KRIPTOVALUTE, BLOKČEJN I BITKOIN

CRYPTOCURRENCY, BLOCKCHAIN, AND BITCOIN

Mario Lukinović
Pravni fakultet Univerziteta Union, Beograd, Srbija

JEL kategorija: **E41, E51**

Apstrakt

Kriptovalute (engl. "cryptocurrency") su digitalne (virtualne) valute, koje iako su sredstvo razmene, još uvek nisu strogo regulisane zakonom u većini država, a u pojedinim su čak i zabranjene. Veliki broj ljudi, uključujući i IT stručnjake i programere ne znaju mnogo o ovoj temi, a šira javnost izjednačava pojmove blokčejna i bitkoina. Tržište kriptovaluta danas iznosi gotovo 770 milijardi dolara. Od pojave prvih digitalnih valuta do danas, nastalo je preko 1.300 aktivnih kriptovaluta koje se razlikuju prema svojim svojstvima i upotrebi. Pre bitkoina bilo je mnoštvo neuspelih pokušaja stvaranja digitalnih valuta (digikeš, heškeš, Fejsbuk kredit i dr.). Utopistička ideja da matematika i fizika mogu rešiti društvene probleme započela je svoj život kroz pojavu bitkoina. Genijalna ideja po kojoj funkcioniše bitkoin zasnovana je na tehnologiji blokčejna, čiji kapacitet doseže daleko iznad kripto valuta. Iako se još uvek vode polemike ko stoji iza pseudonima Satoši Nakamoto, njegova zaostavština ima potencijal da promeni svet. Uspeh bitkoina leži u prednostima koje ima u odnosu na druge slične valute, ali njegov značaj prevazilazi i pogodnosti koje je doneo. Banke nisu potrebne za čuvanje podataka o novcu, evidenciju o imovini i svakoj transakciji bitkoina čuvaju računari svih korisnika mreže u zajedničkoj bazi podataka blokčejnu. Sve transakcije su mnogo brže od bankarskih, bez taksi, uz drastično lakše plaćanje preko državnih granica. Bitkoin svojim korisnicima pruža bezbednosti bez identifikacije, iako blokčejn beleži transakciju, ne beleži ko stoji iza nje. U radu su predstavljeni osnovni principi na kojima su zasnovani bitkoin i druge kriptovalute, pojašnjen odnos između blokčejna i bitkoina.

Keywords: *kriptovalute, digtalni novac, kriptografija, blokčejn, bitkoin.*

Abstract

Cryptocurrencies are digital (virtual) currencies, which, although they are a means of payment, are not yet strictly regulated by law in most states, and in some, they are even prohibited. Many people, including IT professionals and programmers, do not know much about this topic, and the general public equates the terms blockade and bitcoin. The crypto-market today amounts to nearly $ 770 billion. Since the emergence of the first digital currencies to date, over 1,300 active crypto sites have appeared, which differ in their properties and uses. Before the bitcoin, there were a lot of unsuccessful attempts to create digital currencies (DigiCash, Hashcash, Facebook credit, etc.). Utopian idea that mathematics and physics can solve social problems began its life through the appearance of bitcoin. The genial idea on which is a bitcoin functioned is based on blockchain technology, whose potential reaches far

Adresa autora:
Mario Lukinović
lukinovicmario@gmail.com

beyond the cryptocurrencies. Although there is still a controversy over the pseudonyms of Satoshi Nakamoto, his legacy has the potential to change the world. The success of bitcoin is in the advantages it has in relation to other similar currencies, but its importance goes beyond the benefits it has made. The banks do not need to store the data on money, property records and every bit of transaction stored by computers of all network users in a common database - blockchain. All transactions are much faster than banking, no tax, with drastically easier payment across state borders. Bitcoin provides to users security without identification, although blockchain registers a transaction, does not record who is behind it. The paper presents the basic principles on which bitcoin and other cryptocurrencies are based, the relationship between blockchain and bitcoin is explained.

Keywords: *cryptocurrencies, digital money cryptography, blockchain, bitcoin.*

1 UVOD

Ideal o novcu koji se ne oslanja na centralne institucije (koje mogu propasti, ali i koje vrše nadzor nad korisnicima), postojao je decenijama. U digitalnom svetu prvi ga je uobličio pisac naučne fantastike Nil Stivenson 1999. godine u svojoj noveli Kriptonomikon. On je opisao podzemni svet koji funkcioniše zahvaljujući digitalnom zlatu zasnovanom na kriptografiji, pri čijoj upotrebi korisnici ne moraju odavati ko su i šta su (Popper, 2016).

Kriptovalute (engl. *cryptocurrency*) su digitalne (virtualne) valute, koje iako su sredstvo razmene, još uvek nisu strogo regulisane zakonom u većini država, a u pojedinim su čak i zabranjene (Jovanović, 2014).

Da bi se razumeo nastanak i funkcionisanje kriptovaluta, neophodno je sagledati ih iz različitih uglova na kojima su one bazirane: matematici, sociologiji, ekonomiji, pravu i politici. To je verovatno i glavni razlog zbog koga veliki broj ljudi (uključujući i IT stručnjake i programere) ne znaju mnogo o ovoj temi. Takođe, šira javnost izjednačava pojmove blokčejna i bitkoina.

Sve kriptovalute su bazirane na jedinstvenom nizu brojeva za svaku jedinicu valute, koje korisnici mogu jedni drugima slati preko mreže. U prošlosti su se ti nizovi mogli lako kopirati i trošiti više puta, zbog čega nisu imali vrednost. Kriptograf Dejvid Čaum je taj problem rešio stvaranjem jedinstvene centralizovane knjige, u kojoj su se čuvale beleške o transakcijama svakog korisnika, čime ni jedna jedinica valute više nije mogla da se nalazi na dva mesta istovremeno (Bertlet, 2016).

Kriptovalute svoj nastanak duguju težnjama levo orijentisanih utopističkih posvećenika IT tehnologija koji su sanjali o univerzalnom novcu koji bi svako mogao da poseduje i troši, čija je vrednost onolika koliko su korisnici voljni da plate (na principu ponude i potražnje), ali pre svega na liniji fronta za onlajn anonimnost i slobodu, bez cenzure i nadzora. Pojavi bitkoina prethodio je Sajberpankerski manifest Done Haravej (Haraway, 1985) koji počinje rečima: „U elektronsko doba, privatnost je neophodan uslov za postojanje otvorenog društva“.

Kriptovalute su univerzalni novac koji se može koristiiti bilo gde u svetu, one su lako prenosive i teško se krivotvore.

Neki podaci pokazuju da tržište kriptovaluta danas iznosi gotovo 770 milijardi dolara. Od pojave prvih digitalnih valuta do danas, nastalo je preko 1.300 aktivnih kriptovaluta koje se razlikuju prema svojim svojstvima i upotrebi.

Prema odredbama Zakona o Narodnoj banci Srbije celokupni unutrašnji promet u Republici Srbiji izražava se u dinarima, osim ako nekim zakonom nije drukčije određeno. „Zakonom o platnom prometu propisano je da se poslovi platnog prometa obavljaju u dinarima, a Zakonom o deviznom poslovanju da se plaćanje, naplaćivanje i prenos između rezidenata i između rezidenata i nerezidenata u Republici Srbiji vrši u dinarima, a izuzetno se može vršiti i u devizama u slučajevima koji su propisani ovim zakonom“ (NBS, 2014).

Tržište kriptovaluta u Srbiji postoji, sve je veći broj rudara. Iako trgovanje kriptovalutama nije nelegalno, Narodna Banka Srbije - NBS je u više saopštenja navela da one ne predstavljaju zakonsko sredstvo plaćanja u Republici Srbiji. Takođe, zbog toga što ih ne izdaje centralna banka, NBS za korišćenje virtuelnih valuta, ulaganje u njih, kao ni za njihovu vrednost. Narodna banka Srbije je više puta upozoravala javnost da virtuelne valute ne predstavljaju

zakonsko sredstvo plaćanja u Republici Srbiji (NBS, Politika – u vezi s bitkoinom, 2017).

Ukoliko kriptovalute promatramo kao novac onda njihove tranksakcije mogu biti upitne shodno Zakonu o sprečavanju pranja novca i finansiranja terorizma, gde je propisana obaveza preduzimanja radnji i mera za sprečavanje pranja novca, kao što su identifikacija stranaka koje trguju preko tih platformi, uzimanjem kopije ličnog dokumenta. Kako poslovanje platformi na kojima se vrše transakcije kriptovalutama nije zakonom regulisano u Republici Srbiji, a uglavnom ni u uporednom pravu, a čl. 552. Zakona o obligacionim odnosima Republike Srbije ((„Sl. list SFRJ“, br. 29/78, 39/85, 45/89 - odluka USJ i 57/89, „Sl. list SRJ“, br. 31/93 i „Sl. list SCG“, br. 1/2003 - Ustavna povelja) predviđa razmenu robe kao jedan od načina trgovine, otvara se put ka legalnoj trgovini kriptovalutama (Bubanja, 2017).

Praksa je pokazala da su se korisnici kriptovaluta kada su imali problem sa njima, obraćali vlastima i njihovim regulatornim telima, zbog čijeg su zaobilaženja i smišljeni. Nažalost, korisnici ne uživaju pravnu zaštitu čak i kada je reč o trgovini putem registrovanih privrednih subjekta.

2 BITKOIN

Prva decentralizovana kriptovaluta koja se pojavila je bitkoin (eng. „Bitcoin“). Termin bitkoin označava istoimenu organizaciju, softver i protokol, kao i jedinicu mere ove kriptovalute (skraćeno BTC) (Bertlet, 2016). Koncept na kome se zasniva bitkoin prvi put je predstavljen 2008. godine u članku "Bitcoin: A Peerto-Peer Electronic Cash System", a u januaru 2009. godine bitkoin je pušten u promet. Njegov tvorac nije poznat do danas i krije se iza pseudonima Satoši Nakomato. Novu vrstu digitalne kriptovalute formirao je tako što je stvorio distribuirani sistem verifikacije. Bitkoin nastaje u procesu koji se naziva „rudarenje“ (engl. mining). Njegova jedinstvenost je u tome što je decentralizovana valuta, iza koje ne stoji nijedna država, niti banka. Bitkoin je digitalna valuta, koja nastaje i čuva se elektronski.

Kriptovalute u cilju maksimizacije bezbednosti, upotrebljavaju metod - dokaz o radu (engl. *proof-of-work*), metod baziran na informacijama koje je teško stvoriti, ali koje ostalim učesnicima u rudarenju obezbeđuju laku proveru i verifikaciju transakcija. Kriptovalute se čuvaju na bitkoin adresama za koje ključ predstavlja jedinstven niz slova i brojeva. Svaka transkacija bitkoinom se beleži u blokovima koji se zovu blokčejn. Transakcije se hronološkiređaju u blokove, u svakom se nalazi digitalni potpis prethodnog bloka, time se uređuje redosled i garantuje da novi blok može da se pridruži lancu samo ako počne na mestu na mestu završetka prethodnog. Jedan od osnovnih činilaca bezbednosti bitkoina je da se kopija svake izvedene transakcije beleži na svakom nalogu na kome je instaliran bitkoin softver. Blokčejnove neprekidno verifikuju računari svih korisnika softvera, tako sistem zna u bilo kom trenutku, koliko bitkoina svaki korisnik u svom novčaniku poseduje. Novčanik je program koji služi za slanje, primanje i skladištenje kriptovaluta. Digitalni novčanik sadrži prikaz količine kriptovalute koju korisnik poseduje, zapise o svim njegovim transakcijama, korisnički tajni ključ i njegove adrese (Bertlet, 2016). Novčanik je moguće instalirati na računar, mobilni telefon i tablet.

Falsifikovanje bitkoina nije moguće, jer iako vlasništvo može da se menja ono se ne može nikada duplirati (Bertlet, 2016). On je pseudo-anoniman, bitkoin mreža čuva sve podatke o svakoj transakciji koja se dogodila unutar mreže. Svako ko ima bitkoin softver i adresu na bitkoin mreži, može videti koliko novca ima na mreži, ali ne i kome oni pripadaju. Za razliku od otvaranja računa u bankama, otvaranje bitkoin računa (adrese) je brzo, bez troškova i „papirologije“. Jedna od glavnih prednosti bitkoin mreže je brzina transakcija.

Svako ko snagu svog računara posveti verifikaciji transakcija u blokčejnu može biti „rudar“. To je proces dodavanja transkacija u registar svih bitkoin transkacija. Rudarenje čini rešavanje matematičkog algoritma za čije se uspešno rešavanje dobija određena količina bitkoina.

Iako bitkoin ima reputaciju nestabilnosti, velikih fluktuacija i nezakonitog poslovanja, čemu mnogi pridodaju i urušavanje tradicionalnog koncepta nacionalnih država, ipak većina se slaže u tome da je njegova pojava najvažnija nova ideja od stvaranja Interneta (Vigna & Casey, 2016).

Razloga za uspeh bitkoina ima više. Finansijska kriza povoljno je uticala na njegov razvoj, poverenje u postojeći finansijski ali i politički

sistem je bilo poljuljano i brojni korisnici su u njemu prepoznali drugačije rešenje.

Anonimnost koju pruža prilikom transakcija jedan je od ključnih razloga njegovog uspeha. Prilikom digitalnog plaćanja bitkoinom u većini slučajeva nije potrebno davanje ličnih podataka. Ovakva vrsta anonimnosti, nažalost pogodovala je i usponu tamne strane upotrebe i popularnosti bitkoina u kriminalnim krugovima.

Računi u bitkoinu nisu opterećeni visokim bankarskim dažbinama.

Takođe, nije beznačajan ni potencijal plaćanja izdataka koji su manji od trenutnih ograničenja u konvencijalnim transakcijama na internetu (npr. naplata čitanja jednog novinskog članka ili preskoči reklamu, koji koštaju manje od 20 ili 30 centi kolika je najmanja transakcija) (Popper, 2016).

Kao što su svi učesnici na internetu povezani protokolima (TCP/IP, FTP, SMTP, HTTP i dr.**)** zahvaljujući kojima mogu međusobno da komuniciraju, bitkoin je stvorio svoje softverske protokole koji uređuju funkcionalna pravila upravljanja sistemom.

Bitkoin je omogućio novi način stvaranja, čuvanja i transfera novca.

Od svog nastanka bitkoin se unapređivao, podržan od internet zajednice, posebno od posvećenika slobodi interneta i anonimosti, mnogi od problema koji su uočeni su rešavani zajedničkim naporom internet zajednice.

3 BLOKČEJN

Blokčejn (engl. blockchain) nije samo bitkoin, on je tehnologija za koju mnogi predviđaju da će promeni svet (OECD, 2018).

Ukoliko bismo pojednostavljeno opisivali blokčejn mogli bismo da kažemo da je to nova vrsta baze podataka, iako bi to bilo pojednostavljeno objašnjenje slično kao kada bi smo imejl (email) opisali kao novi način za slanje pisama.

Iako blokčejn jeste nova vrsta baze podatka, to ne objašnjava u dovoljnoj meri genijalnost načina na koji funkcioniše.

Kada bilo gde i bilo kada položimo novac, oslanjamo se na zapis u bazi podataka treće strane, banke, firme i sl. Poverenje u banke zasnovano je na zakonu koji reguliše rad banke, poverenju u državu da će u slučaju propasti banke država nadoknaditi klijentima njihov ulog.

Kada plaćamo on line usluge ili vršimo neku drugu transakciju kreditnim karticama, poklanjamo poverenje kompanijama koje posreduju u našem plaćanju (Mastercard, VISA i dr.) koje za to uzimaju određenu materijalnu nadoknadu. Čak i prilikom tradicionalnih oblika plaćanja gotovinom u papirnom novcu, mi dajemo papir na kome je ispisana vrednost za koju prodavac veruje da će mu biti isplaćena (ili garantovana) od strane vlade koja ju je štampala. Digitalno plaćanje zbog prisustva trećih strana (banke, kreditne kompanije i dr.) uvek je bilo moguće pratiti. I kod plaćanja gotovinom klijenti veruju bankama i kreditnim kompanijama koje rukovode platnim karticama, da imaju pouzdane baze podataka. I vlade država veruju da banke i kreditne kompanije vode baze podataka koje su tačne i pouzdane.

Baze podataka sadrže mnoštvo ličnih podataka, od npr. medicinske dokumentacije u domu zdravlja koja sadrži važne informacije o nama i našem zdravstvenom stanju, kada smo i od koje bolesti bolovali, koje lekove smo koristili i sl. I druge baze podataka sadrže mnoštvo naših ličnih podataka koje su važne ne samo za nas, već i za državu, grad, privredu, druge građane itd.

Osim što omogućava anonimne i sigurne transakcije, blokčejn ima i potencijal da sačuva sve vredne informacije, od podataka o rođenim i umrlim, preko osiguranja, do katastara nepokretnosti, pa čak i glasova (Tapscott, 2018).

Sagledavši mogućnosti koji blokčejn nudi u transformaciji industrija i tržišta, povećanju transparentnosti i poverenja između građana, kao i olakšanom pristupu tržištu (uz bolju efikasnost transakcija), ali i rizicima koje sa sobom nosi, Organizacija za ekonomsku saradnju i razvoj - OECD organizovala je od 4. do 5. septembra 2018. godine Forum politike OECD-a za blokčejn. To je bila ujedno i prva glavna međunarodna konferencija na kojoj se razmatrao uticaj blokčejna na aktivnosti vlada i javnih prioriteta. Forum se bavio prednostima i rizicima blokčejna za ekonomiju i društvo, pokušajem određivanja adekvatnog regulatornog pristupa, kao i javnih politika prema blokčejnu.

Učesnici Foruma su diskutovali o mogućnostima globalnog ekonomskog uticaja blokčejna,

njegovim implikacijama na privatnost i sajber bezbednost, upotrebi blokčejn tehnologija za povećanje inkluzivnosti, njegovoj upotrebi u promovisanju zelenog rasta i održivosti, kao i jačanju kapaciteta javne uprava i primene u praksi (OECD, 2018).

4 ZAKLJUČAK

Pre bitkoina bilo je mnoštvo neuspelih pokušaja stvaranja digitalnih valuta (digikeš, heškeš, Fejsbuk kredit i dr.). Uspeh bitkoina leži u prednostima koje ima u odnosu na druge slične valute, ali njegov značaj prevazilazi i pogodnosti koje je doneo.

Svaki korisnik bitkoina ima potpunu kontrolu nad novcem na svom računu (adresi), jedino osoba sa privatnim ključem može pristupiti bitkoinima na toj adresi. Banke nisu potrebne za čuvanje podataka o novcu, evidenciju o imovini i svakoj transakciji bitkoina čuvaju računari svih korisnika mreže u zajedničkoj bazi podataka blokčejnu. Sve transakcije su mnogo brže od bankarskih, bez taksi, uz drastično lakše plaćanje preko državnih granica.

Bitkoin svojim korisnicima pruža bezbednosti bez identifikacije, iako blokčejn beleži transakciju, ne beleži ko stoji iza nje. Zahvaljujući peer-to-peer komunikaciji i kriptografiji, povezivanje bitkoin transakcija sa osobom u stvarnom životu je veoma teško. To je u ujedno možda i njegova najveća mana, jer su oporezivanje i nadzor nad korisnicima krajnje teški.

Garancija vrednosti bitkoina osmišljena je po uzoru na plamenite metale kojih ima ograničeno u prirodi. Zbog toga je Satoši u kodu bitkoina odredio da ih ima maksimalno 21 milion, te da ukoliko bitkoin protokol ostane isti, poslednji bitkoin će biti izrudaren 2140. godine. Do sada je izrudareno oko 17 miliona bitkoina, što znači da je ostalo 4 miliona, ili oko 19%.

Do sada je bitkoin uspeo da prevlada sve krize koje su ga zahvatile (u više slučajeva nestajali su iznosi koji su dostizali i 400 miliona dolara). Kakva god sudbina bitkoina bila u budućnosti, njegova uloga se neće moći zanemariti, prvenstveno zbog toga što je zahvaljujući njemu iznedren blokčejn. Bez obzira na skepticima u vezi sa kriptovalutama, teško se mogu osporiti mogućnosti koje blokčejn pruža, pre svega u zaštiti baza podatka.

CITIRANA DELA

Bertlet, D. (2016). *Darknet: u digitalnom podzemlju.* Beograd: Laguna.

Bubanja, B. (2017). *Sve što bi trebalo da znate o trgovini kriptovalutama.* PC Press.

Haraway, D. J. (1985). *A Cyborg Manifesto.* Manifestly Haraway, University of Minnesota Press. Preuzeto sa users.uoa.gr/~cdokou/HarawayCyborgManifesto.pdf

Jovanović, U. (2014). *Kriptovalute.* Beograd: Matematički fakultet. Preuzeto sa http://poincare.matf.bg.ac.rs/~vladaf/Courses/Matf%20MNSR/Prezentacije%20Individualne/

NBS. (2014, 10 2). *Narodna banka Srbije upozorava da bitkoin ne predstavlja zakonsko sredstvo plaćanja u Srbiji.* Preuzeto sa Narodna banka Srbije, Kabinet guvernera: http://www.nbs.rs/internet/latinica/scripts/showContent.html?id=7605

NBS. (2017, 11 3). *Politika – u vezi s bitkoinom.* Preuzeto sa Narodna banka Srbije, Kabinet guvernera: https://www.nbs.rs/internet/latinica/scripts/showContent.html?id=12079&konverzija=yes

OECD. (2018). Distributed Ledgers: Opportunities and Challenges. *OECD Blockchain Policy Forum.* OECD Conference Centre, Paris: OECD.

Popper, N. (2016). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money.* Harper Paperbacks.

Tapscott, D. (2018). *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World.* Portfolio.

Vigna, P., & Casey, M. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order.* Picador.