use national currencies that benefit from special status of the legal tender imposed by state, and until recently we have used them exclusively in this role. On the wings of the belief of a renowned economist who argued that the exclusive right attached to the state of issuing money and regulating monetary flows did not produce any better money than the one that would otherwise have existed, gave rise to the advent of new private digital currencies headed by its most prominent member - bitcoin. The paper includes sections on the first self-contained economic vision of the private currency, the emergence and features of digital currencies, the technology of payments and validation of payment transactions in the digital currency system, as well as the assessment of their achievements so far. Digital currencies can be worthy competitors to national currencies only if they are able to perform three economic functions of money. They account for a remarkable technical and conceptual achievement, but it is not entirely clear whether they are new money, new gold or a new financial investment, since they incorporate something from all categories listed that makes them unique. The paper proposes a distinction to be made between the relative position of the three groups of currencies, the official currencies of the developed countries, the official currencies of the less developed countries and digital currencies in further analyses and investigations vis-à-vis ultimate impact of digital currencies. Neither all official currencies are the same nor will they be equally susceptible to persistent digital currencies' assaults. The design of digital currencies is not perfect and it suffers from defects that can turn out to be fatal at some point. In addition, they encounter a strong odium

* Docent, Ekonomski fakultet u Beogradu.

of official institutions. To give a firm prediction how their future will look like is impossible, but envisioning the future without them in it would surely be a cardinal mistake.

Key words: digital currency, bitcoin, block chain, monetary economics

1. UVOD

Sve transakcije u robnoj privredi ostvaruju se putem novca. Usled toga monetarni sistem prožima ukupno funkcionisanje ekonomije. Neravnoteže koje mogu da nastanu na raznim sektorima ekonomije dobijaju novčani izraz i reflektuju se kao neravnoteže na monetarnom sektoru¹. Pojava novca i razvoj monetarnog sistema su direktna posledica opipljivih društvenih koristi. Prednosti podele rada omogućene uvođenjem novca se ističu kao njegov fundamentalni, ali ne i jedini, *raison d'etre*. Adam Smit ukazuje da kad se podela rada jednom potpuno uvede ostaje veoma malen deo potreba koje čovek može podmiriti proizvodima vlastitog rada². Činjenica da je ukupna proizvodnja ljudske zajednice u kojoj se svako specijalizuje za proizvodnju određenih proizvoda ili usluga veća nego u slučaju da svako u toj zajednici proizvodi sve proizvode za svoju potrošnju samostalno, opravdava postojanje monetarnog sistema bez kojeg specijalizacija ne bi bila izvodiva.

Novac kao fenomen je društvena tvorevina, koja se izdigla do neslučenih i neočekivanih značenja. Država je relativno rano prisvojila novac i pravo regulisanja novčanog optičaja uvidevši njegov značaj. Prvi takav slučaj zabeležen je u Lidiji u VI veku p.n.e. kada je kralj Krez (*Croesus*) prvi počeo da kuje novac. Otada kovanje i štampanje novca su se učvrstili kao prerogativ države, kao ekskluzivno pravo suverene zemlje da emituje svoju valutu kojom će se obavljati plaćanja u njenim granicama. Žan Bodin (*Jean Bodin*), istaknuti srednjevekovni francuski filozof i pravnik i tvorac teorije suvereniteta, uvrštava pravo kovanja novca kao sastavni element suvereniteta zemlje. Ono je sa jedne strane izvor državne moći, jasna manifestacija državnog uticaja, a sa druge strane veoma privlačan izvor državnih prihoda. Neretko, pojedine nacije, ponosne na svoj novac, svrstavaju nacionalnu valutu među sopstvene nacionalne simbole. Tako se pored zastave, grba i himne u pojedinim državama u istu ravan po veličini afiniteta svrstava i nacionalna valuta. Ona tada simboliše snagu i veličinu ekonomskog sistema zemlje i doživljava se kao prepoznatljivi znak njenog ekonomskog uspeha³.

Novac danas ima neopozivo višestruk značaj – nacionalni, društveni, ekonomski i politički, zbog čega se monetarna problematika konstantno nalazi u žiži javnosti.

Osnivanjem prvih centralnih banaka države su postavile temelje savremenog i suverenog upravljanja monetarnim sistemom u nacionalnim okvirima. Uvedene su nacionalne valute kojima je pravno obezbeđen status jedinog zakonskog sredstva plaćanja i prometa. Pa ipak, u današnje vreme nedodirljivost ovog monopola je uzdrmana razvojem i mogućnostima savremenih tehnologija i pojavom digitalnih valuta.

Novac je istorijski gledano artefakt koji se konstantno usavršava. Era savremenih tehnologija otvara vrata njegovom oblikovanju kako u realnom, tako i u virtuelnom, digitalnom svetu. Bilo je očekivano da u eri dematerijalizacije i fizičko svojstvo novca postepeno gubi na značaju, ali je malo ko predvideo da to može da vodi i prvim znacima istiskivanja nacionalnog (državnog) novca novim formatima novca koji su fundamentalno različitog, privatnog karaktera.

2. IDEJA PRIVATNIH VALUTA U EKONOMSKOJ TEORIJI

¹ Čirović, M. (1988). *Monetarna ekonomija*. Beograd: Ekonomski fakultet u Beogradu.

² Smit, A. (1998). *Istraživanje prirode i uzroka bogatstva naroda*. Novi Sad: Global Book.

³ Lukić, V., Popović, S. (2016). „Uzdizanje novih valuta u senci nacionalnih valuta“, u S. Tuševljak, Č. Očić i B. Mašić (eds), *Ekonomija danas – slobode, konkurencija, subvencije*. Istočno Sarajevo: Univerzitet u Istočnom Sarajevu, pp. 495-508.

Pojava ideje o privatnoj emisiji novca ima svoje teorijsko uporište koje nije razvijeno u sadašnjem trenutku. Fridrih Hajek je u jednom od svojih dela, kojem njegovi savremenici nisu svojevremeno pridavali zapaženiju pažnju, preispitivao fokalni postulat organizovanja monetarnog sistema u svetlu razrešenja tadašnjeg akutnog problema inflacije⁴. Dovodeći u pitanje postulat državnog monopola na emisiju novca Hajek je pružio nesvakidašnju interpretaciju alternativnog, ali po njemu uspešnijeg, načina koncipiranja monetarnog sistema. On nije mogao da se pomiri sa bespogovornim prihvatanjem univerzalnog učenja po kojem je svaka zemlja večno osuđena na državno snabdevanje novcem koje je oličeno u posebnoj i isključivoj nacionalnoj valuti. Ovo uverenje Hajek izjednačava sa dogmom koja ne bi trebala da odvraća intelektualno nadahnute pojedince od razmišljanja i otkrivanja drugih jednako dobrih ako ne i boljih rešenja.

U najblažem obliku formulisan, stav Hajeka je da isključivo pravo na emitovanje novca i regulisanje monetarnih tokova od strane države nije proizvelo ništa bolji novac od onoga koji bi drugačije postojao da svega toga nema, a verovatnije je da je novac kakav danas imamo zapravo i lošiji. Glavni dobitnik u postojećem stanju stvari je država, jer joj ekskluzivitet emisije novca služi kao glavni instrument za sprovođenje svih državnih politika i najsnažniji oslonac u daljem jačanju vladine moći. U osnovi, država može po svojoj volji da stvori novac i učini da javnost prihvati bilo koju količinu novca koja na taj način bude kreirana. Pogodnosti i nesumnjive prednosti prava emisije novca upućuju da nijedna vlada neće biti spremna da se razreši ovoga tradicionalnog prava bez krupnog otpora. Širenje uticaja i moći savremenih vlada je nezamislivo bez raspoloživih izdašnih finansijskih resursa kojima se pokrivaju budžetski deficiti, a među kojima se deficitarno finansiranje afirmisalo kao najpouzdaniji mehanizam za podmirenje troškova raznorodnih državnih programa.

Istorijski tokovi, kojima se prati sudbina državnog novca još od vremena kovanog novca, su beskrajno ispunjeni ponavljajućim pričama o zloupotrebama prava emisije novca i pratećim obmanama javnosti. Najčešća prevara koja je preduzimana do XVII veka, jer tada papirni novac počinje da dobija na značaju, sastojala se od smanjenja sadržaja plemenitih metala u novčanoj jedinici čiji krajnji rezultat je bio rast broja iskovanih kovanica koje se mogu proizvesti od određene količine plemenitih metala. Ideja koja je koliko jednostavna toliko i delotvorna, jer omogućava laku i brzu zaradu u formi emisije dobiti. Ali ista ideja je aplikativno usavršena kako se postepeno prelazi na papirni novac, obmana javnosti je sada još jeftinija i brža. Svakodnevni život nas uči da sa lakoćom i brzinom zarade raste i stepen surovosti koju subjekat koji ostvaruje takvu zaradu ispoljava, a emisija papirnog novca nije izuzetak. U većini društava u kojima je cirkulisao papirni novac se odbijanje njegovog prihvatanja kažnjavalo na najokrutniji način. Kazne su se kretale od višegodišnje, pa i višedecenijske robije kao što je bio slučaj u Francuskoj, pa do smrtne kazne. U engleskom pravu je čin neprihvatanja papirnog novca bio klasifikovan kao delo uvrede visočanstva (*lese majesty*), a u toku građanskog rata u SAD-u isto delo se tretiralo kao akt veleizdaje sa fatalnom kaznom⁵.

Hajekova vizija redefinisavanja monetarnog sistema polazi od premise da privatno preduzeće, čije poslovanje i opstanak zavise od njegove sposobnosti da održi stabilnom vrednost novca kojeg emituje, jeste najbolje doraslo zadatku obezbeđenja pouzdanog i dobrog sredstva plaćanja za društvo. On stoga agituje za globalnu mrežu institucija koje bi uživale slobodu emisije novčanica na konkurentskim osnovama i otvaranja računa koji su denominirani u istim novčanim jedinicama kao i emitovane novčanice, a čije ime bi te institucije samostalno odabrale. Naziv te privatne valute bi uživao pravnu zaštitu kakvu ima žig ili registrovani zaštitni znak. Pošto se u prometu već nalaze brojne nacionalne valute stavljanje novih valuta u promet bi se moglo nasloniti na postojeće valute. Institucija koja želi da emituje svoju valutu bi tako prvo odabrala njen naziv, a zatim preuzela obavezu da svaku emitovanu novčanicu ili depozit izražen u njoj isplati na zahtev i po želji imaoća u više od jedne etablirane i cenjene nacionalne valute po predeterminisanom kursu, ali u prvom redu

⁴ Hayek, F. (1976). *Denationalisation of Money*. London: Institute of Economic Affairs.

⁵ Nussbaum, A. (1950). *Money in the Law*. Brooklyn: Foundation Press.

nacionalne valute one zemlje u kojoj institucija obavlja poslovanje. Predeterminisani kurs bi imao karakter donje granice, što znači da se ne bi smelo dogoditi da se npr. za jednu jedinicu privatne valute dobije manje jedinica nacionalne valute od onog broja deklarisanog kursom. Svaka institucija bi trebala da obznanu svoju misiju da je njen cilj da čuva kupovnu snagu valute što je bliže moguće konstantnom. Iz toga bi proizašla i obaveza da se precizno definiše koja je to kupovna snaga, u smislu specifikovane korpe dobara koja se jedinicom valute može kupiti, u odnosu na koju se ocenjuje održanje vrednosti valute približno konstantnom. Primarni tok emisije privatne valute bi u početku trebalo da bude regularna kupovina nove valute drugim nacionalnim valutama, bilo putem šaltera ili organizovanjem aukcija za veće emisije, da bi u perspektivi to trebalo da bude kratkoročno kreditiranje koje je sastavni deo redovnog bankarskog poslovanja i način emisije novčane mase u važećem monetarnom sistemu.

Mehanizam istiskivanja nacionalnih valuta privatnim počinje da deluje jednom kada zbog inflacije nacionalne valute počnu da gube svoju realnu kupovnu snagu. Kao posledica toga tekući kurs razmene između nove i nacionalnih valuta bi se izdigao iznad predeterminisanog kursa, pa bi se nove valute menjale uz premiju. Ovaj razvoj događaja ne bi bio moguć da standard realne vrednosti novih valuta nije definisan kod njihove prve emisije, u smislu njihove tadašnje kupovne snage, i da zadatak privatnih emisionih institucija nije da ga očuvaju što je više moguće nepromenjenim sa protekom vremena. Dalja kontinuirana depresijacija postojećih valuta bi pojačavala tražnju za alternativnim stabilnijim valutama što bi podstaklo konkurenciju i umnožio bi se broj privatnih emisionih institucija.

Trenutak potiskivanja nacionalnih valuta ne bi ipak bio kraj već početak ustrojavanja novog monetarnog sistema u kojem se kontrola vrednosti novca obezbeđuje kroz konkurentsko delovanje i ponašanje emisionih institucija. Emisione institucije bi se nalazile pod konstantnim pritiskom konkurencije koja bi nastojala da bude uspešnija u očuvanju vrednosti svojih valuta, pa nijedna emisiona institucija ne bi imala veliki izbor, ako namerava da opstane, već bi se morala povinovati nametnutoj tržišnoj disciplini. Time bi oportuno ponašanje monopolističke centralne banke polako palo u zaborav, a verovatno i sama ona, dok bi bespoštedno nadmetanje za naklonost korisnika novca postalo novi standard ponašanja.

Teza o nadmoćnosti tržišnog mehanizma spram bilo kog oblika državne intervencije u ekonomiji nije neobična imajući u vidu kompletan Hajekov naučni opus. Zato on i ističe da je zapravo konkurencija ta kojoj se duguje glatko funkcionisanje novog sistema, jer ona deluje jače i neposrednije nego bilo kakva obaveza koju emisiona institucija može javno da preuzme u smislu isplate njene valute nekom fiksnom količinom ili korpom dobara ili plemenitih metala; ili izjavom da će ona nastojati da održi vrednost valute konstantnom. Hajek je i detaljno izložio načine regulacije količine nove valute u opticaju kako bi se njena ponuda držala u ravnoteži sa tražnjom za njom, putem pravovremenih ekspanzija i kontrakcija novčane mase, a time i obezbedila stabilnost njene vrednosti.

Hajekov predlog je izložen u smiraj bretonvudskog međunarodnog monetarnog poretka, u vreme kada su definitivno odbačeni zlatni standard i režim fiksnih deviznih kurseva. U trenutku kada stari sistem nije mogao da se održi, a nijedan drugi nije uživao vanrednu podršku kojom bi se samouvereno nametnuo kao hegemonistički. Optimalno rešenje po Hajeku je zamena nacionalnih valutnih sistema sa slobodnom konkurencijom između privatnih emisionih banaka. Kao dodatni argument Hayek ističe zasluge Pokreta za slobodnu trgovinu koji je bio zapažen u XVIII veku, a koje je malo ko mogao predvideti dok je pokret bio u povoju i zbog kojeg je Velika Britanija postala 1860. god. prva nacija koja je prihvatila slobodnu trgovinu. Na sličnim principa i sa identičnim namerama, Hajek smatra i da je kucnuo čas za Pokret za slobodni novac čije će delovanje u konačnom dovesti do društvenog konsekvencija o potrebi, prednostima i koristima prelaska na privatni novac. Prema njegovim predviđanjima, kada se to zaista bude i desilo društvo će se ratosiljati reverzibilnih akutnih inflacija izazvanih neodmerenom državnom potrošnjom, ali i ekonomskih kriza i perioda stagnacije privredne aktivnosti koje su inherentne vladajućem monetarnom sistemu, a koje mnogi prispisuju samom društvenom uređenju – kapitalizmu.

3. POJAVA I OBELEŽJA PRIVATNIH DIGITALNIH VALUTA

Pojava i razvoj novih tehnologija zalaze u svaku poru života, pa tako nisu zaobišli ni monetarnu sferu. Glavna prepreka uvođenju privatnih valuta dugo vremena je bilo nepostojanje mogućnosti za njihov transfer. Oslanjanje na zvanični bankarski sistem nije bilo izvodivo jer se banke moraju povinovati strogim propisima, a njima je jasno bilo definisano kojim valutama one smeju da trguju i u kojim da otvaraju račune. Za privatne valute tu nije bilo mesta, a drugi mehanizmi za njihov prenos nisu bili na raspolaganju. Smetnja je otklonjena novim tehnologijama koje su na prvom mestu značajno transformisale način na koji dolazi do razmene dobara i usluga među ljudima. Ekspanzija korišćenja interneta, njegova rastuća geografska pokrivenost i dostupnost, kao i unapređena brzina, podstiču digitalnu interakciju među ljudima, internet trgovinu, u koju se savršeno uklapaju digitalne valute koje prirodno pripadaju tom virtuelnom svetu. Često se zato paralelno sa pojmom digitalne valute koristi sa istim značenjem i pojam virtuelne valute.

Zvaničnim definicijama virtuelnih valuta su sklone zvanične institucije. Virtuelna valuta je digitalna reprezentacija priznate vrednosti koju emituju privatna lica i koja je denominirana u obračunskoj jedinici koju su oni sami odredili⁶. Virtuelna valuta je vrsta neregulisanog, digitalnog novca, kojeg emituju i kontrolišu njegovi stvaraoci, a koji je prihvaćen i koristi se između članova specifične virtuelne zajednice⁷.

Bitcoin (*Bitcoin*) je pionir digitalnih valuta. Prvi bitcoini su emitovani početkom 2009. god. pa se on polako približava prvoj deceniji svog postojanja. Suština ove valute je koncizno izložena u svega 8 strana rada⁸ autora koji svoj identitet, sem navodnog imena, nije podelio sa javnošću. Kao ideja vodilja za nastanak bitcoina je navedena potreba za postojanjem elektronskog sistema plaćanja koji bi se zasnivao na kriptografskim elementima umesto na poverenju kao etičkoj kategoriji, a koji bi omogućio da dve strane koje zaključuju transakciju (*peer-to-peer transaction*) mogu direktno da završe posao bez potrebe za posredovanjem treće strane koja uživa njihovo poverenje. Usavršavanje formata novca i pratećih platnih sistema je istorijska zakonomernost. Bitcoin u tome ne bi predstavljao izuzetak. Stremljenje ka efikasnijim i sigurnijim sistemima plaćanja je legitimno i društveno korisno, pa stoga i sveukupno poželjno. Pa ipak, nijedan takav konkretan poduhvat do sada nije podrazumevao dovođenje u pitanje vladajuće monetarne paradigme sa tri okosna elementa, zvanična nacionalna valuta, centralna banka i finansijske institucije.

Kod bitcoina se pojavljuje zasebna valuta iza koje ne stoji nikakav ni državni ni privatni autoritet. Za njegovu emisiju nije potrebna centralna banka, već sve odrađuje programerski kod. Na kraju, ni finansijske institucije nisu nužne za njegovu svakodnevnu upotrebu, u smislu transfera i plaćanja, jer za to postoji blokčein (*blockchain*). Iz ovih razloga mnogi doživljavaju bitcoin kao revolucionarnu inovaciju koja će radikalno izmeniti obličje finansijskog sistema.

3.1. VALIDACIJA TRANSAKCIJA I TEHNOLOGIJA PLAĆANJA KOD PRIVATNIH DIGITALNIH VALUTA

Kao što smo primetili još kod Hayeka, postojala je namera i dobra volja da se uvedu privatne valute još pre nekoliko decenija, a verovatno i neuporedivo duže, ali nije postojao sistem koji bi to efektivno omogućio. Kod bitcoina ovu ulogu vrši blokčein. U konvencionalnom monetarno-finansijskom sistemu sistem plaćanja je hijerarhijski uređen. Inicijativu za plaćanje pokreće platilac (fizičko ili pravno lice) koji ima otvoren račun kod banke. Banka platioca smanjuje saldo na računu platioca i prosleđuje centralnoj instituciji zaduženoj za kliring i poravnanje detalje transakcije.

⁶ He, D. et al. (2016). Virtual Currency and Beyond: Initial Considerations. *IMF Discussion Note*, SDN/16/03.

⁷ European Central Bank. (2012). *Virtual Currency Schemes*, Frankfurt: European Central Bank.

⁸ Nakamoto, S. (2008). Bitcoin: A peer-to-peer Electronic Cash System. Preuzeto sa: <https://bitcoin.org/bitcoin.pdf>. Pristupljeno 10.3.2017.god.

Centralna banka, koja se nalazi na vrhu hijerarhije platnog sistema, vrši prenos sredstava sa računa banke platioca na račun banke primaoca, što se i evidentira u njenoj glavnoj knjizi. Ona je zadužena za održavanje pouzdane i tačne evidencije svih međubankarskih platnih transakcija, i.e. validiranje svake pojedinačne transakcije, što onemogućava neosnovana plaćanja bez pokrića (*problem duple potrošnje*) i promet falsifikata. Naposljetku banka primaoca evidentira u svojoj glavnoj knjizi priliv na račun primaoca. Saobrazno održavanju računa poslovnih banaka kod centralne banke i vođenju evidencije plaćanja, poslovne banke održavaju račune svojih klijenata i vode svoje glavne knjige.

Blokčejn je javna glavna knjiga u kojoj su evidentirane sve transakcije ikada realizovane. Za njeno ažuriranje nije zadužena nijedna centralna institucija. U prirodi blokčejna je decentralizovanost. Umesto jedne centralne evidencije koju održava centralna institucija u jednom ili par primeraka, blokčejn se slobodno distribuira svima. To znači da u svakom trenutku egzistira neprebrojiv broj kopija glavne knjige koje se nalaze u posedu privatnih subjekata koji su članovi bitcoin mreže. Blokčejn se nalazi u kontinuelnoj ekspanziji kako se zbivaju nove transakcije koje je neophodno validirati i upisati u njega.

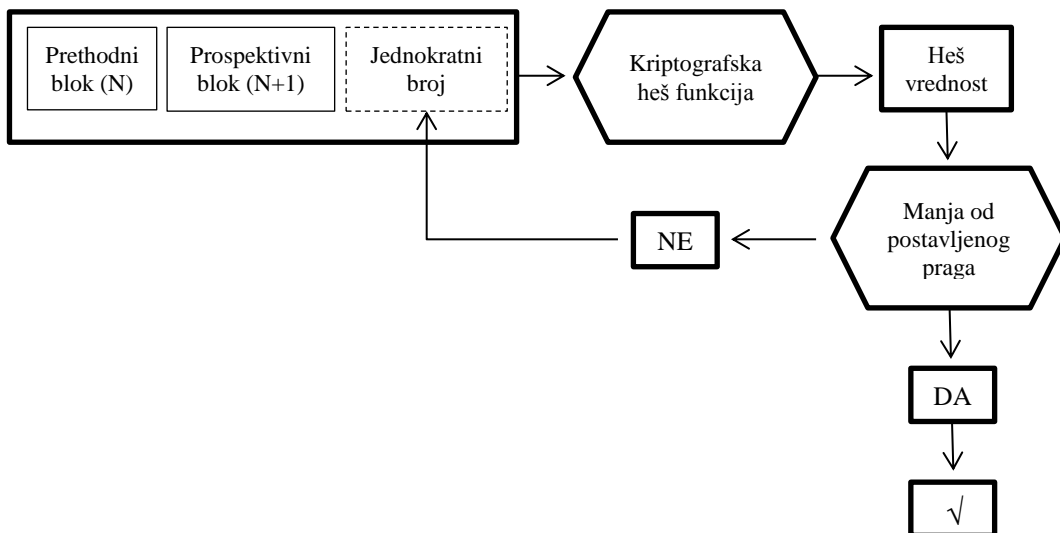
Proces validacije transakcija je specifičan i kompletna novina u sistemima plaćanja. Tehnologija koja omogućava validaciju nazvana je blokčejn tehnologija, a po njoj je i javna glavna knjiga dobila ime, i oslanja se na računarsku tehnologiju i rapidan rast računarske snage, kao i na kriptografiju. Funkcionisanje validacije će biti objašnjeno na sledećem primeru. Prvi korak u transakciji je dogovor između platioca i primaoca o izvršenju plaćanja. Osnova za plaćanje može biti dogovorena komercijalna transakcija ili pak finansijska transakcija u kojoj se vrši kupovina bitcoina nekom od regularnih valuta. Platilac u tom slučaju generiše poruku sa tri osnovna elementa: referenca na prethodnu transakciju kojom je platilac došao u posed dovoljne količine bitcoina da izvrši plaćanje, podaci o osobi koja je primalac i iznos za plaćanje. Podatak o količini bitcoina kojima raspolaže jedan učesnik u mreži se izvodi na osnovu uvida u prethodno obavljene transakcije koje su inkorporirane u blokčejn. Nakon što je poruka generisana, platilac je potpisuje digitalnim potpisom.

Digitalni potpis pruža matematički dokaz da je određenu poruku sačinio određeni subjekat. On se sastoji od dva odvojena, ali matematički povezana ključa: privatnog i javnog. Javni ključ je dostupan svim korisnicima mreže i on služi za identifikaciju pojedinačnih korisnika, odnosno kao njihova zvanična adresa ili broj računa. Ipak, ključ sa kojim će platilac potpisati poruku je privatni ključ koji je poznat samo njemu. Preko privatnog ključa platilac kodira poruku. Obzirom da svi korisnici znaju javni ključ platioca, nakon generisanja kodirane poruke jednostavno je sprovesti njeno dekodiranje javnim ključem čime se verifikuje identitet platioca, odnosno potvrđuje da je lice koje vrši plaćanje zaista generisalo poruku kojom se doznavaaju sredstva primaocu a ne neko drugi ko bi se lažno predstavio. Nakon što je poruka kodirana, ona je spremna za distribuciju u mreži. Poruka u prvom redu mora biti distribuirana do onih učesnika koji obavljaju ulogu rudara (*bitcoin miners*). Svi računari koji su aktivni u mreži vrše transmitovanje poruke, pri čemu se mreža veza među njima formira neformalno i bez posebnih pravila, pa tako dva računara mogu imati uspostavljenu vezu koja nije po definiciji dvosmerna. Oni računari do kojih poruka prvo stigne će je transmitovati drugim računarima sa kojima su povezani, koji će je dalje preneti narednim računarima i proces se nastavlja sve dok poruka ne stigne do poslednjeg računara. Transmisija poruke je brza i efikasna.

Najosetljiviji deo validacionog procesa jeste verifikacija transakcije. Ona se sastoji iz dva dela. Prvi deo podrazumeva proveru digitalnih potpisa na porukama, i on nije zahtevan, dok je drugi deo od krucijalne važnosti. Svaki rudar sačinjava svoj prospektivni blok sazdan od transakcija koje čekaju na validaciju. Da bi rudar stekao pravo da svoj blok doda u blokčejn obavezan je da priloži dokaz rada (*proof of work*). Posao koji rudari obavljaju se odnosi na uspešno rešavanje kriptografske heš funkcije (*cryptographic hash function*). Distinktivno obeležje funkcije jeste da može uzeti bilo koju količinu informacija kao input, pri čemu njena vrednost uvek ima standardnu dužinu (*hash value*). Kriptografsko obeležje funkcije se reflektuje u činjenici da se njena vrednost menja na jedinstven način sa svakom i najmanjom promenom u ulaznim vrednostima inputa tako da je nemoguće unapred predvideti koju vrednost funkcije će proizvesti određena kombinacija inputa. Prema bitcoin

protokolu rudari unose tri inputa u funkciju: referencu na prethodni blok, svoj prospektivni blok i jednokratni broj (*nonce*). Cilj za rudare je da vrednost funkcije do koje su oni došli bude manja od postavljenog praga. Kako su dva inputa, referenca na prethodni blok i prospektivni blok, nepromenljiva rudarima preostaje da variranjem jednokratnog broja postignu svoj cilj. Sam postupak se može opisati kao niz pokušaja i grešaka, pri čemu veći broj rudara i rast broja pokušaja koje jedan rudar može da izvrši u određenoj vremenskoj jedinici skraćuju potrebno vreme za uspešno rešavanje zadatka. Slika 1. opisuje postupak traganja za dokazom rada.

Slika 1. Šema dokaza rada u bitcoin protokolu



Izvor: Ali, R., Clews, R., Southgate, J. (2014). Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin 2014 Q3*, pp. 262-275.

Intencija bitcoin protokola jeste da se prosečno vreme za rešavanje zadatka kreće oko 10 minuta. Da bi se ova namera sproveda u delo protokol periodično sistematski vrši kalibraciju težine zadatka, tako da rast bitcoin mreže i prosečne računarske snage, što je nezaustavljiva tendencija, ne izazovu skraćenje vremena potrebnog za rešavanje zadatka, a što ima odraza na tempo rasta količine bitcoina u opticaju. Konceptija dokaza rada je osmišljena tako da bude teško da se do njega dođe, ali da je zato veoma lako proveriti njegovu valjanost. Prvi rudar koji reši zadatak distribuira rešenje svim članovima mreže na proveru. Ako je proveru pokazala da se radi o tačnom rešenju postiže se konsenzus na nivou mreže i svaki član vrši dodavanje novog bloka na svoju kopiju blokčaina i nastavlja sa traganjem novog tačnog rešenja za sledeći blok koji se uključuje u blokčein.

Kovanicom „rudarenje“ opisuje se proces traganja za tačnim rešenjem. On iziskuje potrošnju resursa kao što su energija i računarska snaga. Procene su da godišnji troškovi energije koje iziskuje rudarenje iznose oko 178 miliona dolara, na osnovu korišćenja prosečne cene struje za fizička lica u SAD-u⁹. Rudari koji neuspešno tragaju za rešenjem nisu materijalno kompenzovani za svoj trud. Za razliku od njih, rudari koji su imali više sreće da ga pronađu bivaju nagrađeni za uspeh emisijom novih bitcoina. U svakom novododatom bloku prva transakcija na listi transakcija u tom bloku je ona kojom se dodeljuju novi bitcoini onom rudaru koji je zaslužan za njegovo ugrađivanje u blokčein. Programirano je da ta nagrada opada tokom vremena. Inicijalna nagrada je iznosila 50 bitcoina. Posle svakih 210 000 blokova ugrađenih u blokčein veličina nagrade se prepolovljava. Ako se uzme u obzir da je projektovano očekivano vreme za formiranje i ugradnju novog bloka 10 minuta, onda se na približno svake 4 godine može očekivati korekcija iznosa nagrade. Trenutno ona iznosi 12,5 bitcoina. Emisija bitcoina kroz kompenzaciju uspešnim rudarim je jedini i isključivi način emisije bitcoina.

⁹ Böhme, R., Christin N., Edelman, B., Moore, T. (2015). “Bitcoin: Economics, Technology and Governance”, *Journal of Economic Perspectives*. Vol (29), pp. 213-238.

3.2.DECENTRALIZOVANI VS CENTRALIZOVANI PLATNI SISTEMI

Izloženi obrazac funkcionisanja platnog sistema kod bitkoina je dijametralno različit u odnosu na postojeći. Sistem je decentralizovan, otvoren i transparentan. Svi korisnici mreže imaju slobodan uvid u zapise u blokčeinu i autorizaciju da ga menjaju, i.e. unose nove transakcije u blokovima u njega. Blokčein u punom smislu predstavlja javno dobro za njegove korisnike. Zahvaljujući njegovom postojanju svi mogu da izvrše proveru postojanja pokrića za transakcije na čekanju. Stabilnost platnog sistema ne zavisi od integriteta centralne institucije čiji zadatak je da blokira lažne transakcije i one bez pokrića. Potreba za integritetom je zamenjena konsenzualnim dogovorom korisnika, pri čemu nijedan korisnik ne mora da zasluži poverenje drugih. U principu, svaki korisnik ima pravo da predloži svoj spisak transakcija koje bi trebalo da se zapišu u blokčein. Ali da bi se taj predlog smatrao kredibilnim, jer iznošenje nekog predloga ne uključuje generalno nikakve konkretne troškove za predlagača, korisnik mora da priloži potvrdu rada kojom se demonstrira da je on podneo određene troškove skopčane sa svojim predlogom na osnovu kojih je došao do rešenja kompleksnog matematičkog problema.

Prednosti decentralizovanog platnog sistema u odnosu na centralizovani mogu da se izlože kroz razmatranje 3 tipa rizika prisutnih u njima. Glavni rizik u centralizovanom sistemu je kreditni rizik koji se ispoljava kao nesolventnost jedne banke koja ima velika dugovanja prema drugim bankama u sistemu. Blisko povezan s njim je rizik likvidnosti koji se vezuje za situaciju u kojoj je jedna banka članica sistema solventna, ali ne i likvidna zbog čega opet nije u stanju da izmiri svoje dospele obaveze prema drugim članicama. Poslednji rizik je operativnog rizik koji se vezuje za moguću zastoj u radu platnog sistema uzrokovan specifičnim vanrednim događajem, kao što je pad informacionog sistema ili nestanak struje. Standardan način za mitigaciju ovih rizika sastoji se u doprinosima banaka članica koji će se, kada se ostvare neki od navedenih rizika, koristiti za pokriće nastalih gubitaka. U decentralizovanim sistemima prva dva rizika se po definiciji eliminišu jer banke članice u njemu uopšte ne postoje. Cela transakcija se odvija samo na realizaciji platilac – primalac. Iako je transakcija bezgotovinska po svim obeležjima, jer drugačija i ne može biti obzirom da je bitkoin digitalna valuta, ona neodoljivo podseća na gotovinsku transakciju.

Pored toga, na prvi pogled deluje da bi decentralizovani sistemi i u pogledu operativnog rizika trebalo da budu otporniji i kapacitativniji. U centralizovanom sistemu kompletan registar platnih transakcija je u nadležnosti i zavisi od stanja jedne proverene i pouzdane institucije. Svaki problem u operativnom funkcionisanju kojem je ona izložena može dovesti do obustave rada kompletnog sistema. Dizajn decentralizovanih sistema isključuje ovu situaciju jer čak i da se određeni korisnici suočavaju sa problemima u svom radu, postoji neizmeran broj drugih korisnika sa svojim kopijama blokčaina koji obezbeđuje nesmetano funkcionisanje sistema.

Kao posebna vrsta rizika u platnom sistemu, nesistematskog karaktera, pojavljuje se rizik krađe. U postojećem platnom sistemu on se može prikazati kroz primer on-line plaćanja karticama. Uvek je prisutan rizik da se određeni detalji kartice podele sa internet trgovcem, koji se kasnije mogu zloupotребiti i poslužiti za plaćanja istom karticom koja nije inicirao njen vlasnik. Sem javnog ključa u decentralizovanim mrežama ne postoji nijedan drugi podatak koji se deli sa ostalim korisnicima. Međutim, rizik gubitka digitalne valute je na određeni način izraženiji u decentralizovanim sistemima. Gubitak privatnog ključa automatski povlači i trajni gubitak pristupa digitalnoj valuti. Nestali ili ukradeni PIN ili šifra kojima se pristupa i raspolaze sredstvima na računu kod banke mogu se resetovati ili povratiti jednostavnim zahtevom upućenim banci. Funkcionisanje blokčaina ne pruža ovakvu mogućnost. Sve transakcije su finalnog karaktera i nema administratora u sistemu koji bi razrešavao ovakve slučajeve. Ipak, ovaj režim upravljanja novčanim sredstvima nije nepoznat korisnicima, jer gotovina koju drže u svom novčaniku teži istoj sudbini kao i digitalna valuta ako se on zagubi.

Granica između centralizovanih i decentralizovanih sistema nije precizno postavljena. Danas razlikujemo dva tipa blokčein protokola, javni i konzorcijalni¹⁰. Javni blokčein je svojstven svim privatnim digitalnim valutama i pristup njemu je otvoren za sve. On je konstruisan na načelu potpune dezintermedijacije. Kao otvoren i slobodan sistem on ne trpi bilo kakvu primenu naknadnih pravila do onih koja su inicijalno bila predviđena kada je sistem koncipiran i lansiran. Među ta pravila, koja mogu da budu od koristi sistemu ali nema mogućnosti da se inkorporiraju u njega, spadaju i pravni propisi kojima se pruža pravna zaštita transaktorima u domenu obligacionih odnosa. Pravna sigurnost nije nešto što odlikuje javni blokčein.

Konzorcijalni blokčein se razvija na ideji da je blokčein tehnologija korisna, ali da se njome može kvazi-centralizovano upravljati. Pravo vršenja upisa u blokčein u konzorcijalnom blokčeinu može da se ograniči samo za određene članove. Kao njegove prednosti, u zavisnosti od načina njegove primene, mogu da se izdvoje unapređenje funkcionisanja tržišta i sniženje transakcionih troškova, ali je noseća prednost izražena u jasnijem pravnom okviru koji obezbeđuje pravnu sigurnost za učesnike. Pristalice konzorcijalnog blokčejna dolaze iz redova finansijskih institucija koje u njemu vide način da eksploatišu novu tehnologiju, i što je mnogo važnije – koncept koji će im omogućiti da i dalje budu potrebne i relevantne. Pravila funkcionisanja konzorcijalnog blokčejna mogu elastično da se postave. Npr. izvodivo je da 15 finansijskih institucija lansiraju blokčein tako da svaka od njih bude učesnik sa povlašćenim pravom upisa novih transakcija u blokčejn, ali da minimum 10 od njih mora da dâ pristanak za svaki blok da bi se on ugradio u njega. Sa druge strane, pravo uvida u blokčein može biti javno, ili pak limitirano¹¹. Ovaj tip blokčejna se naziva i delimično decentralizovanim sistemom.

Kao kuriozitetan slučaj javlja se mogućnost potpuno privatnih blokčejna. Kod takvog tipa blokčejna bi pravo upisa transakcija bilo rezervisano samo za jednu organizaciju. U pogledu prava uvida u njegov sadržaj ostalo bi na volju dotičnoj organizaciji da sama odluči da li je ono opravdano ili ne. Svakako da u određenim slučajevima, ukoliko su u pitanju privatne baze jedne kompanije, za javnim uvidom nema potrebe. Zamislivo je da se centralna banka prikloni u nekom trenutku ovom tipu blokčejna, pod uslovom da se ova tehnologija nametne kao standard čime bi se dobio kriptografski centralizovani sistem.

4. OCENA DOSADAŠNJIH POSTIGNUĆA DIGITALNIH VALUTA

Kod relevantnih radova u oceni dosadašnjih rezultata koje su postigle digitalne valute, u prvom redu bitcoin kao njihov začetnik, po nekom nepisanom pravilu polazi se od njihovog kompariranja sa zvaničnim valutama¹². Digitalne valute mogu biti dostojni izazivači nacionalnih valuta samo ako su sposobne da obavljaju tri ekonomske funkcije novca.

Prva među jednakim funkcija novca je funkcija sredstva plaćanja. Širina baze korisnika neke valute opredeljuje uspešnost u vršenju ove funkcije. Trenutno su na raspolaganju informacije koje pružaju brojni učesnici u bitcoin ekosistemu o različitim statistikama bitcoina¹³. Među tim statistikama trenutno ne figurira, mada ranije u nekoj formi jeste, ona o broju korisnika bitcoina. Razlog tome je generalna priroda decentralizovanosti mreže gde ne postoji centralni agregator podataka već pojedinačni subjekti vode svoje evidencije, ali i pseudoanonimnost koju pruža korišćenje bitcoina.

¹⁰ Roupheal, R. (2017). Blockchain applications for finance: just a passing fad or is this a revolution. Preuzeto sa: <https://medium.com/belem-blockchain/blockchain-applications-for-finance-just-a-passing-fad-or-is-this-a-revolution-6ee22cadd37>. Pristupljeno 22.09.2017.god.

¹¹ Buterin, V. (2015). On Public and Private Blockchains. Preuzeto sa: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>. Pristupljeno 20.3.2017.god.

¹² Lo, S., Wang, J.C. (2014), Bitcoin as Money. *Current Policy Perspectives*, No. 14-4, Federal Reserve Bank of Boston. Luther, W., White, L. (2014), Can Bitcoin Become a Major Currency, George Mason University, *Working paper in Economics*, No. 14-17. Yermack, D. (2013), Is Bitcoin a Real Currency? An Economic Appraisal, *NBER Working Paper No. 19747*.

¹³ Npr. www.blockchain.info, www.bitcoincharts.com, www.bitcoinity.org itd.

Korisnici se raspoznaju u sistemu preko njihovog javnog ključa, ali je nemoguće povezati taj javni ključ sa stvarnim identitetom korisnika. U proceni broja korisnika polazi se od okvirnog broja otvorenih virtuelnih novčanika¹⁴. Ako se uzmu u obzir samo podaci kompanija koje se zvanično vode da pružaju usluge virtuelnog novčanika dobijamo da je njihov broj četverostruko porastao sa 8,2 miliona u 2013. god. na 35 miliona u 2016. god¹⁵. Međutim, tumačenje realnog broja korisnika mora da uzme u obzir da nije promet po svim novčanicima isti, negde je on učestao dok je kod nekih srazmerno redak. Grube procene kompanija koje nude uslugu vođenja virtuelnog novčanika ukazuju da se broj aktivnih novčanika kreće između 7,5% i 30,9% od njihovog ukupnog broja, pri čemu se kao kriterijum redovne aktivnosti najčešće posmatra nedeljna aktivnost vlasnika novčanika koja može podrazumevati logovanje u virtuelni novčanik ili obavljanje barem jedne transakcije. Na osnovu toga može se konzervativno zaključiti da se broj aktivnih korisnika trenutno kreće između 5,8 i 11,5 miliona¹⁶. Pošto broj novčanika koje jedan korisnik može otvoriti nije limitiran i ne može se precizno utvrditi, valjalo bi biti predostrožan u konačnoj proceni broja korisnika bitkoina. Uprkos većem ponderu značaja aktivnih novčanika ne može se osporiti značaj za bitkoin ekosistem korisnika koji stoje iza neaktivnih novčanika.

Takođe, saldo na virtuelnom novčaniku može da služi kao indikator korišćenja bitkoina kao sredstva plaćanja. Broj novčanika u kojima se nalaze bitkoini u vrednosti većoj od 1\$, 100\$, 1000\$ i 10 000\$ iznosi 14 875 778, 4 639 481, 1 908 272 i 518 439, respektivno¹⁷. Logično bi bilo pretpostaviti da bi minimalni operativni saldo, koji omogućava normalnu svakodnevnu upotrebu, morao biti minimum 100\$, a realno i nešto više. Broj takvih novčanika nije veliki.

Sa druge strane, praktičnost i izvodivost korišćenja bitkoina u svakodnevnom životu je uslovljena brojem prodavaca koji ga prihvataju. Sveobuhvatan spisak kompanija koje prihvataju plaćanje bitkoinom ne postoji, pa se najčešće navode najveće kompanije koje su spremne da ga prihvate. Među njima se izdvajaju Microsoft, Dell, Overstock, eGifter, Tigerdirect, CheapAir, Expedia, Steam i drugi. Manja preduzeća koja prihvataju bitkoin koriste to pre kao vid sopstvene promocije¹⁸ i način animiranja novih kupaca. Ograničen broj kompanija koje ga prihvataju automatski znači i ograničen broj proizvoda i usluga koji se njime mogu kupiti. Među njima dominiraju kompjuterski hardver i softver, turističke usluge i usluge online striminga i gaminga ili igara na sreću, pri čemu su malobrojni klasični online trgovci koji u ponudi imaju robu široke potrošnje. Generalno, online kompanije su poznate po inovativnosti u poslovanju i plasmanu svojih proizvoda zbog čega su sklonije i da eksperimentišu sa plaćanjem u bitkoinima u odnosu na one već etablirane.

Globalno gledano, zanemarljiv broj trgovaca prihvata bitkoin kao način plaćanja, a još je zanemarljiviji deo ukupnog prometa tih trgovaca realizovan u bitkoinu. Kao zaključak može se konstatovati da ograničeni načini sticanja bitkoina korespondiraju skućenim opcijama njegove potrošnje.

Funkcija obračunske jedinice je druga funkcija koju mora obavljati pravi novac. Tvorci bitkoina su ovu funkciju izgleda stavili u drugi plan. Bitkoin teško da može razumno da odgovori zahtevu da se putem njega iskazuje i upoređuje vrednost dobara i usluga. Kada bi se cene većine proizvoda izrazile u bitkoinima onda bi one bile istaknute u četvrtoj, pa čak i petoj decimali. Npr. cena hleba u našoj zemlji izražena u bitkonima bi bila oko 0,00006. Najmanja bitkoin jedinica se naziva Satoshi i predstavlja sto milioniti deo jednog bitkoina, zaokruživanje na osmoj decimali. Cene u decimalnom

¹⁴ To su specijalni softveri instalirani najčešće na računarima i mobilnim telefonima koji se koriste za skladištenje i obavljanje plaćanja digitalnim valutama

¹⁵ U realnosti ovaj broj korisnika bi se mogao tumačiti kao prag njihovog ukupnog broja koji se verovatnije kreće iznad granice od 40 miliona.

¹⁶ Hileman, G., Rauchs, M. (2017), Global Cryptocurrency Benchmarking Study, Cambridge Centre for Alternative Finance, University of Cambridge.

¹⁷ Preuzeto sa www.bitcoincharts.com. Pristupljeno 20.11.2017.god.

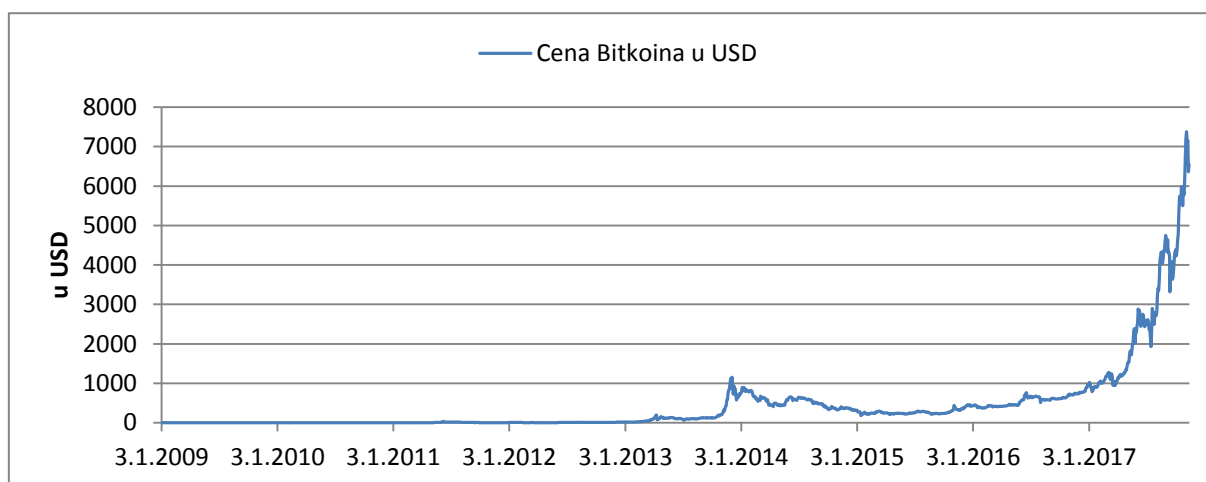
¹⁸ Preuzeto sa: www.politika.rs/sr/clanak/391903/I-u-Beogradu-rucak-placaju-virtuelnim-novcem. Pristupljeno 15.11.2017.god.

obliku nisu nešto što potrošači očekuju i na šta bi bili spremni da se lako i brzo priviknu. Pre bi se mogla očekivati psihološka nelagoda i konfuzija kod kupaca.

Trgovci koji prihvataju bitcoin zato ne izražavaju cene svojih proizvoda u bitcoinima već u zvaničnim valutama. Tek u određenoj fazi finalizacije porudžbine kupac može da bira da plati u bitcoinima, kada bira način plaćanja, a ako izabere tu opciju ima kratak rok od 10-15 minuta da izvrši plaćanja inače dolazi do korekcije cene izražene u bitcoinima u skladu sa promenom njegove vrednosti na tržištu. Da li zbog pravnih, računovodstvenih ili nekih drugih razloga nijedna kompanija koja prihvata plaćanje bitcoinom, barem zvanično, nije potvrdila da poseduje virtuelni novčanik. Umesto toga one imaju ugovore sa određenim kompanijama iz bitcoin ekosistema specijalizovanim za asistenciju trgovcima u ovakvim plaćanjima. Sporazumom se predviđa da specijalizovane kompanije, od kojih je najveća Coinbase, za sebe zadrže bitcoine a trgovcima prebace na njihov regularan bankarski račun protivvrednost u zvaničnoj valuti. Obzirom da funkcija obračunske jedinice vrši važnu društvenu ulogu koordinacije ekonomske aktivnosti i usmeravanja resursa na osnovu promena u relativnim cenama, jasno je da ovu fundamentalnu ulogu bitcoin teško da može da vrši. Bitcoin je barem za sada veoma varljivo merilo vrednosti. Jedina smisljena mera vrednosti koju bitcoin može da ima jeste njegov kurs zamene, ili terminologijom zvaničnih valuta – devizni kurs.

Konačno, treću funkciju sredstva očuvanja vrednosti bitcoin takođe ne uspeva da obavi na valjan način. Smisao ove funkcije se sastoji u obezbeđenju medijuma za prenošenje tekuće kupovne snage iz sadašnjosti u budućnost. Minimum očekivanja subjekata je da u trenutku trošenja novac ima približno istu realnu vrednost, odnosno kupovnu snagu, kao u momentu u kojem su ga oni stekli. U ovom smislu novac se afirmisao kao neprikosnoveno sredstvo očuvanja vrednosti, uprkos određenim diskreditujućim momentima u njegovoj povesti. Ono što upada prvo u oči kod bitcoina jeste volatilitet njegove cene. Dnevna promena vrednosti, deviznih kurseva, gotovo svih zvaničnih valuta u svetu je u ovom veku veoma umerena i bez krupnih kratkotrajnih oscilacija. Sa bitcoinom nije isti slučaj, njegov dnevni volatilitet se izražava dvocifrenim brojem i između 15 i 20 puta je veći od volatilitea deviznih kurseva vodećih svetskih valuta. Iz tog ugla posmatrano može da se konstatuje da je on, u kraćem roku posmatrano, inferioran medijum za očuvanje vrednosti. Međutim, ako bi se stvari sagledale iz ugla drugog vremenskog horizonta, srednjoročnog i dugoročnog, on se ne može blanko otpisati kao potencijalno sredstvo očuvanja vrednosti, jer je zapravo drastično dobio na vrednosti. Grafikon 1. pokazuje istorijsko kretanje cene bitcoina. Tekuća godina bi slobodno mogla da se proglasi zlatnom godinom bitcoina jer mu se cena uosmostručila, sa nešto ispod 1000\$ na početku godine na preko 8000\$ sredinom novembra 2017. god. Pitanje koje se nameće onda jeste šta determiniše cenu bitcoina što bi moglo objasniti ovaj skok i opšte kretanje?

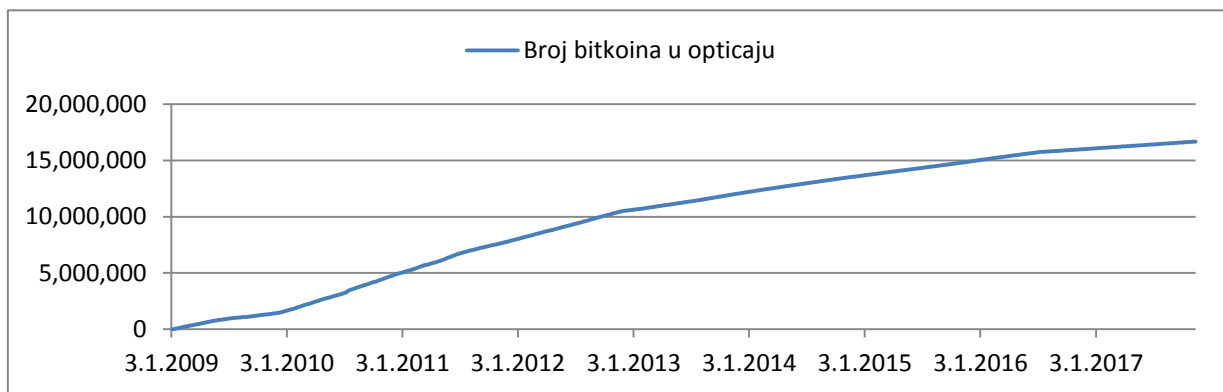
Grafikon 1. Kretanje cene bitcoina



U valuaciju bitcoina ne može se krenuti sa istim premisama koje se koriste kod zvaničnih valuta. Dok se u cirkulaciji nalazio robni novac koji poseduje intrinzičnu vrednost, npr. zlato se može koristiti za proizvodnju ili potrošnju, pitanje determinante njegove fundamentalne vrednosti je bilo jasno razrešeno. Sa druge strane, zvanična valuta uživa potporu države, jer on na kraju krajeva predstavlja njenu obligaciju, što definiše njenu fundamentalnu vrednost. Bitcoin ne odlikuje ništa od toga. Njegova tržišna cena u potpunosti zavisi od očekivanja tržišnih subjekata. Ako oni očekuju da će u budućnosti dovoljan broj subjekata biti voljan da koristi bitcoin u transakcijama, a njegova materijalno-fundamentalna vrednost je faktički jednaka nuli, on će imati pozitivnu vrednost. Iz ovakvih očekivanja proističe tražnja za bitcoinom, a iz njenog odnosa sa ponudom njegova cena.

Bitcoin delimično svoju vrednost duguje svojoj limitiranoj ponudi. Bitcoin protokol predviđa ne samo tempo rasta ponude bitcoina već i njegovu ukupnu količinu. Projektovano je da ukupan iznos bitcoina u opticaju iznosi 21 000 000, pri čemu će poslednji bitcoin biti emitovan 2140. god, mada će se najveći deo emitovati do 2040. god. Grafikon 2. pokazuje sumu do sada emitovanih bitcoina. Za njegovih nepunih 9 godina postojanja pušteno je u opticaj 16,7 miliona bitcoina. Tempo njegove emisije nije ni proizvoljan ni ujednačen. Stopa rasta ponude bitcoina ima opadajuću tendenciju obzirom na programirano prepolovljavanje nagrade za uspešne rudare. Ograničena ukupna ponuda bitcoina ima važno korektivno dejstvo na kretanje njegove cene. U načelu, da bi neka roba bila cenjena, da bi očuvala svoju vrednost i da bi njena tražnja uvek bila dovoljna u odnosu na ponudu, njena oskudnost i retkost tome bitno potpomažu.

Grafikon 2. Kretanje broja emitovanih bitcoina



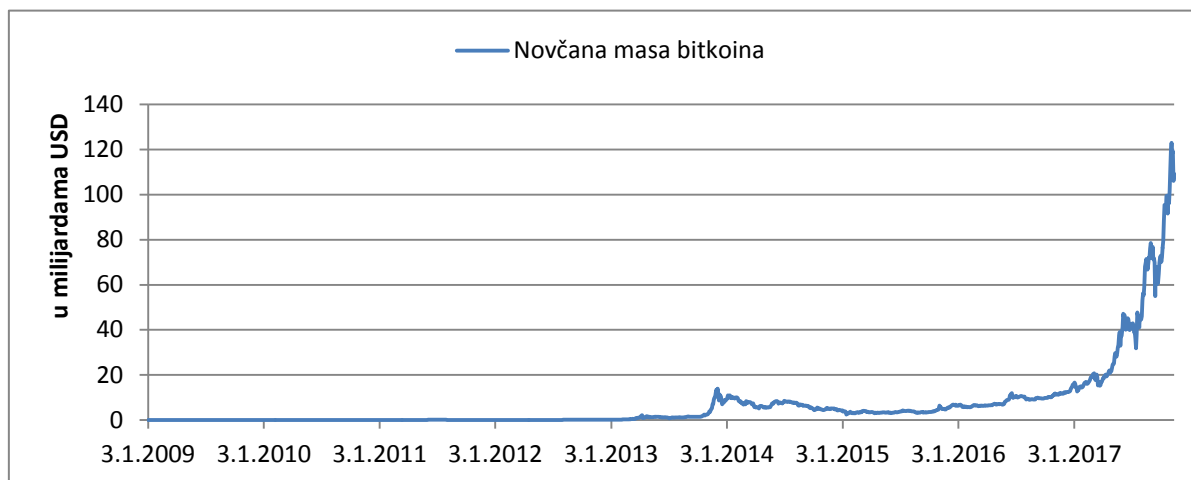
Izvor: www.blockchain.info

Konstrukcija vrednosti bitcoina je oslonjena u potpunosti na snagu dejstva samoostvarujućih očekivanja. Optimistička očekivanja podstiču vrtoglavo visoku vrednost bitcoina. Ofek i Richardson (2003) su istraživali mehur cena akcija internet kompanija početkom ovoga veka došli do zapažanja da kada subjekti sa širokim heterogenim očekivanjima nemaju priliku da sprovedu prodaju na kratko, i.e. da pozajme neku aktivu i prodaju je u očekivanju pada njene cene, ona postaje precenjena jer njena tržišna cena pretežno odražava očekivanja optimističnih subjekata. Dodatni razlog za precenjenost bitcoina jeste što dobar deo korisnika na njega gleda kao na vid finansijske investicije i ne pravi razliku između investiranja u njega u odnosu na neku drugu finansijsku aktivu. Što je strategijski privlačniji kao finansijska investicija on privlači i veće iznose ulaganja što podstiče stvaranje finansijskog mehura. Sa druge strane, oni koji ga kupuju sa tim razlogom nisu motivisani da ga u kratkom roku prodaju jer čekaju na rast njegove vrednosti, što dodatno proizvodi nestašicu u njegovoj tekućoj ponudi i izaziva rast cene.

Važna dimenzija u oceni potencijala bitcoina da uzurpira poziciju i status zvaničnih valuta jeste njegova veličina u poređenju sa drugim zvaničnim valutama. Veličina novčane mase je pogodno merilo u tom pogledu. Grafikon 3. prikazuje promenu veličine novčane mase bitcoina koja je posledica rasta njegovog kvantuma i kretanja njegove cene. Sve do kraja prošle godine, novčana masa nije uspevala da se, sem u par vanrednih slučajeva, uzdigne iznad granice od 10 milijardi

dolara, što je svako izučavanje praktičnog uticaja bitcoina svodilo na bavljenje kuriozitetom, kao što se neki prirodnjački istraživači bave zaštićenim vrstama jer im je broj ugrožen.

Grafikon 3. Novčana masa bitcoina izražena u dolarima



Izvor: www.blockchain.info

Međutim, stanje stvari se bitno menja počev od tekuće godine. Prema trenutnim podacima Narodne banke Srbije, M1 izražen u dolarskoj protivrednosti preračunatoj po tekućem deviznom kursu iznosi oko 6 milijardi dolara, a M3 kao najširi monetarni agregat nešto ispod 22 milijarde¹⁹. Referentni monetarni agregat u SAD-u je M2 čija je aktuelna suma veoma blizu veličine od 13,5 biliona dolara²⁰. Od početka tekuće godine novčana masa bitcoina je porasla sa 15 milijardi \$ na 110 milijardi \$. Novčana masa bitcoina je time prevazišla obe mere količine novca u Srbiji. Konsekventno, monetarni sistem koji okružuje bitcoin je veličinom nadmašio srpski monetarni sistem. Njegov monetarni sistem je na isti način prevazišao i monetarne sisteme najvećeg broja zemalja u svetu. Bitcoin više nije ekstravagantan monetarni eksperiment i trivijalna valuta.

Predlog autora je da se u daljem razmatranju i proučavanjima krajnjih dometa digitalnih valuta napravi distinkcija između relativnog položaja tri grupe valuta, zvaničnih valuta razvijenih zemalja, zvaničnih valuta manje razvijenih zemalja i digitalnih valuta. Nisu sve zvanične valute iste i neće sve biti u podjednakom stepenu podložne upornim atacima digitalnih valuta. Tabela 1. daje presek nekih od važnih kriterijuma i dimenzija koje mogu biti smernice

Tabela 1. Komparacija zvaničnih i digitalnih valuta

	Zvanične valute razvijenih zemalja	Zvanične valute manje razvijenih zemalja	Digitalne valute
Fizički format	Da	Da	Ne
Digitalni format	Da (u formi elektronskog novca)	Da (ukoliko postoji pravna regulativa za elektronski novac) / Ne (u odsustvu takve regulative)	Da
Naziv novčane jedinice	Propisuje država	Propisuje država	Proizvoljno određuju tvorci
Konvertibilnost	Visoka	Niska do osrednja	Visoka (u valute razvijenih zemalja) / Niska (u valute manje razvijenih zemalja)
Geografski opseg prihvatljivosti	Regionalni do globalni	Lokalni	Globalni
Zavisnost od ekonomskog stanja u zemlji	Visoka	Visoka	Bez uticaja

¹⁹ Preuzeto sa: www.nbs.rs. Pristupljeno 20.11.2017.god.

²⁰ Preuzeto sa: www.fred.stlouisfed.com. Pristupljeno 20.11.2017.god.

Deljivost na manje jedinice	Osrednja (npr. 1\$=100 centi)	Osrednja (npr. 1 RSD=100 para)	Visoka (zavisi od dizajna digitalne valute)
Transferabilnost	Visoka (Zbog razvijenosti metoda plaćanja)	Osrednja (zbog slabije razvijenosti metoda plaćanja)	Visoka (ali uslovljena pristupom internetu)
Podložnost falsifikovanju	Osrednja (samo za novac u fizičkom formatu)	Osrednja (samo za novac u fizičkom formatu)	Niska
Mogućnost krađe	Visoka (za novac u fizičkom formatu / Niska (za novac u digitalnom formatu)	Visoka (za novac u fizičkom formatu / Niska (za novac u digitalnom formatu)	Niska
Kredibilitet emitenta	Visok	Srednji	Nizak
Ponuda novca	Diskreciono određena i neograničena	Diskreciono određena i neograničena	Predeterminisana i limitirana

Izvor: Autor

Ako bismo status tri tipa valuta nastojali da utvrdimo na osnovu višekriterijumskog pristupa izloženog u Tabeli 1, onda bi se na dnu uređene hijerarhije našle zvanične valute manje razvijenih zemalja, potom digitalne valute i na njenom vrhu zvanične valute razvijenih zemalja. Redosled u hijerarhiji nije fiksiran, s tim što je u njoj distanca između zvaničnih valuta razvijenih i manje razvijenih zemalja postojana u dužem vremenskom periodu, dok se odgovarajuća distanca kod digitalnih valuta još uvek nije stabilizovala.

Esencijalna distinkcija između zvaničnih i digitalnih valuta tiče se uticaja relevantnih ekonomskih i finansijskih faktora na kretanje njihovih vrednosti. Ekonomsko stanje u nekoj zemlji se neposredno prenosi na vrednost njene valute. Snažan privredni rast u jednoj zemlji i njene povoljne sveukupne ekonomske performanse deluju privlačće na strani kapital koji je u potrazi za visokim i sigurnim prinosisima. Dok ekonomsko snaženje zemlje samo po sebi jeste praćeno i jačanjem njene valute, priliv inostranog kapitala pojačava njenu apresijaciju. Obrnuto, loše ekonomske performanse, visoki deficiti i nezaposlenost ne pogoduju vrednosti domaće valute i bivaju praćeni njenim umanjnjem u varirajućem stepenu. U krajnjoj liniji, staranje o vrednosti domaće valute je zadatak države i centralne banke koja svojom monetarnom strategijom i optimalnim merama monetarne politike nastoji da pruži stabilan oslonac nacionalnoj valuti. Kretanje vrednosti valute se stoga može izraziti kao funkcija raznorodnih ekonomskih, finansijskih i monetarnih varijabli. U bitcoin ekosistemu izostaje sprega između ovih varijabli i njegove vrednosti. Iz toga dalje proishodi nekorelisano kretanje vrednosti bitcoina u odnosu na sve ostale nacionalne valute²¹.

Za skoro sve nacionalne valute u svetu danas, sa izuzetkom možda Zimbabvea, moguće je zadovoljavajuće precizno odmeriti neki razuman raspon u kome se njihovi devizni kursevi, prema glavnim valutama, mogu kretati u budućnosti. Raspon može biti manji ili veći, ali ne i prevelik. Kretanjem deviznih kurseva u nadolazećem periodu mogu upravljati šokovi sa strane ponude ili tražnje. Promena pravca monetarne politike izaziva promenu na strani ponude koja se može transmitovati na vrednost valute. Ekspanzijom količine novca u opticaju daje se impuls smanjenju njegove vrednosti, i obratno u slučaju vođenja restriktivne monetarne politike. Kod bitcoina je takva promena isključena, njegova ponuda je neelastična. Korekcijom ponude nije moguće inicirati ostvarenje poželjnih ekonomskih kretanja da se dese, niti je skok u tražnji moguće delimično umiriti dodatnom ponudom. Pri neelastičnoj ponudi kretanje cene neke robe u potpunosti postaje determinisano promenama u tražnji za njom. Takva je i sudbina bitcoina.

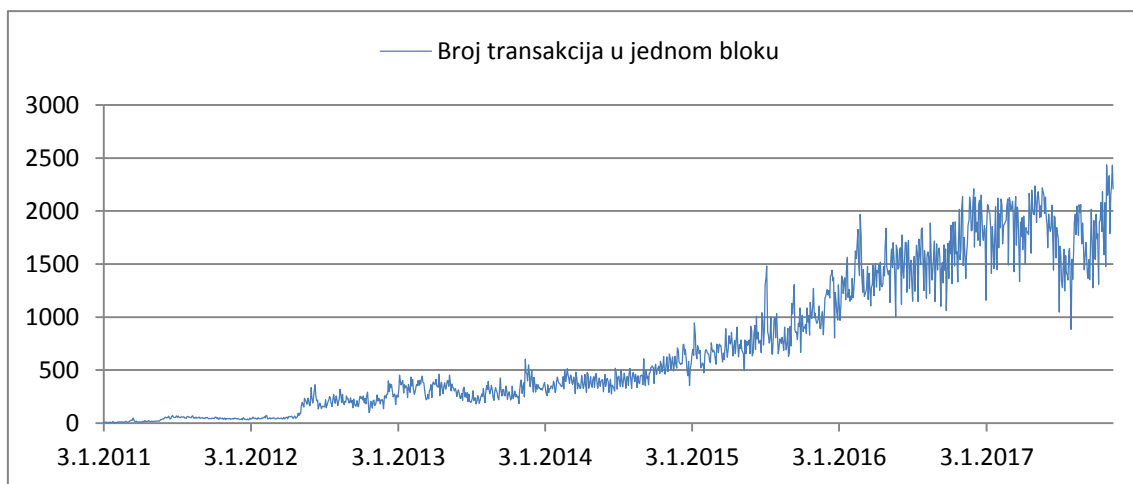
Svaka nova infomacija koja se povezuje sa prospektivnom upotrebom bitcoina u plaćanjima u budućnosti će se odraziti na njegovu tražnju i posledično cenu. Ako se rašire vesti o prevarama sa bitcoinima, npr. krah svojevremeno njegove najveće berze Mt. Gox, ili se u nekoj od zemalja donesu propisi kojima se izričito zabranjuje plaćanje ili trgovina bitcoinima, u skorije vreme iz Kine stižu takve vesti, onda će doći do snažnog depresiranja cene bitcoina. Sa druge strane, ako se

²¹ Yermack, D. (2013), Is Bitcoin a Real Currency? An Economic Appraisal, *NBER Working Paper No. 19747*. Dwyer, G.P., (2015), "The Economics of Bitcoin and Similar Private Digital Currencies", *Journal of Financial Stability*, Vol 17, pp.81-91.

objave vesti o rastu mreže trgovaca koji prihvataju plaćanje bitkoinom, pogotovo ako se radi o zvučnim i renomiranim kompanijama, ili se objave naznake da regularni bankarski sistem razmatra korišćenje bitkoina, ili mu se da legitimitet od strane uvažanih institucija²² onda to može podstaći ozbiljan skok njegove cene. Kretanjem cene bitkoina u potpunosti upravljaju šokovi na strani tražnje. Publicitet koji je kreiran oko bitkoina doprinosi njegovoj popularnosti, ona motiviše nove kupce da se aktivno uključe, ako ništa drugo ono iz znatiželje da isprobaju njegovo korišćenje, što izaziva pozitivan šok tražnje i njegova cena nezadrživo raste. Početkom 2013. god. bitkoin je vredeo oko 13 \$, da bi krajem novembra preskočio granicu od 1100 \$. Prvih dana januara tekuće godine bitkoin je vredeo oko 900 \$, da bi se krajem novembra vinuo do skoro 10 000 \$. Da li ćemo opet videti opadajuću tendenciju cene, nakon perioda eksplozivnog rasta, i u narednom periodu kao što se već desilo u 2013-oj? Zbog neuhvatljive prirode faktora koji je determinišu teško je reći.

Poslednja konsideracija u vezi sa dostignućima bitkoina se odnosi na realne kapacitete i performanse njegovog platnog sistema. Prema glavnom bitkoin protokolu platioci i primaoci nisu izloženi nikakvim troškovima ili provizijama pri izvršenju transakcija. Međutim, ovaj model ima i svoje naličje. Kapaciteti bitkoin mreže su ograničeni njenom konfiguracijom. Veličina jednog bloka iznosi 1 MB i u njega može da stane oko 2000 transakcija. Pri prosečnom vremenskom trajanju pridodavanja novog bloka u blokčein od 10 minuta dolazimo do maksimalnog dnevnog kapaciteta bitkoin platnog sistema od nešto ispod 300 000 transakcija. Funkcionalnost veličine jednog bloka nije dolazila u pitanje kada je broj transakcija bio skroman, ali kako taj broj rapidno raste kapaciteti sistema se dovode do krajnjih limita. Grafikon 4. opisuje ovaj rast.

Grafikon 4. Kretanje broja transakcija koje su sadržane u jednom bloku



Izvor: www.blockchain.info

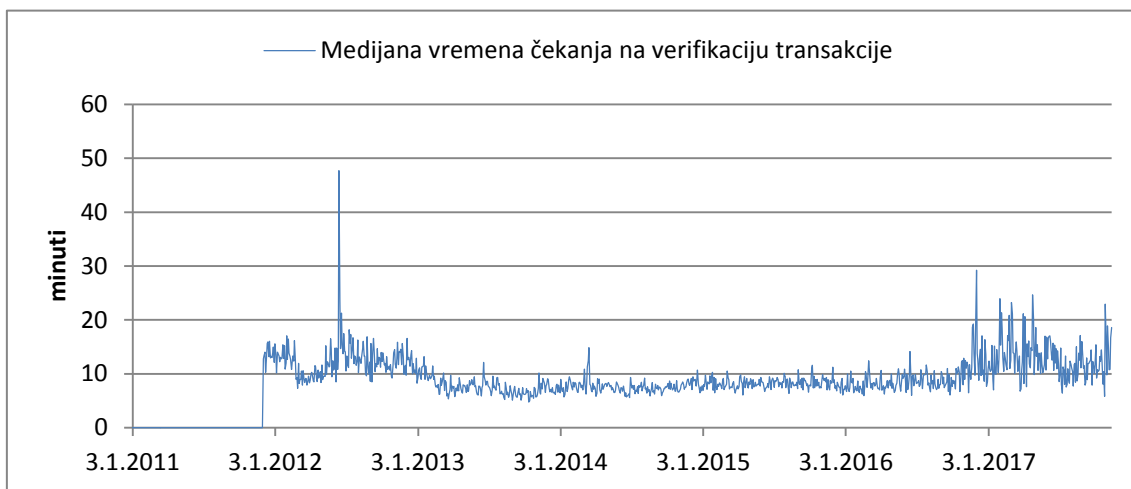
Prema poslednjim podacima dnevni broj realizovanih transakcija se kreće iznad 300 000 i dostiže i 380 000²³, što se može objasniti varirajućim vremenom potrebnim za ekstrakciju jednog bloka koje je češće ispod nego iznad projektovanih 10 minuta. Naprezanje sistema do krajnjih granica dovodi do specifične forme diskriminacije među učesnicima. Naime, iako se eksplicitno ne zahteva plaćanje provizija za transakcije ono nije ni zabranjeno što pruža mogućnost učesnicima zainteresovanijim za realizaciju njihovih transakcija da dobrovoljno plate izvestan iznos kako bi im se transakcije što brže obavile. Dugoročno gledano, plaćanje provizija je jedino rešenje koje bitkoin sistem može učiniti samoodrživim jednom kada se svi bitkoini emituju, a verovatno i mnogo ranije kada kompenzacija za uspešne rudare sveže emitovanim bitkoinima postane materijalno simbolična. Iz ovoga ponašanja proishodi novi problem da se prioritet daje transakcijama koje uključuju naplatu

²² Lagarde, C. (2017), Central Banking and Fintech – A Brave New World?, Govor na konferenciji pod pokroviteljstvom Centralne banke Engleske. Preuzeto sa: <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>. Pristupljeno 22.11.2017.god.

²³ Preuzeto sa www.bitcoincharts.com. Pristupljeno 22.11.2017.god.

provizije nauštrb onih bez nje. Grafikon 5. daje pregled očekivanog vremena čekanja izražen u vidu medijane.

Grafikon 5. Očekivano vreme čekanja na uključivanje transakcije u novi blok



Izvor: www.blockchain.info

Vreme potrebno za validaciju transakcije ispoljava tendenciju rasta u tekućoj godini, pri čemu raste i njegov volatilitet. Ipak, očekivano vreme izraženo u vidu medijane, jer je samo taj podatak javno dostupan, prikriva činjenicu da postoje transakcije koje neodmereno dugo čekaju na validaciju samo iz razloga što se njihovi učesnici pridržavaju inicijalnog bitcoin protokola. Iz perspektive postojećeg finansijskog sistema ovo vreme nije prekomerno, ali je zato u koliziji sa očekivanjima učesnika kojima je obećano da će bitcoin sistem obezbediti momentalni obračun plaćanja. Takođe, trebalo bi navesti i da trenutak validiranja nije i trenutak finalizacije transakcije. Da bi se transakcija smatrala finaliziranom neophodno je da pet sukcesivnih blokova bude pridodato blokčeinu posle bloka u kome se nalazila transakcija. Vreme potrebno za obavljanje transakcije se tako dodatno produžuje, a time i nelagodnost za učesnike u njima kao i za moguće naknadne komplikacije.

Troškovi korišćenja bitcoin sistema se ovim ne iscrpljuju. Korisnici bitcoina moraju biti spremni i na izmirivanje transakcionih provizija kada žele da obave njegovu kupovinu zvaničnim valutama ili da obave prodaju bitcoina i izvrše transfer kupoprodajne vrednosti na račun u banci. Svi ovi troškovi nisu trivijalni. Iz praktične perspektive posmatrano, obećanja o besplatnom i slobodnom elektronskom sistemu plaćanja su svakim danom sve dalje od njihovog ostvarenja. Sa druge strane, bitcoin ekosistem je toliko narastao i nastavlja da raste čime postaje sve solidniji i kompaktniji, a u pogledu svog sveukupnog impakta i relevantniji u digitalnoj finansijskoj sferi.

5. ZAKLJUČAK

Svaki subjekat, pa tako i država, ili možda obrnutim redom, bi načelno trebalo da uživa slobodu u izboru vrste i metode plaćanja u transakcijama u kojima učestvuje, odnosno sredstva kojim se njemu plaća. Država tako ima puno pravo da insistira da joj se porezi plaćaju u valuti koju je ona emitovala, ili da zahteva da u istoj valuti budu iskazani ugovori koje ona zaključuje. Ali ni država nije dosledna u insistiranju na plaćanju u sopstvenoj valuti. Preduzeća namenske industrije u državnom vlasništvu prodaju svoje proizvode pri čemu valuta plaćanja češće jeste neka druga, a ne nacionalna valuta. Neretko se i vrednost ugovora o izgradnji domaće infrastrukture izražava u nekoj drugoj valuti, a broju sličnih takvih ugovora tu nije kraj. Države su danas solidarne. Ako se desi da se napravi poneki presedan i uskrati neprikosновенost nacionalnoj valuti, onda je to još uvek u korist neke druge, tuđe nacionalne valute.

Paralelni virtuelni valutni univerzum zbog toga negoduje. Digitalne valute priželjkuju ista prava za sebe. Njihov radni motor jeste blokčein, inovativni način umrežavanja i koordinacije računara i postavljanja im zadataka što u konačnom ima svoj ekonomski smisao i praktičnu primenu. Za razliku od bitcoina, blokčein ne nailazi na odijum finansijskog establišmenta. Sve bi bilo danas

drugačije da je blokčein ugledao svetlost dana pod pokroviteljstvom institucija vladajuće monetarne paradigme. A možda još uvek za to nije kasno, ako se imaju u vidu planovi nekih javnih i komercijalnih institucija da lansiraju svoje projekte zasnovane na njemu.

Društvo u celini i na duži rok teži progresu u svim područjima, iako on nije ravnomeran u njima. Težnja ka bržim, bezbednijim i jeftinijim načinima plaćanja i transferisanja sredstava je jedno od njih, a bitcoin je jedno od mogućih rešenja. Njegova tehnologija je mlada, ali nije nedonošče. Zato se pojavljuju novi protokoli koji upošljavaju blokčein u kojima se unapređuju neki nedostaci uočeni kod izvornog bitcoin protokola. Rad na takvim poboljšanjima će se nastaviti i u budućnosti. Nikada nije postojao nijedan deo, niti će postojati, u sistemu plaćanja etabliranog finansijskog sistema koji se ne može dodatno unaprediti. Ozbiljna opasnost može biti ako se razgradnja i zamena postojećeg sistema pokažu kao pogodnije i jeftinije rešenje u odnosu na postepenu reformu njegovih sastavnih delova. Povezivanje digitalnih valuta sa aktuelnim sistemom bi verovatno donelo sinergijske efekte. Poslednji signali koji dolaze sa vrha piramide aktuelnog međunarodnog monetarnog poretka upravo idu u tom smeru.

Dok postoji elektronska trgovina, postojaće i elektronski sistemi plaćanja. U tom miljeu su ponikle i nove privatne valute. Digitalne valute su zadivljujuće tehničko i idejno postignuće. Iako nije do kraja jasno da li su one novi novac, novo zlato ili nova finansijska investicija. One inkorporiraju ponešto od svega toga, što ih i čini jedinstvenima. Dati čvrsto predviđanje kako će izgledati njihova budućnost je nemoguće, ali predvideti budućnost bez njih u njoj bi sigurno bila kardinalna greška.

LITERATURA

- Böhme, R., Christin N., Edelman, B., Moore, T. (2015). "Bitcoin: Economics, Technology and Governance", *Journal of Economic Perspectives*. Vol (29), pp. 213-238.
- Buterin, V. (2015). On Public and Private Blockchains. Preuzeto sa: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>. Pristupljeno 20.3.2017.god.
- Ćirović, M. (1988). *Monetarna ekonomija*. Beograd: Ekonomski fakultet u Beogradu.
- Dwyer, G.P., (2015), "The Economics of Bitcoin and Similar Private Digital Currencies", *Journal of Financial Stability*, Vol 17, pp.81-91.
- European Central Bank. (2012). *Virtual Currency Schemes*, Frankfurt: European Central Bank.
- Hayek, F. (1976). *Denationalisation of Money*. London: Institute of Economic Affairs.
- He, D. et al. (2016). Virtual Currency and Beyond: Initial Considerations. *IMF Discussion Note*, SDN/16/03.
- Hileman, G., Rauchs, M. (2017), Global Cryptocurrency Benchmarking Study, Cambridge Centre for Alternative Finance, University of Cambridge.
- Lagarde, C. (2017), Central Banking and Fintech – A Brave New World?, Govor na konferenciji pod pokroviteljstvom Centralne banke Engleske. Preuzeto sa: <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>. Pristupljeno 22.11.2017.god.
- Lo, S., Wang, J.C. (2014), Bitcoin as Money. *Current Policy Perspectives*, No. 14-4, Federal Reserve Bank of Boston.
- Lukić, V., Popović, S. (2016). „Uzdizanje novih valuta u senci nacionalnih valuta“, u S. Tuševljak, Č. Očić i B. Mašić (eds), *Ekonomija danas – slobode, konkurencija, subvencije*. Istočno Sarajevo: Univerzitet u Istočnom Sarajevu, pp. 495-508.
- Luther, W., White, L. (2014), Can Bitcoin Become a Major Currency, George Mason University, *Working paper in Economics*, No. 14-17.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer Electronic Cash System. Preuzeto sa: <https://bitcoin.org/bitcoin.pdf>. Pristupljeno 10.3.2017.god.
- Nussbaum, A. (1950). *Money in the Law*. Brooklyn: Foundation Press.

Rouphael, R. (2017). Blockchain applications for finance: just a passing fad or is this a revolution. Preuzeto sa: <https://medium.com/belem-blockchain/blockchain-applications-for-finance-just-a-passing-fad-or-is-this-a-revolution-6ee22cadd37>. Pristupljeno 22.09.2017.god.

Smit, A. (1998). *Istraživanje prirode i uzroka bogatstva naroda*. Novi Sad: Global Book.

Yermack, D. (2013), Is Bitcoin a Real Currency? An Economic Appraisal, *NBER Working Paper No. 19747*.

www.bitcoincharts.com

www.bitcoinity.org

www.blockchain.info

www.fred.stlouisfed.com.

www.nbs.rs

www.politika.rs