Tehnički, ekonomski i pravni aspekti digitalnog novca

Tomašić, Marijan

Sveučilište u Zadru

Odjel za ekonomiju
Diplomski sveučilišni studij menadžmenta (jednopredmetni)

Tehnički, ekonomski i pravni aspekti digitalnog novca

Diplomski rad

Zadar, 2017.

Sveučilište u Zadru

Odjel za ekonomiju
Diplomski sveučilišni studij menadžmenta (jednopredmetni)

Tehnički, ekonomski i pravni aspekti digitalnog novca

Diplomski rad

Student/ica:

Marijan Tomašić

Mentor/ica:

doc. dr. sc. Mladen Rajko

Zadar, 2017.

Izjava o akademskoj čestitosti

Ja, Marijan Tomašić**,** ovime izjavljujem da je moj diplomski rad pod naslovom Tehnički, ekonomski i pravni aspekti digitalnog novca rezultat mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na izvore i radove navedene u bilješkama i popisu literature. Ni jedan dio mojega rada nije napisan na nedopušten način, odnosno nije prepisan iz necitiranih radova i ne krši bilo čija autorska prava.

Izjavljujem da ni jedan dio ovoga rada nije iskorišten u kojem drugom radu pri bilo kojoj drugoj visokoškolskoj, znanstvenoj, obrazovnoj ili inoj ustanovi.

Sadržaj mojega rada u potpunosti odgovara sadržaju obranjenoga i nakon obrane uređenoga rada.

Zadar, 2017.

SADRŽAJ

Sažetak:

U ovom radu se analiziraju tehnički, ekonomski i pravni aspekti digitalnih valuta, njihov odnos sa klasičnim novcem, pregled tržišta, procjena trendova. Dan je pregled njihovih tehničkih specifičnosti kako bi se lakše sagledali sigurnosni aspekti, te njihovog trenutnog pravnog statusa kako bi se mogle postaviti određene pretpostavke glede trendova. Vidljivo je da je ogromna količina transakcija rezultat trgovine digitalnih valuta međusobno, a manji dio posljedica je razmjene dobara. Očito je da je pokretač ovog trenda popularnosti špekulativni val, uzrokovan znatiželjom, željom za profitom, i jednim dijelom i neznanjem, odnosno zanemarivanjem činjenice da su digitalne valute u velikoj mjeri međusobni supstituti. Iako je u sustavu sve transparentno, oni koji prvi ulaze (kreatori) imaju najveću šansu za zaradu ukoliko određena valuta „zaživi". Naravno da je stanje moguće promijeniti na način prilagodbe pravnog sustava novim okolnostima, i na taj način spriječiti negativnosti a zadržati pozitivne strane digitalnih valuta. Postavljena hipoteza je da u društvu u kojem živimo, a koje je po svojoj prirodi centralizirano i organizirano hijerarhijski, fenomeni poput digitalnih valuta koji iako u tehničkom smislu mogu biti decentralizirano upravljani, ipak ne mogu u potpunosti ispuniti takvu pretpostavku bez odgovarajućeg odgovora institucija, koje upravljaju društvom kreirajući odgovarajuće pravno-ekonomske regulatorne okvire.

Ključne riječi:

digitalne valute, kriptovalute, virtualne valute, virtualni novac, digitalni novac, blockchain, bitcoin, virtualne valutne sheme

1 UVOD

Zadnjih nekoliko godina digitalni novac općenito, a posebno nove digitalne valute sve više postaju predmet interesa javnosti. Velika praktičnost i brzina obavljanja elektroničkih transakcija u odnosu na klasične, su čimbenici koji već sada nedvojbeno utječu na porast popularnosti različitih oblika elektroničkog plaćanja. Digitalne valute na ovom polju donose nove mogućnosti uporabe. Postoje naravno i brojni čimbenici koji koče ili usporavaju trend razvoja digitalnih valuta. Neki od njih su složenost tehničkih rješenja na kojima su utemeljene digitalne valute i nerazumijevanje načina funkcioniranja spomenutih tehničkih rješenja. Nepostojanje centralnog autoriteta koji bi stajao iza takvih valuta, i zabrinutost za potencijalne sigurnosne nedostatke takvog sustava također su demotivirajući faktor uporabe za značajan broj korisnika.

U okviru istraživanja ovog rada postavlja se hipoteza: digitalni novac odnosno digitalne valute bazirane na Blockchain tehnologiji nude puno novih mogućnosti za unapređenje dosadašnje uloge novca u ekonomiji i društvu općenito. Bez odgovarajućeg pravno-ekonomskog okvira definiranog od strane institucija, te mogućnosti je teško u potpunosti iskoristiti.

1.1 Problem istraživanja

Ukupna tržišna kapitalizacija nekoliko glavnih digitalnih valuta, od 2009. godine i pojave Bitcoina kao prvijenca, u stalnom je porastu, a naročito zadnje tri do četiri godine. U vrijeme pisanja ovog rada ona premašuje 25 milijardi USD.[1] Promjene na ovom tržištu se odvijaju munjevitom brzinom što za posljedicu donosi vrlo veliku volatilnost svih značajnih digitalnih valuta na tržištu. Stoga su one često predmet špekulativnog i visoko rizičnog investiranja, bilo na kraći ili duži rok.

[1] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/. [Pristupljeno: 31-ožu-2017]

Prema mnogim autorima, anonimnost transakcija otvara mogućnosti korištenja za ilegalne djelatnosti (prijevare, utaja poreza, ilegalna trgovina, pranje novca).[2] Pitanje je koliko na te zlouporabe utječu same digitalne valute sa svojim specifičnostima, a koliko neprilagođena pravna regulativa. Treba reći da anonimnost i decentraliziranost sustava možemo promatrati i u pozitivnom i u negativnom kontekstu. Teoretski govoreći, potpuno anonimne i decentralizirane transakcije nisu podložne nikakvom regulatornom autoritetu, što znači da njihova kontrola nije moguća niti od strane vlasti, što se može podjednako tumačiti kao mogućnost slobodnog i potpuno anonimnog obavljanja financijskih transakcija, ali i kao značajno sigurnosno ograničenje.

Sa ekonomskog aspekta, vrlo je izvjesno da će digitalne valute u budućnosti imati značajan utjecaj. Od ubrzavanja i pojeftinjenja transakcija, sigurnosnih prednosti (i nedostataka?), pa do pristupačnosti i praktičnosti, pogotovo generacijama koje dolaze i kojima nije strano korištenje novih tehnologija. Novim tehnologijama stvaraju se i nove potrebe, te se nude i novi načini njihovog zadovoljenja. Primjer za to su velika pogodnost za internetsku trgovinu i internetsko plaćanje. Nove, još ne realizirane mogućnosti takozvanih programiranih transakcija odnosno pametnih ugovora (*eng. smart contracts*)[3], te primjena *blockchain*[4] tehnologije izvan područja digitalnih valuta, npr. u raspodjeli udjela tvrtki ili nekih drugih vrijednosti također su moguće i izvjesne.[5] [6]

[2] BRYANS, Danton, Bitcoin and money laundering: mining for an effective solution, *Ind LJ*, sv. 89, 2014, str. 441

[3] OMOHUNDRO, Steve, Cryptocurrencies, smart contracts, and artificial intelligence, *AI Matters*, sv. 1, izd. 2, 2014, str. 19–21

[4] MATTILA, Juri, The Blockchain Phenomenon, *'Book Blockchain Phenomenon'Berkeley Roundtable Int. Econ. 2016 Edn*, 2016, str. 6

[5] 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 Cryptography 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]

[6] 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]

Uz sve navedeno, već na prvi pogled i bez dublje analize, može se pretpostaviti da će spomenuti trendovi već u relativno bliskoj budućnosti ostaviti značajan trag, te utjecati na korjenite promjene načina poslovanja, trgovine, plaćanja, ali i svakodnevnih navika.

1.2 Ciljevi i svrha istraživanja

Cilj ovog rada je analizirati trenutno stanje na tržištu digitalnih valuta sa tehničkog, ekonomskog i pravnog aspekta, kako bi se utvrdio njihov značaj i uloga u svakodnevnom životu i postavile određene pretpostavke glede daljnjeg razvoja i trendova.

Pri tome je potrebno jasno i dovoljno detaljno opisati način funkcioniranja digitalnih valuta u tehničkom smislu, kako bi zainteresirane strane mogle samostalno i što kvalitetnije procijeniti sigurnosne rizike korištenja digitalnih valuta. Pokušat će se, onoliko koliko je to moguće u opsegu rada, pojasniti pojedine tehničke specifičnosti ovakvih sustava kako bi ih se približilo širem krugu potencijalnih korisnika. Bolje poznavanje tehničkih detalja omogućava svakome da samostalno i neovisno prosuđuje koliko je sigurna uporaba digitalnih valuta u tehničkom smislu, te koje su prednosti i nedostaci pojedinih varijanti tehničke izvedbe.

Pokušat će se objasniti što su digitalne valute, u kojoj mjeri se mogu uspoređivati sa klasičnim novcem ili njegovim elektroničkim inačicama, te analizirati kako se digitalne valute uklapaju u klasične definicije novca. 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. Na taj način će se olakšati prognoziranje budućih trendova na ovom području, kao i adaptacija na buduće okolnosti, svima koji su za to zainteresirani. Veći interes javnosti potaknut će masovniju uporabu valuta baziranih na *blockchain* tehnologiji, ali i dati određeni doprinos novim idejama za uporabu ove tehnologije, otkrivanju novih načina primjene, te čak i kreiranju novih potreba društva, koje bi se na ovaj način mogle zadovoljiti.

S pravnog gledišta, vidljivo je da većina društvenih autoriteta (vlasti, zakonodavci, nacionalne banke) kasne sa donošenjem određenih stavova glede pravnog statusa digitalnih valuta. Kao i mnogo puta u povijesti, tehnologija napreduje puno brže od društvenog razvoja, postajući zapravo glavni čimbenik i generator promjena u društvu. Kroz pregled stavova najvažnijih financijskih, ekonomskih i pravnih subjekata, pokušat će se sagledati pravni položaj digitalnih valuta u današnjem društvu, te njihova perspektiva u budućnosti.

1.3 Istraživačka pitanja

Kao rezultat istraživanja očekuje se:

- saznati kakvo je trenutno stanje i trendovi na tržištu digitalnih valuta,
- razlučiti razlike najčešćih tehničkih sustava, te doznati njihove prednosti i nedostatke.
- saznati na koji način digitalne valute postižu tržišnu vrijednost, kako i zašto stječu povjerenje korisnika, te kako se koriste.
- odrediti utjecaj digitalnih valuta na način trgovanja i korištenja novca općenito, te iz prikazanih trendova potvrditi određene prognoze.
- prikazati položaj digitalnih valuta iz pravnog aspekta, te njihov utjecaj i pogodnost za legalne i ilegalne načine korištenja.

1.4 Metodologija

Metodologija istraživanja u prvom dijelu će se bazirati na pojašnjenju osnovnih pojmova i definicija, kao što su digitalni novac, digitalne valute, *blockchain*[7] tehnologija itd. (metode definicije i deskripcije). Prilikom proučavanja s različitih aspekata, a pogotovo tehničkog i

[7] PILKINGTON, Marc, Blockchain technology: principles and applications, *Res. Handb. Digit. Transform.*, ruj. 2015, str. 4,5

ekonomskog, koristit će se metoda analize i dedukcije. U obradi prikupljenih izvora i prilikom njihovog korištenja, te pregleda trenutnog stanja na tržištu, kao i pregleda dosadašnjih radova s promatranog područja, koristit će se jednim dijelom i metoda kompilacije. Prilikom donošenja određenih zaključaka, kao i odgovora na istraživačka pitanja, bit će korištena i metoda sinteze.

2 PRETPOSTAVKE RAZVOJA NOVCA I SUSTAVA PLAĆANJA

U ovom poglavlju prikazane su i ukratko opisane osnovne pretpostavke koje su se morale ispuniti kako bi moglo doći do pojave digitalnog novca. To su prije svega razvoj trgovine i razvoj različitih oblika klasičnog novca, koji su međusobno uzročno-posljedično tijesno povezani, zatim razvoj određenih grana tehnologije i znanosti koji su zaslužni za tehnička rješenja potrebna za korištenje digitalnog novca.

2.1 Uloga razvoja trgovine u razvoju različitih oblika novca

Od davnih vremena ljudi imaju potrebu razmjenjivati vrijednosti. Već razvojem oruđa u prvobitnoj ljudskoj zajednici počinju se stvarati prvi viškovi roba. Kao logična posljedica, javljaju se dvije nove potrebe: potreba razmjene dobara i potreba čuvanja dobara i vrijednosti.[8] Ispočetka se razmjena dobara odvijala direktno, kao trampa. U direktnoj ili bilateralnoj trampi dobra se izmjenjuju direktno, bez uplitanja treće strane. Često nije bilo moguće pronaći partnera za trampu koji bi trebao vaše proizvode, a istovremeno imao viška robe koja vam je potrebna. Zato nastaje potreba za mijenjanjem viškova roba i vrijednosti za one vrijednosti za koje se pretpostavljalo da će se kasnije moći zamijeniti za ono što nam bude trebalo. Nastaje multilateralna trampa, odnosno zamjena roba između više strana. Ako se ta zamjena ne odvija istovremeno, možemo govoriti o robnom novcu, tj. određenim robama koje su funkcionalno postale medij razmjene.[9]

Zbog ograničene praktičnosti trampe, javlja se snažna potreba unapređenja procesa razmjene, koja se pokušava zadovoljiti traženjem adekvatnih sredstava koja bi mogla poslužiti kao medij razmjene. Već tada je bilo jasno da takav medij mora zadovoljavati određene kriterije, kako bi bio prihvaćen od zajednice.[10] Tijekom vremena, različite robe služile su kao mediji razmjene. Neki od prvih medija razmjene bili su osim hrane koja je bila

[8] INNES, A. Mitchell, What is money?, *Bank. Law J.*, svi. 1913, str. 377–408

[9] Ibid.

[10] Ibid.

tražena i **lako utrživa** ali kratkotrajna i pokvarljiva roba, i predmeti iz prirode, kosti, školjke, puževi itd. koji su pak bili **trajni** ali ponekad teško utrživi. Pokazalo se da je za dobar medij bitna njegova **ograničena dostupnost**, kako se ne bi dogodilo da netko olako dođe u posjed veće količine i na taj način stekne nepoštenu prednost u trgovini, ili da se osigura očuvanje vrijednosti novca na dulji rok. Određene robe se počinju sve češće koristiti u razmjeni, prije svega plemeniti metali zlato i sredstvo. Budući da zlato i srebro ne hrđaju, niti ne trunu, a lako su utrživi i teško dostupni, idealni su primjer ekonomskih dobara. S vremenom su postali preferirani medij razmjene.[11]

Većina ekonomista objašnjava povijest nastanka novca kao specijalizaciju u trgovini društva koja se zaustavila na određenim robama, obično metalima kao mediju razmjene. Kasnije, kovanjem metala u novčiće, dolazi do standardizacije količine i čistoće metala što su preduvjeti da bi novac imao kredibilitet. Mali je korak od kovanica do papirnog novca, koji predstavlja ugovor između donositelja i banke ili vlade.[12]

Nastanak novca osim što je posljedica razvoja, i sam postaje generator razvoja trgovine i ekonomije uopće. Razvoj tehnologije i tehnike, kao i razvoj ekonomske teorije i prakse stalno pronalaze nove oblike novca i načine plaćanja. Na taj način zajednica uživa nove efikasnije i naprednije mehanizme razmjene vrijednosti, stvarajući doprinos društvenom probitku.

U idealnom slučaju, novac ima tri ključne karakteristike; on služi kao sredstvo razmjene, kao mjerilo vrijednosti i kao ekonomsko dobro.

2.2 Reprezentativni novac, fiat novac i elektronički novac

Za razliku od robnog novca čija vrijednost leži stvarnoj uporabljivosti samog novca ili materijala od kojih je sačinjen, postupno se ukazala potreba za novim vrstama novca kao što

[11] Ibid.

[12] RITTER, Joseph A., The transition from barter to fiat money, *Am. Econ. Rev.*, sv. 85, izd. 1, ožu. 1995, str. 134

su reprezentativni novac i fiat novac. Povijesno gledano, upotreba reprezentativnog novca prethodi izumu novca. U drevnim imperijima Egipta, Babilona, Indije i Kine, hramovi i palače često su imali robna skladišta koja su izdavala potvrde ili priznanice, kao dokaz za potraživanje dijela robe pohranjene u skladištu. Takve potvrde su jedan od najranijih primjera reprezentativnog novca.[13]

Mnoge svjetske valute do 20. stoljeća bile su reprezentativni novac, vezan za zlato ili srebro. Najpoznatiji primjer je USD, koji je do 1971. godine garantirao donosiocu određenu količinu zlata iz federalnih rezervi. Skupom ekonomskih mjera nazvanih „Niksonov šok" stavljen je izvan snage dotadašnji *Bretton Woods system*, skup ekonomsko monetarnih regulativa između najjačih svjetskih ekonomija, koji je do tada regulirao monetarno djelovanje zemalja članica sporazuma. Potrebe za velikim količinama novca nakon toga više se nisu mogle pokrivati zalihama zlata i USD postaje tzv. *fiat* novac.[14]

Fiat novac je valuta ustanovljena kao novac vladinim propisom ili zakonom. Izraz proizlazi iz latinskog izraza *fiat* ("neka postane", "postat će") koji se koristi u smislu odredbe ili dekreta.[15] On s razlikuje od reprezentativnog novca jer nije više vezan za stvarnu vrijednost. Njegova prihvaćenost propisana je zakonom, a povjerenje je vezano za povjerenje u vlast ili autoritet države. Elektronički novac nastao je kao logična posljedica razvoja telekomunikacijskih i informatičkih tehnologija. On predstavlja svaki oblik novca koji se pojavljuje u elektroničkom odnosno virtualnom obliku, bez obzira dali je ta pojavnost isključiva (kao npr. kod digitalnih valutnih shema) ili se radi o elektroničkoj verziji klasičnog, fiat novca (kao na primjer u slučaju internetskog bankarstva). Zajednička karakteristika svih oblika elektroničkog novca je da se koriste uz pomoć raznih tipova uređaja (računala) i određenih tehnologija.

[13] MUNDELL, Robert A., *The birth of coinage*. Citeseer, 2002, Dostupno na: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1009.8953&rep=rep1&type=pdf. [Pristupljeno: 29-tra-2017]

[14] IRWIN, Douglas A., The Nixon shock after forty years: the import surcharge revisited, National Bureau of Economic Research, 2012, Dostupno na: http://www.nber.org/papers/w17749. [Pristupljeno: 29-tra-2017]

[15] MANKIW, N. Gregory, The data of Macroeconomics, u *Principles of macroeconomics*, Cengage Learning, 2014, str. 220

2.3 Čimbenici u funkciji razvoja digitalnih valuta

Osnovni čimbenici u funkciji razvoja digitalnih valuta su počevši od općenitih kao što su razvoj tehnologije i znanosti, pa do konkretnih, kao što su kvalitativni i kvantitativni razvoj internetske mreže, razvoj kriptografije kao posebne znanstvene discipline te razvoj specifičnih tehnoloških rješenja kao što je na primjer Blockchain software.

2.3.1 Razvoj interneta

Svjedoci smo eksponencijalnog rasta interneta i tehnologija baziranih na internetu kao mediju prijenosa informacija. Razvoj telekomunikacijskih tehnologija od kojih je Internet sigurno najznačajnija infrastrukturna komponenta u masovnoj uporabi, odražava se na sve aspekte življenja, od tehnoloških do znanstvenih, ekonomskih, pa i socijalnih i psiholoških. Bilo je samo pitanje dana kada će se Internet početi koristiti i kao medij za ekonomske transakcije.

Prema nekim izvorima, broj korisnika interneta povećao se sa 35 miliona 1995. na 2.8 milijardi 2014. godine, pa danas imamo oko 39% svjetske populacije koja koristi internet.[16] Istovremeno, Internet je značajno unaprijeđen u tehničkom smislu, brzine pristupa svakodnevno se povećavaju, povećava se pristupačnost širenjem telekomunikacijskih mreža i razvojem tehnologije. Taj trend je, očekivano, u početnoj fazi bio najsnažniji u najrazvijenijem dijelu svijeta gdje se broj korisnika u nekim državama penje i na 89% pismene populacije.[17] Danas i nerazvijene zemlje razvijaju Internet gledajući na to kao strateški interes i preduvjet sveopćeg ekonomskog razvoja.

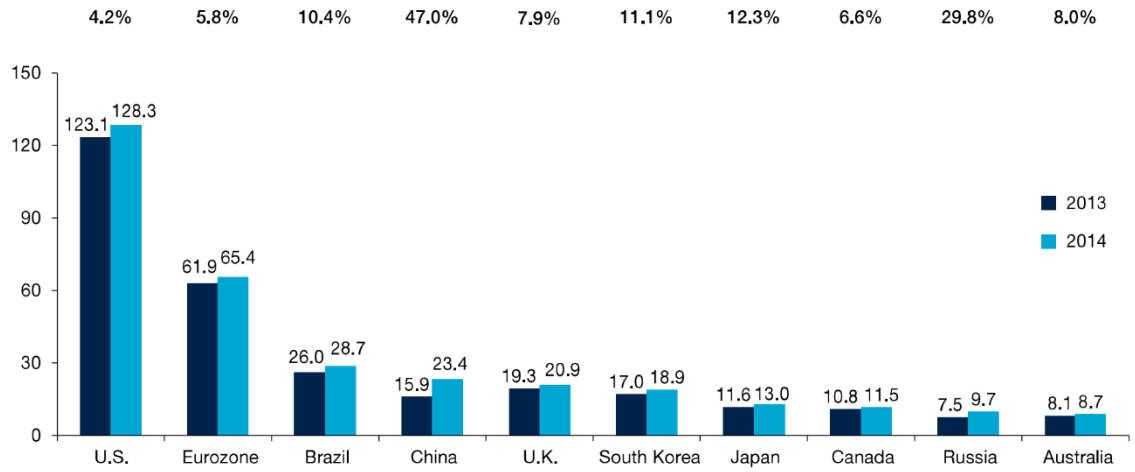
Stvaranjem kritične mase korisnika, pokrenut je vjerojatno ireverzibilan proces unapređenja i razvoja sustava za plaćanje i pohranu vrijednosti. U takvim uvjetima, očekivano, razvile su se prvo elektroničke inačice postojećih valuta i sustava plaćanja, npr. internetsko bankarstvo

[16] 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]

[17] 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

i kartično plaćanje kao najpoznatiji. Slijedeća slika na primjeru iz 2014. godine prikazuje koliki su razmjeri porasta udjela bezgotovinskog plaćanja u najznačajnijim svjetskim ekonomijama.

Slika 1 - Relativni godišnji porast bezgotovinskog plaćanja za 2014. godinu prema svjetskim regijama[18]



Slika pokazuje relativni jednogodišnji porast bezgotovinskog plaćanja podijeljen prema značajnim ekonomskim regijama, za godinu 2014. Vidljivo je povećanje u svim regijama a najviše u zemljama sa brzorastućim ekonomijama, Kini (47%) i Rusiji (29,8%).

Za očekivati je da porast bezgotovinskog plaćanja potiče traženje novih, pogodnijih načina plaćanja, pogotovo plaćanja preko interneta, za što su nove digitalne valute posebno pogodne.

2.3.2 Razvoj kriptografije

Kriptografija je multidisciplinarna znanost, bazirana uglavnom na područjima matematike i računalnih znanosti, u svrhu što efikasnijeg kodiranja i dekodiranja podataka. Pri tome je cilj uspješno poslati informacije primatelju, bez bojazni da će te informacije doći u posjed treće strane (odnosno uz određeni stupanj sigurnosti). Razvojem računalne tehnologije, a posebno

[18] World Payments Report, Dostupno na: https://www.worldpaymentsreport.com/. [Pristupljeno: 20-tra-2017]

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 primiti niz podataka bilo koje duljine, i za njega će proizvesti specifičan „potpis“ odnosno niz znakova unaprijed zadane duljine. Pri tome je važno da svaka i najmanja izmjena ulaznog niza znakova uzrokuje značajne promjene izlaznog niza, a brzina cijelog procesa direktno utječe na uporabljivost funkcije. Sama funkcija je „jednosmjerna“ tj. lako je i brzo izračunati hash ulaznih podataka, ali je nemoguće iz hash-a dobiti originalni niz podataka.[19]

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

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

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

Osim toga, moguće je ustanoviti jednakost podataka bez uvida u njihov sadržaj. Na primjer, ako želite provjeriti dali netko zna lozinku, bez da vam je kaže (npr. nema povjerenja u vas ali vam mora dokazati da mu je lozinka poznata), dovoljno je da vam dostavi hash lozinke. Uspoređujući hash ispravne lozinke sa dobivenim možete ustanoviti njenu ispravnost. Na

[19] 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]

ovaj način entitet u sustavu koji provodi validaciju određenih podataka (u ovom primjeru lozinke, ali to može biti bilo kakav podatak) može obavljati svoju funkciju bez pristupa aktualnim podacima. Na sličnom principu bazira se i jedna od poznatijih teoretskih zagonetki, takozvani „Problem bizantskih generala“ (*The Byzantine generals problem*)[20].

Ovo svojstvo 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.[21] Različiti tipovi ovih funkcija namijenjeni su za različite namjene, i zbog svoje ogromne važnosti, predmet su stalnog razvoja i usavršavanja od strane znanstvene zajednice. Razvoj elektroničkih računala i uređaja, osim što doprinosi kvaliteti života, pomaže i onima koji imaju kriminalne namjere. Tehnologija podjednako ide na ruku i onih koji rade protiv sustava, npr. u pokušajima probijanja sigurnosnih sustava. Računala velike procesorske snage danas su vrlo pristupačna i sve lakše se mogu iskoristiti u takve svrhe. 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.

2.3.3 Blockchain tehnologija

Blockchain tehnologija u smislu temelja sustava virtualnih valutnih shema, predstavljena je svijetu 2009. godine. Pod pseudonimom Satoshi Nakamoto objavio ju je nepoznati autor ili organizacija u vidu software-a otvorenog koda (*eng. Open source*), na web stranici

[20] LAMPORT, Leslie, SHOSTAK, Robert, PEASE, Marshall, The Byzantine generals problem, *ACM Trans. Program. Lang. Syst. TOPLAS*, sv. 4, izd. 3, 1982, str. 382–401

[21] BURR, William E., Selecting the advanced encryption standard, *IEEE Secur. Priv.*, sv. 99, izd. 2, 2003, str. 43–52

https://bitcoin.org.[22] Iako postoje brojne špekulacije, do danas nije sa sigurnošću utvrđen identitet autora. Kako osnovna verzija software-a (koji se od 2009. godine stalno unapređuje i razvija od zajednice) sadrži preko 31000 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).

Blockchain je baza podataka u digitalnom obliku, koja sadrži dnevnik svih transakcija učinjenih u sustavu. Decentralizirana je u smislu da svaki sudionik sustava ima mogućnost pohraniti kod sebe vlastitu kopiju. Sudionici ili čvorovi u sustavu (*eng. nodes*)[23] su ravnopravni svjedoci i kontrolori autentičnosti svake pojedinačne transakcije. Transakcije su grupirane kronološki, u tzv. Blokove transakcija. Svaki blok transakcija digitalno je „potpisan" odnosno pridružena mu je određena digitalna šifra (*eng. hash*) koja je garancija da je blok autentičan, tj. svaki pokušaj promjene sadržaja bloka je vrlo lako otkriti. Uz navedeno, osim određenog broja transakcija, svaki blok sadrži i hash prethodnog bloka, što znači da ako netko želi promijeniti sadržaj određenog bloka (npr. dodajući ili mijenjajući transakcije), mora izmijeniti sve blokove u nizu nakon izmijenjenog bloka. Blokovi su na taj način povezani ili ulančani, odakle i potječe naziv Blockchain.[24]

Ovo je pojednostavljen prikaz funkcioniranja Blockchain tehnologije i tu nisu opisani svi detalji sustava kao ni njegove varijante. Cilj je istaknuti funkcionalnost cijelog sustava baziranog na ravnopravnoj mreži sudionika i tehničkom rješenju, a bez određenog centraliziranog sustava autorizacije[25], kao što je slučaj kod Internet bankarstva, gdje banka autorizira i kontrolira transakcije.

[22] NAKAMOTO, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009, Dostupno na: https://bitcoin.org/bitcoin.pdf. [Pristupljeno: 29-ožu-2017]

[23] ROGOJANU, Angela, BADEA, Liana, OTHERS, The issue of competing currencies. Case study–Bitcoin, *Theor. Appl. Econ.*, sv. 21, izd. 1, 2014, str. 107

[24] ABRAMOWICZ, Michael, Cryptocurrency-Based Law, *Ariz Rev*, sv. 58, 2016, str. 359

[25] 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

2.4 Bitcoin - prva valuta bazirana na blockchain tehnologiji

Bitcoin je digitalna, decentralizirana, pseudo anonimna valuta, koja se ne oslanja na vlade ili druge pravne osobe, i čija vrijednost nije garantirana zlatom ili drugim robama. Ona se oslanja na ravnopravnu mrežu računala i održava integritet uz pomoć kriptografije. Treba reći da postoje radovi koji proučavaju u kojoj mjeri je ova definicija ispravna, pogotovo glede decentraliziranosti i anonimnosti, iako se u načelu ona može prihvatiti kada se uspoređuje sa klasičnim sustavima plaćanja.[26]

Bitcoin je složen sustav, a njegova implementacija uključuje kombinaciju kriptografije, distribuiranih algoritama i usuglašenog ponašanja zajednice korisnika. Štoviše, najnoviji razvoj događaja ukazuje na činjenicu da Bitcoinove operacije mogu uključivati rizike čija priroda i udio su vrlo malo (ako uopće) razumljivi.[27]

Njegovi zagovornici 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*).[28] 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.[29]

Iako Bitcoin ekonomija cvjeta, korisnici su zabrinuti za pravni status Bitcoin-a 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

[26] GERVAIS, Arthur *i ostali*, Is Bitcoin a decentralized currency?, 2014, str. 1

[27] BADEV, Anton I., CHEN, Matthew, Bitcoin: Technical background and data analysis, 2014, str. 2

[28] GRINBERG, Reuben, Bitcoin: An innovative alternative digital currency, 2011, str. 206

[29] ROTHBARD, Murray N., Austrian definitions of the supply of money, *New Dir. Austrian Econ.*, 1978, str. 143–156

omogućava anonimne transakcije čime se olakšava pranje novca, utaje poreza, kockanje, trgovina drogom, dječja pornografija i slične kriminalne djelatnosti.[30] [31]

Bitcoin kao kriptovaluta oslanja se na kriptografski protokol koji određuje na koji način valuta nastaje, mijenja ili kako se njome trguje. Za razliku od nekih prijašnjih digitalnih valuta (poput Second Life-ovog Linden dolara, ili World of Warcraft zlata) koje su izdane i regulirane od strane centralnog servera, Bitcoin je širom svijeta distribuirana, decentralizirana cripto valuta upravljana samo i isključivo od strane kriptografskog protokola otvorenog koda: nema vlade, tvrtke ili banke zadužene za izdavanje ili upravljanje Bitcoinom.[32]

Bitcoin je digitalna valuta koja korisnicima omogućuje slanje uplata u decentraliziranoj, ravnopravnoj mreži računala (eng. izraz *Peer to peer*), te je jedinstven po tome što ne zahtijeva središnju novčanu instituciju za autorizaciju transakcija. Korisnici moraju imati internetsku vezu i Bitcoin softver za plaćanja prema drugom javnom računu odnosno adresi.[33]

Engleski izraz *Peer to peer* (isti sa istim ili svaki sa svakim) u tehnologiji računalnih mreža podrazumijeva koncept umrežavanja računala bez poslužitelja, gdje je svako računalo inteligentna radna stanica, koja pronalazi druga računala putem emitiranja paketa podataka (poruka), i komunicira s njima izravno, bez potrebe autorizacije na nekom centralnom poslužitelju.[34]

Satoši je najmanja jedinica Bitcoina; 1 Bitcoin sadrži 100 milijuna Satošija. Prema dizajnu cijelog sustava, ukupna količina svih Bitcoina ne može biti veća od 21 milijuna (2100

[30] GRINBERG, Reuben, Bitcoin: An innovative alternative digital currency, 2011, str. 206

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

[32] DE FILIPPI, Primavera, Bitcoin: a regulatory nightmare to a libertarian dream, *Brows. Download This Pap.*, 2014, str. 1

[33] WOO, David, GORDON, Ian, IARALOV, Vadim, Bitcoin: a first assessment, *FX Rates*, 2013, str. 2

[34] BANDARA, HMN Dilum, JAYASUMANA, Anura P., Collaborative applications over peer-to-peer systems–challenges and solutions, *Peer--Peer Netw. Appl.*, sv. 6, izd. 3, 2013, str. 257–276

milijardi Satošija). Ukupna količina Bitcoin u opticaju se povećava planirano i očekivano, na temelju programskog koda, do postizanja maksimalne količine u 2140. godini.[35]

Javna povijest svih transakcija kontinuirano se ažurira i ovjerava od strane „rudara" koji prikupljaju serije novih transakcija u blokove i pripajaju te blokove na kraj „Blockchain-a" Ova javna povijest ili dnevnik čini knjigu transakcija u kojima se prati svaki Satoši od prvog vlasnika do današnjih vlasnika. Provjerom svih transakcija za određenog kupca, jamči se da kupac zapravo posjeduje potreban broj Bitcoina za željenu transakciju, te se na taj način sprečavaju prijevare.[36]

Količina Bitcoin-a u opticaju povećava se sa svakim novim blokom transakcija dodanim u javni dnevnik (tj. Blockchain). Provjerom novih transakcija „rudari" ih pakiraju u blokove. Međutim, tu je i računalni zadatak za svaki blok visokog stupnja težine, sustavno dizajniran za ograničavanje povećanja novčane mase, bez obzira koliko sporo ili brzo funkcionira cjelokupna mreža. Bez obzira koliko transakcija sadrži blok, svaki uspješan upis bloka u centralni dnevnik donosi sustavom određeni broj Bitcoin-a rudaru. Doista, prvih nekoliko tisuća blokova jednostavno su služili kao isplata rudaru iako nisu sadržavali druge transakcije (trenutno blokovi sadrže evidenciju stotina transakcija). Na taj način je značajna početna količina novca distribuirana rudarima koji su podnijeli spekulativni rizik uspjeha Bitcoina.[37]

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 17 milijardi USD, sa svakom pojedinačnom jedinicom u vrijednosti preko 1000 USD. Ova ogromna vrijednost se održava isključivo na povjerenju između korisnika uključenih u Bitcoin transakcije.[38]

[35] WOO, David, GORDON, Ian, IARALOV, Vadim, Bitcoin: a first assessment, *FX Rates*, 2013, str. 2

[36] Ibid.

[37] Ibid.

[38] KAPLANOV, Nikolei, Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, *Loy Consum. Rev*, sv. 25, 2012, str. 115

3 TEHNIČKI ASPEKTI DIGITALNIH VALUTA

Kao primjer u proučavanju digitalnih valuta[39], u radu je najviše korišten Bitcoin, jer je trenutno najpopularniji predstavnik spomenutog koncepta, a zbog velike sličnosti (gledano u tehničkom, ekonomskom i pravnom smislu) većina izrečenog 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.

3.1 Pojavni oblici digitalnih valuta

Bitcoin zapravo nema materijalni oblik, iako se može 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 sama novčanica u fizičkom smislu i u originalnom izdanju predstavlja vrijednost i kao takva se ne može (legalno) kopirati, odnosno kopija nema vrijednost iako može biti gotovo istovjetna originalu.

Bitcoin adresa je oznaka ili broj koji možemo usporediti sa brojem klasičnog tekućeg računa u banci. Za svaku postojeću adresu 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. private key*). Ako znate adresu, možete imati potpuni uvid u stanje, ali ne možete trošiti sredstva s računa. Za trošenje vam je potreban privatni ključ.[40]

[39] 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

[40] FAIRFIELD, Joshua AT, BitProperty, *Cal Rev*, sv. 88, 2014, str. 820

Dakle, možemo reći da je bitcoin zapravo broj računa (adresa) koji sadrži određeni saldo izražen u bitcoin jedinicama. Sastoji se od bitcoin adrese kao javnog dijela, i privatnog ključa koji omogućava trošenje.

Na slijedećoj slici vidimo primjer Bitcoin-a tiskanog na papiru. Glavni dio je privatni ključ i bitcoin adresa (javni ključ) koji se jednostavno mogu prepisati na običan papir a da pri tome ne izgube vrijednost. Privatni ključ potrebno je čuvati u tajnosti, jer omogućava otuđenje vrijednosti sa računa (adrese). Javni ključ ili adresa mogu se dijeliti u javnosti i potrebni su onome tko želi doznačiti sredstva na račun (adresu). Na slici su vidljivi i tzv. QR kodovi za svaki od ključeva koji omogućavaju praktično korištenje i očitavanje pomoću pametnog telefona i odgovarajuće aplikacije, kako bi se izbjeglo ručno utipkavanje kodova.

Slika 2 - Primjer Bitcoin-a tiskanog na papiru: s prikazom adrese (lijevo) i privatnog ključa (desno)[41]

Svaka bitcoin adresa i pripadajući privatni ključ su međusobno povezani na način da je adresa rezultat određene kriptografske funkcije provedene nad privatnim ključem. Znači da znajući adresu ne možemo utvrditi privatni ključ, ali znajući privatni ključ, možemo utvrditi adresu odnosno račun vlasnika primjenom odgovarajuće funkcije, odnosno služeći se javno

[41] Bitcoin u papirnatom obliku, Dostupno na: http://i.imgur.com/s4kv4.jpg. [Pristupljeno: 13-tra-2017]

dostupnim web servisima za pojedinu valutu. Princip je više puta opisivan u literaturi (*Public-Key Encryption* - PKE).[42]

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).

3.2 Prednosti i nedostaci različitih tipova novčanika

Bitcoin je zapravo informacija odnosno broj, koji predstavlja takozvanu bitcoin adresu, 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*)

Moderni bitcoin novčanici[43] raspolažu sa više korisnih funkcija. U njima možete čuvati podatke o puno adresa i pripadajućih ključeva, automatski će vam prikazivati ukupno stanje salda, vršiti provjeru transakcije prije nego je pošalju u sustav itd.

Najviše funkcija imaju novčanici u izvedbi za **klasična računala**. Mnogi od njih su u mogućnosti čuvati cjelokupnu bazu podataka svih transakcija (cijeli blockchain) i u stvarnom vremenu vršiti provjere pojedinih transakcija preko priključenih čvorova mreže. Na taj način moguće je pružiti preduvjete za zadovoljenje najviših sigurnosnih standarda u tehničkom smislu, jer nisu potrebni kompromisi oko veličine uređaja, količine memorije,

[42] DOWD, Kevin, HUTCHINSON, Martin, Bitcoin will bite the dust, *Cato J*, sv. 35, 2015, str. 359,364

[43] GOLDFEDER, Steven *i ostali*, Securing bitcoin wallets via threshold signatures, 2014, str. 13

potrošnje energije, brzine interneta i slično. Osnovni nedostatak je što klasična računala nisu uvijek dostupna, odnosno praktična za prenošenje.

Ovdje dolazimo do **mobilnih uređaja ili pametnih telefona**. Uz korištenje mnogobrojnih mobilnih aplikacija ovi uređaji poprimaju sve više funkcija, pa tako i funkcionalnost mobilnih bitcoin novčanika. Ovako implementirana rješenja vrlo su praktična i dostupna. Funkcionalnost u nekim slučajevima i nadmašuje onu kod klasičnih računala, jer su dostupne kamere za skeniranje kodova, te moderna NFC tehnologija za bez-kontaktno plaćanje. Nedostatak je što se mobilni uređaji lako izgube ili bivaju ukradeni, pa se na taj način gubi i vrijednost pohranjena u njima.

Web aplikacije u funkciji novčanika vrlo su praktične. Sadrže sve prednosti klasičnih novčanika uz nemogućnost gubljenja i izuzetnu dostupnost, svuda gdje postoji pristup internetu. Sredstva su uvijek i svuda dostupna, nije potrebno imati posebne uređaje, niti ih moramo posjedovati, web novčanici pristupačni su sa svakog računala spojenog na Internet koje ima internetski preglednik. Nedostatak ovih rješenja je pouzdanost, odnosno potrebno je imati povjerenje u organizaciju koja nudi navedene usluge.[44] U slučaju da sustav nije dobro osiguran, postoji opasnost od krađe. Ovakav tip kriminala se dogodio već nekoliko puta do sada.[45] [46] [47] [48]

Specijalizirani uređaji u funkciji novčanika po svojim prednostima i nedostacima mogu se usporediti sa onima za pametne telefone, pa za njih vrijedi isto što i za mobilne uređaje.

---

[44] The Ill Wind of Bitcoin Exchange Hackings - Once Bitten, Twice Shy!! (Part 1), *NEWSBTC*, 20-ruj-2015, Dostupno na: http://www.newsbtc.com/2015/09/20/the-ill-wind-of-bitcoin-exchange-hackings-once-bitten-twice-shy-part-1/. [Pristupljeno: 15-svi-2017]

[45] HERN, Alex, Bitcoin site Inputs.io loses £1m after hackers strike twice, *The Guardian*, 08-stu-2013, Dostupno na: https://www.theguardian.com/technology/2013/nov/08/hackers-steal-1m-from-bitcoin-tradefortress-site. [Pristupljeno: 15-svi-2017]

[46] WHITTAKER, Zack, Bitstamp exchange hacked, $5M worth of bitcoin stolen, *ZDNet*, Dostupno na: http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/. [Pristupljeno: 15-svi-2017]

[47] Nearly $2M in bitcoins feared lost after Chinese cryptocurrency exchange hack, *Tech in Asia*, 16-velj-2015, Dostupno na: https://www.techinasia.com/bitcoins-lost-after-china-cryptocurrency-exchange-hack-bter. [Pristupljeno: 15-svi-2017]

[48] HURLBURT, George F., BOJANOVA, Irena, Bitcoin: Benefit or Curse?, *IT Prof.*, sv. 16, izd. 3, 2014, str. 13

Zapis adresa na bilo kakvom mediju je još jedna od opcija. Ukoliko nemate povjerenja u tehničke naprave, bitcoin-e možete jednostavno isprintati na papir i kako takve čuvati na načine kako se čuvaju klasične papirne novčanice.

3.3 Bitcoin transakcije

Bitcoin transakcija realizira se u obliku razmjene poruka između računala platitelja odnosno pošiljatelja vrijednosti i sustava računala bitcoin mreže, tzv. skupina rudara (*Mining pools*) koji sudjeluju u procesu potvrde transakcija.[49] Komunikacija se odvija putem standardnog internetskog komunikacijskog protokola u šifriranom obliku. Komunikacijski protokol je detaljno definiran i javno dostupan svima. U tehničkom smislu to je dosta kompliciran proces i na sreću, obični korisnik ga nema potrebu detaljno razumjeti. Ovdje će biti prikazani samo najosnovniji principi, kako bi se moglo pristupiti analizi primjenjivosti i omogućiti korištenje na zadovoljavajućem sigurnosnom nivou.

[49] ZOHAR, Aviv, Bitcoin: under the hood, *Commun. ACM*, sv. 58, izd. 9, 2015, str. 108,110

Slika 3 - Prikaz nekoliko bitcoin transakcija[50]

Prilikom prijenosa određenog iznosa novčanih jedinica s jednog računa na drugi, računalni program elektroničkog novčanika prvo provjerava trenutno stanje salda korisnika, provjeravajući 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 algoritmom pokušava se kombinirati traženi iznos iz postojećih adresa. Ukoliko je to kombiniranje moguće, transakcija se šalje svim čvorovima (*eng. nodes*) na potvrdu ili ovjeru. U slučaju da je nemoguće iskombinirati traženi iznos, uzima se najbliži mogući veći iznos, a ostatak se kroz istu transakciju vraća pošiljatelju na neku od njegovih postojećih adresa. Na prethodnoj se slici vide tri transakcije. Lijevo od zelene strelice su adrese sa kojih se šalje određeni iznos novca na adresu ili adrese s desne strane. Vidljivo je kako se pojedina transakcija često odvija između nekolicine polaznih i najčešće dvije dolazne adrese, jedna primatelja novca i druga pošiljateljeva radi povrata viška iznosa. Treća transakcija je primjer s povratom dijela iznosa na istu adresu s koje je izvršen transfer.

[50] Bitcoin Block Explorer - Blockchain, Dostupno na: https://blockchain.info/. [Pristupljeno: 11-velj-2017]

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.

3.4 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 svih korisnika (odnosno njihovih eloktroničkih novčanika). Primljene transakcije spremaju se u memorijski prostor primatelja (*eng. memory pool*) gdje čekaju da budu zapakirane u novi blok transakcija, 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.[51] Svakim slijedećim 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 samih transakcija, oznake bloka, potpisa prethodnog ovjerenog bloka itd. u blok ugrađuje i jedan proizvoljan broj (*u eng. jeziku nazvan nonce*), promjenom kojega (pošto su sve ostale komponente bloka strogo definirane) može utjecati na potpis (*eng. hash*) samog bloka. Sustav je projektiran tako da zahtjeva hash manji od zadane vrijednosti.[52] 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

[51] DWYER, Gerald P., The economics of Bitcoin and similar private digital currencies, *J. Financ. Stab.*, sv. 17, 2015, str. 81–91

[52] ZOHAR, Aviv, Bitcoin: under the hood, *Commun. ACM*, sv. 58, izd. 9, 2015, str. 108,110

količinom novostvorenih novčanih jedinica. Na taj način motiviraju se rudari za svoj doprinos i istovremeno u opticaj pušta nova količina novca.[53]

Brzina kojom se dodaju novi blokovi u centralni dnevnik sustavno je regulirana i podešena na približno 10 minuta. Ona ovisi o ukupnoj procesorskoj snazi sustava koji računa hash (*eng. hashrate*) i težini zadatka, odnosno zahtijevajući hash manji od određene vrijednosti. Ukoliko se *hashrate* sustava ubrza i novi blokovi počnu pristizati brže, sustav se automatski korigira povećavajući težinu zadatka sve dok ne postigne željenu brzinu zapisa od jednog bloka svakih 10 minuta.

To znači da za potvrdu bitcoin transakcije treba čekati bar 10 minuta, a ako se radi o većim transakcijama, preporuka je čekati nekoliko (5-6) potvrda, što znači približno 1 sat. Ovako dugo vrijeme ovjere transakcije jedan je od najjačih odbijajućih tehničkih čimbenika za prihvaćanje blockchain tehnologije od strane banaka.

Ovakav način potvrde transakcija naziva se *eng. Proof of work*[54] 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. U teoriji, za zapis lažne transakcije u sustav potrebno je raspolagati sa više od pola ukupne procesorske snage sustava (kontrolirati više od pola čvorova pod uvjetom da su jednake snage).[55] To je u praksi teško postići i o tome pišu brojne studije. 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

[53] DWYER, Gerald P., The economics of Bitcoin and similar private digital currencies, *J. Financ. Stab.*, sv. 17, 2015, str. 81–91

[54] OKUPSKI, Krzysztof, Bitcoin Developer Reference, *Availabl E Httpenetium ComresourcesBitcoin Pdf*, 2014, str. 2

[55] HARWICK, Cameron, Cryptocurrency and the Problem of Intermediation, 2015, str. 571

električne energije. Iz tog razloga javljaju se alternativna rješenja korištena u mnogim novim digitalnim valutama.

3.5 POS odnosno „proof of steak“ nasuprot POW sustavu

Za razliku od POW[56] sustava kojega koristi Bitcoin, ideja POS sustava bazira se na pretpostavci da najveći većinski vlasnici valute imaju najveću motivaciju za održavanje vjerodostojnosti sustava. Stoga u takvom sustavu nema potrebe za tzv. rudarenje. Ovjera bloka vrši se konsenzusom, 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, promjena software-a, protokola i slično. Sustav bi u takvim slučajevima prestao biti decentraliziran.

Osim POW i POS algoritama, postoje i drugi, kao i kombinacije spomenutih algoritama. Cijeli sustav blockchain-a u tehničkom smislu zamišljen je tako da se pojedini dijelovi mogu unapređivati i po potrebi mijenjati, ako postoji volja većine da se nove promjene i prihvate.

Sustav je predstavljen u obliku otvorenog koda, transparentan je i kao takav pristupačan zajednici za korištenje i unapređivanje. Iz toga razloga je malo vjerojatno da bi se kao prepreka u korištenju i prihvaćanju digitalnog novca, mogla ispriječiti neka tehnička osobina sustava (dugoročno gledano).

[56] OKUPSKI, Krzysztof, Bitcoin Developer Reference, *Availabl E Httpenetium ComresourcesBitcoin Pdf*, 2014, str. 2

4 EKONOMSKI ASPEKTI DIGITALNIH VALUTA

U ovom poglavlju daje se pojmovno određenje digitalnih valuta, njihova usporedbe s elektroničkim novcem i kategorizacija prema stavovima vodećih europskih i svjetskih financijskih institucija. Analiziraju se najvažnija obilježja digitalnih valuta, kao i njihova pristupačnost i praktična uporaba.

4.1 Pojmovno određenje digitalnih valuta

Da bismo odgovorili na ovo pitanje, potrebno je objasniti neke osnovne pojmove koji se ovdje spominju. U literaturi se koristi nekoliko naziva za digitalne valute. Najčešći su još i kriptovalute (*eng. cryptocurrencies*), virtualne valute (*eng. Virtual currencies*), virtualni novac (*eng. Virtual money*), digitalni novac (*eng. Digital money*), digitalne valute (*eng. Digital currencies*). U ovom radu koristi se posljednji termin „digitalne valute“, odabran isključivo po kriteriju popularnosti na internetu. On se može uzeti kao sinonim za ostale navedene popularne izraze, kojima se nazivaju valute bazirane na blockchain sustavu.

Europska centralna banka odlučila se za naziv „*Virtual currency schemes"* što bi se moglo prevesti sa „virtualne valutne sheme“. U nazivu je dodana riječ shema kako bi se naglasilo da se radi o sustavu više komponenti, od kojih je jedna (ključna i karakteristična) komponenta i sam informacijski sustav na kojem se temelji postojanje valute, odnosno bez čije pomoći valuta ne bi mogla funkcionirati.[57] Gotovo sve funkcije tog sustava u praksi se moraju obavljati uz uporabu računala i telekomunikacijske tehnologije, pa stoga ima smisla promatrati virtualne valute na ovaj način, (kao sustav) jer drugačije ne mogu postojati. Nasuprot tome, klasični novac može ispuniti svoju funkciju i u digitalnom obliku i u klasičnom obliku, pa za njegovu uporabu teorijski gledano informacijska tehnologija nije presudna (iako je danas nezamisliva isključivo klasična uporaba novca, bez korištenja informacijske tehnologije).

[57] Virtual currency schemes, lis-2012, Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. [Pristupljeno: 20-ožu-2017]

Pojedini korišteni pojmovi kod različitih autora često nemaju u potpunosti jednaka značenja, pa ih je potrebno definirati. Navedene definicije preuzete su od Europske centralne banke:[58]

- **Novac** je sve što se uobičajeno koristi za razmjenu vrijednosti. Djeluje kao sredstvo razmjene, skladištenje vrijednosti i obračunska jedinica. U tom smislu, pojam novca širi je od pojma valute.
- **Valuta** je kovani ili tiskani novac, obično ima oblik novčića i novčanica. Kada se odnosi na (određenu) valutu, poput eura ili američkog dolar, značenje postaje konceptualno, tj. zastupa vrijednosti koje su nastale na osnovu zakona i/ili države.
- **Fiducijarna valuta (novac)** je valuta bez vlastite vrijednosti, ona dobiva svoju vrijednost od povjerenja koje imaju korisnici u izdavatelja valute.
- **Fiat valuta (novac)** je uspostavljena od strane vlade ili središnje banke kao jedna vrsta medija za obavljanje transakcija (npr. euro, dolar, kuna).
- **Virtualna valuta** je digitalni prikaz vrijednosti, koji ne izdaje središnja banka, kreditna institucija ili institucija za e-novac, a koja se u nekim okolnostima, može se koristiti kao alternativa za novac.
- **Virtualna valutna shema** (*eng. Virtual currency scheme*) se koristi za opisivanje oba aspekta prijenosa vrijednosti, odnosno virtualnih valuta i izgrađenih tehničkih sustava ili mehanizama koji osiguravaju da ta vrijednost može biti prenesena odnosno korištena.
- **Blockchain** je dnevnik ili knjiga zapisa svih transakcija, grupiranih u blokove, napravljenih s (decentraliziranim) sustavom virtualne valute sheme.

Treba napomenuti da se pojmovi virtualnog i digitalnog ili elektroničkog novca kod nekih autora spominju i u kontekstu digitalne odnosno elektroničke inačice klasičnog novca. Kao primjer možemo uzeti sustav elektroničkog bankarstva ili sustav kartičnog plaćanja. Takvi primjeri nisu primarna tema ovog rada. Umjesto toga, fokus je stavljen na decentralizirane digitalne valute bazirane na blockchain tehnologiji.

[58] Ibid.

4.2 Odnos virtualnih valutnih shema i elektroničkog novca

Osnovne sličnosti i razlike između decentraliziranih virtualnih valutnih shema i elektroničkog novca bile bi slijedeće:[59]

- **Format, pojavnost novca**: U oba slučaja valuta se pojavljuje u digitalnom obliku. Postoji mogućnost prijenosa vrijednosti virtualnih valutnih shema na druge medije, npr. tisak na papir, ali to ne treba miješati sa tiskom klasičnih novčanica. Funkcija takvog medija je isključivo kao materijalnog nositelja informacije, nemoguće ga je falsificirati u klasičnom smislu riječi jer je nositelj vrijednosti skup znakova, koji predstavlja određeni ključ potreban za trošenje novca. Poznavanje ključa je ujedno i posjedovanje vrijednosti.
- **Obračunska jedinica**: Kod elektroničkog novca obračunska jedinica je klasična valuta (USD, EUR, GBP, HRK…). Virtualne valutne sheme obračunavaju se u vlastitim obračunskim jedinicama (Bitcoin, Litecoin, Ethereum …)
- **Stjecanje valute**: Elektronički novac stječemo preuzimanjem direktno od izdavača, u digitalnom ili stvarnom obliku, koji se zajednički prate na računu korisnika, ili primanjem uplata na račun ili u naravi po različitim osnovama. Virtualne valutne sheme stječu se kupovinom ili trgovinom unutar virtualne zajednice korisnika.
- **Pravna reguliranost:** Elektronički novac u potpunosti podliježe regulativi klasičnih valuta, koju provode nacionalne institucije država (nacionalne banke i vlast). Virtualne valutne sheme nisu centralizirano upravljane, a često nisu niti pravno regulirane, odnosno u njihovoj regulaciji sudjeluje svaki član zajednice. Konsenzus većine korisnika proveden korištenjem određenih tehničkih sustava je osnovni regulator sustava.
- **Izdavač:** Kod elektroničkog novca to je legalno ustanovljena institucija. Kod virtualnih valutnih shema izdavač je privatna tvrtka, pojedinac ili udruga. Bilo tko u tehničkom smislu zapravo može biti izdavač svoje valute.
- **Ponuda novca:** Ponuda elektroničkog novca posljedica je ponude i potražnje bazne ili klasične valute. Regulirana je od strane izdavatelja (vlasti) i ujedno služi kao fiskalni regulator ekonomije izdavatelja. Puštanje u optjecaj ili povlačenje novca iz

[59] Ibid.

opticaja podložno je strogoj kontroli i regulativi. Nasuprot tome, kod virtualnih valutnih shema ponuda je najčešće fiksna ili slijedi neki unaprijed predvidivi algoritam. Moguća je i varijanta kod koje izdavatelj regulira ponudu, ali takva rješenja nisu popularna iz jednostavnog razloga što se poništava osnovna prednost sustava, decentraliziranost.

- **Mogućnost otkupa sredstava:** Elektronički novac kao ekstenzija zakonskog sredstva plaćanja podrazumijeva neograničenu mogućnost otkupa od strane izdavača. Tečaj je uglavnom rezultat tržišta klasičnih valuta i u većini slučajeva je relativno stabilan. Kod virtualnih valutnih shema, ne postoji garancija otkupa sredstava, odnosno takva garancija nema previše smisla ako se kao obračunska jedinica koristi sama virtualna valuta. Tržište odnosno ponuda i potražnja glavni su regulatori tečaja u odnosu na klasične valute.[60] Volatilnost je vrlo velika i vrijednost valute nije garantirana. Zapravo mogućnost otkupa i prihvaćenost valute direktno utječu na njenu tržišnu vrijednost.
- **Nadzor i kontrola:** Kod elektroničkih inačica klasičnih valuta nadzor i kontrola provode se jednako kao i za klasični novac, od strane legalnih institucija. Pravni okvir je definiran, a sudska praksa je obimna. Virtualne valutne sheme vrlo su slabo pravno regulirane i mnoge države se još nisu u dovoljnoj mjeri odredile glede njihovog statusa. U većini slučajeva gdje se ne smatraju novcem u pravnom smislu, prema njima se odnosi kao prema vrijednosnicama.
- **Sigurnost i rizik:** Elektronička inačica klasičnih valuta donosi novu, tehničku komponentu sustava te s tim i novi faktor rizika. U praksi ovo je operativni rizik i ne predstavlja prepreku za korištenje, odnosno dobrobit sustava nadmašuje nedostatke. Kod virtualnih valutnih shema osim operativnog rizika, postoje značajni pravni i ekonomski rizici, koje korisnici u potpunosti preuzimaju. Takvi rizici u konačnici značajno utječu na vrijednost valute, odnosno na tečaj i likvidnost, te su puno značajniji od tehničkih i operativnih rizika.

[60] PLASSARAS, Nicholas A., Regulating digital currencies: bringing Bitcoin within the reach of IMF, *Chic. J. Int. Law*, sv. 14, 2013, str. 377

4.3 Jesu li digitalne valute novac?

U kojoj mjeri je neko sredstvo korišteno u ulozi novca varira od osobe do osobe i od vremena do vremena. U teoriji, digitalne valute mogle bi poslužiti kao novac za bilo koga s podrškom za internet i uz korištenje odgovarajućih računala ili uređaja. Trenutno, međutim, digitalne valute ispunjavaju ulogu novca samo u određenoj mjeri i samo za mali broj ljudi. Broj ljudi koji ih koristi u punom smislu kao novac vjerojatno se može mjeriti u tisućama, a njihova uporaba je čak i onda samo usporedo s tradicionalnim valutama korisnika, a ne isključivo.[61] Ipak, promatrajući trendove, teško je vjerovati da će tako ostati.

Jedan od načina potvrde digitalnih valuta kao novca je i promatranje u kojoj mjeri one ispunjavaju tri osnovne funkcije novca, kao jedinice mjere vrijednosti (obračunske jedinice), kao sredstva razmjene vrijednosti i kao sredstva za pohranu odnosno čuvanje vrijednosti.[62] Kako je Bitcoin najraširenija valuta, na njegovom primjeru je načinjena većina analiza.[63]

Zbog same prirode digitalnih valuta odnosno anonimnosti, teško je procijeniti koliko pojedina valuta ima korisnika. Moguće je saznati koliko je digitalnih novčanika (*eng. Digital wallet*) za većinu valuta, ali kako svaki korisnik može imati neograničen broj novčanika, možemo jedino sa sigurnošću reći da je broj korisnika značajno manji.[64] Mnogi korisnici koriste mogućnost posjedovanja više novčanika, a postoji i dosta napuštenih ili izgubljenih novčanika koje su njihovi korisnici otvorili za određene potrebe testiranja samog sustava, i nakon prestanka uporabe ih jednostavno napustili.

Digitalne valute kao obračunske jedinice: Postoji vrlo malo podataka o bilo kojoj digitalnoj valuti koji bi upućivali na korištenje digitalne valute kao obračunske jedinice. Iako se obavlja jedan mali broj transakcija između pojedinaca u kojem su se stranke dogovarale za cijenu u npr. bitcoin-ima, to su uglavnom izolirani i nepovezani slučajevi.

[61] ALI, Robleh *i ostali*, The economics of digital currencies, 2014, str. 279

[62] Ibid.

[63] LO, Stephanie, WANG, J. Christina, Bitcoin as money?, 2014, str. 4

[64] RAYMAEKERS, Wim, Cryptocurrency Bitcoin: Disruption, challenges and opportunities, *J. Paym. Strategy Syst.*, sv. 9, izd. 1, 2015, str. 32

Trgovci koji bi svoje cijene iskazivali u nekoj od digitalnih valuta, morali bi ih ažurirati vrlo često kako bi održali željenu vrijednost odnosno stabilnu cijenu u odnosu tradicionalne valute, npr. EUR ili USD. To je naravno posljedica visoke volatilnosti digitalnih valuta.

Iako sve veći broj tvrtki radi olakšavanja plaćanja i pojednostavljenja iskazuju svoje cijene u npr. bitcoin-ima, to čine paralelno sa korištenjem klasičnih cjenika, koristeći digitalnu valutu kao privremeni medij plaćanja. Banke zapravo nisu svjesne ovih transakcija, jer u konačnici na račune dolazi klasični novac.[65]

Digitalne valute kao medij razmjene vrijednosti: Jedan od pokazatelja u kojoj mjeri se valuta koristi kao sredstvo razmjene je broj trgovaca koji su je spremni prihvatiti u plaćanju. Trenutno, postoji nekoliko tisuća trgovaca diljem svijeta (uglavnom, ali ne isključivo, internetskih trgovina) koje primaju uplate u bitcoin-ima. Spremnost trgovaca da prihvate digitalnu valutu sama po sebi ne podrazumijeva, da se ta mogućnost naširoko koristi.

Jači pokazatelj da određena digitalna valuta vrijedi kao sredstvo razmjene je broj transakcija provedenih od strane svojih korisnika u određenom vremenskom razdoblju, kao i vrijednost ukupnog broja transakcija u određenom periodu. U tom smislu vidljiv je značajan trend porasta. Prema coinmarketcap.com, vidimo da ukupna vrijednost dnevnog prometa prvih 100 najjačih digitalnih valuta premašuje 900 000 000 USD.[66]

Digitalne valute kao medij za čuvanje ili pohranu vrijednosti: Vrijednost novca općenito bazira se na sadašnjem i budućem vjerovanju korisnika u njegovu ponudu i potražnju. Kako u slučaju decentraliziranih digitalnih valuta ne postoji centralni autoritet koji ih kontrolira, njihova je vrijednost isključivo u povjerenju korisnika. Ponuda je uglavnom predvidljiva i relativno sigurna zahvaljujući ugrađenim mehanizmima samih sustava, ali potražnja ovisi o više čimbenika i prilično je neizvjesna. Zbog toga digitalne valute zasigurno nisu pogodan medij za kratkoročno čuvanje vrijednosti. Što se tiče dugoročnog čuvanja vrijednosti, mišljenja su podijeljena u dvije struje. Prva koju čine formalne institucije i banke govori da su ulaganja u digitalne valute visoko rizična. Druga pak, kaže da se može očekivati velik

[65] ALI, Robleh *i ostali*, The economics of digital currencies, 2014, str. 279

[66] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/. [Pristupljeno: 31-ožu-2017]

porast vrijednosti, pa bi zato bilo zgodno ulagati u digitalne valute. Oba stava imaju određene argumente. U svakom slučaju, nedovoljna pravna reguliranost digitalnih valuta je već sama po sebi razlog za njihovo nekorištenje za dugoročnu čuvanje vrijednosti, osim u slučajevima spremnosti na visok špekulativni rizik.[67]

4.4 Pregled tržišta digitalnih valuta

Danas na tržištu postoje brojne digitalne valute, prema mnogim izvorima procjenjuje se da ih ima preko 700 aktivnih, a računajući i one ugašene broj se penje značajno iznad 1000.[68] Trenutno je još uvijek vidljiv trend porasta i broja valuta i tržišne kapitalizacije. Pri tome valja naglasiti da dobar dio valuta zbog vrlo male kapitalizacije nema ekonomskog značaja.

Najbolji pokazatelji popularnosti digitalnih valuta su tržišna kapitalizacija i dnevni promet.

Prema tržišnoj kapitalizaciji na dan 31.03.2017. :

- preko 10000 mil. USD vrijedi 1 digitalna valuta
- preko 1000 mil. USD vrijede 2 digitalne valute
- preko 100 mil. USD vrijedi 9 digitalnih valuta
- preko 10 mil. USD vrijede 42 digitalne valute
- preko 1 mil. USD vrijedi više od 100 digitalnih valuta

Ukupna kapitalizacija prvih 100 valuta iznosi više od 25 milijardi $. Za usporedbu, u veljači 2014. godine svega 34 valute vrijedilo je preko 1 mil. $.[69] Aktualnim trendom, ukupna kapitalizacija se svake godine gotovo utrostruči.

[67] ALI, Robleh *i ostali*, The economics of digital currencies, 2014, str. 279

[68] KOBLITZ, Neal, MENEZES, Alfred J., Cryptocash, cryptocurrencies, and cryptocontracts, *Des. Codes Cryptogr.*, sv. 78, izd. 1, 2016, str. 9

[69] GANDAL, Neil, HALABURDA, Hanna, Competition in the Cryptocurrency Market, *Bank Can. Work. Pap.*, sv. No. 2014-33, 2014, str. 8

Moguće je izvući određene zaključke uporabe i iz usporedbe transakcija prema najvažnijim klasičnim valutama. Gledajući primjer Bitcoin-a u razdoblju od 30 dana 2014 godine [70] :

- 60% transakcija obavljeno je za CNY
- 32% transakcija obavljeno je za USD
- 3% transakcija obavljeno je za EUR
- 1,2% transakcija obavljeno je za GBP

Tablica 2 - Porast tržišne kapitalizacije svih značajnijih virtualnih valuta zadnje 3 godine prema coinmarketcap.com[71]

Datum:	Tržišna kapitalizacija svih značajnijih virtualnih valuta u 1.000.000.000 USD
05.04.2017.	26,96
05.04.2016.	8,15
01.04.2015.	3,87

Prema coinmarketcap.com[72] trenutno je 782 aktivne digitalne valute, od kojih 605 ima zabilježenu bilo kakvu tržišnu kapitalizaciju.

Ovaj popis nije potpun. Mnoge valute nastaju gotovo svakodnevno, a samo one najlikvidnije predmet su trgovine na tržištu i nabrojane na coinmarketcap.com, dok su ostale izostavljene zbog premale likvidnosti. Međutim, postojanje mnogih nevažnih digitalnih valuta ne umanjuje činjenicu da važnost tzv. altcoin valuta raste u smislu alternativnih investicijskih opcija.[73] Altcoins se nazivaju alternativne implementacije digitalnih valuta baziranih na blockchain tehnologiji (**alt**ernativa bit**coin**-u, odakle dolazi i naziv).

[70] ALI, Robleh *i ostali*, The economics of digital currencies, 2014, str. 279

[71] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/. [Pristupljeno: 31-ožu-2017]

[72] All Currencies | CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/all/views/all/. [Pristupljeno: 05-tra-2017]

[73] ELENDNER, Hermann *i ostali*, The Cross-Section of Crypto-Currencies as Financial Assets: An Overview, Sonderforschungsbereich 649, Humboldt University, Berlin, Germany, 2016, Dostupno na: https://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2016-038.pdf. [Pristupljeno: 05-tra-2017]

Slika 4 - Prikaz kretanja cijene zadnjih godinu dana - Ethereum[74]

Slika 5 - Prikaz kretanja cijene zadnjih godinu dana - Litecoin[75]

[74] All Currencies | CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/all/views/all/. [Pristupljeno: 05-tra-2017]

[75] Ibid.

Slika 6 - Prikaz kretanja cijene zadnjih godinu dana - Ripple[76]

Na dan 31.8.2016. udio Bitcoina u tržišnoj kapitalizaciji iznosio je 81%.[77] Na dan 31.3.2017. je udio Bitcoina 67%.[78] Očiti je jači trend rasta alternativnih valuta u odnosu na Bitcoin. U 2014. godini, nove altcoin valute su se stvarale gotovo svaki dan, s brojem od 69 u siječnju 2014. do 590 u prosincu 2014. Rast u aktivnih altcoina je usporen do lipnja 2015. tako da se broj aktivnih valuta od tada kreće između 650 do 770.

Postoje dvije vrste digitalnih valuta prema načinu implementacije. Primjeri valuta kao Bitcoin, Litecoin, Peercoin, Dogecoin itd. bazirani su na implementaciji vlastite blockchain arhitekture, dok npr. Augur, MadeSafeCoin, Golem, DigixDAO, StorjcoinX koriste platforme treće strane.

Implementacija vlastite blockchain tehnologije složen je i zahtjevan proces, koji zahtijeva veliko tehničko znanje za stvaranje, pa čak i samo za kloniranje postojeće blockchain tehnologije. Stvaranje digitalne valute na bazi postojeće tehničke osnove je, s druge strane relativno jednostavan proces i ne zahtijeva veliku tehničku stručnost. Radi se na principu korištenja tehničkih usluga dostupnih uglavnom kao internetski servis.

[76] Ibid.

[77] ELENDNER, Hermann *i ostali*, The Cross-Section of Crypto-Currencies as Financial Assets: An Overview, Sonderforschungsbereich 649, Humboldt University, Berlin, Germany, 2016, Dostupno na: https://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2016-038.pdf. [Pristupljeno: 05-tra-2017]

[78] All Currencies | CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/all/views/all/. [Pristupljeno: 05-tra-2017]

Tablica 3 - Pregled 50 najznačajnijih digitalnih valuta prema tržišnoj kapitalizaciji, na dan 31.03.2017.[79]

	Naziv valute	Tržišna kapitalizacija (mil. $)	Tečaj ($)	Broj jedinica u opticaju	Dnevni promet ($)	% Promjena cijene (24h)
1	Bitcoin	16.939,15	1042,63	16.246.562	403.362.000	0.13%
2	Ethereum	4.627,32	51,26	90.265.018	110.927.000	-3.08%
3	Ripple	665,69	0,017804	37.388.960.792	39.526.700	67.72%
4	Dash	560,18	77,84	7.196.855	26.183.000	-7.19%
5	Litecoin	336,68	6,68	50.419.907	209.775.000	53.89%
6	Monero	295,07	20,77	14.209.408	5.778.410	-1.64%
7	Ethereum Classic	242,86	2,69	90.223.401	22.969.800	13.94%
8	NEM	130,86	0,01454	8.999.999.999	616.650	-2.97%
9	Augur	110,45	10,04	11.000.000	1.385.860	6.17%
10	MaidSafeCoin	70,71	0,15624	452.552.412	596.408	-3.62%
11	Zcash	67,76	69,04	981.581	4.864.620	10.26%
12	Golem	66,53	0,081136	820.000.000	9.845.100	16.20%
13	Tether	54,95	1	54.950.856	29.270.000	0.00%
14	Decred	52,64	11,53	4.563.830	1.723.900	-5.93%
15	Iconomi	52,43	0,602631	87.000.000	992.324	-8.57%
16	PIVX	46,07	0,87449	52.686.558	1.495.880	32.43%
17	DigixDAO	42,02	21,01	2.000.000	485.676	6.45%
18	Steem	41,59	0,176379	235.796.032	840.980	12.60%
19	Waves	37,34	0,373397	100.000.000	365.596	-7.69%
20	Dogecoin	35,96	0,000331	108.755.928.597	2.359.740	22.54%
21	Factom	33,71	3,85	8.753.219	3.408.300	-9.87%
22	Lisk	32,82	0,312421	105.056.650	986.454	-7.56%
23	First Blood	31,73	0,370898	85.558.371	2.301.800	0.68%
24	Round	31,73	0,037326	850.000.000	121.500	193.34%
25	SingularDTV	28,15	0,046918	600.000.000	36.442	-4.66%
26	Bytecoin	21,56	0,000118	182.678.307.367	687.100	-21.01%
27	Ardor	21,13	0,02115	998.999.495	87.898	0.97%
28	GameCredits	20,27	0,32882	61.659.500	208.176	2.82%
29	BitConnect	19,87	3,43	5.785.821	317.231	2.26%
30	Melon	19,17	31,98	599.400	170.043	0.87%
31	Stellar Lumens	18,84	0,002695	6.991.236.609	2.691.020	31.44%
32	Stratis	18,83	0,191524	98.326.995	464.184	-9.15%
33	Siacoin	18,62	0,000757	24.607.743.872	860.496	18.62%
34	BitShares	17,85	0,006885	2.592.350.000	930.258	6.64%
35	Komodo	16,92	0,167911	100.770.034	156.515	-0.64%
36	Peercoin	15,46	0,644895	23.979.495	834.068	12.28%
37	Nexus	15,08	0,313122	48.150.366	43.312	-5.23%
38	Nxt	14,09	0,014102	998.999.983	482.401	8.69%
39	Emercoin	13,41	0,336983	39.791.344	250.487	-1.37%
40	Namecoin	10,43	0,7078	14.736.400	1.374.020	22.57%
41	AntShares	10,33	0,206602	50.000.000	427.253	-2.69%
42	BitcoinDark	10,29	7,98	1.288.862	1.630.450	3.57%
43	ShadowCash	9,78	1,47	6.645.046	205.480	-2.91%
44	Storjcoin X	9,59	0,187827	51.053.144	71.710	-6.37%
45	Counterparty	9,32	3,56	2.619.561	99.459	-2.88%
46	Byteball	9,21	67,03	137.442	29.369	9.92%
47	SysCoin	9,03	0,017239	523.750.980	1.128.120	-10.01%
48	Gulden	8,62	0,025137	342.899.445	20.020	-1.02%
49	Xaurum	8,43	0,093736	89.971.116	41.146	0.24%
50	ZCoin	8,24	4,65	1.774.505	616.326	-5.41%

4.5 Kategorizacija digitalnih valuta prema interakciji sa klasičnim valutama

Prema Europskoj centralnoj banci (ECB), postoji više tipova virtualnih valutnih shema, prema tome u kakvom su odnosu prema stvarnim valutama, i prema načinima kako se stječu. Neki tipovi uopće nisu decentralizirani niti bazirani Blockchain tehnologiji, ali ih je potrebno spomenuti zbog potpunijeg pregleda i analize njihovog utjecaja na nastanak novih decentraliziranih valuta.

Odnosi virtualnih valutnih shema prema stvarnim valutama jedan su od boljih pokazatelja njihovog općeg ekonomskog značaja, i uz odgovarajuću teoretsku osnovu omogućuju lakše prognoziranje njihovog razvoja i uloge u budućnosti. Njihova interakcija sa stvarnim novcem odvija se kroz razmjenu pojedine virtualne valute za stvarni novac, te kroz mogućnost kupnje i prodaje dobara. Promatrajući moguće smjerove tijeka stvarnog novca u takvim razmjenama, možemo razlučiti tri karakteristična tipa virtualnih valutnih shema:[80]

- Zatvoreni sustavi virtualnih valutnih shema
- Virtualne valutne sheme s jednosmjernim protokom
- Virtualne valutne sheme s dvosmjernim protokom

Zatvoreni sustavi virtualnih valutnih shema

Zatvoreni sustavi virtualnih valutnih shema nemaju gotovo nikakvih ekonomskih, financijskih niti monetarnih učinaka, ili bar ne više nego bilo koja roba ili usluga dostupna na tržištu. Koriste se za kupnju i prodaju virtualnih roba i usluga u zatvorenim sustavima (virtualnim tržištima). Nije ih moguće koristiti izvan tih virtualnih zajednica, ili je takvo korištenje zabranjeno. U pravnom smislu, takve valute najčešće se ograđuju od uloge konkurenta stvarnom novcu. Primjer su različite valute ili „zlato“ u računalnim igrama. Način stjecanja takvog novca moguć je isključivo kroz postizanje određenih rezultata ili ciljeva u igri. Trgovanje izvan sustava je najčešće zabranjeno od strane autora, kako bi se

[79] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/. [Pristupljeno: 31-ožu-2017]

[80] Virtual currency schemes, lis-2012, Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. [Pristupljeno: 20-ožu-2017]

izbjegao sukob sa zakonom. Smisao ovakvih sustava je u omogućavanju određenih funkcija i mogućnosti u pruženoj usluzi ili prodanom proizvodu, odnosno dodanoj vrijednosti.

Iako ovakve valute nisu namijenjene trgovini izvan svog matičnog sustava, u određenim slučajevima javlja se efekt njihove stvarne ponude i potražnje, te trgovine ili razmjene za stvarni novac. Kao posljedica, takve valute ravnopravno mogu poslužiti i za različite ilegalne aktivnosti, npr. igre na sreću ili slične aktivnosti.

U takvim slučajevima, moglo bi se govoriti o određenim ekonomskim efektima, ali su oni zbog gotovo beznačajnog udjela takve trgovine na tržištu zanemarivi.

Virtualne valutne sheme s jednosmjernim protokom

Virtualne valutne sheme s jednosmjernim protokom mogu se kupovati za stvarni novac, ali se za njih ne može dobiti stvarni novac (ne mogu se prodavati). Najsličnije su nekim tipovima bonova za koje možemo dobiti određene virtualne ili stvarne usluge i proizvode. Uvjeti konverzije i tečaj kontrolirani su od strane izdavatelja. Jednako kao i kod zatvorenih sustava, radi se o centraliziranim valutama.

Jedan od poznatijih primjera su tzv. Facebook krediti (FB) (*eng. Facebook credits*) predstavljeni 2009. godine, korišteni za kupovinu dobara i usluga iz aplikacija na Facebook platformi. Valuta je startala kao zamjena za dolar, odnosno mogla se kupiti po tečaju 1 FB = 1 USD, dok zamjena u obrnutom smjeru nije bila moguća. Mogla se koristiti za kupnju stvarnih roba i usluga oglašavanih na Facebook platformi. Stjecanje valute bilo je moguće putem kreditnih kartica i PayPal sustava plaćanja. Par godina kasnije, 2012. kompanija je odlučila konvertirati salda korisnika u lokalne valute, zbog pojednostavljenja korištenja usluge, ali vjerojatno i zbog izbjegavanja sukoba sa različitim pravnim regulativama pojedinih zemalja.[81]

[81] Introducing subscriptions and local currency pricing, *Facebook for Developers*, Dostupno na: https://developers.facebook.com/blog/post/2012/06/19/introducing-subscriptions-and-local-currency-pricing/. [Pristupljeno: 24-tra-2017]

Virtualne valutne sheme s dvosmjernim protokom

Virtualne valutne sheme s dvosmjernim protokom moguće je razmjenjivati za stvarne valute, njihova vrijednost utvrđena je tržišnim tečajem i kao takve vrlo su slične digitalnim inačicama stvarnih valuta. Mogu biti centralizirane valute pod kontrolom izdavatelja ili decentralizirane, bazirane na Blockchain tehnologiji. Dvosmjerne valutne sheme u tehničkom smislu mogu se smatrati novcem. Eventualne prepreke mogu biti ekonomske ili pravne prirode, jer po definiciji novac je osim sredstva razmjene dobara i sredstvo čuvanja vrijednosti i jedinica za mjerenje vrijednosti. U tom smislu može se raspravljati koliko su decentralizirane valute uopće novac, obzirom da se, (bar za sada) gotovo uopće ne koriste kao mjera vrijednosti dobara.

Što se pak tiče centraliziranih valuta, one su najčešće elektronička inačica klasičnih valuta, pa za njih vrijedi i primjenjuje se postojeća pravna i ekonomska regulativa. Osim u raznovrsnijem načinu uporabe i tehničke realizacije, po ničemu drugom ne razlikuju se od klasičnih valuta. U teoriji, mogu biti realizirane i bez uporabe tehničke infrastrukture, za razliku od decentraliziranih, koje egzistiraju isključivo zahvaljujući korištenju modernih tehničkih i tehnoloških rješenja.

4.6 (De)centraliziranost autoriteta izdavatelja kao čimbenik digitalnih valuta

Prije svega ovdje se misli na centraliziranost u smislu postojanja autoriteta izdavatelja, a ne na centraliziranost u smislu izvedbe tehničkog rješenja ili u zemljopisnom smislu.

Jedno od najvažnijih obilježja svake pa i digitalne valute je izdavatelj ili kreator valute. Izdavatelj svake valute, prije pojave digitalnih valuta baziranih na Blockchain tehnologiji, bio je određeni pravni (ili fizički) subjekt, kojega je moguće identificirati, odnosno koji je imao interes biti poznat, jer je jamčio vrijednost i autentičnost valute. Zapravo povjerenje u autoritet izdavatelja ključno je za prihvaćanje svakog fiat novca. Taj autoritet odnosno izdavatelj je najčešće država ili institucija vlasti, iako u praktičnom smislu to može biti bilo tko, čak i bilo koja pravna ili fizička osoba, pod uvjetom da može osigurati usklađenost s važećom pravnom regulativom i povjerenje potencijalnih korisnika valute.

Izdavatelj valute ili sustava plaćanja ključni je čimbenik i za kontrolu sustava. Ako se radi o tiskanom novcu ili novčanicama, on osigurava zadovoljavajuću razinu kvalitete novca kako bi se spriječilo i otežalo krivotvorenje, a ako se radi o elektroničkom sustavu (npr. elektroničkom bankarstvu ili sustavu plaćanja karticama) osigurava primjerenu kvalitetu i sigurnosnu razinu tehničkog rješenja i brine se za njegovo održavanje.

U slučajevima mogućih sporova između korisnika valute, do kojih može doći pri korištenju valute, izdavatelj je taj koji raspolaže relevantnim informacijama potrebnim da se spor razriješi (dnevnici transakcija, evidencije i sl.). Ako postoji tehnička mogućnost poništenja transakcije, on je taj koji to omogućava i kontrolira. Izdavatelj također ima i pravnu odgovornost prema korisnicima valute ili sustava plaćanja, jer upravlja čuvanjem vrijednosti svojih korisnika. U određenim situacijama on i materijalno odgovara za štete u sustavu, proizašle iz nepredviđenih ili kriminalnih događaja koji mogu prouzročiti materijalne gubitke (npr. tehnički kvar bankomata ili sigurnosni propust sustava elektroničkog plaćanja).

Dakle, izdavatelj je bit svake centralizirane valute ili sustava plaćanja, i prema toj činjenici usklađena je i sva pravna regulativa donesena prije pojave decentraliziranih valuta.

Nasuprot tome, Blockchain tehnologija donosi brojne nove mogućnosti i uvodi potpuno novu perspektivu u područje novca, valuta i sustava plaćanja. Za razliku od svih prijašnjih pristupa, sada je moguće korištenjem tehnologije, formalno decentralizirati sustav, odnosno iz njega izbaciti izdavatelja, a njegove ključne funkcije zamijeniti automatiziranim tehničkim rješenjima. Tehnički sustav preuzima funkciju izvršenja i kontrole transakcija, te uz pomoć kriptografije održava zadovoljavajuću razinu sigurnosti. Svi parametri sustava su ili unaprijed programirani, ili su podložni promjeni uz konsenzus većine korisnika. Cijeli sustav je transparentan, od povijesnog pregleda svake pojedine transakcije, do uvida u svaku liniju programskog koda sustava. Svaki korisnik participira u radu sustava, a izdavatelj kao autoritet ne postoji, odnosno cijela zajednica korisnika može se u određenim okolnostima smatrati izdavateljem. Sve relevantne informacije cirkuliraju prema svim korisnicima sustava, omogućavajući uvid i kontrolu svakome.

Na taj način tehnologija se može koristiti za stvaranje novih organizacija baziranih na software-u, koje se nazivaju decentralizirane organizacije (DOs) i/ili decentralizirane autonomne organizacije (DAO). Te organizacije mogu ponovno implementirati određene

aspekte tradicionalnog korporativnog upravljanja pomoću softvera, čime stranke mogu uživati prednosti formalnih korporativnih struktura, uz istodobno zadržavanje fleksibilnosti i opsega neformalnih online grupa. Takve organizacije također mogu egzistirati anonimno, bez pomoći izvan sustava. One mogu posjedovati, razmjenjivati ili trgovati resursima i stupiti u interakciju s drugim ljudima ili strojevima, postavljajući nova pitanja oko tradicionalnih pojmova pravne osobnosti, individualne agencije i odgovornosti.[82]

Uz sve korisne efekte ovog pristupa, javljaju se i neki negativni, od kojih su najznačajniji pitanje odgovornosti za kontrolu sustava, nemogućnost identifikacije kod rješavanje sporova i nemogućnost poništenja transakcije. Jasno je da neke funkcije izdavatelja mogu lako biti automatizirane, a neke (npr. odgovornost) ne. Nepostojanje subjekta odgovornosti sigurno je i jedno od najspecifičnijih obilježja sustava digitalnih valuta.

Postoje i autori koji sumnjaju u decentraliziranost Bitcoin sustava zbog činjenice da su glavne „rudarske" snage koncentrirane u nekoliko velikih čvorova (zbog maksimiziranja zarade od rudarenja), a već samo prva tri najjača čvora premašuju 50% procesorske snage sustava što bi ukoliko se udruže, zadovoljilo teorijski minimum za mogućnosti kompromitiranja sustava.[83]

4.7 Anonimnost digitalnih valuta baziranih na Blockchain sustavu

U teoriji, Blockchain je potpuno automatizirani sustav s mogućnošću pružanja potpune anonimnosti korisnicima. Ipak, pošto svi živimo i djelujemo u određenim pravnim okruženjima i u organiziranim zajednicama vođenim od određenih autoriteta, teško je garantirati anonimnost preko razine koju to dopusti aktualno pravno okruženje. Isto vrijedi i za digitalne valute.

[82] WRIGHT, Aaron, DE FILIPPI, Primavera, Decentralized blockchain technology and the rise of lex cryptographia, 2015, str. 2,3

[83] GERVAIS, Arthur *i ostali*, Is Bitcoin a decentralized currency?, 2014, str. 1

Iako samo tehničko rješenje omogućava praktično potpunu anonimnost transakcija, ono se oslanja na postojeću telekomunikacijsku strukturu koja u određenoj mjeri može biti kontrolirana od strane vlasti. U kombinaciji sa transparentnošću sustava, ova činjenica stvara određene indirektne načine kako ta anonimnost potencijalno može biti narušena.

Analitička obrada kompletnog dnevnika transakcija (Blockchain-a) omogućava povezivanje i grupiranje pojedinih transakcija prema raznim parametrima, kao što su adresa pošiljatelja, adresa primatelja, vrijeme transakcije, iznos, (u određenim slučajevima i IP adresa pošiljatelja) i sl. Kombinirajući navedene podatke, moguće je dobiti kronologiju događanja za svaku pojedinu adresu, uključujući i povezanost (preko transakcija) sa drugim adresama sustava (postoje različiti pokušaji daljnjeg unapređenja anonimnosti sustava kombiniranjem transakcija, npr. *CoinJoin*, *CoinShuffle*[84]) . Rezultat toga je potpuna transparentnost sustava do razine vlasništva adrese, jer se za svaku adresu zna sve, ali se ne može direktno povezati adrese sa njihovim vlasnicima.[85] Kako svaki korisnik može imati neograničen broj adresa unutar svojih novčanika, i anonimno ih stvarati, nemoguće je direktno ugroziti privatnost. Međutim, ukoliko bi se na neki način uspjelo povezati korisnika i adrese, privatnost bi u potpunosti nestala. U teoriji, postoje određene situacije kada bi tako nešto bilo moguće izvesti, uz određene okolnosti koje su ovdje navedene:

- **Kontrola pristupa internetu**: prva je točka gdje anonimnost sustava može biti kompromitirana. Svaki novčanik mora imati pristup internetu da bi obavljao transakcije. Davatelj usluge pristupa internetu ima mogućnost kontrole internetskog prometa za svakog korisnika, i premda je ta komunikacija najčešće kriptirana, dostupne su mu krajnje IP adrese, i vrijeme transakcija. Na taj način postoji određena mogućnost kombinacije ovih podataka sa podacima iz originalnog dnevnika transakcija (vrijeme transakcija, IP adrese i identitet korisnika interneta) i značajno reduciranje broja mogućih kombinacija koje povezuju korisnika internetske usluge i adrese računa. Ovo se odnosi na novčanike korištene s privatnih računala, bilo stolnih ili mobilnih.

[84] SELIJ, Jan-Willem, CoinShuffle anonymity in the Block chain, 2015, Dostupno na: http://rp.delaat.net/2014-2015/p77/report.pdf. [Pristupljeno: 17-svi-2017]

[85] DOGUET, Joshua J., The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System, *La. Law Rev.*, sv. 73, izd. 4, 2012, str. 1119

- **Identifikacija računala s kojeg se obavljaju transakcije**: uređaji koji pristupaju internetu preko mobilne mreže registrirani su kod operatera preko jedinstvenog IMEI broja uređaja, a u velikoj većini slučajeva i preko identifikacije SIM kartice. Na taj način operater ima uvid u kompletan internetski promet određenog uređaja, a osim podataka iz prethodnog odjeljka, dostupni su i određeni podaci o lokaciji korisnika dobiveni preko internetske pristupne točke. To donosi iste rizike kao u prethodnom primjeru.
- **Identifikacija uređaja ili korisnika preko operacijskog sustava uređaja**: gotovo sve nove verzije operacijskih sustava (Android, Windows, IOS, itd.) za svoj rad traže od korisnika identifikaciju. Iako postoji mogućnost davanja netočnih identifikacijskih podataka, svaki korisnik je pojedinačno određen, pa čak iako je dao krive podatke (moguće ga je prepoznati u skupini korisnika, ali bez imena). Na ovaj način skupu dostupnih podataka dodajemo i lokaciju određenu preko satelita ako je dostupna na uređaju, e-mail korisnika, te statistiku korištenja koja ga obilježava, a koju vodi sam operativni sustav uređaja.
- **Identifikacija preko aplikacije novčanika**: pošto je za obavljanje transakcija i čuvanje digitalne valute potrebno imati određenu aplikaciju (koju prosječni korisnik neće sam izraditi nego će koristiti neke od dostupnih), treba biti svjestan da aplikacija novčanika ima potpuni uvid u sve transakcije adresa koje sadrži, kao i uvid u privatne ključeve potrebne za otuđenje sredstava (trošenje). Ukoliko je autor aplikacije ugradio u aplikaciju određeni nedokumentirani mehanizam komunikacije, to predstavlja rizik u smislu anonimnosti ali i sigurnosti. Takve radnje bi se vremenom vrlo vjerojatno otkrile, no ipak su značajan rizik čak i za gubitak novca. Iako nas Blockchain sustav rješava potrebe za povjerenjem u autoritet, ostaje potreba za povjerenjem u autore tehničkih komponenti sustava, ili izrada vlastitog.
- **Identifikacija preko malicioznog software**-a: instalacijom malicioznog software-a (razni tipovi računalnih virusa, i slično) javljaju se isti rizici kao u prethodnoj točki.

Kombinirajući navedene okolnosti vidimo da u određenim (iako teško ostvarivim) okolnostima anonimnost korisnika može biti ugrožena od strane određenih tehnički naprednih subjekata koji participiraju u sustavu ili autoriteta koji su im nadređeni. Iako je gotovo nemoguće da običan korisnik sazna određene zaštićene podatke Blockchain sustava, ta mogućnost je puno pristupačnija autoritetima vlasti, koji pravnom regulativom i

kontrolom određenih strateških točki sustava, ako požele, mogu stvoriti takve uvjete da im je jako teško ili gotovo nemoguće nešto sakriti.

4.8 Kontrola količine novca kod digitalnih valuta (pitanje inflacije)

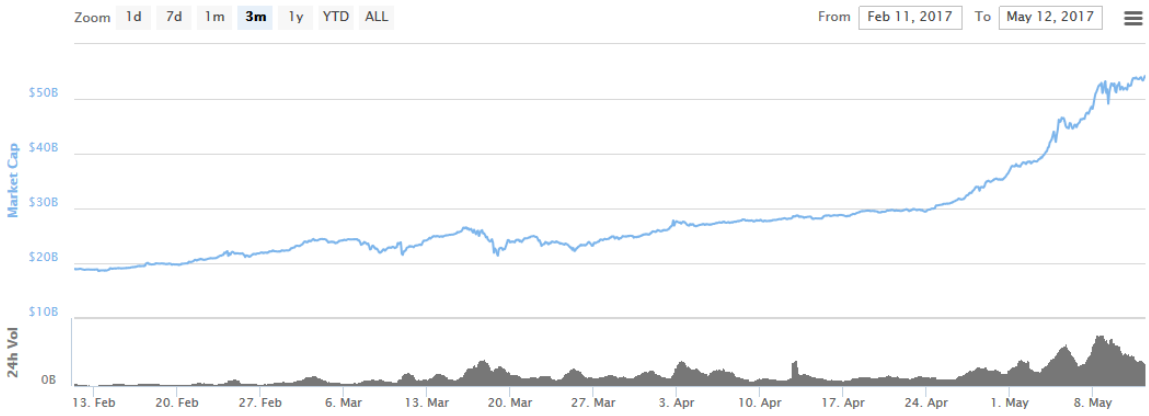
Kod predstavljanja Blockchain valute, kao jedna od ključnih prednosti navedena je neovisnost sustava od centralnih banaka u smislu nekontroliranog i netransparentnog „tiskanja“ novog novca. Ponuda novca pojedinih digitalnih valuta unaprijed je određena ili transparentna, najčešće određenim tehničkim ograničenjima, kao na primjer rudarenjem i auto-regulacijom stvaranja novih blokova u Blockchain sustavu Bitcoin valute. Pitanje inflacije jedno je od najznačajnijih pitanja pri procjeni vrijednosti pojedine valute. U tom smislu gledajući pojedinačno, većina digitalnih valuta, zbog unaprijed određene (programirane) količine jedinica, uz istovremenu mogućnost gubitka ili nestajanja jedinica iz sustava (gubitak, tehnički kvar i sl.), dugoročno pokazuju stabilne ili deflatorne trendove. U najmanju ruku, ako je inflacija i moguća u pojedinom slučaju, ona je potpuno predvidljiva.

Posebno je pitanje kada govorimo o inflaciji, a pošto tržište digitalnih valuta djeluje u sinergiji, mogu li se promatrati ukupni zajednički efekti proizvedeni od svih aktivnih digitalnih valuta. Kako se na tržištu gotovo svakodnevno pojavljuju nove valute sa značajnom tržišnom kapitalizacijom, jasno je da je sve veća vrijednost pohranjena u to zajedničko tržište. Sve je više mjenjačnica koje omogućuju jednostavnu konverziju između pojedinih digitalnih valuta. Kako ovdje ne postoje ekonomije pojedinih država kao svojevrsni faktor sigurnosti i faktor diferencijacije pojedinih valuta, kao što je to slučaj kod klasičnih valuta, postavlja se pitanje dali nove digitalne valute na tržištu utječu na cijenu svih ostalih. Moglo bi se pretpostaviti da među pojedinim digitalnim valutama, pogotovo onima baziranim na istoj tehnologiji, postoji značajan faktor supstitucije, utoliko više što su trendovi promjene vrijednosti pojedinih valuta vrlo slični. Razlike su najčešće posljedica nekih tehničkih specifičnosti i sigurnosnih propusta u pojedinim sustavima, koje uzrokuju značajne gubitke vrijednosti a nerijetko i nestajanje takvih valuta. Prema dostupnim podacima vidljivo je da većina digitalnih valuta koja skupi određenu kapitalizaciju, nastavlja rasti i pratiti zajednički trend. Čak što više, u zadnje vrijeme primjetan je sve veći trend rasta

alternativnih valuta u odnosu vodeći Bitcoin, što još više potvrđuje postavljenu tezu. Za primjer možemo ukupnu tržišnu vrijednost Bitcoina i svih ostalih valuta (*Altcoins*):

Slika 7 - Ukupna tržišna kapitalizacija Bitcoin-a, zadnjih 3 mjeseca[86]

Slika 8 - Ukupna tržišna kapitalizacija Altcoins-a, zadnjih 3 mjeseca[87]



[86] All Currencies | CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/all/views/all/. [Pristupljeno: 05-tra-2017]

[87] Ibid.

4.9 Pristupačnost digitalnih valuta

Uporaba digitalnih valuta, iako u snažnom porastu, još uvijek je ograničena na relativno mali udio populacije. Pretpostavka je da su to uglavnom korisnici koji dolaze iz tehničkih i financijskih područja djelatnosti, s određenom razinom tehničkih znanja, ali i razni drugi, entuzijasti željni upoznavanja novih tehnologija i špekulanti skloni podnijeti značajne rizike. Naravno, realno je pretpostaviti da postoji i određeni udio uporabe u ilegalne svrhe.[88]

Praktičnost, prihvaćenost, visina provizije kod zamjene za klasičnu valutu, transakcijske provizije, raspoloživost bankomata samo su neki su od čimbenika koji mogu utjecati na masovnost uporabe digitalnih valuta. Iako je cirkulacija valute unutar zajednice relativno jednostavna a transakcije jeftine, akcije ulaska ili izlaska s tržišta (kupnja ili prodaja Bitcoin-a ili druge valute za klasični novac) još uvijek podrazumijeva određene prepreke. Ovakvu situaciju na tržištu možemo potvrditi na primjeru Bitcoin-a, kao najpopularnije valute, dok je kod altcoin-a ona još izraženija. Velika volatilnost valute i neprihvaćenost od vlada također su značajni uzroci neprihvaćenosti.[89]

Kupnja Bitcoina nije uvijek jednostavna kao što možda očekuju novi korisnici. Dobra vijest je da broj opcija stalno raste. Neke čak ne moraju nužno zahtijevati elektronički novčanik ili pristup internetu. Osim dolje nabrojanih, ostale opcije uključuju Bitcoin debitne kartice, fizičke Bitcoin-ove „novčiće“ i tzv. prepaid kartice.[90]

Osobna prodaja dostupna je za one koji žive u sredinama s većom koncentracijom korisnika, npr. u velikim svjetskim gradovima. Ovaj način prodaje omogućuje najnižu cijenu transakcije, pod uvjetom da postoji povjerenje između prodavatelja i kupca. Do određene mjere moguće je ostati anoniman. Postoje i određene internetske stranice koje olakšavaju pronalazak partnera za trgovinu.[91]

---

[88] TRAUTMAN, Lawrence J., Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?, 2014, str. 8

[89] LUTHER, William J., Cryptocurrencies, network effects, and switching costs, *Contemp. Econ. Policy*, 2015, str. 2

[90] COINDESK, How can I buy bitcoins?, *CoinDesk*, 20-kol-2013, Dostupno na: http://www.coindesk.com/information/how-can-i-buy-bitcoins/. [Pristupljeno: 05-svi-2017]

[91] Find your people | Meetup, Dostupno na: http://www.meetup.com/. [Pristupljeno: 05-svi-2017]

Mjenjačnice za Bitcoin i ostale digitalne valute prisutne su u sve većem broju i realizirane gotovo u pravilu kao internetski servisi. Pošto je cijeli proces moguće automatizirati, nema potrebe za angažiranjem ljudskog rada, što se povoljno odražava na troškove. Najčešći načini plaćanja su kreditne kartice, Paypal i slični servisi elektroničkog plaćanja, te bankovni transferi. Provizije su relativno velike i najčešće se kreću u rasponu od 3-10% za kartice i Paypal, dok se kod bankovnih transfera može postići niži trošak kod nacionalnih transakcija. Takvu mogućnost je moguće iskoristiti samo ako postoji mjenjačnica unutar države, što je slučaj samo u zemljama razvijene ekonomije, dok u većem dijelu svijeta ona nije dostupna. Prihvaćene su uglavnom najvažnije svjetske valute, USD, EUR, GBP i druge, dok korisnici ostalih manje značajnih valuta moraju prvo konvertirati svoje valute za neku koja se prihvaća u mjenjačnici. Što se anonimnosti tiče, ona u ovom slučaju nije moguća jer svaki od navedenih sustava plaćanja zahtijeva određeni oblik autorizacije. Pozitivno je što na ovaj način, a posebno kod plaćanja bankovnim transferima, postoji značajan stupanj sigurnosti. Mnoge mjenjačnice u ponudi imaju više aktivnih digitalnih valuta, te vrlo jednostavno i jeftino omogućuju njihovu zamjenu. Iznenađujuće, ovisno gdje se nalazite, još uvijek nije lako kupiti Bitcoin-e kreditnom karticom ili PayPal-om. To je zato što se takve transakcije lako mogu poništiti telefonskim pozivom tvrtki za kartice (storniranje uplata). Budući da je teško dokazati da je bilo kakva roba promijenila ruke u prijenosu Bitcoina, mjenjači izbjegavaju takav način plaćanja i kao i većina privatnih prodavača.[92]

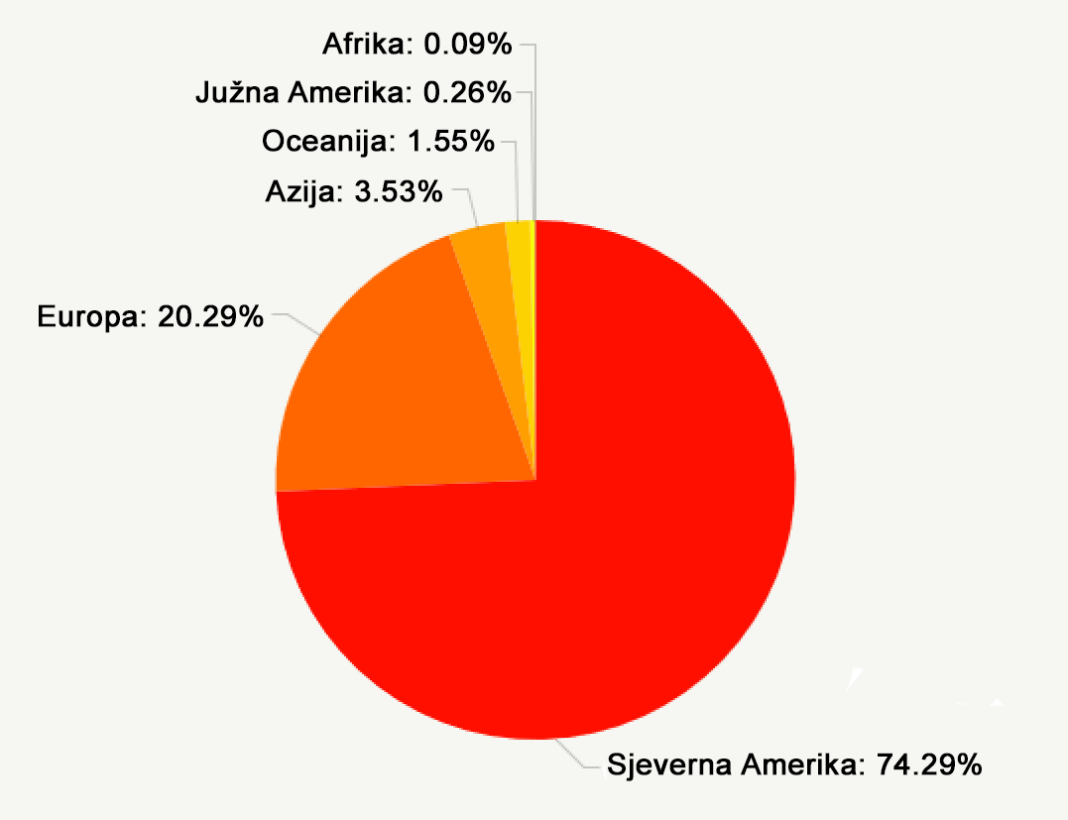
Specijalizirani bankomati ukoliko su dostupni, jednostavna su i praktična opcija za trgovanje digitalnim valutama. Obavljanje transakcija je relativno brzo i jednostavno a postoji i mogućnost anonimnosti ako se plaća gotovinom. Provizije za Bitcoin se u najvećem broju slučajeva kreću u rasponu od čak 0,5% do 10%, ovisno o lokaciji i načinu plaćanja. Prosječna prodajna provizija je 6,01%, a kupovna 9,73%. Relativno niske provizije mogu se pronaći uglavnom samo na jako prometnim uređajima u zemljama sa velikom uporabom valute, kao što su Velika Britanija i SAD. Prema coinatmradar.com trenutno je evidentirano 1163 Bitcoin bankomata u svijetu.[93] Prema trenutnom trendu, svake godine broj se gotovo

[92] COINDESK, How can I buy bitcoins?, *CoinDesk*, 20-kol-2013, Dostupno na: http://www.coindesk.com/information/how-can-i-buy-bitcoins/. [Pristupljeno: 05-svi-2017]

[93] Bitcoin ATM Map, Dostupno na: https://coinatmradar.com/. [Pristupljeno: 05-svi-2017]

udvostruči. U Hrvatskoj je trenutno instalirano 3 uređaja, po jedan u Zagrebu, Rijeci i Splitu. Apsolutno najveći broj uređaja je u SAD-u. Slika prikazuje raspored prema kontinentima:

Slika 9 - Raspored Bitcoin bankomata prema kontinentima[94]



Iz slike se može u određenoj mjeri pretpostaviti i rasprostranjenost korisnika valute, jer je za ekonomsku održivost pojedinog bankomata nužna određena količina transakcija.

Investicijski fondovi su još jedna zanimljiva mogućnost ulaganja u digitalne valute. Za korisnike koji žele uložiti u Bitcoin, a raspoložive metode im se čine kompliciranе i nesigurne, ovakvi fondovi mogli bi ponuditi profesionalnu uslugu. Trenutno je poznato nekoliko pokušaja osnivanja takvih fondova, *Bitcoin Investment Trust* (BIT)[95] i *Winklevoss*

[94] Ibid.

[95] GRAYSCALE, Dostupno na: https://grayscale.co/. [Pristupljeno: 05-svi-2017]

ETF[96] [97], *The Bitcoin Superfund*[98]. I u ovom slučaju nedostatak pravne definiranosti koči ovakvu inicijativu zbog osnovane bojazni vlasti o mogućnosti prevare. Javnost s nestrpljenjem očekuje reviziju odluke Američke agencije za vrijednosnice o zabrani osnivanja *Winklevoss ETF-a* koja treba biti donesena 15.svibnja 2017. U slučaju ukidanja zabrane, očekuje se novi vjetar u leđa investitorima.

[96] BUKHARI, Jeff, Bitcoin: Winklevoss ETF May Not be Dead Yet, *Fortune*, Dostupno na: http://fortune.com/2017/03/23/why-the-winklevoss-bitcoin-etf-may-not-be-dead-yet/. [Pristupljeno: 05-svi-2017]

[97] SEC Rejects Winklevoss Bitcoin ETF Bid, *CoinDesk*, 10-ožu-2017, Dostupno na: http://www.coindesk.com/sec-shoots-winklevoss-bitcoin-etf-bid/. [Pristupljeno: 05-svi-2017]

[98] New Active Trading Bitcoin Fund Seeks UK Investors, *CoinDesk*, 28-ožu-2014, Dostupno na: http://www.coindesk.com/new-active-trading-bitcoin-fund-seeks-uk-investors/. [Pristupljeno: 05-svi-2017]

5 PRAVNI ASPEKTI DIGITALNIH VALUTA

Digitalne valute u pravnom smislu tretiraju se na različite načine. Reakcije zakonodavaca pojedinih država idu od ignoriranja do zabrane. Upravo je ta neodređenost veliki sigurnosni rizik za korisnike, i uzrok uglavnom špekulativnom pristupu digitalnim valutama. Primjer je veliki pad Bitcoin valute s početkom u prosincu 2013. godine, nakon izdanog upozorenja Kineske centralne banke financijskim institucijama i tvrtkama da ne koriste Bitcoin. Kako je Kinesko tržište korisnika Bitcoin valute jedno od najvećih, ovaj potez Kineske centralne banke bio je snažan okidač za prodaju uz veliki pad tečaja. Iako se formalno radi o decentraliziranim valutnim sustavima bez nadređenog autoriteta, vlast ima na raspolaganju snažne mehanizme kojima može uspostaviti kontrolu nad uporabom digitalnih valuta, ako to u nekom momentu poželi.

Nedovoljno definirani pravni okvir u mnogim slučajevima dodatno motivira zlouporabu digitalnih valuta, umanjujući potencijalno pozitivne efekte koje bi proizvela šira uporaba blockchain tehnologije.

5.1 Pravni status digitalnih valuta u Republici Hrvatskoj i Europskoj Uniji

Od nastanka prve digitalne valute Bitcoin-a do danas objavljeno je svega nekoliko preporuka i naputaka o korištenju digitalnih valuta u Hrvatskoj. Prije svega za javnost je bitno znati dali je uporaba takvih valuta legalna, kako se pravno definira status virtualnih valuta, te kako se one tretiraju u smislu oporezivanja. Hrvatska nacionalna banka 2013. provela je raspravu o kruženju digitalne valute i zaključila da Bitcoin nije ilegalan u Hrvatskoj. Prema Zakonu o HNB-u, jedina službena valuta je kuna, a iznimno se može dopustiti i plaćanje u drugim valutama. HNB Bitcoin i ostale digitalne valute ne definira ni kao valutu, odnosno službeno sredstvo plaćanja, ni kao elektronički novac, već se poziva na mišljenje Europske središnje banke iz listopada 2012.[99] Iz tog razloga trgovanje digitalnim valutama u Hrvatskoj nije ilegalno. Što se tiče oporezivanja, porezna uprava poziva se na tumačenje članka 40. stavka

[99] Virtual currency schemes, lis-2012, Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. [Pristupljeno: 20-ožu-2017]

1. Zakona o porezu na dodanu vrijednost (Narodne novine broj 73/13, 99/13, 148/13, 153/13 i 143/14, u daljnjem tekstu: Zakon o PDV-u):

„ … U skladu s navedenim, mišljenja smo da se za potrebe oporezivanja PDV-om "bitcoin" može smatrati prenosivim instrumentom u smislu članka 40. stavka 1. točke d) Zakon-a o PDV-u te da se oslobođenje od plaćanja PDV-a iz toga članka može primijeniti na transakcije, uključujući posredovanje u vezi s virtualnim valutama kao što je "bitcoin".“[100]

Znači da se trgovina digitalnim valutama promatra zapravo kao trgovina ekonomski bezvrijednim objektima. Mogućnost uporabe digitalnih valuta kao sredstva plaćanja na ovaj način je zanemarena u pravnom smislu. To otvara određene opcije njihove uporabe u sivoj ekonomiji.

Osim spomenutih priopćenja, HNB upućuje potencijalne korisnike na dokument[101] upozorenja EBA-e o korištenju digitalnih valuta, iz 2013. godine.[102] Jasno je da se stavovi HNB i općenito hrvatskog zakonodavstva oslanjaju na pravni sustav EU, i za očekivati je da će se prilagođavati eventualnim promjenama stajališta EU.

Treba napomenuti da je Švedski Vrhovni Upravni Sud 2. lipnja 2014. godine Europskom sudu pravde podnio zahtjev za prethodnu odluku (predmet C-264/14) kojim je zatraženo očitovanje o poreznom tretmanu "bitcoin-a" te da će u skladu s tim nakon donošenja presude biti moguće promjene u poreznom tretmanu "bitcoina" i u Republici Hrvatskoj. Naime, presude Europskog suda pravde dio su pravne stečevine Europske unije te su ih sve države članice Europske unije obvezne primjenjivati.[103]

[100] popis_misljenja - Posredovanje pri kupnji i prodaji virtualne..., Dostupno na: https://www.porezna-uprava.hr/HR_publikacije/Lists/mislenje33/Display.aspx?id=19252. [Pristupljeno: 02-svi-2017]

[101] EBA warns consumers on virtual currencies - View press release - European Banking Authority, Dostupno na: https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies. [Pristupljeno: 02-svi-2017]

[102] E-novac - HNB, Dostupno na: https://www.hnb.hr/o-nama/zastita-potrosaca/bezgotovinska-placanja/e-novac. [Pristupljeno: 02-svi-2017]

[103] popis_misljenja - Posredovanje pri kupnji i prodaji virtualne..., Dostupno na: https://www.porezna-uprava.hr/HR_publikacije/Lists/mislenje33/Display.aspx?id=19252. [Pristupljeno: 02-svi-2017]

U Europskoj uniji uporaba digitalnih valuta trenutno nije regulirana. Stajalište Europske nacionalne banke je da sustav nacionalnih banaka ne prepoznaje termine poput "virtualne valute" ili "virtualne valutne sheme" u smislu novca, te ne smatra da bi ovi koncepti pripadali svijetu novca ili valuta koji se koriste u ekonomskoj literaturi. Niti je virtualna valuta novac, niti je valuta s pravne perspektive.[104]

S pravne perspektive za ECB novac je sve što se široko koristi za razmjenu vrijednosti u poslovanju. Pojam valuta se koristi za "klasične" forme novca, koji se obično pojavljuje u obliku kovanica ili novčanica. U više konceptualnom smislu, valuta predstavlja specifičan oblik novca koji se generalno koristi u nekoj zemlji. Obzirom da sheme virtualnih valuta nisu široko korištene za razmjenu vrijednosti, nisu u pravnom smislu novac i u odsutnosti materijalne verzije nisu ni valuta, te zato virtualna valuta zapravo nije valuta.[105]

Nadalje, za prihvaćanje novca za plaćanje, samo novčanice i kovanice eura su zakonsko sredstvo plaćanja u zemljama euro-zone, i stoga po zakonu samo Euro mora biti prihvaćen kao sredstvo plaćanja duga u tim zemljama. Različiti oblici elektroničkog novca, sustavi za plaćanje preko interneta, različite verzije bankovnog novca, i elektronički novac (*eng. e-money*) u nominiran u eurima, u strogom smislu nisu zakonsko sredstvo plaćanja. Ipak, ovi oblici novca su široko prihvaćeni za sve vrste plaćanja po izboru. Euro kao valuta može zauzeti oblik novčanica, kovanica, bezgotovinskog novca i elektroničkog novca.[106]

To nije slučaj za virtualne valute. Sheme virtualnih valuta, kao što je Bitcoin, koriste vlastitu denominaciju. Sheme virtualne valute nisu bezgotovinski, elektronski, digitalni ili virtualni oblici određenje valute. One su nešto drugo, različito od drugih valuta. Niti jedna virtualna valuta, za sada, nije službeno deklarirana kao valuta neke države. Stoga vjerovnik nije dužan prihvatiti plaćanje s virtualnom valutom kako bi dužnika odriješio duga. To znači da se

[104] Virtual currency schemes - a further analysis, velj-2015, Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf? [Pristupljeno: 18-velj-2017]

[105] Ibid.

[106] Ibid.

virtualna valuta može koristiti samo kao ugovorni novac, kada postoji sporazum između kupca i prodavatelja uz uvjet da se dana virtualna valuta prihvaća kao sredstvo plaćanja.[107]

Malo je drugačija situacija u Velikoj Britaniji. Iako bitcoini nisu regulirani, prihodi od njihove trgovine klasificirani su kao i prihodi od trgovine jednokratnim bonovima, čime je svaka transakcija podložna porezu na dodanu vrijednost od 10-20%. Takva regulativa je snažno kritizirana od strane zajednice korisnika i velika kočnica za jačanje britanske Bitcoin industrije. Već duže vrijeme postoje najave da će se ovo oporezivanje ukinuti i izjednačiti status digitalnih valuta sa statusom koji imaju u Europskoj zajednici.

5.2 Pravni status digitalnih valuta u SAD-u

Američko zakonodavstvo je primjer postupnog i temeljitog pristupa ovom problemu. Primjetni su veliki napori u osmišljavanju pravnog okvira koji bi mogao biti uvod u povećanu upotrebu digitalnih valuta, i koji bi pružio odgovarajuću potrošačku zaštitu i regulatorne zaštitne mjere. Prema američkim zakonima, Bitcoin se ne smatra vrijednosnicom, pa za njegovu regulativu nije nadležna Komisija za vrijednosne papire (*Securities and Exchange Commission* - SEC). Nedostatak legitimnog autoriteta koji prepoznaje i dodjeljuje vrijednost Bitcoinu pruža nadzornu mogućnost Uredu za financijsku zaštitu potrošača (*Consumer Financial Protection Bureau* - CFPB), koji ima za cilj osigurati financijsku sigurnost potrošača.[108]

Ne treba očekivati da će vlada Sjedinjenih Država ili bilo koja druga vlada u tom smislu, dopustiti bilo kakvu značajnu pohranu vrijednosti u nekoj od novokreiranih "valuta" bez odluke o reguliranju izdavatelja ili uključenje valute pod pravno okrilje središnje burze.[109]

[107] Ibid.

[108] MAESE, Vivian A., Divining the Regulatory Future of Illegitimate Cryptocurrencies, *Wall Str. Lawyer*, sv. 18, izd. 5, 2014, str. 9

[109] HUGHES, Sarah Jane, MIDDLEBROOK, Stephen T., Regulating cryptocurrencies in the United States: Current issues and future directions, 2014, str. 845

U nastojanju da se pomogne saveznim državama u razvoju propisa i licenci za nadzor operacija virtualnih valuta, konferecija državnih nadzornih tijela banaka (*eng. Conference of State Bank Supervisors – CSBS*), objavila je model pravnog okvira za državnu regulaciju aktivnosti određenih vitrualnih valuta (*CSBS Model Framework*) 15. rujna 2015. koji uključuje komponente koje je CSBS identificirala kao ključ režima regulacije virtualnih valuta koji štiti potrošače i veće tržište, dok u isto vrijeme podržava odgovorne inovacije. Pravni okvir utjelovljuje regulatornu shemu koja je slična vrsti regulacija trenutno primjenjivim pod državnim zakonom za financijske tvrtke koje obavljaju transakcije s američkim dolarima ili drugim novcem. On uključuje zahtjeve za superviziju, ispitivanje i provedbu autoriteta nad poslovima vezanim za virtualne valute i njihove aktivnosti. Model specificira kako državni režim virtualnih valuta treba obuhvaćati licenciranje, kapitalne i ulagačke standarde, zaštitu potrošača i sukladnost standardima. Nadalje, postavlja standard za državnu regulaciju aktivnosti virtualnih valuta pomoću entiteta koji nisu uključeni u državne regulacije depozitarnih institucija. Model preporučuje državama usvajanje zakona koji obuhvaćaju tvrtke i aktivnosti vezane za korištenje virtualnih valuta. Obuhvaća prijenose virtualnih valuta i razmjenu virtualnih valuta između tvrtki. Također uključuje i tvrtke koje pružaju usluge izdavanja i razmjene virtualnih valuta, kao što su dobavljači "novčanika". Model ne uključuje posebni režim za nove kompanije. Umjesto toga, CSBS savjetuje svaku državu na izabiranje odvojenog aranžmana za nova poduzeća kako bi se osmislila adekvatna zaštita potrošača.[110]

5.3 Pravni status digitalnih valuta u drugim državama

Izvan Sjedinjenih Američkih Država, pronalazimo ograničenu regulaciju digitalnih valuta. Neke zemlje kao što su Kina, Island, Ruska federacija, i Tajland donijele su uredbe koje učinkovito zabranjuju korištenje Bitcoina u svrhu plaćanja na svojim domaćim tržištima. Druge zemlje su se usredotočile na reguliranje digitalnih valuta samo u ograničene svrhe. Primjerice, neke su se zemlje bavile poreznim pitanjima povezanim s virtualnim valutama,

[110] State Regulators Issue Model Regulatory Framework for Virtual Currency Activities, Dostupno na: https://www.csbs.org/news/press-releases/pr2015/Pages/PR091515.aspx?PF=1. [Pristupljeno: 03-svi-2017]

a neke su najavile svoje planove za regulaciju virtualnih valuta kao roba. Vlade su izdale upozorenja o rizicima korištenja virtualnih valuta, i najavile namjeru primjene postojećih zakona protiv pranja novca i izvještavanja o transakcijama u virtualnoj valuti. Međutim, prevladavaju propisi koji se usredotočuju na oporezivanje i okvire koji sprečavaju upotrebu digitalnih valuta. Samo je švicarska vlada najavila svoju namjeru da ne regulira Bitcoin.[111]

Australija na primjer, dozvoljava entitetima trgovanje, izdavanje ili kupnju bitcoina. Australski porezni ured (ATO) tretira transakcije virtualnih valuta kao trampu, koje su kao takve podložne odgovarajućim porezima ovisno o korištenju i korisniku.[112]

Obično plaćanje roba ili usluga u Bitcoin-ima (na primjer, pribavljanje osobnih dobara ili usluga na internetu putem Bitcoina) ne podliježe oporezivanju na dobit ili imovinu. Kod korištenja Bitcoin-a za kupnju roba ili usluga za osobnu uporabu ili potrošnju, bilo koji kapitalni dobitak ili gubitak od prodaje Bitcoina neće se uzimati u obzir kod oporezivanja pod uvjetom da je visina transakcije do 10.000 AUD.

Kanada općenito održava pozitivan stav prema Bitcoin-u i virtualnim valutama, uz ulaganje napora u osiguranje da se one ne koriste za pranje novca. Bitcoin se smatra robom od strane Agencije za priznavanje prihoda Kanade (*Canada Revenue Agency* - CRA). To znači da se Bitcoin transakcije smatraju trampom, a ostvareni prihod smatra se poslovnim prihodom. Porez također ovisi o tome dali se radi o poslovima kupnje ili investiranja.

Razmjene Bitcoin-a i sličnih valuta predstavljaju financijske usluge. To ih dovodi pod djelokrug zakona protiv pranja novca (*Anti Money Laundering* - AML). Transakcije spomenutih valuta trebaju se registrirati u Centru za analizu financijskih transakcija i izvješća (*Financial Transactions and Reports Analysis Centre* - FINTRAC), prijaviti sve sumnjive transakcije, i čak čuvati određene dnevnike transakcija. Pored toga, kanadska vlada

[111] HUGHES, Sarah Jane, MIDDLEBROOK, Stephen T., Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries, *Yale J Reg*, sv. 32, 2015, str. 495

[112] OFFICE, Australian Taxation, Tax treatment of crypto-currencies in Australia - specifically bitcoin, Dostupno na: http://agov-display-g2.prod.atohnet.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?default. [Pristupljeno: 03-svi-2017]

je zadužila Odbor za bankarstvo senata za izradu smjernica za zakonodavstvo virtualnih valuta.

2013. godine centralna banka Kine i četiri središnja vladina ministarstva zajednički izdaju "Obavijest o mjerama opreza od rizika Bitcoina", te ga definiraju kao specijalnu "virtualnu robu". U obavijesti stoji kako po prirodi Bitcoin nije valuta te nebi trebao biti u opticaju i korišten na tržištu kao vauluta. Bankama i platnim institucijama u Kini zabranjeno je trgovanje u Bitcoinima. "Obavijest o mjerama opreza od rizika Bitcoina" zahtjeva da u ovoj fazi, financijske i platne institucije ne smiju koristiti Bitcoin za produkte ili usluge, prodavati ili kupovati ih niti omogućiti kupcima direktnu ili indirektnu uslugu vezanu za Bitcoin, uključujući registraciju, razmjenu ili druge usluge. Obavijest dalje zahtjeva jačanje nadzora nad internetskim stranicama koje pružaju uslugu registracije Bitcoina, trgovanja i ostalo. Također je upozoreno o rizicima korištenja Bitcoina kao sredstva za "pranje novca".

U lipnju 2016. proglašen je dopunjeni zakon Japanske banke koji uključuje zakon o plaćanju usluga. Zakon definira Bitcoin i ostale virtualne valute kao vrijednost imovine koju mogu koristiti nespecificirane osobe za isplatu protuvrijednosti za kupljenu robu ili uslugu, a koje se mogu prodati nespecificiranim osobama te se mogu prenositi preko elektroničkog sustava za obradu podataka. Izmijenjeni zakon će zahtijevati da se razmjena virtualnih valuta u Japanu mora registrirati u Financial Services Agency (FSA). Zakon zahtjeva da se razmjena virtualnih valuta upravlja odvojeno od vlastitih. Nadzor upravljanja mora biti obavljen od strane ovlaštenih javnih računovođa ili računovodstvenih tvrtki. Subjekti koji obavljaju razmjene virtualnih valuta bit će obavezni provjeriti identitet korisnika koji otvaraju račun i obavijestiti vlasti na moguće sumnjive transakcije. Zakon treba stupiti na snagu 1. travnja 2017.[113] [114]

[113] Bitcoin regulation overhaul in Japan » Brave New Coin, Dostupno na: https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/. [Pristupljeno: 22-svi-2017]

[114] Japan's Bitcoin Law Goes Into Effect Tomorrow, *CoinDesk*, 31-ožu-2017, Dostupno na: http://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/. [Pristupljeno: 22-svi-2017]

6 RASPRAVA

Mnogi uspoređuju pojavu blockchain-a s drugom revolucionarnom tehnologijom, Internetom, i predviđaju da će ova tehnologija promijeniti ravnotežu moći od centraliziranih vlasti ka zajednici, u području komunikacija, poslovanja, pa čak i politike ili zakona. Blockchain može potaknuti novo razdoblje karakterizirano globalnim platnim sustavima, digitalnim sredstvima, decentraliziranom upravljanju, pa čak i decentraliziranim pravnim sustavima. Blockchain omogućuje kolektivima, organizacijama i društvenim zajednicama da postanu fluidnije i promoviraju svoje sudjelovanje kao demokratske institucije. Tehnologija bi mogla utjecati na tržišta kapitala, omogućujući običnim građanima izdavanje financijskih vrijednosnih papira koristeći samo nekoliko redaka programskog koda.[115] [116]

Digitalne valute daju nam potpuno novi model sustava. On predstavlja pravi fenomen u smislu nove vrijednosti koja je nastala bez ikakve prethodne potrebe i bez određene temeljne vrijednosti. Očiti uspon Bitcoin-a prema statusu valute koja se već sada može koristiti za kupnju stvarnih proizvoda, ističe da je novac društveni koncept ili oblik interakcije između ljudi.[117]

Puno je pitanja kada se raspravlja o Bitcoin-u, blockchain-u i digitalnim valutama općenito. Ipak, ona se mogu klasificirati ili grupirati u nekoliko ključnih o kojima se najčešće govori, odnosno koja su vjerojatno najznačajnija:

- Definicija digitalnih valuta, odnosno njihovo pojmovno određenje i klasifikacija u jezičnom, pravnom i ekonomskom smislu
- Tehnički i praktični aspekti sigurnosti uporabe digitalnih valuta
- Uporabljivost, prihvaćenost i dostupnost digitalnih valuta
- Različiti aspekti utjecaja digitalnih valuta na ekonomiju i trendovi

[115] ANDREESSEN, Marc, Why Bitcoin Matters, *DealBook*, 21-sij-2014, Dostupno na: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/. [Pristupljeno: 20-svi-2017]

[116] WRIGHT, Aaron, DE FILIPPI, Primavera, Decentralized blockchain technology and the rise of lex cryptographia, 2015, str. 2,3

[117] BORNHOLDT, Stefan, SNEPPEN, Kim, Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies, *ArXiv Prepr. ArXiv14036378*, 2014, str. 4

Počevši od same definicije i pravnog određenja, jasno je da je zbog nepostojanja sličnog modela u prošlosti, kao i zbog pojedinačnih specifičnosti pojedine valute ovo pitanje jedan od najvećih izazova, prije svega za pravnike i zakonodavce. U posljednjih nekoliko godina napisano je puno analiza, prijedloga zakona, naputaka i članaka s ciljem definiranja pojmova i lakšeg stvaranja pravnih okvira za regulaciju. Svi lokalni i globalni društveni subjekti, počevši od nacionalnih vlada i banaka, znanstvene zajednice, međunarodnih institucija uključili su se u ovu problematiku, prepoznavši definiranje i rješavanje ovog problema kao globalni i opći interes.

Mišljenja su različita, pa tako npr. Bayern u svom radu pokušava odrediti u koji tip imovine bi se mogao ili trebao svrstati Bitcoin. Pitanje je vrlo složeno, s jedne strane niti jedna dosadašnja pravna stečevina ne može se u potpunosti primjeniti na ovakav tip imovine ili novca, a s druge strane pojedinačni pokušaji nacionalnih zakonodavstava krenuli su u različitim smjerovima. Da bi uopće bilo moguće ustanoviti određene pravne okvire, prvo je potrebno postići konsenzus na svjetskoj razini oko definicije digitalnih valuta i pojmova vezanih za tu tematiku. Dali je Bitcoin roba, valuta, kolekcionarska rijetkost, pravo ili nešto sasvim drugo? Svaki od ponuđenih odgovora ima određeni smisao. Čini se da u ovom slučaju nije moguće primjeniti ni jedan postojeći koncept kao takav, već je potrebno stvoriti novi i prema njemu graditi pravne okvire.[118]

Može se reći da je Bitcoin roba jer se njime trguje i postoji u ograničenoj količini, ali s druge strane on nema materijalni oblik već predstavlja informaciju čiji nositelj ili medij može poprimiti različite oblike. Nemoguće je doslovno posjedovati bitcoin-e, korisnik je zapravo samo u posjedu privatnog ključa koji mu omogućava otuđenje određene količine novčanih jedinica. Cijeli sustav se sastoji zapravo od skupa evidencija prometa za svaku adresu, te na taj način "zna" koliko svaka adresa odnosno njen "vlasnik" ima pravo otuđiti (potrošiti).[119]

Ako ga promatramo kao pravo, ili nekakav tip mjenice zadovoljit ćemo jedan dio potreba regulative, ali u tom slučaju također postoje dvojbe; pravo se u konačnici odnosi na stvarnu

[118] BAYERN, Shawn, Dynamic common law and technological change: the classification of Bitcoin, *Wash Lee Rev Online*, sv. 71, 2014, str. 22

[119] Ibid.

vrijednost, dug ili robu, a bez općeprihvaćenog korištenja bitcoina kao mjerila vrijednosti robe, i ova definicija pokazuje nedostatke.[120]

Prepoznajući hitnost problema, najzanimljivije rješenje je donio je Japan. Inicirano kao odgovor na neke prethodne kriminalne događaje, ono je odličan kompromis u nedostatku globalnog konsenzusa i pronalaska bolje i šire prihvaćene definicije, jer ne sputava legalnu uporabu digitalnih valuta, a u isto vrijeme nudi određenu pravnu zaštitu korisnicima. Radi se o zakonu koji je stupio na snagu u travnju 2017. a kojim se definira posebni registar za transakcije digitalnim valutama, slično kao i za klasične ali odvojen zasebno.[121] [122] Uspostava takvog registra je osnova za proglašenje Bitcoina legalnim sredstvom plaćanja u Japanu, i omogućuje korištenje digitalnih valuta u platnom prometu. Donošenjem takvog zakona u ogromnoj mjeri je povećan stupanj zaštite korisnika valute od potencijalnih prijevara, ili sličnih kriminalnih radnji, kao i same države od potencijalne uporabe valute u ilegalne svrhe. Glavni nedostatak ovakvog rješenja je nedostatak anonimnosti, kao jednog od ključnih koncepata digitalnih valuta. Korisnici su prisiljeni odreći se anonimnosti kako bi pronašli sigurnost pod okriljem državne regulative. Većini ovaj nedostatak neće predstavljati problem, dok će u isto vrijeme biti velika zapreka za pokušaje zlouporabe. Ovo je do sada najliberalniji stav zakonodavstva neke države prema regulaciji uporabe digitalnih valuta, i prvi slučaj prihvaćanja digitalnih valuta u platnom prometu neke države. Kako je cijeli koncept u trenutku pisanja ovog rada vrlo svjež može se samo pretpostaviti kako će se odraziti na popularnost digitalnih valuta u Japanu, te kako će utjecati na ostala nacionalna zakonodavstva.

Promatrajući tehničku stranu, postojeće digitalne valute pate od brojnih ograničenja. Vjerojatno najveće je njihova slaba skalabilnost: Bitcoin mreža, koja se trenutno najviše koristi, može se nositi s najviše 7 transakcija u sekundi i suočava se sa značajnim izazovima u povećanju ove stope. Sustav za plaćanje PayPal obrađuje više od 100 transakcija u sekundi, a poznata kartična tvrtka Visa obrađuje u prosjeku od 2000 do 7000 transakcija. Ovaj

[120] Ibid.

[121] Bitcoin regulation overhaul in Japan » Brave New Coin, Dostupno na: https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/. [Pristupljeno: 22-svi-2017]

[122] Japan's Bitcoin Law Goes Into Effect Tomorrow, *CoinDesk*, 31-ožu-2017, Dostupno na: http://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/. [Pristupljeno: 22-svi-2017]

nedostatak skalabilnosti posljedica je oslanjanja na POW sustav potvrde transakcija. Kao drugi nedostatak najčešće se spominje potreba za potrošnjom znatne količine računalnih resursa (električne energije i uređaja) u procesu kontrole transakcija, koja je prema nekim procjenama usporediva s potrošnjom energije velike elektrane. Alternativne digitalne valute kao što su npr. Litecoin ili Permacoin pokušavaju uporabom različitih tehničkih modifikacija sustava smanjiti ove troškove.[123] [124]

Osim toga postoje i sumnje u tvrdnje da su decentralizirani sustavi efikasniji. Prema njima, cijene održavanja centraliziranih sustava i cijene njihovih transakcija skuplje su kao posljedica nedostatka konkurencije i visokih marži, a ne samog koncepta.[125]

Drugi značajni nedostatak je ovisnost digitalnih valuta o tehničkim uređajima i sustavima. Koliko god takvi sustavi doprinose općem boljitku i efikasnosti, oni prisiljavaju korisnike na ovisnost o tehničkim uređajima. Neki oblici slobode se čak i gube ovakvim sustavima, npr. izaći u kupovinu ili nekakav izlazak sa samo par novčanica u džepu, bez pametnih telefona ili sličnih tehničkih uređaja.

Nedovoljna dostupnost mjenjačnica i bankomata također su značajna prepreka, kao i visoke mjenjačke provizije. Što se tiče prihvaćenosti od strane trgovaca, ona je još uvijek više egzotična nego značajna. Mnogi od trgovaca koji prihvaćaju Bitcoin, zbog još uvijek malog udjela takvih transakcija, više se oslanjaju na možebitne marketinške učinke takve odluke nego na njene ekonomske efekte.

U ekonomskom smislu gledano, ključno ograničenje postojećih decentraliziranih digitalnih valuta je gubitak kontrole nad monetarnom opskrbom, što za makroekonomsku politiku nudi

[123] DANEZIS, George, MEIKLEJOHN, Sarah, Centrally banked cryptocurrencies, *ArXiv Prepr. ArXiv150506895*, 2015, str. 1

[124] HAYES, Adam S., Cryptocurrency Value Formation: An empirical study leading to a cost of production model for valuing Bitcoin, *Telemat. Inform.*, 2016, str. 18

[125] EVANS, David S., Economic aspects of bitcoin and other decentralized public-ledger currency platforms, 2014, str. 19

malu ili nikakvu fleksibilnost u regulaciji, te ekstremna volatilnost njihovih vrijednosti kao valuta.[126]

Analizirajući koliko se Bitcoin koristi kao sredstvo plaćanja, a koliko kao špekulativno ulaganje, ispitivane su namjere novih korisnika s obzirom na ove dvije opće moguće svrhe. Rezultati daju snažne pokazatelje da novo privučeni korisnici prvenstveno ograničavaju svoj odnos prema Bitcoinu na trgovanje na burzama digitalnih valuta. Iako je Bitcoin sustav plaćanja i dalje dominantan u pogledu apsolutnih količina transakcija, utvrđeno je da je trenutni fokus i rast korisnika ograničen na trgovanje na burzama s ciljem visoko rizičnog špekulativnog ulaganja i stjecanja profita na osnovu trenutnog snažnog rasta valute, a ne na korištenju u međusobnoj trgovini robama i uslugama, kao alternativni sustav transakcija.[127]

Zanimljivo je da tržište alternativnih valuta (*altcoins*) raste po još bržoj stopi od samog Bitcoina. Uz činjenicu kako je prihvaćenost alternativnih valuta općenito značajno manja nego Bitcoin-a, to još više potkrepljuje gore navedene zaključke. Ovakva situacija povećava opasnost stvaranja balona, kao su već i prije upozoravale brojne međunarodne institucije (ECB, IMF…) u svojim priopćenjima i analizama. Svjedočimo (u vrijeme pisanja ovog rada) kako udio Bitcoina opada u ukupnoj kapitalizaciji digitalnih valuta, te kako se prvi konkurenti značajno približavaju prijeteći da će zauzeti vodeću poziciju. U isto vrijeme ukupna kapitalizacija raste ogromnom brzinom, stvarajući stanje slično povijesnim razdobljima prije velikih padova na svjetskim burzama vrijednosnica.[128] [129] [130]

Treba naglasiti da Blockchain tehnologija nije ograničena samo na stvaranje valuta. Primjenjiva je na mnogim područjima od financija, uprave, državne administracije i sl. U ovoj fazi primjene nije ni moguće predvidjeti sve njene mogućnosti, one će se razvijati postupno i kroz praksu i uporabu širiti na različita područja primjene. Mnoge ideje već sada

[126] DANEZIS, George, MEIKLEJOHN, Sarah, Centrally banked cryptocurrencies, *ArXiv Prepr. ArXiv150506895*, 2015, str. 1

[127] GLASER, Florian *i ostali*, Bitcoin-asset or currency? revealing users' hidden intentions, 2014, Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247. [Pristupljeno: 17-svi-2017]

[128] ABREU, Dilip, BRUNNERMEIER, Markus K., Bubbles and crashes, *Econometrica*, sv. 71, izd. 1, 2003, str. 2

[129] LUX, Thomas, Herd behaviour, bubbles and crashes, *Econ. J.*, 1995, str. 881–896

[130] AVERY, Christopher, ZEMSKY, Peter, Multidimensional uncertainty and herd behavior in financial markets, *Am. Econ. Rev.*, 1998, str. 724–748

postoje. Uglavnom se radi o automatizaciji funkcioniranja različitih registara imovine ili prava, koji se uporabom ovakve tehnologije mogu izdvojiti iz državne administracije i decentralizirati. Dobar primjer bio bi implementacija blockchain tehnologije u sustav vrijednosnica gdje bi vršio funkciju središnje depozitarne agencije, ili na području uprave gdje bi se koristio kao evidencija vlasništva nekretnina, i slično. U literaturi se također dosta spominju i pametni ugovori, kod kojih se može automatizirati sam proces određene pravne radnje, bez potrebe ovjere od treće strane. Moguće je na primjer stvoriti sustav u kojem je osiguran i potpuno automatiziran proces kupoprodaje nekretnine bez potrebe različitih ovjera kod bilježnika, potvrda iz gruntovnice i slično.[131] [132] [133]

Primjena Blockchain tehnologije i digitalnih valuta vrlo je pogodna za proširenje funkcionalnosti umrežavanja uređaja (*eng. Internet of Things* - IoT), trenda koji je nastao širenjem interneta i uporabe minijaturnih računala koja se mogu ugraditi u različite uređaje stvarajući od njih takozvane pametne (*smart*) verzije. Takvi uređaji mogli bi izvršavati automatizirane transakcije međusobno, na osnovu programiranih obrazaca odnosno algoritama. Na primjer električni auto čije baterije punimo na javnoj punionici mogao bi automatizirano vršiti uplatu za primljenu energiju, ili platiti sam za sebe parkirnu kartu na javnom parkingu.[134] [135]

Neki autori idu i dalje, govoreći o takozvanim „etičkim valutama“, kod kojih je svrha i namjena određene digitalne valute programirana unaprijed od strane autora i koje na

[131] CROSBY, Michael *i ostali*, Blockchain technology: Beyond bitcoin, *Appl. Innov.*, sv. 2, lip. 2016, str. 6–10

[132] JUELS, Ari, KOSBA, Ahmed, SHI, Elaine, The ring of gyges: Using smart contracts for crime, *aries*, sv. 40, 2015, str. 54

[133] DUPONT, Quinn, MAURER, Bill, Ledgers and Law in the Blockchain, *Kings Rev. 23 June 2015 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-svi-2017]

[134] BECK, Roman *i ostali*, Blockchain–The Gateway to Trust-Free Cryptographic Transactions, *ECIS 2016 Proc.*, 2016, str. 1–14

[135] JAYARAMAN, Prem Prakash *i ostali*, Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation, *Future Gener. Comput. Syst.*, 2017, Dostupno na: http://www.sciencedirect.com/science/article/pii/S0167739X17303308. [Pristupljeno: 24-svi-2017]

određeni način „sudjeluju u odlučivanju“ na koji način i za koju namjenu mogu biti potrošene.[136]

[136] GLADDEN, Matthew E., Cryptocurrency with a conscience: Using artificial intelligence to develop money that advances human ethical values, 2015, str. 90

7 ZAKLJUČAK

Prema njihovim zagovornicima, digitalne valute imaju nekoliko glavnih obilježja koja se navode kao velika prednost i razlog za prihvaćanje njihove uporabe. Ova obilježja nalaze se na puno mjesta gdje se objašnjava definicija neke digitalne valute, kao na primjer Bitcoin-a, a to su prije svega:

- decentraliziranost kontrole takvog sustava, bazirana na uporabi blockchain tehnologije
- ograničenost količine novčanih jedinica bilo tehnički, algoritmom ili konvencijom zajednice korisnika
- anonimnost korištenja
- praktičnost i efikasnost korištenja, pogotovo u internetskoj trgovini

Gledajući redom, pojam decentraliziranosti naglašava se u kontekstu nepostojanja autoriteta kontrole nad sustavom, što bi na određeni način trebalo implicirati veću demokratičnost sustava. Decentraliziranost se često dodatno pokušava naglasiti umanjivanjem važnosti uloge kreatora sustava, te kako je slučaj s Bitcoinom, njegovom anonimnošću. Činjenica jest da se države kao kontrolori svojih ekonomija koriste regulacijom količine novca u opticaju kao jednom od važnih makroekonomskih poluga. Kontrola novčanih transakcija nužna je za realizaciju svakog poreznog sustava, koji je opet cijena življenja u uređenom društvu.

U radu je prikazana određena analiza centraliziranosti valuta baziranih na blockchain-u, iz koje se vidi da ona ni u ovom slučaju nije apsolutna, odnosno u određenim teoretskim okolnostima (npr. udruživanje nekoliko najvećih čvorova kod Bitcoin sustava) takav sustav bi postao centraliziran, bez obzira što sama tehnologija to ne traži niti uvjetuje. Društvo u kojem živimo organizirano je na principu hijerarhije i samim tim centralizirano u nekim ključnim aspektima. Pitanje je koliko je uopće moguća ideja realizacije potpuno decentralizirane valute u takvom društvenom uređenju, glede utjecaja na socijalnu politiku, poreznog aparata itd. Zato je za očekivati da će društveni sustav pružati snažan otpor svakoj inicijativi koja remeti njegove temeljne koncepte, a to bi u ovom slučaju bila apsolutno decentralizirana valuta. Ukoliko se situacija u društvu promjeni, imamo spremnu tehnologiju.

Zajednica je u određenoj mjeri svjesna ovog problema i svaka strana pokušava se prilagoditi za opću korist. Afirmacijska grupa radi na unapređenju sustava i njihovoj prilagodbi sadašnjim društvenim okvirima kako bi popularizirala uporabu novih valuta, dok vlasti i institucije rade na uređenju i unapređenju pravnih okvira kako bi se na opću korist uredila uporaba digitalnih valuta.

Pitanje odnosno problem anonimnosti također je analizirano i može se vidjeti da je ono posljedica nedovoljne zainteresiranosti institucija u počecima stvaranja digitalnih valuta. Jasno je da nova tehnologija nudi tehnička rješenja za postizanje značajnog stupnja anonimnosti, ali opet kao što je to slučaj i s centralizacijom, takav koncept moguće je realizirati samo u onoj mjeri u kojoj ne ugrožava temeljne društvene interese. Institucije imaju mehanizme kojima mogu značajno utjecati na stupanj anonimnosti, ukoliko to žele, a to i čine postupno kroz razvoj pravne regulative.

Sve veća baza korisnika digitalnih valuta, i sve veća pozornost javnosti i medija prema njima u zadnje vrijeme, uzrokovana je najčešće velikim porastom tečaja (ili bolje reći cijene?) gotovo svih digitalnih valuta na tržištu. Stvara se izuzetno primamljiva prilika za špekulativna ulaganja i ostvarivanje velikih prinosa. Takve situacije su u povijesti uvijek bile interesantne i dizale veliku prašinu u javnosti.

Jasno je također da nove digitalne valute donose novu dimenziju u razmjeni vrijednosti i trgovini, u praktičnom smislu, boljom efikasnošću, novim mogućnostima, uštedama u vremenu i cijeni i slično, ovisno od primjene do primjene. U tom smislu, ova tehnologija je dobitak za društvo.

Možda najzanimljivije, je pitanje regulacije količine novca u opticaju. Iako je broj novčanih jedinica pojedine digitalne valute kontroliran i predvidljiv, često se zanemaruje da su digitalne valute u velikoj mjeri međusobni supstituti. Iz prethodne analize vidljivo je da je i ogromna količina transakcija rezultat trgovine digitalnih valuta međusobno, a manji dio posljedica je razmjene dobara. U prilog tezi ide i činjenica da su visine prosječnih provizija kod zamjene za klasične valute u prosjeku značajno veće od provizija kod međusobne razmjene digitalnih valuta, te činjenica kako je rast alternativnih valuta značajno veći unatoč njihovoj manjoj prihvaćenosti od trgovaca i manjoj pristupačnosti. Očito je da je pokretač ovog trenda popularnosti špekulativni val, uzrokovan znatiželjom, željom za profitom, i

jednim dijelom i neznanjem. Činjenica je da iako je u sustavu sve transparentno, oni koji prvi ulaze (kreatori) imaju najveću šansu za zaradu ukoliko određena valuta „zaživi“. Naravno da je stanje moguće promijeniti na način prilagodbe pravnog sustava novim okolnostima, i na taj način spriječiti negativnosti a zadržati pozitivne strane digitalnih valuta.

Vrijeme koje dolazi bit će obilježeno značajnim događanjima na polju novca i plaćanja općenito. Inercija tržišta nastala velikim špekulativnim interesom pogurat će sve društvene i ekonomske čimbenike i utjecati na stvaranje određenih interesnih skupina, stvarajući pritiske na cijelu zajednicu, kako bi se adaptirala na novostvorene mogućnosti. Sve veća kritična masa posjednika digitalnih valuta, stvara interese za njihov razvoj i implementaciju u svakodnevni život, nastaju potrebe za reakcijom institucija, zakonodavstava, ekonomija i ostalih društvenih čimbenika. Neovisno u kojem smjeru će se stvari razvijati, činjenica je da digitalne valute istovremeno donose nove mogućnosti ali i nove nedostatke i probleme. Kao i mnogo puta ranije, nove tehnološke mogućnosti mogu se iskoristiti i u pozitivnom i u negativnom smislu. Digitalne valute su novi ekonomski alat, čiji značaj, doprinos i korisnost ovise prije svega o okolnostima i načinu korištenja

LITERATURA

[1] ABRAMOWICZ, Michael, Cryptocurrency-Based Law, *Ariz Rev*, sv. 58, 2016, str. 359, {13}

[2] ABREU, Dilip, BRUNNERMEIER, Markus K., Bubbles and crashes, *Econometrica*, sv. 71, izd. 1, 2003, str. 2, {61}

[3] ALI, Robleh, BARRDEAR, John, CLEWS, Roger, SOUTHGATE, James, The economics of digital currencies, 2014, str. 279, {30,31,32,33}

[4] ANDREESSEN, Marc, Why Bitcoin Matters, *DealBook*, 21-sij-2014, Dostupno na: https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/. [Pristupljeno: 20-svi-2017]. , {57}

[5] AVERY, Christopher, ZEMSKY, Peter, Multidimensional uncertainty and herd behavior in financial markets, *Am. Econ. Rev.*, 1998, str. 724–748, {61}

[6] BADEV, Anton I., CHEN, Matthew, Bitcoin: Technical background and data analysis, 2014, str. 2, {14}

[7] BANDARA, HMN Dilum, JAYASUMANA, Anura P., Collaborative applications over peer-to-peer systems–challenges and solutions, *Peer--Peer Netw. Appl.*, sv. 6, izd. 3, 2013, str. 257–276, {15}

[8] BAYERN, Shawn, Dynamic common law and technological change: the classification of Bitcoin, *Wash Lee Rev Online*, sv. 71, 2014, str. 22, {58,59}

[9] BECK, Roman, STENUM CZEPLUCH, Jacob, LOLLIKE, Nikolaj, MALONE, Simon, Blockchain–The Gateway to Trust-Free Cryptographic Transactions, *ECIS 2016 Proc.*, 2016, str. 1–14, {62}

[10] BORNHOLDT, Stefan, SNEPPEN, Kim, Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies, *ArXiv Prepr. ArXiv14036378*, 2014, str. 4, {57}

[11] BRYANS, Danton, Bitcoin and money laundering: mining for an effective solution, *Ind LJ*, sv. 89, 2014, str. 441, {2}

[12] BUKHARI, Jeff, Bitcoin: Winklevoss ETF May Not be Dead Yet, *Fortune*, Dostupno na: http://fortune.com/2017/03/23/why-the-winklevoss-bitcoin-etf-may-not-be-dead-yet/. [Pristupljeno: 05-svi-2017]. , {49}

[13] BURR, William E., Selecting the advanced encryption standard, *IEEE Secur. Priv.*, sv. 99, izd. 2, 2003, str. 43–52, {12}

[14] 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, {17}

[15] 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, {9}

[16] COINDESK, How can I buy bitcoins?, *CoinDesk*, 20-kol-2013, Dostupno na: http://www.coindesk.com/information/how-can-i-buy-bitcoins/. [Pristupljeno: 05-svi-2017]. , {46,47}

[17] CROSBY, Michael, PATTANAYAK, Pradan, VERMA, Sanjeev, KALYANARAMAN, Vignesh, Blockchain technology: Beyond bitcoin, *Appl. Innov.*, sv. 2, lip. 2016, str. 6–10, {62}

[18] DANEZIS, George, MEIKLEJOHN, Sarah, Centrally banked cryptocurrencies, *ArXiv Prepr. ArXiv150506895*, 2015, str. 1, {60,61}

[19] DE FILIPPI, Primavera, Bitcoin: a regulatory nightmare to a libertarian dream, *Brows. Download This Pap.*, 2014, str. 1, {15}

[20] DELMOLINO, Kevin, ARNETT, Mitchell, KOSBA, Ahmed, MILLER, Andrew, SHI, Elaine, Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, u *International Conference on Financial Cryptography 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], {2}

[21] DOGUET, Joshua J., The Nature of the Form: Legal ad Regulatory Issues Surrounding the Bitcoin Digital Currency System, *La. Law Rev.*, sv. 73, izd. 4, 2012, str. 1119, {42}

[22] DOWD, Kevin, HUTCHINSON, Martin, Bitcoin will bite the dust, *Cato J*, sv. 35, 2015, str. 359,364, {19}

[23] DUPONT, Quinn, MAURER, Bill, Ledgers and Law in the Blockchain, *Kings Rev. 23 June 2015 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-svi-2017], {62}

[24] DWYER, Gerald P., The economics of Bitcoin and similar private digital currencies, *J. Financ. Stab.*, sv. 17, 2015, str. 81–91, {23,24}

[25] ELENDNER, Hermann, TRIMBORN, Simon, ONG, Bobby, LEE, Teik Ming, OTHERS, The Cross-Section of Crypto-Currencies as Financial Assets: An Overview, Sonderforschungsbereich 649, Humboldt University, Berlin, Germany,

2016, Dostupno na: https://sfb649.wiwi.hu-berlin.de/papers/pdf/SFB649DP2016-038.pdf. [Pristupljeno: 05-tra-2017], {33,35}

[26] EVANS, David S., Economic aspects of bitcoin and other decentralized public-ledger currency platforms, 2014, str. 19, {60}

[27] FAIRFIELD, Joshua AT, BitProperty, *Cal Rev*, sv. 88, 2014, str. 820, {17}

[28] GANDAL, Neil, HALABURDA, Hanna, Competition in the Cryptocurrency Market, *Bank Can. Work. Pap.*, sv. No. 2014-33, 2014, str. 8, {32}

[29] GERVAIS, Arthur, CAPKUN, Vedran, CAPKUN, Srdjan, KARAME, Ghassan O., Is Bitcoin a decentralized currency?, 2014, str. 1, {14,41}

[30] GLADDEN, Matthew E., Cryptocurrency with a conscience: Using artificial intelligence to develop money that advances human ethical values, 2015, str. 90, {63}

[31] 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-svi-2017], {61}

[32] GOLDFEDER, Steven, BONNEAU, Joseph, KROLL, J. A., FELTEN, E. W., Securing bitcoin wallets via threshold signatures, 2014, str. 13, {19}

[33] GRINBERG, Reuben, Bitcoin: An innovative alternative digital currency, 2011, str. 206, {14,15}

[34] HARWICK, Cameron, Cryptocurrency and the Problem of Intermediation, 2015, str. 571, {24}

[35] HAYES, Adam S., Cryptocurrency Value Formation: An empirical study leading to a cost of production model for valuing Bitcoin, *Telemat. Inform.*, 2016, str. 18, {60}

[36] HERN, Alex, Bitcoin site Inputs.io loses £1m after hackers strike twice, *The Guardian*, 08-stu-2013, Dostupno na: https://www.theguardian.com/technology/2013/nov/08/hackers-steal-1m-from-bitcoin-tradefortress-site. [Pristupljeno: 15-svi-2017], {20}

[37] HUGHES, Sarah Jane, MIDDLEBROOK, Stephen T., Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries, *Yale J Reg*, sv. 32, 2015, str. 495, {55}

[38] HUGHES, Sarah Jane, MIDDLEBROOK, Stephen T., Regulating cryptocurrencies in the United States: Current issues and future directions, 2014, str. 845, {53}

[39] HURLBURT, George F., BOJANOVA, Irena, Bitcoin: Benefit or Curse?, *IT Prof.*, sv. 16, izd. 3, 2014, str. 13, {20}

[40] INNES, A. Mitchell, What is money?, *Bank. Law J.*, svi. 1913, str. 377–408, {6,7}

[41] IRWIN, Douglas A., The Nixon shock after forty years: the import surcharge revisited, National Bureau of Economic Research, 2012, Dostupno na: http://www.nber.org/papers/w17749. [Pristupljeno: 29-tra-2017], {8}

[42] JAYARAMAN, Prem Prakash, YANG, Xuechao, YAVARI, Ali, GEORGAKOPOULOS, Dimitrios, YI, Xun, Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation, *Future Gener. Comput. Syst.*, 2017, Dostupno na: http://www.sciencedirect.com/science/article/pii/S0167739X17303308. [Pristupljeno: 24-svi-2017], {62}

[43] JUELS, Ari, KOSBA, Ahmed, SHI, Elaine, The ring of gyges: Using smart contracts for crime, *aries*, sv. 40, 2015, str. 54, {62}

[44] KAPLANOV, Nikolei, Nerdy money: Bitcoin, the private digital currency, and the case against its regulation, *Loy Consum. Rev*, sv. 25, 2012, str. 115, {16}

[45] KOBLITZ, Neal, MENEZES, Alfred J., Cryptocash, cryptocurrencies, and cryptocontracts, *Des. Codes Cryptogr.*, sv. 78, izd. 1, 2016, str. 9, {32}

[46] KOSBA, Ahmed, MILLER, Andrew, SHI, Elaine, WEN, Zikai, PAPAMANTHOU, Charalampos, 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], {2}

[47] LAMPORT, Leslie, SHOSTAK, Robert, PEASE, Marshall, The Byzantine generals problem, *ACM Trans. Program. Lang. Syst. TOPLAS*, sv. 4, izd. 3, 1982, str. 382–401, {12}

[48] LO, Stephanie, WANG, J. Christina, Bitcoin as money?, 2014, str. 4, {30}

[49] LUTHER, William J., Cryptocurrencies, network effects, and switching costs, *Contemp. Econ. Policy*, 2015, str. 2, {46}

[50] LUX, Thomas, Herd behaviour, bubbles and crashes, *Econ. J.*, 1995, str. 881–896, {61}

[51] MAESE, Vivian A., Divining the Regulatory Future of Illegitimate Cryptocurrencies, *Wall Str. Lawyer*, sv. 18, izd. 5, 2014, str. 9, {53}

[52] MANKIW, N. Gregory, The data of Macroeconomics, u *Principles of macroeconomics*, Cengage Learning, 2014, str. 220, {8}

[53] MARIAN, Omri Y., Are Cryptocurrencies' Super'Tax Havens?, 2013, Dostupno na: http://scholarship.law.ufl.edu/facultypub/358. [Pristupljeno: 18-velj-2017], {15}

[54] MATTILA, Juri, The Blockchain Phenomenon, *'Book Blockchain Phenomenon'Berkeley Roundtable Int. Econ. 2016 Edn*, 2016, str. 6, {2}

[55] 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}

[56] 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], {11}

[57] MUNDELL, Robert A., *The birth of coinage*. Citeseer, 2002, Dostupno na: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1009.8953&rep=rep1&type=pdf. [Pristupljeno: 29-tra-2017], {8}

[58] NAKAMOTO, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009, Dostupno na: https://bitcoin.org/bitcoin.pdf. [Pristupljeno: 29-ožu-2017]. , {13}

[59] OFFICE, Australian Taxation, Tax treatment of crypto-currencies in Australia - specifically bitcoin, Dostupno na: http://agov-display-g2.prod.atohnet.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?default. [Pristupljeno: 03-svi-2017]. , {55}

[60] OKUPSKI, Krzysztof, Bitcoin Developer Reference, *Availabl E Httpenetium ComresourcesBitcoin Pdf*, 2014, str. 2, {24,25}

[61] OMOHUNDRO, Steve, Cryptocurrencies, smart contracts, and artificial intelligence, *AI Matters*, sv. 1, izd. 2, 2014, str. 19–21, {2}

[62] PILKINGTON, Marc, Blockchain technology: principles and applications, *Res. Handb. Digit. Transform.*, ruj. 2015, str. 4,5, {4}

[63] PLASSARAS, Nicholas A., Regulating digital currencies: bringing Bitcoin within the reach of IMF, *Chic. J. Int. Law*, sv. 14, 2013, str. 377, {29}

[64] RAYMAEKERS, Wim, Cryptocurrency Bitcoin: Disruption, challenges and opportunities, *J. Paym. Strategy Syst.*, sv. 9, izd. 1, 2015, str. 32, {30}

[65] RITTER, Joseph A., The transition from barter to fiat money, *Am. Econ. Rev.*, sv. 85, izd. 1, ožu. 1995, str. 134, {7}

[66] ROGOJANU, Angela, BADEA, Liana, OTHERS, The issue of competing currencies. Case study–Bitcoin, *Theor. Appl. Econ.*, sv. 21, izd. 1, 2014, str. 107, {13}

[67] ROTHBARD, Murray N., Austrian definitions of the supply of money, *New Dir. Austrian Econ.*, 1978, str. 143–156, {14}

[68] SELIJ, Jan-Willem, CoinShuffle anonymity in the Block chain, 2015, Dostupno na: http://rp.delaat.net/2014-2015/p77/report.pdf. [Pristupljeno: 17-svi-2017], {42}

[69] TRAUTMAN, Lawrence J., Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?, 2014, str. 8, {46}

[70] 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, {13}

[71] WHITTAKER, Zack, Bitstamp exchange hacked, $5M worth of bitcoin stolen, *ZDNet*, Dostupno na: http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/. [Pristupljeno: 15-svi-2017]. , {20}

[72] WOO, David, GORDON, Ian, IARALOV, Vadim, Bitcoin: a first assessment, *FX Rates*, 2013, str. 2, {15,16}

[73] WRIGHT, Aaron, DE FILIPPI, Primavera, Decentralized blockchain technology and the rise of lex cryptographia, 2015, str. 2,3, {41,57}

[74] ZOHAR, Aviv, Bitcoin: under the hood, *Commun. ACM*, sv. 58, izd. 9, 2015, str. 108,110, {21,23}

[75] All Currencies | CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/all/views/all/. [Pristupljeno: 05-tra-2017]. , {33,34,35,45}

[76] Bitcoin ATM Map, Dostupno na: https://coinatmradar.com/. [Pristupljeno: 05-svi-2017]. , {47,48}

[77] Bitcoin Block Explorer - Blockchain, Dostupno na: https://blockchain.info/. [Pristupljeno: 11-velj-2017]. , {22}

[78] Bitcoin regulation overhaul in Japan » Brave New Coin, Dostupno na: https://bravenewcoin.com/news/bitcoin-regulation-overhaul-in-japan/. [Pristupljeno: 22-svi-2017]. , {56,59}

[79] Bitcoin u papirnatom obliku, Dostupno na: http://i.imgur.com/s4kv4.jpg. [Pristupljeno: 13-tra-2017]. , {18}

[80] CryptoCurrency Market Capitalizations, Dostupno na: https://coinmarketcap.com/. [Pristupljeno: 31-ožu-2017]. , {1,31,33,37}

[81] EBA warns consumers on virtual currencies - View press release - European Banking Authority, Dostupno na: https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies. [Pristupljeno: 02-svi-2017]. , {51}

[82] E-novac - HNB, Dostupno na: https://www.hnb.hr/o-nama/zastita-potrosaca/bezgotovinska-placanja/e-novac. [Pristupljeno: 02-svi-2017]. , {51}

[83] Find your people | Meetup, Dostupno na: http://www.meetup.com/. [Pristupljeno: 05-svi-2017]. , {46}

[84] GRAYSCALE, Dostupno na: https://grayscale.co/. [Pristupljeno: 05-svi-2017]. , {48}

[85] Introducing subscriptions and local currency pricing, *Facebook for Developers*, Dostupno na: https://developers.facebook.com/blog/post/2012/06/19/introducing-subscriptions-and-local-currency-pricing/. [Pristupljeno: 24-tra-2017]. , {38}

[86] Japan's Bitcoin Law Goes Into Effect Tomorrow, *CoinDesk*, 31-ožu-2017, Dostupno na: http://www.coindesk.com/japan-bitcoin-law-effect-tomorrow/. [Pristupljeno: 22-svi-2017]. , {56,59}

[87] Nearly $2M in bitcoins feared lost after Chinese cryptocurrency exchange hack, *Tech in Asia*, 16-velj-2015, Dostupno na: https://www.techinasia.com/bitcoins-lost-after-china-cryptocurrency-exchange-hack-bter. [Pristupljeno: 15-svi-2017]. , {20}

[88] New Active Trading Bitcoin Fund Seeks UK Investors, *CoinDesk*, 28-ožu-2014, Dostupno na: http://www.coindesk.com/new-active-trading-bitcoin-fund-seeks-uk-investors/. [Pristupljeno: 05-svi-2017]. , {49}

[89] popis_misljenja - Posredovanje pri kupnji i prodaji virtualne..., Dostupno na: https://www.porezna-uprava.hr/HR_publikacije/Lists/mislenje33/Display.aspx?id=19252. [Pristupljeno: 02-svi-2017]. , {51}

[90] SEC Rejects Winklevoss Bitcoin ETF Bid, *CoinDesk*, 10-ožu-2017, Dostupno na: http://www.coindesk.com/sec-shoots-winklevoss-bitcoin-etf-bid/. [Pristupljeno: 05-svi-2017]. , {49}

[91] State Regulators Issue Model Regulatory Framework for Virtual Currency Activities, Dostupno na: https://www.csbs.org/news/press-releases/pr2015/Pages/PR091515.aspx?PF=1. [Pristupljeno: 03-svi-2017]. , {54}

[92] The Ill Wind of Bitcoin Exchange Hackings - Once Bitten, Twice Shy!! (Part 1), *NEWSBTC*, 20-ruj-2015, Dostupno na: http://www.newsbtc.com/2015/09/20/the-ill-wind-of-bitcoin-exchange-hackings-once-bitten-twice-shy-part-1/. [Pristupljeno: 15-svi-2017]. , {20}

[93] Virtual currency schemes, lis-2012, Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. [Pristupljeno: 20-ožu-2017]. , {26,27,28,37,50}

[94] Virtual currency schemes - a further analysis, velj-2015, Dostupno na: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf? [Pristupljeno: 18-velj-2017]. , {52,53}

[95] World Payments Report, Dostupno na: https://www.worldpaymentsreport.com/. [Pristupljeno: 20-tra-2017]. , {10}

TECHNICAL, ECONOMIC AND LEGAL ASPECTS OF DIGITAL MONEY

Summary:

This paper analyzes the technical, economic and legal aspects of digital currencies, their relationship with classical money, market reviews, and trend estimates. An overview of their technical specifications is provided to help them better understand the security aspects and their current legal status in order to set certain assumptions about trends. It is evident that huge volumes of transactions are the result of a digital currency trading, and a minor part of the result is the exchange of goods. It is obvious that the driving force behind this trend of popularity is the speculative wave, caused by curiosity, desire for profit, and partly by ignorance, or by neglecting the fact that digital currencies are largely mutually substitutable. Although the system is transparent, those who enter first (creators) have the highest chance of earning if a particular currency "comes to life". Of course, the situation can be changed in ways of adjusting the legal system to new circumstances, thus preventing negativity and keeping the positive side of digital currencies. The hypothesis is that in the society in which we live, which is by its nature centralized and hierarchically organized, phenomena such as digital currencies, despite the technical possibilities, can not fully fulfill their task without the proper response of the institutions that manage the society by creating the appropriate legal and economic regulatory frameworks.

Keywords:

digital currencies, cryptocurrencies, virtual currencies, virtual money, digital money, blockchain, bitcoin, virtual currency schemes

PRILOZI