Pregledni rad
UDK 004.738.5:339
DOI 10.7251/MFP1701161R
COBISS.RS-ID 6752280

ANALIZA TEHNIČKOG ASPEKTA DIGITALNOG NOVCA

Mladen Rajko[2], Marijan Tomašić[3]

SAŽETAK

U posljednjih nekoliko godina digitalni novac i nove digitalne valute sve više postaju predmet interesa stručnih i znanstvenih krugova te javnosti. Velika brzina obavljanja elektroničkih transakcija te poboljšana praktičnost u odnosu na klasične su čimbenici, koji nedvojbeno utječu na porast uporabe i popularnosti različitih oblika elektroničkog plaćanja – i digitalnog novca. Digitalni novac donosi nove mogućnosti uporabe i korištenja, no postoje i brojni čimbenici koji koče trend razvoja digitalnog novca. Jedan od najčešćih je složenost tehničkih rješenja na kojima su utemeljene digitalne valute te nerazumijevanje načina funkcioniranja potrebnih tehničkih rješenja. Za sada ne postoji centralni autoritet koji bi stajao iza takvih valuta, a zabrinutost za potencijalne nedostatke takvog sustava je demotivirajući faktor uporabe za veliki broj korisnika. U ovome radu, digitalni se novac, promatra s tehničkog akspekta, analizirajući pojavne oblike digitalnih valuta, prednosti i nedostatke različitih tipova novčanika, funkcije čvorova te POS i POW sustav. Definirana tema je vrlo slabo istražena u znanstvenoj literaturi, a u okviru istraživanja ovog rada postavljena je hipoteza da je za daljnji razvoj i uporabu digitalnog novca potrebno održavati stabilnim sve tehničke aspekte digitalnih valuta. Osim brige o ekonomskim aspektima digitalnih valuta, potrebno je uspostaviti stabilan ekonomski i pravni sustav koji će upravljati digitalnim valutama te ukupnu operativu uskladiti s zakonskom legislativom zemlje u kojoj se transakcije provode.

Ključne riječi: *digitalni novac, tehnički aspekt digitalnog novca, Blokchain sustav*

ABSTRACT

In the last couple of years, digital money and new digital currencies are increasingly becoming a subject of interest of professional and scientific circles as well as of the wider public. The high speed of performing electronic transactions and their improved viability, compared to the classical currencies, are factors that undoubtedly affect the increase in the use and the popularity of diverse forms of electronic payments - and of digital money. Digital money brings forth new opportunities of use, though there are also many factors that hinder the digital currency development trend. One of the most common is the complexity of technical solutions on which digital currency is based and lack of understanding of how the required technical solutions operate. At present, there is no central authority behind such currencies and a concern about some potential disadvantages of such systems is a demotivating factor for a large number of users. In this paper, through an analysis of the emerging forms of digital currencies, the advantages and disadvantages of various types of digital wallets, node functions and POS and POW systems, digital money is approached from a technical perspective. Our subject of research is poorly explo-

2 Doc. dr sc Mladen Rajko**,** Sveučilište u Zadru, Odjel za ekonomiju, mrajko@unizd.hr
3 Marijan Tomašić, mag. oecc., Sveučilište u Zadru, Odjel za ekonomiju mtomasic@unizd.hr

red in scientific literature, and the hypothesis of this paper is that, in order to assure the further development and use of digital currencies, the technical aspects of their use need to be stable. Besides maintaining stable their technical aspects, it is compelling to establish a stable economic and legal system that would manage digital currencies and to align the overall functioning of the legal framework of the country where transactions are conducted.
Key words: digital money, technical aspects of digital money, Blockchain system

1 UVOD

S ekonomskog aspekta, vrlo je izvjesno da će digitalne valute u budućnosti imati značajan utjecaj na ukupno poslovanje i financijske transakcije. Od ubrzavanja i pojeftinjenja transakcija, sigurnosnih prednosti, do pristupačnosti i praktičnosti, pogotovo onim generacijama koje dolaze i koje se više koriste ovim tehnologijama. Novim tehnologijama stvaraju se postepeno i nove potrebe, te se pojavljuju i novi načini njihovog zadovoljenja. Primjer za to su velika pogodnost za internetsku trgovinu i internetsko plaćanje. Nove, još nerealizirane mogućnosti takozvanih programiranih transakcija odnosno pametnih ugovora (*eng. smartcontracts*)[4], te primjena *blockchain*[5] tehnologije izvan područja digitalnih valuta, npr. u raspodjeli udjela tvrtki ili nekih drugih vrijednosti također su moguće i izvjesne.[6][7] Bez dublje analize, moguće je pretpostaviti da će spomenuti trendovi već u relativno bliskoj budućnosti ostaviti značajan trag, utjecati na temeljne promjene načina poslovanja, trgovine, plaćanja te svakodnevnih navika potrošača.

Cilj ovog rada je analizirati trenutno stanje na tržištu digitalnih valuta s tehničkog aspekta, kako bi se utvrdio njihov značaj i uloga u svakodnevnom životu te analizirale određene pretpostavke glede daljnjeg razvoja i trendova. U radu će se objasniti koji su pojavni oblici digitalnih valuta, koje su prednosti i nedostaci različitih tipova novčanika, koje su funkcije čvorova te POS i POW sustav. Prikazat će se aktualni pregled tržišta digitalnih valuta kroz trendove uporabe, prikaz tržišne kapitalizacije, broja transakcija, vrijednosti transakcija, tečaja i drugih veličina kako bi se što preciznije odredio njihov udio i značaj u financijskom sektoru i utjecaju na ekonomiju. Pretpostavka je da će veći interes javnosti potaknuti masovniju uporabu valuta baziranih na blockchain tehnologiji te dati određeni doprinos novim idejama za uporabu ove tehnologije, otkrivanju novih načina primjene te kreiranja novih potreba društva, koje bi se na ovaj način mogle zadovoljiti.

Novac, kao jedan od najvažnijih entiteta ekonomije ima ulogu ponajprije osigurati razmjenu dobara u svojoj sinergijskoj cjelini te alocirati resurse. Po uzoru na prirodne procese, ekonomiju možemo promatrati kao eko-sustav ili organsku tvorevinu, u kojoj zdravlje cjeline ovisi ponajviše o samoj strukturi katalizirajućeg medija, odnosno novca, koji cirkulira između gospodarstava i pojedinaca. Prema nekim autorima, posljednja globalna financijska kriza može se uzeti kao dokaz kako će uska usmjerenost prema većoj učinkovitosti financijskih tržišta najvjerojatnije generirati sistemsku nefleksibilnost do točke krhkosti i

4 OMOHUNDRO, Steve, Cryptocurrencies, smartcontracts, andartificialintelligence, *AI Matters*, sv. 1, izd. 2, 2014, str. 19–21

5 MATTILA, Juri, TheBlockchainPhenomenon, *'BookBlockchainPhenomenon'BerkeleyRoundtableInt. Econ. 2016 Edn*, 2016, str. 6

6 DELMOLINO, Kevin*i ostali*, Stepbysteptowardscreating a safesmartcontract: Lessonsandinsightsfrom a cryptocurrencylab, u *International Conference on Financial Cryptographyand Data Security*, 2016, str. 79–94, Dostupno na: http://link.springer.com/chapter/10.1007/978-3-662-53357-4_6. [Pristupljeno: 18-velj-2017]

7 KOSBA, Ahmed *i ostali*, Hawk: Theblockchain model ofcryptographyandprivacy-preservingsmartcontracts, u *SecurityandPrivacy (SP), 2016 IEEE Symposium on*, 2016, str. 839–858, Dostupno na: http://ieeexplore.ieee.org/abstract/document/7546538/. [Pristupljeno: 14-velj-2017]

sloma. Kako bi se cjelokupan sustav suočio sa izazovima strukturnih mana trenutnog sustava potrebno je razumijevati, kultivirati i njegovati kompleksne i prilagodljive komponente ekonomskog sustava. Alternativne valute su sve one valute koje se koriste kao alternativa dominantnom nacionalnom ili međunarodnom sustavu i najčešće se navode kao lokalne valute ili komplementarne valute, te su se postupno proširile po svijetu. Kako se radi o relativno neistraženom području te velikom broju varijacija, nejasan je pravi utjecaj primijenjenih alternativnih valuta na razvoj lokalnih zajednica. Sam aspekt razvoja kao pojma može lako postati kompleksan pošto se ne koncentrira isključivo na ekonomsku domenu. Istraživanjem se došlo do saznanja da ne postoji mnogo autora koji istražuju područje tehničkog aspekata digitalnog novca, tako da je ova tema poprilično nova. Jerome Blanc istražuje tehnčke i ekonomske aspekte digitalnog novca s naglaskom na njegovu socijalnu dimenziju i lokalne valute. Georgina M. Gomez istražuje tehničke aspekte digitalnog novca temeljeći svoja istraživanja na primjeru Argentine, a Leander Bindewald istražuje tehničke aspekte alternativnog novca kao komplementarne valute. U radu je na temelju provedenog istraživanja obranjena hipoteza da je za daljnji razvoj i uporabu digitalnog novca potrebno održavati stabilnim sve tehničke aspekte digitalnih valuta, a otvoreno je i jedno novo područje mogućeg istraživanja vezano uz mjerenje efikasnosti korištenja alternativnog digitalnog novca na lokalnim tržištima.

2 ČIMBENICI U FUNKCIJI RAZVOJA DIGITALNIH VALUTA

Najbitniji čimbenici u funkciji razvoja digitalnih valuta su razvoj tehnologije, znanosti te kvalitativni i kvantitativni razvoj internetske mreže, razvoj kriptografije kao zasebne znanstvene discipline te razvoj posebnih tehnoloških rješenja - na primjer Blockchain tehnologija.

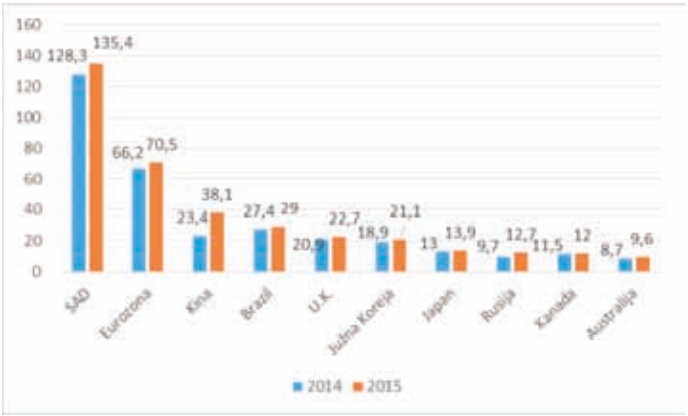
2.1 Razvoj interneta

Ubrzani razvoj telekomunikacijskih tehnologija od kojih je internet zasigurno najznačajnija infrastrukturna komponenta u masovnoj uporabi, odražava se na sve aspekte života, od tehnoloških do znanstvenih, ekonomskih, pa i socijalnih i psiholoških. Bilo je samo pitanje vremena kada će se internet početi koristiti i kao medij za ekonomske transakcije. Broj korisnika interneta povećao se s 35 milijuna 1995. na 2,8 milijardi 2014. godine, pa danas ima oko 39% svjetske populacije koja koristi internet.[8] Od samih začetaka, internet je značajno unaprijeđen u tehničkom smislu, brzine pristupa svakodnevno se povećavaju, a povećava se i pristupačnost širenjem telekomunikacijskih mreža svakim daljnjem razvojem tehnologije. Taj je trend, očekivano, u početnoj fazi, bio najsnažniji u najrazvijenijem dijelu svijeta gdje broj korisnika u nekim državama dostiže i 89% pismene populacije.[9] Danas i nerazvijene zemlje razvijaju internet gledajući na to kao strateški interes i preduvjet sveopćeg ekonomsko-tehnološkog razvoja. Stvaranjem prve kritične mase korisnika, pokrenut je proces unapređenja i razvoja sustava za plaćanje i pohranu vrijednosti. U takvim uvjetima razvile su se prvo elektroničke inačice postojećih valuta i sustava plaćanja, npr. internetsko bankarstvo i kartično plaćanje. Slijedeća slika na primjeru iz 2015. godine

8 MEEKER, Mary, Internet trends 2015-Code conference, *Glokalde*, sv. 1, izd. 3, 2015, Dostupno na: http://dergipark.ulakbim.gov.tr/glokalde/article/view/5000135231. [Pristupljeno: 29-ožu-2017]

9 CHENG, Cecilia, LI, AngelYee-lam, Internet addictionprevalenceandqualityof (real) life: A meta-analysisof 31 nationsacrosssevenworldregions, *CyberpsychologyBehav. Soc. Netw.*, sv. 17, izd. 12, 2014, str. 755–760

prikazuje koliki su razmjeri porasta udjela bezgotovinskog plaćanja u najznačajnijim svjetskim ekonomijama.



Grafikon1: Broj godišnjih transakcija u bezgotovinskom plaćanju za razdoblje 2014-2015. godinu prema svjetskim regijama10

Grafikon pokazuje relativni jednogodišnji porast bezgotovinskog plaćanja podijeljen prema značajnim ekonomskim regijama, za 2015. godinu. Vidljivo je povećanje u svim regijama, a najviše u zemljama s brzorastućim ekonomijama - Kini, Rusiji i Južnoj Koreji. Većina se stručnjaka slaže da porast bezgotovinskog plaćanja potiče traženje novih, pogodnijih načina plaćanja, pogotovo plaćanja preko interneta, za što su nove digitalne valute posebno pogodne.

2.2. Razvoj kriptografije

Kriptografija je multidisciplinarna znanost, zasnovana uglavnom na područjima matematike i računalnih znanosti, a u svrhu što efikasnijeg kodiranja i dekodiranja podataka. Cilj je da pošiljatelj informacije može vrlo uspješno poslati informacije primatelju, bez bojazni (ili sa određenom sigurnošću) da će sve te informacije doći u posjed treće strane. Razvojem računalne tehnologije, a posebno mikroprocesora, stvorili su se uvjeti za nastanak sve efikasnijih i bržih implementacija kriptografskih funkcija u računalnim (software-skim) funkcijama. Jedno od područja kriptografije je i razvoj tzv. hash funkcija. To su funkcije koje za ulaz mogu uzeti niz podataka bilo koje duljine, a za njega će izraditi specifičan „potpis" odnosno niz znakova koji je unaprijed zadane duljine. Pri tome je izrazito važno da svaka najmanja izmjena ulaznog niza znakova uzrokuje značajne promjene izlaznog niza, dok brzina cijelog procesa direktno utječe na uporabljivost funkcije. Sama funkcija je „jednosmjerna" tj. lako je izračunati hash ulaznih podataka, ali je nemoguće iz hasha dobiti originalni niz podataka.[11]U tablici 1 dan je primjer nekoliko kodiranih nizova znakova.

10 World PaymentsReport, dostupno na: https://www.worldpaymentsreport.com/reports/noncash#transactions-volumetop-10-markets [Pristupljeno: 30.08.2017.]

11 MIRONOV, Ilya, OTHERS, Hashfunctions: Theory, attacks, andapplications, *Microsoft Res. Silicon Val. CampusNoviembre De*, 2005, Dostupno na: http://www.engr.uconn.edu/~akiayias/cse281sp08/CSE281_Computer_Security/Reading_files/hash_survey.pdf. [Pristupljeno: 30-ožu-2017]

Ulazni niz podataka	SHA-256 kodirani hash u heksadecimalnom obliku
a	ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb
A	559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd
Ovo je test	0e12c87d069f5ca7b7d7b66fb3e9e4f4e60a12a9b337c7f2f0057a953f1ecad1
Ovo je test.	93135b502c42cec40bd0815a0a3deec07cbc09464b47a74be084257924203c08

Tablica 1- Primjer nekoliko kodiranih nizova znakova SHA-256 algoritmom12

Ovakva se tehnologija koristi za osiguranje autentičnosti ili kontrolu podataka, na način da se provjerom potpisa (hasha) - kojeg je moguće lako i brzo izvršiti, može sa zadovoljavajućom razinom vjerojatnosti garantirati i potvrditi autentičnost originalnih podataka. Npr. u tablici 1 prikazan je primjer nekoliko ulaznih i pripadajućih izlaznih vrijednosti za hash funkciju SHA-256. Izlaz te funkcije je 256 bitni broj, što znači da je maksimalni broj kombinacija izlazne vrijednosti jednak 2^{256}, odnosno vrijednosti većoj od 10^{77}.

Svojstvo kriptiranja je vrlo važno u projektiranju virtualnih valutnih sustava jer omogućava strojnu, automatiziranu provjeru podataka, bez prisustva čovjeka. Razvoj digitalnih valuta, pa i samih digitalnih inačica klasičnog novca, ne bi bio moguć bez odgovarajućeg stupnja razvoja kriptografije. Osim funkcije sigurnosne zaštite transakcija u općenitom internetskom poslovanju, kod virtualnih valutnih shema kriptografija je temeljna i ključna komponenta sustava. Neke od najpoznatijih i najviše korištenih hash funkcija danas su MD5, SHA-160, SHA-256, SHA-512 itd.[13] Različiti tipovi ovih funkcija namijenjeni su za različite namjene, i zbog svoje ogromne važnosti, predmet su stalnog razvoja i usavršavanja od strane znanstvene zajednice. Stoga je razvoj i unapređenje kriptografije svakako nužan preduvjet za razvoj novih elektroničkih sustava plaćanja i unapređenje njihove sigurnosti, a s tim i raznih oblika digitalnog novca.

2.3. Blockchain tehnologija

Blockchain tehnologija kao temelj sustava virtualnih valutnih shema, predstavljena je 2009. godine. Pod pseudonimom Satoshi Nakamoto objavio ju je nepoznati autor (ili organizacija) u vidu softwarea otvorenog koda (*eng. Open source*), na web stranici https://bitcoin.org.[14] Iako postoje brojne špekulacije, do danas nije sa sigurnošću utvrđen identitet autora. Kako osnovna verzija softwarea (koji se od 2009. godine stalno unapređuje i razvija od zajednice) sadrži preko 31.000 linija koda, što bi uz neke prosječne standarde značilo minimalno 2-3 godine rada uz puno radno vrijeme za jednog programera, jasno je zašto mnogi sumnjaju da je cijeli projekt djelo jednog čovjeka (iako je i ta mogućnost realna).[15]

12 TOMAŠIĆ, M., Tehnički, ekonomski i pravni aspekti digitalnog novca, diplomski rad, Sveučilište u Zadru – Odjel za ekonomiju, Zadar, 2017., str. 11.
13 BURR, William E., Selectingtheadvancedencryption standard, *IEEE Secur. Priv.*, sv. 99, izd. 2, 2003, str. 43–52
14 NAKAMOTO, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009, Dostupno na: https://bitcoin.org/bitcoin.pdf. [Pristupljeno: 29-ožu-2017]
15 TOMAŠIĆ, M., Ibid., str., 12.

Blockchain je baza podataka u digitalnom obliku, sadrži dnevnik svih transakcija izvršenih u sustavu. Decentralizirana je na način da svaki sudionik sustava ima mogućnost pohranjivanja kod sebe vlastite kopije. Sudionici ili čvorovi u sustavu (*eng. nodes*)[16] su ravnopravni svjedoci i kontrolori autentičnosti svake pojedinačne transakcije. Transakcije se grupiraju kronološki, u tzv. Blokove transakcija. Svaki blok transakcija se digitalno „potpisuje" - odnosno pridružena mu je određena digitalna šifra (*eng. hash*) koja je garancija da je blok autentičan te je svaki pokušaj promjene sadržaja bloka vrlo lako otkriti. Uz navedeno, svaki blok sadrži i hash prethodnog bloka, a to znači da ako netko želi promijeniti sadržaj određenog bloka (npr. dodajući ili mijenjajući transakcije), mora izmijeniti i sve blokove u nizu nakon izmijenjenog bloka. Blokovi su na taj način povezani - ulančani, odakle i potječe naziv Blockchain.[17] Iz prethodnog je vidljivo da se cijeli sustav temelji na funkcionalnosti mreže sudionika u kojoj su svi ravnopravni i postavljenom tehničkom rješenju, bez određenog centraliziranog sustava autorizacije[18], kao što je slučaj kod internet bankarstva, gdje banka autorizira i kontrolira transakcije.

2.4. Bitcoin - prva valuta bazirana na blockchain tehnologiji

Bitcoin je digitalna, decentralizirana, pseudoanonimna valuta, koja se ne oslanja na vlade ili druge pravne osobe, i čija vrijednost nije garantirana zlatom ili drugom robom. Ona se oslanja na ravnopravnu mrežu računala i održava integritet uz pomoć kriptografije.[19] Bitcoin je vrlo složen sustav, a njegova implementacija uključuje kombinaciju kriptografije, distribuiranih algoritama i usuglašenog ponašanja zajednice korisnika. Zagovornici Bitcoina tvrde da Bitcoin ima mnoga svojstva koja bi ga mogla učiniti idealnom valutom za trgovinu. Na primjer, bitcoini su vrlo likvidni, imaju niske troškove transakcije, mogu se koristiti za brzo slanje novca preko interneta, a mogu se praktično koristiti za obavljanje plaćanja u malim iznosima (*eng. micropayments*).[20] Decentralizirano upravljanje valutom koje onemogućava nekontrolirano tiskanje novog novca i generiranje inflacije, također se navodi kao prednost, mada postoje i mišljenja kako je upravo ta mogućnost regulacije količine novca bitan mehanizam financijskog upravljanja društvom, na način da se time uravnotežuju ciklusi ekonomskih kriza i procvata.[21]

Iako Bitcoin ekonomija cvjeta, korisnici su zabrinuti za pravni status Bitcoina i mogućnost eventualne zabrane uporabe od strane vlasti. Američka vlada je npr. procesuirala i zatvorila kreatore digitalne valute bazirane na vrijednosti zlata, e-gold, zbog kršenja državnih i saveznih propisa za urotu, pranje novca, kao i za pružanje usluga koje su klasificirane kao prijevare s kreditnim karticama, i investicijske prijevare. Činjenica jest da Bitcoin omogućava anonimne transakcije čime se olakšava pranje novca, utaje poreza, kockanje, trgovina drogom, dječja pornografija i slične kriminalne djelatnosti.[22][23]

16 ROGOJANU, Angela, BADEA, Liana, OTHERS, Theissueofcompetingcurrencies. Casestudy–Bitcoin, *Theor. Appl. Econ.*, sv. 21, izd. 1, 2014, str. 107

17 ABRAMOWICZ, Michael, Cryptocurrency-BasedLaw, *ArizRev*, sv. 58, 2016, str. 359

18 TURPIN, Jonathan B., Bitcoin: Theeconomiccase for a global, virtualcurrencyoperatinginanunexploredlegalframework, *Indiana J. Glob. Leg. Stud.*, sv. 21, izd. 1, 2014, str. 339

19 TOMAŠIĆ, M., Ibid., str., 14.

20 GRINBERG, Reuben, Bitcoin: Aninnovative alternative digitalcurrency, 2011, str. 206

21 ROTHBARD, Murray N., Austriandefinitionsofthesupplyofmoney, *New Dir. AustrianEcon.*, 1978, str. 143–156

22 GRINBERG, Reuben, Bitcoin: Aninnovative alternative digitalcurrency, 2011, str. 206

23 MARIAN, Omri Y., Are Cryptocurrencies' Super'TaxHavens?, 2013, Dostupno na: http://scholarship.law.ufl.edu/facultypub/358. [Pristupljeno: 18-velj-2017]

Bitcoin nema intrinzičnu vrijednost pa ipak se njime trguje širom svijeta za prilično velike iznose. Ukupna vrijednost Bitcoina u opticaju u trenutku pisanja ovog rada iznosi oko 75 milijardi USD, sa svakom pojedinačnom jedinicom u vrijednosti preko 4.500 USD. Ova ogromna vrijednost se održava isključivo na povjerenju između korisnika uključenih u Bitcoin transakcije.[24] Osim Bitcoina, sljedeća tablica prikazuje pregled pet najznačajnijih digitalnih valuta na svjetskom tržištu.

R.br.	Naziv valute	Tržišna kapitalizacija (mil $)	Vrijednost u $	Broj jedinica u opticaju	Dnevni promet u milijunima
1	Bitcoin (BTC)	75,74	4.581,51	16.531.600	2.474,8
2	Ethereum (ETH)	35,12	372,41	94.317.688	1.184,2
3	Bitcoin Cash (BCH)	8,86	535,32	16.551.938	320,4
4	Ripple (XRP)	8,40	0,22	38.343.841.883	291,8
5	Litecoin (LTC)	3,30	62,63	52.690.857	322,2

Tablica 2: Pregled pet najznačajnijih digitalnih valuta prema tržišnoj kapitalizaciji na dan 26.08.2017.25

3 TEHNIČKI ASPEKTI DIGITALNOG NOVCA

Kao primjer proučavanja digitalnih valuta[26] u radu je najviše korišten Bitcoin, jer je trenutno najpopularniji predstavnik spomenutog koncepta, a zbog velike sličnosti (u tehničkom, ekonomskom i pravnom smislu) većina iskazanog moglo bi se odnositi na bilo koju aktivnu digitalnu valutu baziranu na blockchain tehnologiji. Osnovne razlike među pojedinim valutama su uglavnom u specifičnostima tehničke prirode, te u prihvaćenosti pojedine valute, odnosno tržišnoj kapitalizaciji.

Pojavni oblici digitalnih valuta

Digitalne valute u većini slučajeva zapravo nemaju materijalni oblik iako se mogu prikazati i čuvati na materijalnom mediju (npr. papiru). Pri tome sam medij nema nikakvu važnost niti vrijednost - kao što je to slučaj kod klasičnog papirnog novca, gdje novčanica u fizičkom smislu i u originalnom izdanju predstavlja vrijednost. Za svaku postojeću adresu kod digitalnih valuta sustav bilježi ulazne i izlazne transakcije, tako da zbroj svih transakcija predstavlja stanje na računu. Pri tome se ne čuvaju salda pojedinih računa nego povijest svih transakcija, iz kojih se može lako izračunati trenutni saldo za svaku adresu. Uz svaku adresu postoji i tzv. privatni ključ (*eng. privatekey*). Ako korisnik poznaje adresu, može imati potpuni uvid u stanje, ali ne može trošiti sredstva s računa. Za trošenje je potreban privatni ključ.[27] Svaka adresa digitalne valute i pripadajući privatni ključ su međusobno povezani na način da je adresa rezultat određene kriptografske funkcije provedene nad privatnim ključem. To znači da se znajući adresu ne može utvrditi privatni ključ, ali

24 KAPLANOV, Nikolei, Nerdymoney: Bitcoin, theprivatedigitalcurrency, andthecaseagainstitsregulation, *LoyConsum. Rev*, sv. 25, 2012, str. 115

25 All Currencies | CryptoCurrencyMarketCapitalizations, Dostupno na: https://coinmarketcap.com/all/views/all/. [Pristupljeno: 26.08.2017.]

26 BUTERIN, Denis, RIBARIĆ, Eda, SAVIĆ, Suzana, Bitcoin – Nova globalna valuta, investicijska prilika ili nešto treće?, *Zb. Veleuč. U Rijeci*, sv. 3, izd. 1, 2015, str. 146

27 FAIRFIELD, Joshua AT, BitProperty, *Cal Rev*, sv. 88, 2014, str. 820

znajući privatni ključ, može se utvrditi adresu odnosno račun vlasnika primjenom odgovarajuće funkcije, odnosno služeći se javno dostupnim web servisima za pojedinu valutu.[28] Prilikom provjere svake transakcije, sustav uz pomoć privatnog ključa provjerava pripada li odgovarajuća adresa tom ključu, a zatim raspolaže li adresa sa dovoljno novca za izvršenje transakcije (je li saldo zadovoljavajući).

Prednosti i nedostaci različitih tipova novčanika

Digitalna valuta (npr. Bitcoin) je zapravo informacija odnosno broj, koji predstavlja takozvanu adresu digitalne valute, koja se može čuvati na više načina, najčešće u digitalnom obliku uz pomoć specijaliziranog računalnog programa. Takvi programi nazivaju se „novčanik" (*eng. Wallet*) i pojavljuju se u više oblika odnosno inačica:

1. Za klasična stolna i prijenosna računala (software za Windows, Mac, Linux)
2. Za mobilne uređaje (pametni telefoni i tableti, Android, iPhone)
3. Kao web aplikacije (*eng. Online web wallets*)
4. Kao specijalizirani uređaji (*eng. Hardware Wallets*)[29]

Moderni Bitcoin novčanici[30] raspolažu sa više korisnih funkcija. U njima možete čuvati podatke o puno adresa i pripadajućih ključeva, automatski će prikazivati ukupno stanje salda te će vršiti provjeru transakcije prije nego je pošalju u sustav.

Prilikom prijenosa određenog iznosa novčanih jedinica s jednog računa na drugi, računalni program elektroničkog novčanika najprije provjerava trenutno stanje salda korisnika, provjerava iznos na svakoj pojedinačnoj pohranjenoj adresi kako bi utvrdio postoji li dovoljna količina novca za realizaciju transakcije. Kada se utvrdi da je saldo zadovoljavajući, posebnim se algoritmom pokušava kombinirati traženi iznos iz postojećih adresa. Ukoliko je to kombiniranje moguće, transakcija se šalje svim čvorovima (*eng. nodes*) na potvrdu ili ovjeru. U slučaju nemogućnosti kombiniranja traženog iznosa, uzima se najbliži mogući veći iznos, a ostatak se kroz istu transakciju vraća pošiljatelju na neku od njegovih postojećih adresa. Na taj način digitalni novčanik ispunjava svoju funkciju. Prilikom kontrole salda neke verzije koriste vlastitu kopiju dnevnika transakcija, a neke (npr. mobilne) za pohranu vlastite kopije nemaju tehničkih uvjeta zbog ograničenosti memorije i slično, pa se za kontrolu salda oslanjaju na čvorove od povjerenja kontrolirajući samo nekoliko zadnje ovjerenih blokova. Za prikaz trenutnog stanja koriste se najčešće funkcije sučelja blockchain sustava koje su javno dostupne kao internetski servis.[31]

Funkcija čvorova za ovjeru transakcija

Svaki mrežni čvor sustava odnosno „rudar" (*eng. miner*) stalno je spojen na internetsku mrežu i prima sve novo emitirane transakcije korisnika (odnosno njihovih eloktroničkih novčanika). Takve primljene transakcije spremaju se u memorijski prostor primatelja (*eng. memorypool*) gdje čekaju da budu zapakirane u novi blok transakcija, zatim ovjerene i dodane u centralni dnevnik transakcija. Dodavanjem bloka u centralni dnevnik (blockchain) sve transakcije u bloku su ovjerene, transparentne i može ih provjeriti bilo tko.[32]

28 DOWD, Kevin, HUTCHINSON, Martin, Bitcoinwill bite thedust, *Cato J*, sv. 35, 2015, str. 359,364
29 TOMAŠIČ, M., Ibid., str. 19.
30 GOLDFEDER, Steven *i ostali*, Securingbitcoinwalletsviathresholdsignatures, 2014, str. 13
31 TOMAŠIĆ. M., Ibid., str.22.
32 DWYER, Gerald P., TheeconomicsofBitcoinandsimilarprivatedigitalcurrencies, *J. Financ. Stab.*, sv. 17, 2015, str. 81–91

Svakim sljedećim dodavanjem novog bloka u centralni dnevnik višestruko se ovjeravaju sve transakcije prethodnih blokova, povećavajući sigurnost sustava i u tehničkom smislu onemogućavajući zlouporabu cijelog sustava. Svaki rudar prilikom formiranja novog bloka transakcija, osim transakcija, oznake bloka i potpisa prethodno ovjerenog bloka u blok ugrađuje i jedan proizvoljan broj (*nonce*), promjenom kojega (pošto su sve ostale komponente bloka strogo definirane) može utjecati na potpis (*hash*) samog bloka. Sustav je projektiran tako da zahtijeva hash manji od zadane vrijednosti.[33] Kako nije moguće predvidjeti izlaznu vrijednost hash funkcije, rudari je moraju pogađati, odnosno ponavljati izračun mijenjajući *nonce* vrijednost, sve dok ne dobiju zadovoljavajući hash. Prvome koji dobije zadovoljavajući hash, sustav dozvoljava upis novog bloka u centralni blockchain, i nagrađuje ga određenom količinom novostvorenih novčanih jedinica. Na taj način motiviraju se rudari za svoj doprinos i istovremeno u opticaj pušta nova količina novca.[34]

Ovakav način potvrde transakcija naziva se *eng. Proofofwork*[35] ili skraćeno POW, zato što je potrebno uložiti određeni računalni rad kako bi se blok transakcija potvrdio. Uloženi rad ujedno je i garancija autentičnosti zapisa, odnosno sigurnosni čimbenik. Prema nekim autorima, ako bi netko kontrolirao više od pola čvorova na mreži, vrlo vjerojatno ne bi imao motiv raditi kriminalne radnje jer bi na taj način utjecao na pad vrijednosti valute zbog čega bi i sam najviše izgubio. Sustav bi tada pokazao tendenciju prijelaza u centralizirani, pa bi primjena blockchain tehnologije izgubila smisao. Brojni stručnjaci nastoje razviti i unaprijediti sustav koji koristi POW, zbog njegovih glavnih nedostataka; vremena za potvrdu transakcija i potrebe za „rudarima" te potrošnjom električne energije. Iz tog razloga javljaju se alternativna rješenja korištena u mnogim novim digitalnim valutama.

POS odnosno „profofsteak" nasuprot POW sustavu

Za razliku od POW[36] sustava kojega koristi Bitcoin, ideja POS sustava bazira se na pretpostavci da većinski vlasnici valute imaju najveću motivaciju za održavanje vjerodostojnosti cijelog sustava. Iz tog razloga, u takvom sustavu nema potrebe za tzv. rudarenje. Ovjera bloka vrši se konsenzusom vlasnika, pri čemu razmjerni udio u vlasništvu valute daje težinu prilikom potvrde bloka transakcija. U odnosu na POW sustav gdje je za kompromitiranje sustava potrebno kontrolirati više od 50% procesorske snage sustava, ovdje je potrebno posjedovati više od 50% novca kao bi se provela ovjera lažne transakcije. Treba primijetiti da slično kao i kod POW sustava, u takvom slučaju vlasnik više od 50% sredstava zapravo ima najmanje motiva za kompromitiranje sustava, jer raspolaže potrebnim konsenzusom za provođenje određenih akcija u sustavu, promjene softwara, protokola i slično. Osim POW i POS algoritama, postoje i drugi sustavi, kao i kombinacije raznih algoritama. Cijeli je sustav blockchaina u tehničkom smislu zamišljen tako da se pojedini dijelovi mogu unapređivati i po potrebi mijenjati, uz uvjet da postoji volja većine da se nove promjene i prihvate. Sustav je predstavljen u obliku otvorenog koda, vrlo je transparentan i kao takav pristupačan zajednici za korištenje i unapređivanje.

33 ZOHAR, Aviv, Bitcoin: underthehood, *Commun. ACM*, sv. 58, izd. 9, 2015, str. 108,110
34 DWYER, Gerald P., TheeconomicsofBitcoinandsimilarprivatedigitalcurrencies, *J. Financ. Stab.*, sv. 17, 2015, str. 81–91
35 OKUPSKI, Krzysztof, BitcoinDeveloper Reference, *Availabl E HttpenetiumComresourcesBitcoin Pdf*, 2014, str. 2
36 OKUPSKI, Krzysztof, BitcoinDeveloper Reference, *Availabl E HttpenetiumComresourcesBitcoin Pdf*, 2014, str. 2

4 ZAKLJUČNA RAZMATRANJA

Digitalni novac u tehničkom i pravnom smislu može se analizirati na razne načine. Zakonodavaci pojedinih država idu od ignoriranja do zabrane, što može predstavljati određeni sigurnosni rizik za korisnike, i uzrok špekulativnom pristupu digitalnim valutama. Korištenje digitalnog novca još je ograničeno na relativno mali udio populacije. Uglavnom su to korisnici koji se bave tehničkim ili financijskim djelatnostima te koji posjeduju potrebnu raznu tehnološkog znanja. Čimbenici koji najviše utječu na masovnost uporabe digitalnih valuta su prihvaćenost, praktičnost, visina provizije kod zamjene za klasičnu valutu, transakcijske provizije te raspoloživost bankomata. Razmjena digitalnog novca između korisnika postaje iz dana u dan sve jednostavnija i jeftinija, no još postoje određene prepreke koje onemogućuju brži razvoj transakcija. Kao jedan od primjera može se navesti veliki pad Bitcoin valute iz 2013. godine, nakon izdanog upozorenja Kineske centralne banke financijskim institucijama i tvrtkama da ne koriste Bitcoin. Kod digitalnih se valuta formalno radi o decentraliziranim valutnim sustavima bez nadređenog autoriteta, no svaka vlast ima na raspolaganju snažne mehanizme kojima može uspostaviti kontrolu nad korištenjem digitalnih valuta, ako to u nekom trenutku poželi. S obzirom na nedefinirani pravni okvir u većini zemalja, postoji rizik od zlouporabe digitalnih valuta, umanjujući potencijalno pozitivne efekte koje bi proizvela veća uporaba blokchain tehnologije. Sve veći razvoj i korištenje digitalnih valuta donosi novu dimenziju u trgovini, uštedama u vremenu i cijenama. Uzimajući u obzir provedeno istraživanje, može se zaključiti da je za održavanje stabilnosti sustava digitalnih valuta neophodna kvalitetana i sigurna tehnička podrška. Može se zaključiti da je tehnički aspekt jedan od najbitnijih čimbenika o kojima je potrebno voditi računa u cilju dugoročno održivog i kontinuiranog razvoja digitalnog novca u budućnosti te je na taj način i potvrđena hipoteza ovog rada.

LITERATURA:

1. ABRAMOWICZ, Michael, Cryptocurrency-Based Law, *Ariz Rev*, sv. 58, 2016, str. 359.
2. ANDREESSEN, Marc, Why Bitcoin Matters, *DealBook*, Dostupno na: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/. [Pristupljeno: 20.05.2017].
3. BORNHOLDT, Stefan, SNEPPEN, Kim, Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies, ArXiv Prepr. ArXiv14036378, 2014.
4. BURR, William E., Selecting the advanced encryption standard, *IEEE Secur. Priv.*, sv. 99, izd. 2, 2003, str. 43–52.
5. BUTERIN, Denis, RIBARIĆ, Eda, SAVIĆ, Suzana, Bitcoin – Nova globalna valuta, investicijska prilika ili nešto treće?, Zb. Veleuč. u Rijeci, sv. 3, pres. 1, 2015.
6. CHENG, Cecilia, LI, Angel Yee-lam, Internet addiction prevalence and quality of (real) life: A meta-analysis of 31 nations across seven world regions, *Cyberpsychology Behav. Soc. Netw.*, sv. 17, izd. 12, 2014, str. 755–760.
7. CryptoCurrency Market Capitalizations, Dostupno na https://coinmarketcap.com/all/views/all/, (Pristupljeno 24.07.2017.).
8. European Central Bank. Eurosystem. 2015. Virtual currency scheme – a further analysis. Frankfurt am Main, Dostupno na https://www.ecb.europa.eu/pub/pdf/ other/virtualcurrency schemesen.pdf, (Pristupljeno 28.08.2017).
9. DELMOLINO, Kevin *i ostali*, Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, u *International Conference on Financial Cryp-*

tography and Data Security, 2016, str. 79–94, Dostupno na: http://link.springer.com/chapter/10.1007/978-3-662-53357-4_6. [Pristupljeno: 18-velj-2017].
10. DOWD, Kevin, HUTCHINSON, Martin, Bitcoin will bite the dust, *Cato J*, sv. 35, 2015, str. 359,364.
11. DUPONT, Quinn, MAURER, Bill, Ledgers and Law in the Blockchain, *Kings Rev., Httpkingsreview Co Ukmagazineblog20150623ledgers--Law---Blockchain*, 2015, Dostupno na: http://iqdupont.com/assets/documents/DUPONT-MAURER-2015-Preprint-Ledgers_and_Law_in_the_Blockchain.pdf. [Pristupljeno: 24.05.2017].
12. DWYER, Gerald P., The economics of Bitcoin and similar private digital currencies, *J. Financ. Stab.*, sv. 17, 2015, str. 81–91.
13. FAIRFIELD, Joshua AT, BitProperty, *Cal Rev*, sv. 88, 2014, str. 820.
14. GLASER, Florian, ZIMMERMANN, Kai, HAFERKORN, Martin, WEBER, Moritz Christian, SIERING, Michael, Bitcoin-asset or currency? revealing users' hidden intentions, 2014, Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247, (Pristupljeno 17.05.2017).
15. GOLDFEDER, Steven *i ostali*, Securing bitcoin wallets via threshold signatures, 2014, str. 13.
16. GRINBERG, Reuben, Bitcoin: An innovative alternative digital currency, 2011, str. 206.
17. KAPLANOV, Nikolei, Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, *Loy Consum. Rev*, sv. 25, 2012, str. 115.
18. KOBLITZ, Neal, MENEZES, Alfred J., Cryptocash, cryptocurrencies, and cryptocontracts, Des. Codes Cryptogr., sv. 78, izd. 1, 2016.
19. KOSBA, Ahmed *i ostali*, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, u *Security and Privacy (SP), 2016 IEEE Symposium on*, 2016, str. 839–858, Dostupno na: http://ieeexplore.ieee.org/abstract/document/7546538/. [Pristupljeno: 14-velj-2017].
20. LUTHER, William J., Cryptocurrencies, network effects, and switching costs, Contemp. Econ. Policy, 2015.
21. MANKIW, N. Gregory, The data of Macroeconomics, Principles of macroeconomics, Cengage Learning, 2014.
22. MARIAN, Omri Y., Are Cryptocurrencies' Super'Tax Havens?, 2013, Dostupno na: http://scholarship.law.ufl.edu/facultypub/358. [Pristupljeno: 18-velj-2017].
23. MATTILA, Juri, The Blockchain Phenomenon, *'Book Blockchain Phenomenon'Berkeley Roundtable Int. Econ. 2016 Edn*, 2016, str. 6.
24. MEEKER, Mary, Internet trends 2015-Code conference, *Glokalde*, sv. 1, izd. 3, 2015, Dostupno na: http://dergipark.ulakbim.gov.tr/glokalde/article/view/5000135231. [Pristupljeno: 29-ožu-2017].
25. MIRONOV, Ilya, OTHERS, Hash functions: Theory, attacks, and applications, *Microsoft Res. Silicon Val. Campus Noviembre De*, 2005, Dostupno na: http://www.engr.uconn.edu/ ~akiayias/cse281sp08/CSE281_Computer_Security/Reading_files/hash_survey.pdf. [Pristupljeno: 30-ožu-2017].
26. NAKAMOTO, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009, Dostupno na: https://bitcoin.org/bitcoin.pdf. [Pristupljeno: 29.03.2017].
27. OMOHUNDRO, Steve, Cryptocurrencies, smart contracts, and artificial intelligence, *AI Matters*, sv. 1, izd. 2, 2014, str. 19–21.
28. PLASSARAS, Nicholas A., Regulating digital currencies: bringing Bitcoin within the reach of IMF, Chic. J. Int. Law, sv. 14, 2013.
29. OKUPSKI, Krzysztof, Bitcoin Developer Reference, *Availabl E Httpenetium ComresourcesBitcoin Pdf*, 2014, str. 2.
30. ROGOJANU, Angela, BADEA, Liana, OTHERS, The issue of competing currencies. Case study–Bitcoin, *Theor. Appl. Econ.*, sv. 21, izd. 1, 2014, str. 107.
31. ROTHBARD, Murray N., Austrian definitions of the supply of money, *New Dir. Austrian Econ.*, 1978, str. 143–156.

32. TOMAŠIĆ, M., Tehnički, ekonomski i pravni aspekti digitalnog novca, diplomski rad, Sveučilište u Zadru – Odjel za ekonomiju, Zadar, 2017.
33. TRAUTMAN, Lawrence J., Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox, 2014.
34. TURPIN, Jonathan B., Bitcoin: The economic case for a global, virtual currency operating in an unexplored legal framework, *Indiana J. Glob. Leg. Stud.*, sv. 21, izd. 1, 2014, str. 339.
35. Virtual currency schemes, lis-2012, Dostupno na https://www.ecb.europa.eu /pub/pdf/other/ virtualcurrencyschemes201210en.pdf., (Pristupljeno 20.03.2017.)
36. ZOHAR, Aviv, Bitcoin: under the hood, *Commun. ACM*, sv. 58, izd. 9, 2015, str. 108,110
37. World Payments Report, Dostupno na: https://www.worldpaymentsreport.com/reports/ noncash#transactions-volumetop-10-markets [Pristupljeno: 30.08.2017]