Ivan Ivljanin[1]

STRUČNI RAD
UDK: 336.7:004]:339.5
DOI: 10.56362/Rev2299089I

DIGITALNI NOVAC U MEĐUNARODNOJ TRGOVINI

UVOD

Svet se užurbano udaljava od fizičkog novca, potpomognut trendom opšte digitalizacije. Protekla decenija neosporno je obeležena ekspanzijom digitalnih valuta, a veruje se da njihovo vreme tek dolazi. Decentralizacija, anonimnost i vrtoglav skok vrednosti učinile su da termini poput blokčejn lanaca, kriptovalute i tokena izađu iz kriptografske i programerske niše i postanu deo svakodnevice mnogo šireg auditorijuma. Šta je zapravo digitalni novac? Ovaj rad teži da približi terminologiju i objasni neke od složenih koncepata u vezi sa razvojem i afirmacijom digitalnog i kriptovanog novca kakvog ga danas poznajemo.

Kriptovaluta je vrsta digitalnog medija za razmenu. Kako bi se kreiranje novih jedinica držalo pod kontrolom, i verifikovale i obezbedile finansijske transakcije, kriptovalute se oslanjaju na kriptografiju. U poređenju sa centralizovanim bankarskim sistemom koji je pod kontrolom država i vlada, kriptovalute su potpuno decentralizovane. Drugim rečima, kriptovalute nisu povezane ni sa jednim monetarnim sistemom, nemaju realno pokriće u zlatu ili drugom reprezentu vrednosti i jedini mehanizam koji je relevantan za određivanje njihove vrednosti jeste tržišna ponuda i potražnja (11) i (9).

Postoje brojni razlozi za stvaranje alternativnih valuta. Većinski konsenzus (8) postignut je oko podele na dve glavne kategorije: materijalne i digitalne valute. One se dele na:

- Valute sa suštinskom upotrebnom vrednošću: njihova vrednost nije apstraktna i takođe ne zavise od bilo kakvog vladinog ili monetarnog instrumenta. Primer toga je situacija kada su vojnici koristili metale ili cigarete za trgovinu u Berlinu posle Drugog svetskog rata.

REZIME

Šta je dovelo do meteorskog rasta i popularnosti kriptovaluta, pre svega bitkoina? Koji su koncepti prethodili razvoju modernih kriptovaluta? Šta je blokčejn i kakva je arhitektura različitih distributivnih javnih knjiga? Koja je upotrebna vrednost digitalnog novca u svakodnevnim transakcijama, a koja u međunarodnoj trgovinskoj razmeni? Ovaj rad pokušava da odgovori na navedena pitanja i da dešifruje visokosložen tehnički žargon koji po pravilu prati temu digitalnog novca.

Ključne reči: kriptovaluta; blokčejn; dupla potrošnja; anonimnost; distributivna javna knjiga.

[1] Stručni konsultant rane biznis faze (startap faze) u IT industriji, e-mail: ivljanin@gmail.com

- Token: ovaj medijum razmene obično je vođen nekim društvenim sporazumima ili geografskom lokacijom. Neki od primera mogu biti lokalne valute poput Brikstonske funte u Ujedinjenom Kraljevstvu. Dizajniran je da podstakne lokalnu proizvodnju i trgovinu.
- Centralizovana digitalna valuta: dobri primeri su bodovi lojalnosti raznih kompanija, vazdušne milje ili valute koje se koriste u zatvorenim sistemima poput video-igara.
- Distribuirana i/ili decentralizovana digitalna valuta: sve kriptovalute spadaju u ovu kategoriju. Sve transakcije mogu se obaviti bez treće strane zahvaljujući blokčejn tehnologiji. Neki od primera kriptovaluta su Bitkoin (Bitcoin), Lajtkoin (Litecoin), Ripl (Ripple), Eter (Ether).

KRIPTOVALUTE

Početak razvoja kriptovaluta seže još u 1983. godinu, kada je Dejvid Čaum (David Chaum) predstavio anonimni kriptografski elektronski novac – *eCash* (5). Ideja iza toga bila je da postoji softver koji će lokalno skladištiti novac u digitalnom formatu, ali je zahtevao posedovanje kriptografskog potpisa banke. Kriptografski protokoli su korišćeni da bi se sprečila dupla potrošnja i da bi korisnici ostali anonimni. To je značilo da osoba koja koristi *eCash* može da troši svoj digitalni novac kod trgovaca koji prihvataju tu alternativnu valutu, ili na internetu. Čaumova kompanija se zvala „Digicash", i pošto je samo ova kompanija upravljala kriptografskom infrastrukturom, smatrala se centralizovanim sistemom. Tokom 90-ih, banke u Sjedinjenim Državama i Evropi (Austriji, Nemačkoj, Švajcarskoj) koristile su ovaj sistem za elektronska plaćanja. Međutim, zbog rastuće popularnosti kreditnih kartica, „Digicash" je prestao da se koristi 1998. godine (10). Tokom godina koje su usledile, kriptovalute su se polako razvijale u formu koja nam je poznata danas. Neke od njih su:

- *E-Gold*: Prva digitalna zlatna valuta. Korisnici su mogli da se registruju na svojoj veb-stranici na kojoj je njihov novac određen u gramima zlata. Mogli su da izvrše trenutne transfere drugim korisnicima platforme. Ustanovljen je 1996. godine i bio je u opticaju do 2009. godine, kada je ugašen zbog pravnih problema. Tokom svog postojanja imao je dve milijarde američkih dolara prometa godišnje (10).

- *Hashcash*: Prvo je korišćen za kontrolu neželjene e-pošte i odbranu od „Denial of Service" napada (DoS attack). Uveo ga je 1997. godine Adam Bek (Adam Back). Koristio je algoritam za proveru rada koji zahteva rešavanje određenih matematičkih problema visoke kompleksnosti, čiji se rezultati naknadno lako mogu proveriti. Algoritam je zasnovan na hešu i kriptografski je. Danas se koristi kao dokaz o radu za rudarenje bitkoina (10) i (1).
- B-novac je prethodnik bitkoina. Uveo ga je Vej Daji (Wei Dai) 1998. godine. On je predložio dva protokola za „anonimni, distribuirani elektronski sistem gotovine". Čak je i Satoši Nakamoto (Satoshi Nakamoto) pomenuo Dajijev rad kada je kreirao Bitkoin. Daji je želeo da predstavi sistem plaćanja koji će se koristiti samo između dve zainteresovane strane, bez posrednika, ali njegov koncept zapravo nikada nije realizovan i ostao je samo na predlogu (4).

Kako je nastupila finansijska kriza 2008. godine, interesovanje za kriptovalute je ponovo počelo da raste. U tom trenutku se činilo da kriptovalute mogu da ponude rešenja za probleme koji su nastali sa sistemom fiat valute. Verovalo se da kriptografski digitalni sistem plaćanja može eliminisati treću stranu od poverenja iz onlajn plaćanja. Centralnim bankama je bilo dozvoljeno da štampaju novac bez pokrića tokom krize, što je izazvalo inflaciju. Sa druge strane, kriptovalute nude ograničenu ponudu i novi novčići se kreiraju samo po unapred određenim pravilima. Dakle, niko nije mogao da proizvede više nego što je planirano na početku. Ogromni državni dugovi, ljudi koji nisu mogli da otplate svoje hipoteke i pad na berzi još više su skrenuli pažnju na kriptovalute. Poverenje u banke i vlade je bilo poljuljano. Stoga su ljudi želeli da razmotre alternativne načine da uštede i ulože svoju imovinu (4).

BLOKČEJN

Kriptovalute pružaju način za verifikaciju svih transakcija. Ovo se postiže korišćenjem distribuirane knjige transakcija. Distribuirana knjiga može se predstaviti kao mreža baze podataka koja može da se deli na više sajtova, institucija ili zemalja. Nema centralizovanog skladište podataka, niti postoji centralni administrator baze podataka. Pošto svi učesnici u mreži imaju sopstvenu identičnu kopiju knjige, svaka promena u bazi podataka će biti prikazana gotovo odmah u

svim primercima glavne knjige. Sigurnost sačuvanih podataka u zajedničkoj knjizi se održava kriptografijom. Ključevi i potpisi se koriste za kontrolu radnji u knjigama. U zavisnosti od pravila mreže, neki ili svi učesnici mogu napraviti promene u zapisu u knjigama.

Jedan od najčešće korišćenih tipova distribuiranih knjiga je blokčejn, ali pominjanje kriptografski obezbeđenog lanca blokova sežu do 1991. godine, kada su Stjuart Haber (Stuart Haber) i V. Skot Storneta (W. Scott Stornetta) osmislili sistem sa mogućnostima kreiranja sigurne i pouzdane vremenske oznake koja se ne može promeniti (7). Nakon nekoliko pokušaja da se modifikuje i učini efikasnijim, prvi blokčejn je 2008. godine kreirao Satoši Nakamoto (12). Dizajn je poboljšan dodavanjem *Hahcash* metode za dodavanje blokova u lanac i sa ovim više nije bilo potrebe da strana od poverenja potpisuje svaki blok koji je dodat u lanac. Nije bio potreban ni pouzdani autoritet niti centralni server. Glavna svrha stvaranja blokčejna bila je da služi kao javna knjiga transakcija bitkoina. Ovo je bio prvi put da je problem dvostruke potrošnje rešen samo korišćenjem kriptografije (13).

Blokčejn je dizajniran na način da se odupre bilo kakvim modifikacijama podataka.

Blokčejn se sastoji od povezanih zapisa koji se mogu dodati jedan za drugim. Zapisi se nazivaju blokovi i povezuju se pomoću kriptografske funkcije. Blokčejn je dizajniran na način da se odupre bilo kakvim modifikacijama podataka. Svaki od blokova u blokčejnu sadrži podatke o transakciji praćene vremenskom oznakom i kriptografskim hešom prethodnog bloka. Jednom kada je blok ubačen u lanac, podaci se ne mogu menjati bez promene svih prethodnih blokova. Ovo se ne može uraditi bez konsenzusa većine mreže, jer blok lanac koristi *peer-to-peer* mrežu za varijaciju novih blokova i komunikaciju između čvorova. Zbog toga se blokčejn smatra decentralizovanim (13). To je u osnovi zajednička baza podataka u kojoj se sve transakcije koje su izvršene distribuiraju među svim učesnicima. Konsenzus većine učesnika u mreži je provera svake izvršene transakcije. Kada ga mreža prihvati, bilo koji zapis koji je deo lanca ne može se menjati ili brisati. To znači da su svi zapisi o transakcijama bezbedno uskladišteni u blok lancu. Ove karakteristike čine bitkoin i druge kriptovalute sigurnijim za svoje korisnike.

Digitalna plaćanja su često povezana sa trećim licima od poverenja. Pošto postoji velika verovatnoća prevara, naknade za platne transakcije su visoke. Sa druge strane, kriptovalute koriste kriptografiju umesto trećih strana od poverenja. To znači da će naknade za takve transakcije biti mnogo manje u poređenju sa tradicionalnim, u koje su uključene treće strane. Svaka transakcija koja se obavi preko blokčejna – sadržaće digitalni potpis (3).

Digitalni potpis se sastoji od javnog ključa i privatnog ključa. Svaka transakcija mora biti poslata primaocu pomoću javnog ključa. Svaka transakcija je prethodno digitalno potpisana privatnim ključem pošiljaoca. Da bi pošiljalac potrošio novac, on ili ona treba da dokaže da su vlasnici privatnog ključa. Primalac proverava da li javni ključ na transakciji odgovara privatnom ključu pošiljaoca. Sve transakcije se emituju svakom čvoru u mreži. Nakon što je transakcija verifikovana, biće evidentirana u javnoj knjizi. Međutim, pre nego što se nepromenljivi podaci o transakciji zadrže, potrebno ih je verifikovati. Čvorovi koji verifikuju transakcije moraju da se uvere da potrošač zaista poseduje tu kriptovalutu i da ima dovoljno kriptovalute na svom nalogu za tu određenu transakciju (3).

Digitalni potpis se sastoji od javnog ključa i privatnog ključa.

I dalje postoji problem oko toga kako mreža odlučuje koji će blok biti sledeći u lancu, jer bilo koji od čvorova može da kreira blok od još uvek nepotvrđenih transakcija. Redosled čvorova u ovom slučaju nije pouzdan jer različiti blokovi mogu doći iz različitih čvorova u isto vreme. Ovaj problem se rešava u blokčejn tehnologiji korišćenjem matematičke slagalice. Svaki od blokova će biti dodat u blokčejn tek nakon rešavanja određenog matematičkog problema – dokaz rada. Čvor u mreži koji je kreirao blok treba da dokaže da je uložio dovoljno računarskih resursa da reši matematički problem. Obično bi bilo potrebno oko 10 minuta da čvor reši zagonetku. Prvi od čvorova koji reše matematički problem deliće blok sa ostatkom mreže. Međutim, moguće je da se istovremeno emituje više blokova. U tom slučaju će oba bloka biti prihvaćena i formiraće se više ogranaka. Pošto su matematički problemi prilično komplikovani, malo je verovatno da će obe grane nastaviti da napreduju istim tempom, a da će jedna od njih na kraju postati duža. Kada se to desi, samo najduži lanac je validan i prihvaćen od strane mreže. Zbog toga je nemoguće da napadač stvori prevaru. Napadač bi morao da generiše lažni blok rešavanjem matematičkog problema i da generiše sledeće blokove brže od dobrih čvorova, kako bi grana koja sadrži loš blok bila najduža. Ovo postaje još teže jer su svi blokovi kriptografski povezani.

DVOSTRUKA POTROŠNJA

Problem dvostruke potrošnje je dobro poznat problem u sistemima digitalnog plaćanja. Odnosi se na problem gde se isti novac može potrošiti više puta. Na primer, korisnik A želi da pošalje 100 evra korisniku B. A može da izvrši transakciju, a B će dobiti 100 evra. Transakciju izvršava A tako

što kreira kopiju od 100 evra i tu kopiju šalje korisniku B. Međutim, nema garancije da je A smanjio iznos novca na svom računu za iznos transakcije. Dakle, korisnik A može ponovo da ih potroši. Sa druge strane, B je već primio transakciju. Na kraju ovakve transakcije ceo sistem će imati 100 evra više nego na početku, a ova razlika nema nikakvo validno pokriće iza sebe. Ovaj problem rešava treća strana od poverenja koja će pravilno upravljati transakcijom, npr. banka. Pružajući ovu uslugu, treća strana će uzeti procenat transakcije da pokrije svoje troškove. I na taj način ovakva transakcija izvršena uz pomoć treće strane povećava transakcione troškove.

Blokčejn tehnologija i verifikacije na nivou celokupne mreže učinili su digitalne transakcije kriptovaluta sigurnim i jeftinijim. Ušteda je pre svega nastala zbog izbegavanja potrebe za trećom stranom od poverenja koja kontroliše transakcije. Dakle, nakon svake uspešne verifikacije transakcije, samo jedan zapis će biti dodat u blokčejn i taj zapis se ne može promeniti ili ukloniti. Sve nove transakcije će se naknadno proveravati u odnosu na već postojeće zapise u blokčejnu i stoga nije moguće potrošiti isti novac dvaput (10).

Da bi se napravio novi blok, rudari moraju da reše matematički zadatak koji predstavlja dokaz rada. Učesnici se utrkuju jedni protiv drugih u rešavanju zagonetke. Prvi učesnik koji ju uspešno dekodira, dobija nagradu u obliku bitkoina. Tim dokazom o radu kreira se evidencija transakcija. Ovaj zapis se ne može promeniti bez ponovnog izvršenja dokaza o radu (10).

Prema Krosbiju (Michael *Crosby)* i saradnicima, digitalna ekonomija će primorati sve industrije da prigrle blokčejn tehnologiju (3). U svetu gde već koristimo Big Data za predviđanje ponašanja i poboljšanje e-trgovine, blokčejn može postati novi „motor rasta" digitalne ekonomije i same industrije. Iako postoji mnogo kontroverzi oko bitkoina, blokčejn tehnologija koja stoji iza bitkoin kriptovalute je sve vreme funkcionisala bez ikakvih problema. Zbog toga je pronašla širok spektar upotrebe kako u finansijskom tako i u nefinansijskom sektoru. Finansijski sektori su nekada videli kriptovalute i blokčejn kao konkurenciju i pretnju tradicionalnim poslovnim modelima. Danas finansijske institucije počinju da uviđaju prednosti blokčejn tehnologije i vide njenu potencijalnu upotrebu u svom poslovanju. Najveće svetske banke postaju otvorene za mogućnosti koje bi blokčejn mogao da donese (3). Upotrebni modeli mogu značajno da se razlikuju. Na primer, blokčejn se može koristiti za bezbedno skladištenje akcija, stanja na bankovnim računima, obveznica i hipoteka. Osim

Blokčejn tehnologija i verifikacije na nivou celokupne mreže učinili su digitalne transakcije kriptovaluta sigur nim i jeftinijim.

toga, i fizička i digitalna sredstva mogu biti uskladištena u blokčejnu. Na primer, kuće, automobili, laptopovi i druge vredne stvari koje se ne mogu lako uništiti ili replicirati. Na ovaj način se lako može dokazati vlasništvo, a istorija transakcija se takođe brzo može proveriti.

TIPOVI BLOKČEJNA

Trenutno postoje tri tipa blokčejna: privatni, javni i partnerski blokčejn. U privatnim blokčejn sistemima samo čvorovi koji dolaze iz jedne određene organizacije mogu da učestvuju u procesu konsenzusa. Pošto svi čvorovi dolaze iz iste organizacije, ovo se smatra centralizovanom mrežom. Za razliku od privatnog blokčejna, u javnom blokčejnu svi javni čvorovi mogu da učestvuju u procesu konsenzusa. Zbog toga se ovo definiše kao decentralizovana mreža. Između ta dva tipa se nalazi partnerski blokčejn, koji podrazumeva samo unapred odabrane čvorove za učešće u procesu konsenzusa. Čvorovi iz više unapred definisanih organizacija mogu učestvovati u mreži i zato se takva postavka blokčejna navodi kao delimično decentralizovana.

Za razliku od privatnog blokčejna, u javnom blokčej nu svi javni čvorovi mogu da učestvuju u procesu konsenzusa.

BITKOIN

Bitkoin je prvi put predstavljen 2008. godine u radu „Bitkoin: Peer-to-peer elektronski gotovinski sistem“ autora Satošija Nakamotoa (12). Identitet Satošija Nakamotoa nije otkriven do danas. Takođe nije poznato da li iza pseudonima stoji samo jedna osoba ili grupa ljudi. Postoje insinuacije da bi ime moglo biti sastavljeno od imena četiri velike tehnološke kompanije: SAmsung, TOSHIba, NAKAmichi i MOTOrola. Međutim, ovo nikada nije dokazano (15). Bitkoin predstavlja jedan od najpopularnijih primera kriptovaluta danas.

Sistem na kome radi ova kriptovaluta je decentralizovana *peer-to-peer* mreža otvorenog koda. Svi čvorovi u mreži su međusobno povezani, što znači da je mreža potpuno razgranatog tipa. Uprkos ovoj transparentnosti, još uvek postoji veliko nepoverenje u bitkoin i druge sisteme kriptovaluta. To se dešava zato što obično nisu povezani ni sa jednim pravnim licem, niti je još uvek jasno ko stoji iza njih, a često nije očigledno ni kako posluju bez treće strane od poverenja (11).

Bitkoin koristi decentralizovani i *peer-to-peer* mrežni model za verifikaciju i obradu svih transakcija. Bitkoin tehnologija se oslanja na kriptografiju za obradu transakcija,

a implementirana je kao sistem otvorenog koda, kako je stajalo u Nakamotovoj publikaciji iz 2008. godine (8). Prvi put u istoriji onlajn plaćanja moguće je izvršiti transakciju bez uključenja treće strane od poverenja i bez plaćanja naknada centralizovanom organu. Sve transakcije se čuvaju u blokčejnu. Takođe, svi čvorovi u mreži su zaduženi za verifikaciju transakcija pomoću kriptografije. Rudari su nagrađeni bitkoinima za dokaz rada, koji predstavlja pronalaženje rešenja zadatog matematičkog problema. Bitkoin se može koristiti za kupovinu proizvoda i usluga. Takođe se može zameniti za druge kriptovalute ili dekretne (fiat) valute (11).

Novac se između ostalog definiše i kao sredstvo razmene, obračunska jedinica i skladište vrednosti. Pošto bitkoin zadovoljava definiciju novca i u digitalnom je obliku, može se definisati kao digitalna valuta. Naziv bitkoin valute koji je u široj upotrebi je BTC, međutim, postoje neke berze koje koriste KSBT umeto BTC (10). Bitkoin izostavlja poverljive treće strane u onlajn transakcijama i rešava problem dvostruke potrošnje korišćenjem *peer-to-peer* mreže. Da bi to obezbedila, mreža hešuje sve transakcije i stavlja ih u lanac. Bitkoin sistem je izgrađen kao softver otvorenog koda, što znači da svako na internetu može da mu pristupi i može da ga pregleda, modifikuje i poboljša.

Očečkuje se da će poslednji bitkoin biti iskopan oko 2040. godi ne.

Satoši Nakamoto je napustio Bitkoin projekat 2010. godine i ostavio ga u rukama zajednice, na taj način otklonivši svaku sumnju da postoji neko ko kontroliše projekat iz pozadine. Osim toga, čak i ako bi neki od programera softvera poželeli da promene izvorni kod, ova promena ne bi bila prihvaćena ukoliko ne postoji potpuni konsenzus svih čvorova koji su trenutno u mreži. Ako dođe do neke promene u sistemu, svi korisnici, uključujući programere, morali bi da se slože oko izmena (10).

Bitkoin kao digitalna valuta dizajniran je sa ograničenom količinom novčića. Taj limit je 21 milion bitkoina. Očekuje se da će poslednji bitkoin biti iskopan oko 2040. godine. Da bi generisali nove novčiće, rudari prikupljaju neobrađene transakcije u bloku i pokušavaju da reše dokaz o radu kako bi njihov blok bio prihvaćen u blok lancu. Ovaj proces se zove *rudarenje*. Kao nagradu ako njihov blok prođe verifikaciju mreže, dobijaju bitkoine. Veličina svakog bloka bitkoina je 1 MB i može sadržati transakcije do svoje maksimalne veličine. Kroz ovaj proces ne samo da će se generisati i izdavati novi bitkoini, već će se obraditi i dodati u blok-lanac nove transakcije. Tako rudari svojom računarskom snagom doprinose održavanju cele mreže i zbog toga dobijaju nagradu.

U proseku, novi blok može se kreirati svakih 10 minuta, a teškoća problema koju rudari treba da reše da bi blok mogao da se kreira je obično prilagođena tom periodu. Ako se novi blokovi generišu prebrzo, teškoća će se povećati, a ako se blokovi generišu presporo, teškoća će se smanjiti. Rudari prikupljaju nove i neproverene transakcije, i pomoću kompjuterskog programa pokušavaju da pogode *Nonce broj* (number used once) koji će omogućiti da njihov blok sa transakcijama bude prihvaćen u lancu. Heš funkcija koja se koristi u bitkoin sistemu je SHA-256. Koristi se za digitalne potpise u transakcijama, bitkoin adrese i verifikaciju plaćanja. Štaviše, ova heš funkcija predstavlja osnovu za matematički problem dokaza rada koji treba rešiti. SHA-256 je naslednik SHA-1 heš funkcije koju je prvi put predstavila NSA u Sjedinjenim Državama i koja je korišćena u *Hashcash*-u (10). Dalje, kriptografija sa javnim ključem se koristi u bitkoin sistemu. Uz pomoć javnih i privatnih ključeva, autentičnost transakcija se može lako odrediti. U ovoj vrsti kriptografije, javni ključ se kreira iz privatnog ključa, ali je nemoguće ponovo kreirati privatni ključ od javnog ključa. Drugim rečima, javnom ključu se može pristupiti i javno ga deliti, dok, sa druge strane, privatni ključ mora biti obezbeđen. Privatni ključ se stoga koristi za kreiranje digitalnih potpisa, dok se javni ključ koristi samo za njihovu validaciju. Kao nova tehnologija, bitkoin donosi mnogo svežih ideja u već afirmisan monetarni sistem. Međutim, zbog nedostatka vladinih regulativa, postoje izvesni rizici u njenoj primeni.

TRŽIŠTA KRIPTOVALUTA

Korišćenje digitalnih valuta nosi ogroman potencijal za poboljšanje efikasnosti sistema plaćanja, koje će dovesti do smanjenjem naknada i troškova transakcije. Mnoge kompanije svoje poslovanje prilagođavaju kriptovalutama, što iz korena menja platne sisteme kakve poznajemo. Kompanije koje su najviše pogođene takvim promenama su kompanije za transfer novca i kreditne kartice, berze hartija od vrednosti, kao i kompanije koje proizvode opremu za realizaciju plaćanja. Međutim, bitkoin i dalje u velikoj meri zavisi od fiat valute kada je u pitanju kupovina i trgovanje. Pošto rudarenje zahteva mnogo opreme, znanja i truda, mnogi bi se radije odlučili da ga kupe na berzi kriptovaluta nego da ga kopaju. Berze kriptovaluta služe kao posrednik između bitkoina i drugih kriptovaluta sa jedne strane i fiat valuta sa druge. Sa popularnošću bitkoina i kriptovaluta uopšte, raste interesovanje za berze koje ih nude (10). Trenutno su najveće berze

kriptovaluta, ako pogledamo procenu zarade i obim trgovanja, Binance (Malta), Kraken (SAD), FTX (Bahami), KuCoin (Sejšeli), CoinBase (SAD), Bitstamp (Velika Britanija).

Ljudi mogu kupiti bitkoin na berzama kriptovaluta za fiat valutu, ili mogu da prodaju bitkoin i zarađuju novac. Ovo važi i za druge kriptovalute. Berze služe kao primarni izvor pristupa mreži kriptovaluta. Cene kriptovaluta određuju samo potražnja i ponuda, pa te razmene imaju veliki uticaj na njihovu vrednost. Na berzama učesnici mogu ne samo da kupuju ili prodaju bitkoine ili druge kriptovalute, već mogu i da menjaju jedne za druge. Primenjuju se kursevi za tu konkretnu valutu. Ove stope mogu da variraju na različitim berzama kriptovaluta. Učesnici na berzi takođe mogu tamo i da čuvaju svoje bitkoine. Svojim računima pristupaju putem bezbedne SSL veze na svojoj veb-stranici. Razmene kriptovaluta su dostupne samo na mreži.

S obzirom na to da postoji mnogo problema povezanih sa kriptovalutama, kao što su pranje novca i trgovanje na crnom tržištu, berze zahtevaju identifikaciju učesnika pre nego što mogu da trguju na njoj. Ona ima identitet učesnika, kao i podatke o njegovom ili njenom računu. Svaki učesnik na berzi ima svoj digitalni novčanik. Berza sa druge strane ima sve privatne ključeve za sve novčanike svojih klijenata. Ako učesnik želi da proda bitkoin, on prenosi željeni iznos iz sopstvenog novčanika u novčanik berze. Transakcije poput uplata i isplata bitkoina se dokumentuju na blokčejnu. Međutim, podaci o trgovi bitkoinima su samo zabeleženi u istoriji transakcija same berze. Identitet klijenta nije prikazan na blokčejnu, umesto toga transakcije se vode kao trgovine same berze. Detalji o klijentu koji je izvršio transakciju čuvaju se samo u internoj bazi podataka berze na kojoj klijent trguje (2).

Ako učesnik želi da proda bitkoin, on prenosi željeni iznos iz sopstvenog novčanika u novčanik berze.

Da bi berza ostala konkurentna na tržištu, potrebno je da zadrži obim trgovine iznad određenog nivoa. Kada se dostigne taj nivo, tada postaje interesantna meta za hakere. Zbog toga su berze kriptovaluta veoma izložene sajber napadima i bezbednosnim pretnjama. Jedan od najvećih napada na berzu kriptovaluta desio se 2011. godine kada je napadnuta Mt. Gox. U 2013. i 2014. godini, pre nego što je proglasio bankrot, Mt. Gox je upravljao sa preko 70% svih bitkoin transakcija širom sveta. Bila je to najveća berza bitkoina u to vreme. U 2011. godini haker je prebacio veliku količinu bitkoina na svoj račun, nezakonito koristeći akreditive jednog od revizora berze. On je manipulisao softverom i stvorio masivnu narudžbu za bitkoine po svakoj ceni. Cena je privremeno porasla, nakon čega je on prodao bitkoine. Posle nekoliko minuta, cena se vratila na normalu. Ovaj incident

je uticao na račune u vrednosti od 8.750.000 dolara na berzi. Da bi povratio poverenje, Mt. Gox je prebacio 424.242 bitkoina iz jednog od svojih hladnih novčanika na svoju adresu.

Drugi incident se dogodio samo nekoliko meseci kasnije, u oktobru 2011. U tom incidentu je 2.609 bitkoina poslato na nevažeću adresu. To je bilo isto kao da su ti bitkoini uništeni, jer privatni ključ za tu adresu ne postoji i skoro ga je nemoguće vratiti (2). U februaru 2014. godine Mt. Gox je prekinuo sve transakcije na berzi. Više od par nedelja berza nije poslovala. Ovo je izazvalo zabrinutost kod njegovih klijenata. Konačno je Mt. Gox proglasio bankrot. Oko 750.000 bitkoina sa privatnih računa je nestalo zajedno sa 100.000 bitkoina sa same berze. U tom trenutku vrednost nestalih bitkoina bila je procenjena na 473.000.000 dolara.

Kolaps Mt. Gox-a bio je jedna od najvećih kriza kriptovaluta do danas. Četvrta najveća berza kriptovaluta u 2013. takođe je uskoro zatvorena zbog kršenja bezbednosnih protokola. Sa ove berze ukradeno je oko 24.000 bitkoina samo tokom jednog napada. U to vreme je već nedostajalo 730.000 bitkoina pre kolapsa Mt. Gox-a. Zajedno sa izgubljenim bitkoinima na Mt. Gox-u, gubitak je predstavljao skoro 6% ukupne ponude bitkoina (2). Prema blokčejnu, u oktobru 2022. godine u opticaju je nešto manje od 19,2 miliona bitkoina. Procenjuje se da je 3,79 miliona bitkoina izgubljeno ili uništeno. Ovo predstavlja vrednost veću od 70 milijardi dolara. To implicira da je između 18% i 20% svih zaliha bitkoina zauvek izgubljeno (Bhaskar & Chuen, 2015).

U incidentu iz 2011. godine, 2.609 bitkoina poslato je na nevažeću adresu.

BITKOIN DANAS

U septembru 2022. godine bitkoin je vredeo približno 20.000 dolara. Pre nego što će svet zahvatiti pandemija korona virusa, mogla su se čuti predviđanja da će njegova vrednost do kraja 2020. godine premašiti 100.000 dolara (14). Predviđalo se čak i će da u narednih 10 godina, počev od 2020, bitkoin moći da dostigne vrednost između jednog i 12,5 miliona dolara. U Hedž fond industriji menadžeri su verovali da bitkoin predstavlja digitalno zlato, zbog svoje sposobnosti da odoleva inflatornim pritiscima, što je i dovelo do njegove ekspanzije u inflatornim periodima posle 2009. godine. Ipak, ne dele svi takvo mišljenje. Varen Bafet (Warren Buffett), jedan od istaknutih fond menadžera, veruje da je bitkoin gotovo bezvredan (6).

Sa početkom 2022. godine, sukobom u Ukrajini i dvocifrenom inflacijom u najvećim ekonomijama sveta, bitkoin

je izgubio preko 60% svoje vrednosti. Njegova budućnost ostaje nepredvidiva. Ipak, jedno je izvesno. Bitkoin i blokčejn koji ga pokreće stvaraju godišnji utrošak od 127 teravat časova električne energije (6). Najveća nuklearna elektrana u Evropi u punom kapacitetu godišnje proizvede manje od polovine te količine. Najveća cena ikada plaćena za bitkoin iznosila je 68,789.63 dolara, u novembru 2021. godine. U trenutku istorijski najveće valuacije, tržište kriptovaluta bilo je procenjeno na dva biliona dolara – približno 40 puta vrednije od bruto domaćeg proizvoda Srbije. Ako se uzme u obzir da je 2009. godine vrednost bitkoina bila nula dolara i energetski uticaj na planetu potpuno zanemarljiv, nameće se zaključak da iako nije prva, i svakako nije ni poslednja, bitkoin ostaje istorijski definišuća kriptovaluta, ona koja je pokrenula zamajac digitalne transformacije.

DIGITAL CURRENCY IN INTERNATIONAL TRADE

SUMMARY

What led to the meteoric growth and popularity of cryptocurrencies, primarily Bitcoin? What concepts preceded the development of modern cryptocurrencies? What is blockchain and what is the architecture of different distributed public ledgers? What is the use value of digital money in everyday transactions and what is the use value in international trade exchange? This paper tries to answer the above questions and decipher the highly complex technical jargon that usually accompanies the topic of digital money.

Keywords: cryptocurrency; blockchain; double-spending; anonymity; distributed public ledger.

LITERATURA

1. Back, A. (2002). Hashcash - a denial of service counter-measure. Tech Report.
2. Bhaskar, N. D., & Chuen, D. L. (2015). Handbook of Digital Currency. Elsevier.
3. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain techno-logy: Beyond bitcoin. Applied Innovation.
4. Dai, W. (1998). B-money. Consulted.
5. David Chaum, A. F. (1988). Untraceable electronic cash. In Conference on the Theory and Application of Cryptography. Davos: Springer.
6. Forbes. (2022). Preuzeto sa: https://www.forbes.com/sites/qai/2022/05/04/warren-buffett-says-crytpo-doesnt-produce-anything/?sh=46f1ed997ee6
7. Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document. In Confe-rence on the Theory and Application of Cryptography. Sydney: Springer.
8. Hileman, G. (2014). From bitcoin to the brixton pound: history and prospects for alternative currencies. In International Conference on Financial Cryptography and Da-ta Security. Springer.
9. Jeffrey Chu, S. N. (2015). Statistical analysis of the exchange rate of bitcoin. PloS one.
10. Lam Pak Nian, D. L. (2015). Introduction to bitcoin. Elsevier.
11. Martina Matta, I. L. (2015). Bitcoin spread prediction using social and web search me-dia. Dublin: UMAP Workshops.
12. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Working Paper.
13. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.
14. NextAdvisor (2022). Preuzeto sa: https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-price-predictions/
15. Wallace, Benjamin. „The rise and fall of bitcoin.“ *Wired*, 2011.

Rad primljen: 4.9.2022 • Prihvaćen: 30.9.2022.