

THE USE OF DECENTRALIZED DIGITAL CURRENCY BITCOIN IN ELECTRIC COMMERCE

PRIMJENA DECENTRALIZIRANE DIGITALNE VALUTE BITCOIN U ELEKTRONI KOM POSLOVANJU

IDLBEK, Robert; BUDIMIR, Verica & HRMIC, Danijela

Abstract: *The mathematical concept of Bitcoin network was introduced in the year 2008. by a person, or group of people under the pseudonym Satoshi Nakamoto. During the next year, the first implementation of software for supporting Bitcoin transactions was put into operation. Today, it supports more than 70,000 daily transactions, and market value in the last five years has reached roughly \$ 7 billion. Therefore, it can be easily seen that that there is a specific need for the application of new forms of digital payment in electronic commerce.*

Keywords: *Bitcoin, digital currency, electronic commerce, cryptocurrency*

Sažetak: *Koncept bitcoin mreže prvi je puta predstavljen 2008. godine od strane osobe ili grupe ljudi pod pseudonimom Satoshi Nakamoto. Ve sljede e godine je pušten u pogon prvi softver za provedbu bitcoin transakcija, a danas se dnevno provede njih više od 70 tisu a. Obzirom na izrazito snažan rast te mreže, ija je vrijednost u posljednjih pet godina dosegla okvirno 7 milijardi USD, jasno je kako postoji konkretna potreba za primjenom novih oblika digitalnih pla anja u elektroni kom poslovanju.*

Ključne riječi: *Bitcoin, digitalna valuta, elektroni ko poslovanje, kripto valuta*



Authors' data: Robert **Idlbek**, dr.sc., Veleu ilište u Požegi, Vukovarska 17, 34000 Požega; ridlbek@vup.hr; Verica **Budimir**, dr.sc., Veleu ilište u Požegi, Vukovarska 17, 34000 Požega, vbudimir@vup.hr; Danijela **Hrmic**, upr.iur., student, Veleu ilište u Požegi, Vukovarska 17, 34000 Požega; dhrmic@vup.hr

1. Uvod u problematiku elektroni kog pla anja

Razvoj razli itih oblika digitalnih pla anja u posljednjih petnaestak godina ima snažan utjecaj na svjetsku ekonomiju i op enito pozitivno prihva anja ideje o sigurnoj razmjeni roba, usluga i financijskih sredstava. Bezgotovinska pla anja temeljena na informati koj tehnologiji postaju osnovni i preferirani na in pla anja za sve ve i broj korisnika ija educiranost i povjerenje u sigurnost sustava raste. Prihva anje novih kanala pla anja koji u svojem nazivu imaju prefikse za „mobilno“ i „elektroni ko“, postaju sve eš i i op e prihva eni. Tome ide u prilog i injenica kako pove anje broja bezgotovinskih transakcija ima o ekivano pozitivan trend u posljednjih deset godina. Taj trend pokazuje kako se broj bezgotovinskih transakcija pove ava na godišnjoj razini okvirno 6-7% u razvijenim zemljama, odnosno oko 15-20% u zemljama u razvoju, što je rezultiralo dosegom od 333 milijarde bezgotovinskih transakcija u 2012. godini [1]. Kroz analizu dostupne literature, isti u se tri osnovna razloga za navedeni porast broja digitalnih oblika pla anja: (1) pove ana penetracija pametnih mobilnih ure aja i korištenja Interneta, (2) napredak u tehnologiji, te (3) inovativni proizvodi i usluge. Dosadašnja iskustva korisnika *online* financijskih usluga za bezgotovinska pla anja (kreditne kartice, PayPal, Skrill te razni sustavi elektroni kog novca) pozitivna su i s pove anjem njihove educiranosti pove ava se i povjerenje prema sigurnosnim mehanizmima na kojima se ti sustavi temelje. Iz perspektive korisnika, primjena sustava za elektroni ka pla anje je uglavnom jednostavna, no zbog izrazito kompleksne sigurnosne infrastrukture i skupa. Sigurnosna infrastruktura se financira kroz naknade za svaku provedenu elektroni ku bezgotovinsku transakciju, a njihov iznos ini 3 do 10% ukupne cijene transakcije. Navedena naknada zara unava se primatelju novca (pružatelju usluge, prodavatelju), što u kona nici znatno poskupljuje uslugu odnosno proizvod. Zbog toga, kao i niza kasnije navedenih razloga, vidljiva je potreba za uvo enjem novih oblika elektroni kih pla anja.

2. Razlozi uvo enja alternativnih na ina za elektroni ka pla anja

Problematika i tehnološki temelji za primjenu elektroni kog pla anja obra eni su u mnogim starijim znanstvenim i stru nim radovima [13, 14]. Analiziraju i promjene u na inima pla anja posljednjih 10-ak godina vidljivo je kako se oni nisu znatnije mijenjali, dok je broj usluga i korisnika na Internetu bitno porastao. Uvo enje novih usluga, u pravilu uvijek temeljenih na mrežnom pristupu i nekom obliku informati ke tehnologije, usporeno je zbog neadekvatnih oblika elektroni kog pla anja. Stoga, sveobuhvatne i funkcionalne promjene mogu e je o ekivati uskoro. Osnovne pokreta ke ideje za promjenu postoje ih elektroni kih oblika pla anja mogu se prikazati u sljede ih pet aspektata:

2.1. Mogu nost obrade transakcija bez obzira na mjesto, vrijeme i pristup mreži

Sve više digitalnih usluga i proizvoda dostupno je ne samo na mreži ve i u svakodnevnom životu pojedinca koji nije vezan uz mrežu. Iako je propagacija mobilnog Interneta izuzetno snažna pojava u posljednjih nekoliko godina [15] usluge

zasnovane na njemu plaćaju se još uvijek na trenutno klasične (PayPal, e-bankarstvo i slično). Svi navedeni oblici elektroničkog plaćanja zahtijevaju od korisnika posjed uređaja spojenog na mrežu što u nekim slučajevima s tehničke strane nije moguće ostvariti. To onemogućuje provedbu elektroničkog plaćanja i zbog toga je fokus informatičke zajednice na uspostavi načina za elektroničko plaćanje u slučajevima kada pristup mreži nije dostupan (eng. offline).

2.2. Brzina obrade transakcija

Za otkrivati je da se elektroničke novane transakcije u današnje vrijeme obrađuju u tzv. realnom vremenu (eng. realtime), što bi za korisnika trebalo predstavljati trenutnu obradu. Međutim, to je u većini slučajeva daleko od realnosti. Transakcije u poslovnim bankama provode se trenutno samo ako su i pošiljatelj i primatelj novca u istoj banci. U slučaju da su oni u različitim bankama, transakcije se dijele u vremenske cikluse koje određuje nacionalno regulatorno i međubankarsko tijelo, a u navedenim ciklusima se provode ukoliko transakcija uključuje dvije banke. U Hrvatskoj je takvo regulatorno tijelo Nacionalni klirinški sustav (NKS), a u pravilu se u toku jednog dana izvrši četiri ciklusa u okviru kojih se provede oko pola milijuna transakcija [4]. Navedeni klirinški sustavi predstavljaju velik problem u brzini i cijeni obrade novanih transakcija ukoliko se novana transakcija provodi bilateralno, zbog čega je i cijena prijenosa novca iz jedne države u drugu visoka.

2.3. Cijena transakcije

Kao što je ranije navedeno, jedan od osnovnih problema u korištenju online načina plaćanja su upravo visoki transakcijski troškovi. Navedeni troškovi variraju, ovisno o financijskom proizvodu odnosno kartičarskoj ili bankarskoj usluzi, no uvijek predstavljaju značajan postotak ukupne cijene usluge. U izračun cijene transakcije uključuje se cijena troškova obrade podataka, autorizacije, kliringa, poravnavanja, detekcije sumnjivih transakcija i slično [5]. Takva visoka cijena obrade transakcije, koja često uključuje visok fiksni trošak ujedno i onemogućuje provedbu tzv. mikrotransakcija. Takva mikroplaćanja, čija ideja je brzo, jednostavno i jeftino prebacivanje manje sume novca s jednog računa na drugi, osnova su mnogih modernih i inovativnih usluga. Mikrotransakcije su predvođene industrijom zabave, odnosno kupovinom digitalnih vrijednosti unutar računalnih igara. Kao primjer mikroplaćanja u Hrvatskoj možemo navesti SMS plaćanje parkinga, plaćanje karte za tramvaj putem SMS-a ili NFC-a, te plaćanje cijene objave oglasa ili preuzimanje sadržaja s nekih web portala. Kao što je vidljivo iz primjera, takav način plaćanja uvijek se odvija između registriranog pružatelja usluga (poduzeća) i korisnika, a plaćanja izvan granice države zbog mogućih visokih troškova mobilnih operatera i roaminga mogu predstavljati opasnost po korisnika. Nadalje, nije moguće provesti transakciju mikroplaćanja između dvije privatne osobe. Upravo zbog tih razloga informatički stručnjaci već niz godina pokušavaju pronaći adekvatno rješenje te omogućiti financijske transakcije koje ne bi bile centralizirane i vezane uz pojedinog pružatelja usluga ili banku: Financijske transakcije trebale bi biti decentralizirane, jeftine, brze i uz visoku razinu sigurnosti i anonimnosti.

2.4. Zavisnost od regulatornih i drugih posredni kih tijela

Svi oblici današnjeg elektroni kog pla anja ovise o regulatornim i posredni kim tijelima, bilo da se oni odnose na banke, klirinške institucije ili karti arske organizacije koje nude usluge pla anja. Takav pristup iako je nužan, znatno otežava transakcije i ovisan je o zakonskim regulativama koje u razli itim zemljama mogu biti potpuno druga ije.

2.5. Sigurnost transakcija i privatnost korisnika

Iako je ova tema obra ena u mnogo stru nih i znanstvenih lanaka, zajedni ki zaklju ak je kako su trenutno dostupni mehanizmi zaštite za korisnika dovoljno prihvatljivo rješenje te kako sigurnost u ve ini slu ajeva ovisi o samom korisniku, a ne tehnologiji. ak i tada, zbog visoke razine profesionalizma te planiranog smanjenja rizika od negativnog publiciteta, banke, karti arske ku e i drugi pružatelji elektroni kih usluga pla anja na vlastiti teret snose eventualne troškove korisnika koji su na bilo koji na in prevareni. U tehni kom smislu privatnost korisnika ne postoji jer su sve elektroni ke transakcije povezane s identitetom osoba koje šalju ili primaju novac.

3. Uvod u problematiku kriptovalute Bitcoin

Bitcoin (BTC) je virtualna digitalna valuta temeljena na kompleksnim matemati kim i sigurnim kriptografskim algoritmima za zaštitu sigurnosti korisnika, sigurnosti transakcija i osiguravanje njihove provedivosti [2]. Vrijednost BTC valute nije vezana za neku postoje u opipljivu vrijednost (npr. zlato), niti je vezana uz bilo kakvo regulatorno tijelo kao što je to nacionalna ili centralna banka. Obzirom kako jedan BTC nema direktnu vezu sa realnom vrijednoš u, to je ujedno i jedna od najve ih mana. Tržišna cijena jednog BTC-a u vrijeme pisanja ovog teksta kre e se oko 313 EUR. U vrijednosti BTC-a mogu e su velike oscilacije u cijeni uslijed njegove ovisnosti o broju korisnika, špekulacijama te budu oj naklonjenosti financijskog tržišta, regulatornih tijela i legislative. Obzirom kako nema realnu vrijednost, koncept korištenja ove kriptovalute temelji se na ideji da e navedenu kriptovalutu koristiti i druga osoba ili poslovni subjekt kao sredstvo pla anja odnosno primanja naknade za svoju uslugu ili proizvod. U posljednje vrijeme sve je ve i broj korisnika koji prima navedenu valutu kao platežno sredstvo, što u ovom trenutku predstavlja pozitivan trend i perspektivnu budu nost. Provedba transakcija vezanih uz bitcoin digitalnu valutu zasniva se na decentraliziranoj peer-2-peer mreži, a sve transakcije vidljive su svim Internet korisnicima okvirno 10 minuta nakon njihove provedbe. Takav pristup omogu uje pra enje svih dosadašnjih transakcija u tzv. realnom vremenu na web stranici blockchain.info te onemogu uje falsificiranje podataka i uplata. Za razliku od klasi nih financijskih transakcija koje su vidljive samo fizi kim ili pravnim osobama koje su u njih uklju ene (primatelj, pošiljatelj i banka), bitcoin transakcije vidljive su svim korisnicima Interneta. Iako neki izvori navode kako su transakcije u bitcoin sustavu anonimne [2], to zapravo nije to no ve se radi o pseudonimnosti [3]. Transakcija je anonimna na na in da jedan korisnik može imati neograni en broj adresa za primanje ili slanje novca, te da one niti na

jedan na in ne odaju identitet korisnika. Me utim, obzirom kako je koncept bitcoin mreže temeljen upravo u njenoj transparentnosti, svi korisnici mogu provjeriti s koje adrese i na koju adresu je stigla uplata, odnosno s koje adrese je ona ispla ena. Olakšavaju a okolnost je u tome što transakcijski ra un odnosno adresa primatelja ili pošiljatelja novca predstavlja alfanumeri ki niz od 27 do 34 znakova (npr: 3J98t1WpEZ73CNmQviecnyiWrnqRhWNLY) što otežava ulazak u trag vlasnika ra una. Isto tako, osoba samostalno može izraditi i imati u posjedu neograni en broj transakcijskih ra una, pa ak i koristiti novi ra un za svaku transakciju. Imaju i to u vidu, ukoliko se poštuje nekoliko osnovnih pravila prilikom pla anja bitcoin valutom, korisnik može biti siguran u svoju anonimnost. Upravo zbog takve anonimnosti se kriptovalu tu bitcoin, kao i gotovinu, povezuje sa raznim nelegalnim aktivnostima i trgovinom [16]. Bitcoin je u obliku nove i tehnološki zanimljive ideje predstavljen 2008. godine u stru nom lanku objavljenom pod pseudonimom Satoshi Nakamoto [6, 7]. Klju ne ideje navedenog lanka predstavljaju: mreža ravnopravnih ra unala (peer-2-peer), sigurnost i elektroni ki sustavi za pla anje. Navedene ideje polaze od toga da postoji matemati ki algoritam koji omogu uje sigurnu provedbu transakcija izme u korisnika i bez potrebe za tre om stranom (npr. bankom). To po iva na injenici kako je matemati ko probijanje odre enih transakcija putem tzv. iste sile (eng. brute force) složen, zahtjevan, spor i esto neprakti an posao, te da e transakcije u bitcoin mreži biti sigurne sve dok ra unala za rudarenje budu imala više procesorske snage od ra unala koja bi se eventualno mogla iskoristiti za hakerski napad [6]. Tehni ka specifikacija mreže pojašnjena u navedenim stru nim radovima stvorila je osnovu za kasniju razradu kripto valuta, od kojih je osim navedene bitcoin mreže nastalo još nekoliko: litecoin, devicon, liquidcoin, namecoin, solidcoin, ixcoin i 10coin [8]. Korisnici bitcoin mreže u posjed navedene valute mogu do i na dva na ina: 1) kupovinom za tradicionalan novac, te 2) pružanjem usluge digitalne obrade podataka, tzv. rudarenjem (eng. mining). Kupovina kripto valute mogu a je putem brojnih online servisa za kupoprodaju kao što je slovenski bitstamp.net, dok je proizvodnja vlastite valute tehni ki znatno zahtjevniji posao. U posljednje vrijeme javljaju se i bitcoin bankomati koji omogu uju kupovinu ili prodaju te valute za gotovinu. Rudarenje se odvija na na in da ra unala spojena na Internet i u našem vlasništvu pružaju odre ene usluge procesiranja operacija koje se u bitcoin mreži provode i koje su nužne za njeno funkcioniranje. Na taj na in, naše ra unalo pomaže u nesmetanom radu mreže preuzimaju i na sebe odre eni posao kao što je to knjiženje novih transakcija u bazu, njihovu provjeru, objavu i sli no. Navedene aktivnosti su izuzetno procesorski zahtjevne i upravo je njihova procesorska intenzivnost temeljna karakteristika koja ne dopušta inflaciju valute. Naime, nakon odre enog procesorski zahtjevnog posla, korisnik-vlasnik ra unala koje provodi rudarenje dobiva odre enu koli inu BTC kripto valute kao nagradu za svoj rad. Obzirom na visoku cijenu hardvera potrebnog za te aktivnosti, neki od relevantnih stru nih lanaka govore o neisplativosti investicija u hardver za rudarenje [8]. Takav hardver mora biti temeljen na skupim multiprocesorskim i višejezgrenim grafi kim procesorima namijenjenim isklju ivo za intenzivnu obradu podataka. Obzirom na njihovu cijenu i potrošnju elektri ne

energije, sve manji broj korisnika se na to odlučuje, a sve veći broj na kupovinu BTC-a putem web stranica.

4. Pravna regulativa

Obzirom kako pojedini bitcoin računali posjeduju više od 100 milijuna USD vrijednosti u BTC valuti [10], a cjelokupno tržište je procijenjeno na više od 7 mlrd. USD [11], sve je veći i zanimanje regulatornih tijela za uvođenje nekog oblika regulacije u transakcije s kriptovalutama. U Republici Hrvatskoj bitcoin kriptovaluta nije definirana kao elektronički novac ili oblik plaćanja te zbog toga niti ne postoji zakonska prepreka za njeno korištenje. Hrvatska narodna banka se u svom priopćenju priklanja europskim liberalnim stavovima i navodi kako bitcoin nije sredstvo plaćanja te kao takvo niti ne podliježe oporezivanju, nadzoru i drugim oblicima regulacije. Takav pristup opremanje stavovima nekih zemalja u kojima je zabranjeno bilo kakvo trgovanje vezano uz bitcoin (Island i Vietnam), dok je u Indiji, Indoneziji, Japanu, Jordanu, Libanonu, Taiwanu i Kini (osim Hong Konga) trgovina uz određena ograničenja dozvoljena.

Obzirom kako regulatorna tijela svih zemalja nemaju sličan stav o tim navedenoj problematici, u slučaju daljnjeg nastavka razvoja bitcoin mreže, za očekivati je usklađivanje regulativa i zakonodavstva u različitim zemljama. Američka administracija bitcoin ne smatra valutom već sredstvom plaćanja koje se može oporezivati [9] što ukazuje na prepoznavanje potencijala ovog oblika plaćanja u budućnosti. Imaju i u vidu snažni razvoj kriptovaluta (u ovom trenutku postoji već 10-ak izvedenica na temelju bitcoin protokola), te sve veći u količinu transakcija vezanih uz kriptovalute, izvjestan je određeni oblik njene regulacije [12].

5. Zaključak na razmatranja

Kriptovalute u budućnosti mogu imati znatan utjecaj na razvoj elektroničkog poslovanja. Imaju i u vidu snažan razvoj novih obrazaca ponašanja korisnika, uglavnom temeljenih na mreži, digitalnim medijima i elektroničkim uslugama, logičan je i dodatan razvoj sadašnjih i budućih oblika elektroničkih plaćanja. Bitcoin kao predstavnik novog i inovativnog oblika plaćanja temeljen na matematičkim algoritmima u obliku kriptovalute, predstavlja zanimljiv idejni koncept.

Iako u ovom trenutku postoji nekoliko objektivnih razloga za opreznost prilikom obavljanja transakcija i posjedovanja bitcoin valute, razvoj ovog koncepta elektroničkog plaćanja u budućnosti bi mogao unijeti promjene u način razmišljanja i pristupa izradi novih proizvoda i usluga te njihovoj trgovini. Imaju i u vidu problematiku moguće inflacije digitalne kriptovalute te njene nevezanosti uz fizičke vrijednosti, djelomičnu anonimnost i nemogućnost nadzora digitalnih transakcija, ukoliko to regulativa i zakonodavstvo određene zemalja dopusti, moguće je očekivati kako će neki od oblika kriptovaluta održati kao platežno sredstvo i izvan okvira Interneta.

6. Literatura

- [1] Word Payments Report 2013 (2013). World Non-Cash Markets and Trends [online], *Dostupno na:* http://www.capgemini.com/resource-file-access/resource/pdf/wpr_2013.pdf *Pristup* 02-04-2014, str. 5.
- [2] Corporate Counsel (2013). Why Not Accept Bitcoin for Goods and Services? [online], *Dostupno na:* http://www.thompsonhine.com/uploads/1137/doc/corpcounsel_com-Why_Not_Accept_Bitcoin_for_Goods_and_Services.pdf *Pristup* 03-04-2014
- [3] Meiklejohn, S.; Pomarole, N. & Jordan G. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names [online], *Dostupno na:* <http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf> *Pristup* 06-04-2014
- [4] FINA (2014). Statistika naloga u NKS-u [online], *Dostupno na:* <http://www.fina.hr/Default.aspx?art=9006>
- [5] More CSI (2014). Transparentnost pove ava cijenu transakcija? [online] *Dostupno na:* <http://www.kartice.ba/banke.php?type=naknade1&page=1&rel=yes> *Pristup:* 9-04-2014
- [6] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System [online], *Dostupno na:* <https://bitcoin.org/bitcoin.pdf> *Pristup* 12-02-2014
- [7] Nakamoto, S. (2010). Bitcoin P2P e-cash paper [online], *Dostupno na:* <http://article.gmane.org/gmane.comp.encryption.general/12588/> *Pristup:* 12-02-2014
- [8] Heid, A. (2013). Analysis of Cryptocurrency Marketplace [online], *Dostupno na:* http://www.hackmiami.org/whitepapers/HackMiami-Analysis_of_the_Cryptocurrency_Marketplace.pdf *Pristup:* 15-03-2014
- [9] Internal Revenue Service (2014). Notice 2014-21. *Dostupno na:* <http://www.irs.gov/pub/irs-drop/n-14-21.pdf> [online], *Pristup:* 22-04-2014
- [10] BitcoinRichList (2014). Top 100 Richest Bitcoin Addresses [online], *Dostupno na:* <http://bitcoinrichlist.com/top100> *Pristup:* 17-04-2014
- [11] CoinMktCap (2014). Crypto-Currency Market Capitalizations [online], *Dostupno na:* <https://coinmarketcap.com> *Pristup:* 16-04-2014
- [12] European Parliamentary Research Service (2014). Bitcoin: Market, economics and regulation [online], *Dostupno na:* [http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI\(2014\)140793_REV1_EN.pdf](http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf) *Pristup:* 19-04-2014
- [13] Asonan, N., Janson, P.A. & Steiner, M. (1997). The State of the Art in Electronic Payment Systems [online] *Dostupno na:* http://www.hit.bme.hu/~buttyan/courses/BMEVIHI5316/Asokan+.SotA_e-payment_systems.1997.pdf *Pristup:* 12-04-2013
- [14] Dahlberg, T., Mallat, N. & Ondrus, J. (2007). Past, present and future of mobile payments research: A literature review [online] *Dostupno na:* <http://www.janondrus.com/wp-content/uploads/2008/05/ecra2007-inpress.pdf> *Pristup:* 27-01-2014
- [15] eMarketer (2014). Nearly Half of Western Europeans Will Use Mobile Web This Year [online] *Dostupno na:* <http://www.emarketer.com/Article/Nearly-Half-of-Western-Europeans-Will-Use-Mobile-Web-This-Year/1010510> *Pristup:* 14-04-2014
- [16] Samani, R., Paget, F. & Hart, M. (2014). Digital Laundry: An analysis of online currencies, and their use in cybercrime. McAfee [online] *Dostupno na:* <http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf> *Pristup:* 24-03-2014