FBIM Transactions
DOI 10.12709/fbim.07.07.02.14

NEVIDLJIVE TRANSAKCIJE U DARK WEB-U

STEALTH TRANSACTIONS IN THE DARK WEB

Sergej Uljanov
Fakultet za poslovne studije i pravo Univerztiteta „UNION – Nikola Tesla“, Beograd, Republika Srbija

Đorđe Milošević
Kriminalističko-policijski univerzitet, Beograd, Republika Srbija

JEL Kategorija rada: **E49, F38, L86**

Apstrakt

Autori u ovom radu razmatraju mogućnosti vršenja novčanih transakcija skrivenih u okruženju dark web-a. Kao ključne komponente ovakve aktivnosti autori ističu fenomenološki tripod, koji čine pojmovi kripto valute, blokčejn tehnologije i virtuelnog novčanika (web wallet). S tim u vezi, autori će prikazati u radu, u posebnim poglavljima, pojmove i vrste virtuelnog novca, web wallet-a i način funkcionisanja blokčejn razmene podataka odnosno jedinica kripto valute. Poseban osvrt biće napravljen u odnosu na pitanja anonimnosti i skrivanja tragova novčanih tokova u Darknetu. Autori teže da objasne razloge zbog kojih nosioci transakcija virtuelnog novca insistiraju na svojoj anonimnosti i nemogućnosti praćenja njihove aktivnosti od strane drugih subjekata prisutnih u tamnom vebu, bez obzira na to da li je reč o hakerima ili organima za primenu zakona. Takođe, autori smatraju značajnim obuhvatno posmatranje želje za anonimnim delovanjem, koja ne podrazumeva uvek i isključivo kriminalnu intenciju. U radu su otvorena pitanja stvarne anonimnosti virtuelnih novčanika, kao i ranjivosti blokčejn modusa u odnosu na sajber napade i zloupotrebu radi skrivanja novčanih transakcija u kriminalne svrhe, te „pranje“ kripto valuta. Autori u radu nastoje da iznesu najnovije podatke koji se odnose na navedenu problematiku, kako bi istraživani fenomen mogao biti sagledan u svojoj aktuelnosti. Namera autora je da svoje zaključke temelje na punoj voluminoznosti ključnih pojmova, čiji značaj predstavlja okosnicu ovog rada.

Ključne reči: *dark web, kripto valuta, blokčejn, web wallet, kripto novčanik, „pranje“ virtuelnog novca, transakcija kripto valute*

Abstract

The authors of this article deem possibilities of doing money transactions covered by the network of the dark web. As key components of such activity, the authors highlight phenomenological tripod made of terms related to cryptocurrency, blockchain technology and virtual wallet (known as web wallet). Thereby, the authors are about to present in this article, as chaptered, terms and kinds of

Adresa autora zaduženog za korespodenciju:
Đorđe Milošević
djodjolos@gmail.com

virtual money, web wallets and the way of running, both, blockchain exchanging of data and of cryptocurrencies units. The special overview is to be done considering questions of anonymity and hiding traces of money transactions in the Darknet. The authors tend to explain the reasons why subjects of cryptocurrency transactions insist to remain stealth and anonymized having their activities untraceable to other subjects presented in the dark web, no matter if it is up to hackers or law enforcement. Also, the authors consider it as important to make a broader view of the phenomenon of having a need for an anonymized way of doing transactions, which is not always to be solely connected to criminal intent. There are issues of virtual wallets anonymity and blockchain modus vulnerability relate to cyber-attacks and misuse of stealth money transactions, both, for illegal purposes and for cryptocurrencies money laundering, to be mattered in this article. The authors strive to express the most recent data on the above-mentioned challenges, to make researched phenomena to be perceived as an actual one. The intention of the authors is to base their conclusions on the full-scale volume of essential terms whose importance represents a framework for this article.

Keywords: *the dark web, cryptocurrency, blockchain, web wallet, dark wallet, cryptocurrency money laundering, cryptocurrency transaction*

1. UVOD

Digitalna era prekinula je i gotovo prevazišla tradicionalno organizovanje baza podataka u svakoj oblasti poslovanja uvodeći standarde koji podrazumevaju njene produkte, kao što su elektronsko trgovanje, društvene mreže, kripto valute, cloud computing i obrada kompleksnih setova podataka. Brz napredak u razvoju i inovacijama digitalnih proizvoda otvorio je mogućnosti za neovlašćen pristup zaštićenim podacima i sajber krađe. Zbog ovakvih pretnji, korisnici se sve više opredeljuju za informatičke proizvode koji štite privatnost i podižu nivo sajber bezbednosti. Korisnici koji se kreću u prostorima digitalnih tržišta, upotrebljavaju elektronski način plaćanja i razmenjuju informacije na grupnim forumima zahtevaju veći stepen anonimnosti za svoje prisustvo i svoje aktivnosti na globalnom vebu, a naročito u njegovom nevidljivom delu Deep Web-u u kome se odvija intenzivna onlajn komunikacija i realizuju novčane transakcije. Platforme koje omogućuju anonimnost podataka, svakako, čine rešenje za ovakav problem korisnika. Ove platforme postoje u formi web wallet odnosno virtuelnog novčanika, poznatog i kao dark wallet, te skrivenih mreža za komunikaciju u dubokom vebu, posebno u njegovoj Darknet zoni. Jedna od ovakvih mreža je, prvenstveno, izraz kapaciteta pretraživača TOR, čija eksploatacija ne eksponira identitet korisnika. Kao ulaznica u polje dark web-a, TOR je značajna karika u lancu kretanja korisnika kroz neprozirne slojeve nevidljivog veba.

Darknet je popularniji nego posećeniji, jer samo manja populacija korisnika poznaje načine njegovog funkcionisanja. Za ogromnu većinu korisnika tamni veb je misteriozni deo dubokog veba, povodom koga i dalje ima više pitanja nego odgovora. U njegovom okruženju, pored ostalih diskretnih aktivnosti, kripto valute svojim tokovima doprinose održavanju i razvoju ilegalnog prometa i jačanju kriminalnih tržišta. Nevidljive transakcije pomoću blokčejn tehnologije privlače brojne korisnike da plasiraju svoj virtuelni novac na „crna“ tržišta Darkneta i tako anonimno dođu do zabranjenih proizvoda odnosno nelegalnih informatičkih sadržaja, usluga i servisa.

Da bi anonimna transakcija kripto valute na kriminalnom tržištu tamnog veba bila ostvariva neophodna je sinergija tripoda njenih komponenti: kripto valuta, blokčejn tehnologije i web wallet-a, kojima posvećujemo sledeće redove.

2. KRIPTOVALUTE

Bitkoin je digitalni fenomen koji je imao iznenađujuće brz razvoj kao monetarni entitet sposoban da očuva vrednost, ali i kao sredstvo razmene. Međutim, rame uz rame sa porastom njegove popularnosti, ovaj virtuelni novac postao je učestala meta krađe i izuzetno tražena platežna jedinica za potrebe ilegalnog poslovanja. S tim u vezi, napomenućemo da kao način odbrane anonimnosti i privatnosti učesnika u transakciji kripto valute, može da posluži dark wallet koji je vrsta web wallet-a odnosno kripto novčanika zaštitnika virtuelnog novca od sajber napada i krađe.

Najveći protivnik kripto valute je nedovoljna obaveštenost javnosti o njenoj svrsi, s obzirom na to da se ovaj digitalni novac predstavlja kao činilac privatnosti korisnika koji se ne može kontrolisati. Ipak, koncept virtuelnog novca nije shvaćen u potpunosti jer je mreža za razmenu bitkoina dostupna na javnom registratoru što smanjuje garanciju potpune anonimnosti korisnika.

Bitkoin nije samo fenomen koji je postavio trend upotrebe virtuelnog načina plaćanja roba i usluga, već je činjenicom svoje upotrebljivosti u decentralizovanoj peer-to-peer mreži (u kojoj su svi učesnici jednaki) postao standard za kreiranje kripto valuta i kao takav izazov i inspiracija za mnoge dizajnere virtuelnog novca.

Pre upoznavanja sa drugim vrstama kripto valuta, koje se uslovno rečeno mogu posmatrati kao alternative bitkoinu, neophodno je najpre sagledati smisao virtuelnog novca uopšte. Naime, reč je o digitalnom novcu, koji ima oblik kovanica. Dok su neke vrste kripto valuta dostupne u fizičkom svetu posredstvom kreditnih kartica, velika većina ovakve vrste novca ostaje potpuno neopipiljiva (Bajpai, 2019).

Tajnost kripto valuta odnosi se na diskretnost složenog postupanja sa digitalnim kovanicama, koje se odnosi na njihovo generisanje, čuvanje i bezbednu transakciju, uz prerogativ anonimnosti. Uz tajnost, kao ključnu karakteristiku, kripto valute odlikuje i decentralizovanost načina upotrebe jer su nastale timskim radom, koji je kodirao proces njihovog izdavanja (često nazivan „iskopavanje rude“) i kontrole tokova njihovog plasiranja (Bajpai, 2019). Kripto valute su dizajnirane na načine koji ih skrivaju od kontrole državnih organa, zbog čega su često izložene javnoj kritici.

Pored bitkoina, sve druge vrste virtuelnog novca nazivaju se alternativne kripto valute i njihovi kreatori nastoje da ih predstave kao izmenjenu ili unapređenu verziju bitkoina. Neke od ovih digitalnih valuta se „iskopavaju“ jednostavnije od bitkoina, ali mogu biti manje likvidne, manje prihvatljive i zato manje vrednosti jer način njihovog generisanja uslovljava njihov kvalitet (Bajpai, 2019).

Nije moguće obuhvatno predstaviti jedinstvenom listom sve postojeće kripto valute jer neprestano nastaju nove. Danas ima više od 1.600 virtuelnih moneta i mnoge od njih su popularne u različitim grupama sponzora i ulagača (Bajpai, 2019). Polje kripto valuta se stalno uvećava, pa se bitcoin već uveliko posmatra kao inicijalna pionirska moneta u odnosu na koju se određuju parametri za kreiranje novih virtuelnih valuta (Bajpai, 2019). Uobičajeno je da se rejting kripto valuta uspostavlja prema njihovoj tržišnoj vrednosti, što je *inter alia* uzeto u obzir prilikom narednog redosleda njihovog izlaganja.

2.1. Vrste kripto valuta

U odnosu na veliki broj postojećih alternativnih kripto valuta, od kojih su među najpopularnijima: ethereum, ripple, bitkoin keš, litecoin, cardano, neo, eos, iota, dash, monero, ark, nem, vechain, tether, lisk, gas, qtum, aelf, icon, zcash, waves, steem, verge, ardor, ox, nano, tron, stellar, dent, salt i dr., podrobnije ćemo razmotriti značaj sledećih virtuelnih moneta:

1. Litecoin, nastala 2011. godine, bila je jedna od prvih virtuelnih valuta koje su pratile uzor bitkoina i često je karakterisana kao srebrna verzija bitkoinovog zlatnika. Ova kripto valuta koncipirana je na globalnoj otvorenoj platnoj mreži, koja nije pod centralizovanom kontrolom. Litecoin kao verifikator koristi algoritamsku šifru čije dekodiranje izvodi glavni procesor na korisničkom nivou. Premda litecoin u velikoj meri podseća na bitcoin, ipak ima veću brzinu u generisanju digitalnih podataka i nudi bržu potvrdu transakcije. U porastu je broj sajber trgovaca koji su prihvatili ovaj kripto novac, kao i onih koji doprinose njegovom razvoju. Početkom februara, 2019. godine, litecoin je imao tržišnu vrednost od 2.630.000.000 američkih dolara, uz pojedinačnu vrednost kovanice u iznosu od 43,41 američka dolara (Bajpai, 2019).
2. Nastala tokom 2015. godine, ethereum je decentralizovana softverska platforma koja omogućuje izradu protokola neposrednih transakcija i mrežnih softvera bez radnog diskontinuiteta angažovanih umreženih računarskih jedinica, mogućnosti prevare, kontrole ili mešanja treće strane. Aplikacije se pokreću na ovoj platformi na svakoj kovanici kripto valute. Kovanice nalikuju vozilima koja se kreću po platformi, pa ulagači svoja

potraživanja drugih kripto valuta obavljaju posredstvom ethereum-a. Tokom 2014. godine, ethereum je plasirao pretprodaju kovanica, koja je naišla na neočekivano veliki odgovor korisnika. Prema devizi svojih kreatora, ova kripto valuta može biti upotrebljena za organizovanje, decentralizovanje, obezbeđivanje i trgovinu svega i svačega. Posle hakerskog napada 2016 godine, od ethereum-a je izdvojen ethereum classic, kao poseban vid ove virtuelne monete. Početkom 2019. godine, tržišna vrednost ethereum-a iznosila je 12.490.000.000 američkih dolara, a vrednost pojedinačne kovanice bila je 118,71 američki dolar (Bajpai, 2019).

3. Zcash je decentralizovana kripto valuta otvorenog tipa, koja je plasirana krajem 2016. godine. Kreatori tvrde da bitkoin svojom važnošću predstavlja http (glavni protokol) za finansije, ali da zcash u tom smislu predstavlja https (obezbeđen glavni protokol). Ova kripto valuta nudi privatnost i selektivnu transparentnost transakcija. Tako, poput https-a, zcash može da obezbedi izuzetan stepen bezbednosti ili privatnosti u slučajevima gde se sve transakcije registruju i izdaju u blokčejn modusu, ali da pri tom podaci o pošiljaocu, primaocu i visini iznosa ostaju u sferi privatnosti. Zcash omogućuje svojim korisnicima zaštićene transakcije, čiji sadržaj je kriptovan upotrebom napredne kriptografske tehnike sa nazivom zk-SNARK, koju kreira isti tim tvoraca ove virtuelne valute. U prva dva meseca 2019. godine, zcash je ima tržišnu vrednost od 291.500.000 američkih dolara, dok je pojedinačna vrednost kripto kovanice iznosila 49,84 američka dolara (Bajpai, 2019).
4. Dash je kripto moneta, poznata i kao darkcoin, koja je diskretnija verzija bitkoina. Dash nudi veći stepen anonimnosti jer funkcioniše preko decentralizovane mreže glavnog koda koja gotovo sasvim onemogućava praćenje tragova transakcije. Ova kripto moneta nastala je 2014. godine i za kratko vreme dobila je veliki broj korisnika. U prvom tromesečju 2015. godine darkcoin je promenio ime u dash, što je skraćenica od digital cash odnosno digitalne gotovine. Ova izmena nije uticala na funkcionalnost informatičkih alata, kao što su DarkSend za mešanje kovanica radi povećanja njihove anonimnosti i InstantX koji omogućava brze digitalne transakcije u rasponu od 3 američka centa do 3.000 američkih dolara. Početkom 2019. godine, tržišna vrednost dash-a bila je 640.760.000 američkih dolara, uz pojedinačnu vrednost kovanice od 74,32 američka dolara (Bajpai, 2019).
5. Ripple je globalna mreža koja u realnom vremenu nudi brzu, pouzdanu i jeftinu mogućnost vršenja uplata na međunarodnom nivou. Nastala je 2012. godine. Njeno potvrđivanje konsenzusom korisnika ne zahteva generisanje „iskopavanjem“ zbog čega se ripple kripto novac odvojio od bitkoina i drugih alternativnih virtuelnih moneta. S obzirom da ripple ne zahteva „iskopavanje“, to umanjuje angažovanje računarskih jedinica i minimizira usporenost mreže. Ideja tvoraca ripple-a je da distribucijom vrednosti motivišu razvoj poslovnosti, podignu nivo likvidnosti provajdera i prodaju ovu kripto valutu institucionalnim kupcima zainteresovanim da investiraju plasiranjem ovog virtuelnog novca. Do sada, ripple je imao uspeha sa ovim modelom funkcionisanja, te je ostao privlačan kao digitalna valuta tradicionalnim finansijskim subjektima, koji traže načine za unapređivanje prekograničnog načina isplate. Na početku 2019. godine, ripple je imao tržišnu vrednost od 12.690.000.000 milijardi američkih dolara, a pojedinačna vrednost njegove kovanice bila je 0,308 američkog dolara (Bajpai, 2019).
6. Monero je bezbedna i anonimna kripto valuta, čije tragove nije moguće pratiti. Ovaj virtuelni novac, otvorenog tipa, nastao je 2014. godine i brzo pobudio interesovanje kriptografske zajednice i entuzijasta. Njegov razvoj je u potpunosti doniran i timski usmeravan. Monero je produkt potrebe za decentralizovanom upotrebom i promenljivom veličinom blokova podataka, što omogućava potpunu privatnost uz upotrebu posebne tehnike zvane prstenasti potpis. Ovo podrazumeva postojanje grupe validnih potpisa, od kojih bar jedan pripada postojećem korisniku, ali se on ne može izdvojiti jer ga krije grupa. Zbog takvog izuzetnog mehanizma zaštite, monero je kao virtuelni novac stekao lošu reputaciju jer se

dovodi u vezu sa kriminalnim operacijama širom sveta. Nebitno da li se ova kripto valuta koristi u dobre ili loše svrhe, ne može se poreći da je njenim nastankom u svet virtuelnih moneta uveden značajni tehnološki pomak. Na početku 2019. godine, tržišna vrednost monera iznosila je 808.500.000 američkih dolara, a vrednost njene kovanice bila je 48,18 američkih dolara (Bajpai, 2019).

7. Bitcoin cash (bitkoin keš) kao kripto moneta zauzima značajno mesto u istoriji alternativnog virtuelnog novca jer je prvi uspešno odvojen od originalnog bitkoina razdvajanjem blokčejn modusa, do kog je došlo usled neslaganja unapređivača ovog kripto novca i onih koji su ga „iskopavali“. Zbog decentralizovane prirode digitalnog novca, obuhvatne promene esencijalnog koda u kovanici moraju biti rezultat konsenzusa svih članova u zajednici korisnika. Ovaj mehanizam varira u zavisnosti od tipa konkretne kripto valute kod koje je došlo do protokolarnog neslaganja u blokčejnu. Bitkoin je, tako, nastao 2017. godine kao rezultat navedenog razdvajanja. Dok je kod bitkoina limit veličine blokova sa podacima striktan i iznosi 1 megabajt, kod bitkoin keša se kreće od 1 do 8 megabajta sa idejom da će veći blokovi doprineti bržem odvijanju transakcije. Ovo je dovelo i drugih promena, kao što je uklanjanje protokola Segregated Witness koji se odnosi na veličinu blokova sa podacima. Početkom 2019. godine, bitkoin keš je imao tržišnu vrednost od 2.230.000.000 američkih dolara, uz pojedinačnu vrednost kovanica od 126,49 američkih dolara (Bajpai, 2019).
8. Neo je nastao 2014. godine pod svojim prvim nazivom AntShares. Do sada, ovo je najzastupljenija kripto valuta koja se pojavila u Kini zbog čega se naziva i kineskim ethereum-om, uzevši u obzir njenu sličnu upotrebu kod ostvarivanja neposrednih transakcija. Tokom 2017. godine, neo je ostvario uspeh sa skokom tržišne vrednosti od 0,16 do čak 162 američka dolara po kovanici, što iznosi uvećanje od neverovatnih 111%. Jedan od razloga za ovakav strelovit uspon leži u podršci koju je ova kripto valuta ostvarila u odnosu na razvoj programskih jezika, kao što su Go, Java, C++ i drugi. Smatramo ključnim afirmativan odnos kineske Vlade prema ovom virtuelnom novcu, imajući u vidu njen rigidan stav prema kripto valutama. Na početku 2019. godine, neo je vredeo na tržištu 492.480.000 američkih dolara, a po kovanici 7,58 američkih dolara (Bajpai, 2019).
9. Cardano je virtuelna moneta kreirana u drugoj polovini 2017. godine, nudeći sve prednosti platforme ethereum u vezi sa neposrednim transakcijama i mobilnim aplikacijama. Tendencija tvoraca ove kripto valute je rešavanje problema interoperabilnosti i veličine blokova podataka u nizu blokčejn modusa. Cardano kripto novac, takođe, je usmeren na prevazilaženje problema međunarodnih isplata, koje su skupe i vremenski zahtevne. Zahvaljujući tako usmerenim naporima kreatora putem ove kripto valute međunarodna isplata bila je realizovana u vremenskom intervalu od nekoliko sekundi. Početkom 2019. godine, cardanova tržišna vrednost iznosila je 1.160.000 američkih dolara, dok je pojedinačna vrednost kovanica bila 0,041 američkog dolara (Bajpai, 2019).
10. Eos spada u najmlađe kripto valute. Nastala je 2018. godine prema dizajnu ethereum-a, tako da nudi platformu za razvoj decentralizovanih aplikacija. Prvi plasman ovog virtuelnog novca doneo je 4.000.000.000 američkih dolara od usluga upućenih masovnom broju korisnika. Eos funkcioniše prema distribuiranom konsenzusu na svojoj mreži u kojoj se razmenjuje prema blokčejn modusu, pri čemu je svaki sledeći blok podataka izabran slučajnom kombinacijom promenljivih faktora, kao što su imovinska vrednost ili starosna dob. Ovo je razlog zašto eos upotrebljava blokove podataka promenljive veličine. Ova kripto valuta ima svoj operativni sistem, koji igra ulogu blokčejn mreže za razmenu eos kovanica. Eos je izuzetno napredan kripto novac jer ne zahteva „rudarenje“ da bi se proizvodile njegove kovanice. Umesto toga, proizvođači blokova podataka bivaju nagrađeni eos kovanicama u zavisnosti od dostignutog stepena ostvarene proizvodnje. Eos podrazumeva složen sistem pravila koja se odnose na upravljanje navedenim procesom, sa ciljem da mreža ovog virtuelnog novca bude više

decentralizovana od sistema rivalskih kripto moneta. Krajem 2018. godine, tržišna vrednost eos-a bila je 2.490.000.000 američkih dolara, dok je pojedinačna vrednost njegove kovanice iznosila 2,47 američkih dolara (Bajpai, 2019).

Bitkoin nastavlja da predvodi ostale kripto valute, prema kriterijumima tržišne vrednosti, baze podataka korisnika i popularnosti. Ipak, virtualne monete kao što su ethereum i ripple, koje se više koriste u preduzetničke svrhe, postaju sve zastupljenije. Vreme će pokazati da li će i koje kripto valute, zbog revolucionarnosti svojih performansi, potisnuti konkurentske alternativne virtuelne monete i prevazići rešenja koja za sada nudi bitkoin. Prema nekim mišljenjima bitkoin nije anoniman zbog čega je podesan za ilegalne aktivnosti i „pranje“ virtuelnog novca (Canellis, 2018), dok ima i tvrdnji koje afirmativno ocenjuju prednosti bitkoina jer omogućava izbegavanje sporosti protokola tradicionalnih finansijskih institucija (Nakamoto, 2009).

2.2. „Pranje” novca zloupotrebom kripto valute

Nasuprot opštem uverenju, nije teško slediti tragove transakcija bitkoina i otkriti podatke onih koji su ih izvršili. Očigledno, blokčejn modus je transparentan, tako da se akteri kriminalnih transakcija bitkoina mogu otkriti. Bitkoin nije anoniman. Za ostale kripto valute i dalje veliki problem predstavlja skrivanje podataka njihovih pošiljaoca, primaoca i potrošača (Canellis, 2018). Ostaje pitanje na koji način nosioci kriminalnih aktivnosti kripto novac, koji potiče iz nezakonite delatnosti, „peru“ i plasiraju u regularne tokove virtuelnih valuta.

Prema nekim mišljenjima ilegalno stečena kripto moneta može se „oprati“ tzv. preturanjem i slobodnom razmenom (Canellis, 2018). Preturanje podrazumeva rasturanje kovanica bitkoina, radi njihovog ponovnog skupljanja. Bitkoini se najpre upućuju na različite adrese, da bi se potom u celokupnom iznosu sve kovanice našle u kripto novčaniku (dark wallet) postavljenom u tamnom vebu (Canellis, 2018). Ovaj postupak ne iziskuje previše pažljivosti, ali nije besplatan. Uobičajeni troškovi iznose 1% do 3% vrednosti virtuelne valute koja se „čisti“ mešanjem. Potrebno je imati jedan web wallet postavljen u regularnoj zoni Interneta, a zatim još dva ili više wallet-a (u ovom slučaju dark wallet-a) koji funkcionišu u okruženju Darkneta. Dalji postupak nalaže da se bitkoini iz web wallet-a pošalju u skrivene dark wallet-e. Ovakva transakcija naziva se „skok“ i može se izvesti više puta u samom tamnom vebu. Svakim „skokom“ više se zameću tragovi transakcije. Kada se niz takvih transakcija završi, bitkoini se prevrću u mešalici odnosno u naročitom informatičkom servisu koji rastura i skuplja kovanice kripto novca, kako bi se još više obezbedio stepen anonimnosti njihovog korisnika. Rasturanje kovanica realizuje se brojnim transakcijama, koje se vrše u nasumičnom intervalu prema bitcoin adresama u TOR-ovoj mreži. Posle mešanja, pretpostavlja se da je kripto valuta „oprana“ odnosno da se ne mogu otkriti podaci njenog korisnika. Takve kovanice razmenjuju se za druge bitkoine, kovanice drugih kripto moneta ili čak legalno izdat nekonvertibilni papirni novac. Neki autori smatraju da ni prikazani postupak ne garantuje bezbednost i privatnost korisnika kripto novca koje se „pere“ jer se ovakvi servisi za preturanje i mešanje virtuelnih valuta koriste u kriminalne svrhe i mogu oštetiti bez kontrole inicijatora navedenih transakcija (Canellis, 2018), dok postoje i osporavanja funkcionalnosti dark wallet-a u TOR-ovoj mreži uz isticanje prevaziđenosti takvog načina postupanja (Khatwani, 2019).

Kao jednostavniji način „pranja“ virtuelnog novca može poslužiti slobodna razmena (Canellis, 2018). Ova razmena se vrši mimo protokola know-your-customer i anty-money-laundering, u kojima je identifikacija korisnika obavezna. Postupak razmene vrši se bez mešanja kripto valute. Potrebno je trgovati bitkoinima na različitim tržištima više puta. Tako korisnik može da izvrši razmenu bitkoina za kovanice alternativnog virtuelnog novca. Svaki put kada se kripto valuta razmeni za drugu virtuelnu monetu povećava se stepen privatnosti, slično „skokovima“ na wallet adrese u Darknetu. Efektivnost razmene uslovljena je kapacitetom informatičkog servisa koji obavlja uslugu, tako da i ovaj način „pranja“ virtuelnih kovanica nije potpuno siguran. Nakon razmene, korisnik može svoj kripto novac uputiti u dark wallet posredstvom još jedne anonimne transakcije. Naposletku razmenjen virtuelni novac može biti

zamenjen i sa „čistom“ nekonvertibilnom legalnom valutom, ali to je ređi slučaj zbog nepostojanosti i kratkotrajnosti održavanja ovakvih tržišta za razmenu kripto valuta sa legalnim novcem. Nesumnjivo, „perači“ kripto moneta opredeljuju se za skrovita peer-to-peer tržišta i ilegalne usluge u TOR-ovoj mreži, kako bi svoje kriminalno stečene virtuelne kovanice pretvorili u legalnu gotovinu.

Holandska policije je 2016. godine je upala u međunarodni lanac za „pranje“ novca, kojom prilikom je zaplenjeno više bankovnih računa, bitkoin kovanice, luksuzna vozila visoke klase i sastojci za pravljenje sintetičke droge. Utvrđeno je da je u ovom slučaju kripto valuta „čišćena“ slobodnom razmenom i to preko država gde gotovo i da se ne primenjuju protokoli za sprečavanje „pranja“ novca, te da je 97% „opranih“ kovanica završilo u državama koje imaju izuzetno blag režim ograničavajućih protokola (Canellis, 2018).

Postoji, takođe, mogućnost „pranja“ kripto novca, možda manje nedozvoljena ali i dalje u sferi sumnjivih aktivnosti, koja podrazumeva mešanje kovanica i dovodi se u vezu sa zabranjenim sajtovima za kockanje virtuelnim novcem (Canellis, 2018). Ovi sajtovi su pod nadzorom Coinbase servisa za vršenje regularnih razmena. U ovom slučaju, digitalni novac dospeva u blokčejn kockarnica pre nego što se plasira u Coinbase zbog čega pruža mogućnost za „pranje“ virtuelnog novca proisteklog iz kriminalne aktivnosti (Canellis, 2018).

Naposletku, navešćemo još jedan modalitet „pranja“ virtuelnih moneta putem zloupotrebe kripto kartica. U aprilu 2019. godine, Coinbase je ostvario partnerstvo sa Paysafe i Visa provajderima, te svojim korisnicama omogućio snabdevanje kripto karticama (Kaminska, 2019). Posrednici u „čišćenju“ digitalnih kovanica, sada mogu da svojim klijentima predaju kripto kartice i pin brojeve. Time se narušava zadati režim korišćenja kripto kartica, ali tome se ne pridaje poseban značaj. Ključna je činjenica da su kripto kartice i pin brojevi bezlični i ne podrazumevaju kontaktiranje ličnim podacima korisnika u ovakvom mehanizmu za „pranje“ kripto novca zbog čega kripto kartice predstavljaju ozbiljan izvor rizika za savesne nosioce (Kaminska, 2019).

3. BLOKČEJN MODUS

U suštini blokčejn je lanac blokova, u kome „blokovi“ predstavljaju grupu digitalnih podataka, koji su pohranjeni u „lance“ odnosno baze podataka. Preciznije, blokovi su sačinjeni od digitalnih delova informacija i imaju tri osnovna dela. U prvom segmentu bloka, nalaze se podaci o datumu, vremenu, te iznosu novca poslednje realizovane nabavke izvršene preko Interneta. U drugom segmentu, blok sadrži podatke o učesnicima transakcije koji su prikazani kroz digitalni potpis, a nisu navedeni doslovno. U trećem segmentu bloka, pohranjen je identifikacioni jedinstveni kod, poznat kao heš, koji omogućuje međusobno razlikovanje blokova zbog čega nije moguće napraviti istu porudžbinu dva puta. Jedan blok u blokčejnu ima kapacitet do 1 megabajta podataka, što bi značilo da u odnosu na veličinu transakcije, u jednom bloku može biti smešteno nekoliko hiljada transakcija.

Primera radi prikazaćemo javni ključ: 1EHYa6X4Jz2uvNExL504nE41pwXhwL6kWn. Ovaj ključ povezan je sa privatnim ključem kojim se pristupa glavnom kripto novčaniku učesnika u transakciji (Khatwani, 2019). Uvidom u blokčejn pretraživač doći ćemo do saznanja da je na ovoj adresi obavljeno više hiljada transakcija, te da je na njoj istovremeno pozicionirano 7 bitkoina (Khatwani, 2019).

Kada se u blok smeste novi podaci, oni se dodaju i celom lancu. Blokčejn obuhvata veći broj blokova zbog čega predstavlja zbir njihovih kapaciteta za pohranjivanje podataka. Da bi jedan blok bio prihvaćen u blokčejn moraju biti ispunjeni sledeći uslovi. Najpre mora doći do transakcije. Potom ona podleže verifikaciji. U slučaju transakcije bitkoina, oko 5.000.000 računarskih jedinica u svetu mrežno će obaviti kontrolu novih podataka, koji se odnose na vreme transakcije, novčani iznos i učesnike. Sledi pakovanje podataka o transakciji u blok, koji će se pridružiti hiljadama drugih takvih blokova u blokčejnu. Na kraju, svaki blok dobija svoj jedinstveni heš kod kojim se razlikuje od drugih blokova, ali i heš koji ga označava kao poslednjeg u nizu blokčejna. Po dodavanju novog bloka lancu, njegov sadržaj postaje javno dostupan. Moguće je ostvariti uvid u podatke koji su predmet transakcije, kao što su oni koju ukazuju na vreme, mesto i korisnika koji je dodao blok u blokčejn.

Blokčejn je javni registar na kome počiva kompletna mreža za razmenu Bitkoina. Sve potvrđene transakcije nalaze se u blokčejnu. On dozvoljava kripto novčanicima da vrše kalkulaciju svog platnog kapaciteta, tako da nova transakcija može biti verifikovana jer pripada potrošaču koji je pokrenuo. Integritet i hronološki poredak u blokčejnu su kriptografski zaštićene kategorije jer se poruke i transakcije kreću kroz različite blokčejn mreže na bezbedan i matematički pouzdan način (Khatwani, 2018).

Sama transakcija je transfer vrednosti koji se odvija između kripto novčanika sa bitkoinima, koji su uvršteni u blokčejn. Web wallet sadrži i tajni deo podatka, koji se zove tajni ključ ili seme. Ovaj ključ se koristi za potpisivanje transakcije i predstavlja matematičku činjenicu da potiče od vlasnika kripto novčanika kome i pripada. Potpis štiti transakciju od neovlašćenog pristupa jer samo vlasnik tajnog ključa može vršiti transfer podataka na bitkoin adrese koje želi (Khatwani, 2019). Ne treba smetnuti s uma da se podaci kodirani i prikazani kao numerički niz (Khatwani, 2019). Sve transakcije u mreži obično se potvrđuju u roku od 10 do 20 minuta postupkom koji se naziva „iskopavanje“. Ovaj postupak je distribuirani sistem koji počiva na konsenzusu radi potvrde transakcije i njenog upakivanja u blokčejn. Time je naložen i hronološki red postavljanja blokova u lanac, kojim se štiti neutralnost mreže blokčejna i odobrava različitim računarskim jedinicama da jednoglasno svoje slaganje sa stanjem u sistemu. Svaki blok podleže strogim kriptografskim pravilima, čije poštovanje verifikuje mreža blokčejna. Ova pravila sprečavaju izmenu u blokovima koji su već postavljeni u lanac jer bi to oštetilo sve naredne blokove. Postupak „iskopavanja“ podseća na takmičarsku lutriju, koja ne dozvoljava dodavanje novih blokova u blokčejn bez poštovanja navedene procedure. Na ovaj način ne može doći do mogućnosti da grupa ili pojedinac ostvare kontrolu nad sadržajem bloka i lanca, niti da izvrše zamenu delova blokčejna kako bi nedozvoljeno povratili svoja sredstava već namenjena realizovanju transakcije.

U svoj svojoj složenosti, blokčejn kao decentralizovani oblik registrovanja podataka ima gotovo neograničeni potencijal. Tehnologija blokčejna uz reduciranje troškova obezbeđuje veću privatnost korisnicima i viši stepen bezbednosti, uz manju mogućnost greške u svojoj mreži. Prednosti blokčejna svakako su: pojačana preciznost, izostavljanje faktora ljudskog uticaja u procesu verifikacija, smanjivanje troškova zbog eliminisanja treće strane kao verifikatora, decentralizovan sistem koji limitira mogućnost neovlašćenog pristupa i izmene podataka, bezbedno i efikasno obavljanje transakcija uz očuvanje privatnosti učesnika, te transparentna tehnologija. Nedostaci blokčejna mogli bi biti: značajni tehnološki troškovi u vezi sa postupkom „iskopavanja“ bitkoina, usporenost transakcija po sekundi, mogućnost ostvarivanja uvida u hronologiju nelegalnih aktivnosti i osetljivost na hakerske napade. Obzirom da je svaka transakcija registrovana u digitalnom javno dostupnom registratoru, lako se mogu uočiti tragovi koji su zabeleženi u istoriji transakcije i vode do bitkoin adrese korisnika (Vladimir, 2019). Ovo naravno može biti iskorišćeno kao međuprostor u kome privatna korporacija ili određeni državni organ mogu diskretno pratiti aktivnosti učesnika transakcije anulirajući njihovu privatnost (Greenberg, 2014).

4. WEB WALLET

Kripto novčanik je namenjen čuvanju virtuelnog novca i prevashodno služi da zaštiti privatnost korisnika. Dark wallet je kripto novčanik koji je vrsta web wallet-a posebno kreirana da omogući anonimnost svog korisnika (Vladimir, 2019). Njemu mogu pristupiti sve kategorije korisnika jer je dobro dizajniran i dostupan. Ipak, zbog imperativa da garantuje anonimnost korisnika rašireno je verovanje da dark wallet najviše upotrebljavaju prekršioci zakona. Postoje mišljenja da je upravo dark wallet-om omogućeno da se u sajber prostoru vrše brojne kriminalne aktivnosti zbog čega je kritikovan u oblasti kripto zaštite (Vladimir, 2019). Bez obzira na različite stavove o ulozi dark wallet-a, činjenica je da se njime nedvosmisleno doprinosi vršenju nevidljivih isplata, te da bez njega mešanje radi „pranja“ virtuelnih kovanica u CoinJoin servisu ne bi bilo moguće. Neki autori navode da je kripto novčanik softver namenjen „pranju“ novca (Greenberg, 2014). Ima tvrdnji da „perači“ novca mešalicama digitalnih moneta neprestano eksploatišu nove adrese wallet-a, koje se generišu automatski, što pogoduje organizatorima sive ekonomije i kriminalnih tržišta da koordiniraju transakcijama u

tamnom vebu radi „čišćenja“ kripto valuta (Kaminska, 2019). Prisutna je i opasnost da se kripto novac poslat radi „čišćenja“ u nečiji virtuelni novčanik, nikada ne vrati pošiljaocu (Kudlovich, 2018).

Kripto novčanik je digitalni alat za zaštitu privatnosti, koji pojačava anonimnost tako što transakcije bitkoina čini nevidljivim. Struktura njegovog dizajna podrazumeva tri obavezna podsegmenta tzv. džepova, koje korisnik može za svoje potrebe kreirati u većem broju. Ovi podsegmenti odnose se na potrošnju, poslovanje i uštedu. Svaki od njih ima svoj poseban „nevidljivi“ mod u kome korisnik može da obavlja privatne transakcije virtuelnim novcem. Međutim i pored navedenih karakteristika dark wallet-a, postoje kritike na račun ne obaziranja njegovih provajdera na potrebe privatnosti, koja bi u dovoljnom stepenu obezbedila samostalno finansijsko delovanje korisnika (Reutzel, 2016).

Dark wallet od ostalih kripto novčanika razlikuju sledeće performanse, koje ga odlikuju. Reč je najpre o modu za skrivanje adrese. On maskira svaku transakciju bitkoina, koja se vrši iz kripto novčanika, što ometa napore praćenja tragova transakcije koji vode do njenog inicijatora. Svaka transakcija je enkriptovana, pa nijedan od učesnika u transakciji ne može znati adrese drugih učesnika. Postoji i opcija mešanja digitalnih kovanica iz najmanje dve transakcije zbog čega se otežava otkrivanje njihovih korisnika, koji te transakcije realizuju. Kad god neki od korisnika pošalje iznos virtuelnih kovanica na određenu adresu, kripto novčanik izabere drugu transakciju koja se vrši istovremeno i meša virtuelni novac iz obe transakcije radi izbegavanja identifikacije korisnika. Neki autori smatraju da je dark wallet, kao TOR-ov kripto novčanik, zastareo, nefunkcionalan i prevaziđen (Khatwani, 2019). Postoje i druge vrste wallet-a za koje se tvrdi da su najefektivniji u 2019. godini (Khatwani, 2019). Reč je o sledećim vrstama kripto novčanika sa ključnim odlikama navedenim u zagradi: Ledger Nano X (anonimni hardver wallet), Ledger Nano S (anonimni hardver i veb wallet), Samourai Wallet (anonimni mobilni wallet), PINT Wallet (anonimni mobilni wallet), Bitcoinpaperwallet.com (anonimni papirni wallet), BitLox (anonimni hardver wallet) i Electrum (desktop i mobilni wallet).

Dark wallet se konstantno unapređuje. Njegova usluga je stalno dostupna za preuzimanje sa zvaničnog veb sajta. Korisnici su obavezni da otvore fajl iz zip moda i sačuvaju ga na radnoj površini svoje računarske jedinice. Posle preuzimanja i otvaranja fajla, korisnik koristi Chrome pretraživač i iz menija usluga se opredeljuje za ekstenzije. Posle pokretanja razvojnog moda iz postavki i njegovog unošenja u otvoreni fajl, korisnik unosi svoje korisničko ime i lozinku u wallet. Od pošiljaoca se zahteva da za dekodiranje upotrebi jednokratnu šifru kako bi otvorio adresu primaoca, što je podatak koji je poznat samo primaocu. Prema nekim shvatanjima, kripto novčanik je softverska kombinacija javnog i tajnog ključa, te ukoliko je registrovana na papiru opredeljuje wallet kao papirni, a ako se nalazi na mobilnom uređaju određuje wallet kao mobilni (Khatwani, 2019).

Oprečna su mišljenja o prirodi dark wallet-a, od onih koja ističu prednost njegovih informatičkih karakteristika koje doprinose očuvanju anonimnosti i privatnosti korisnika, do drugih koja kritikuju njegov potencijal za skrivanje kriminalnih aktivnosti i ometanje kapaciteta organa za primenu zakona. Ove zabrinutosti su realne, ali ipak ne može se poreći zaštitna uloga kripto novčanika koju ostvaruje jačanjem stepena privatnosti učesnika transakcija i pravljenjem brane prema sajber kradljivcima digitalnih privatnih dobara.

5. ZAKLJUČCI

Paradoks kripto valute je njena dihotomna priroda, zbog čega je bitkoin istovremeno i javan i anoniman (Kudlovich, 2018). Sve transakcije u mrežama tamnog veba ostavljaju svoje tragove, iako javni ključevi ne ukazuju na podatke svojih vlasnika. Kritičan trenutak kada kripto valuta gubi plašt anonimnosti jeste kada korisnik vrši plaćanje ili razmenu odnosno kada bitkoin napušta okrilje dark wallet-a radi plasiranja u tokove transakcije.

Ipak, postoje razni načini zaštite privatnosti korisnika u blokčejn modusu. Jedan od njih je mešalica kripto valute, koja održava anonimnost korisnika virtuelnog novca. Algoritam je jednostavan i podrazumeva da korisnik uputi svoj virtuelni novac na adresu mešalice koja se se za svakog korisnika vodi posebno. Potom se jedinice

kripto valute mešaju sa jedinicama iz transakcija drugih korisnika ili se distribuiraju na pozicije stotine hiljada drugih web wallet-a koji su povezani sa određenom mešalicom. Kada se ovaj postupak okonča, „čisti“ bitkoini se prenose u web wallet koji pripada njihovom prethodnom ili novom vlasniku. Alternativan način ovom postupku predstavljaju posebni web wallet-i, koji obezbeđuju visok stepen privatnosti, kao što je Electrum. Zatim, postoje i wallet-i sa ugrađenim opcijama za mešanje virtuelnog novca (Kudlovich, 2018). Jedan od web wallet-a, dark wallet, ima svoju integrisanu performansu pod nazivom CoinJoin, koja omogućuje da se sve jedinice kriptovalute u transakciji mešaju, te nije moguće otkriti inicijalnog vlasnika plasiranog virtuelnog novca. Više korisnika wallet-a podiže stepen anonimnosti transakcija u Dark Web-u (Kudlovich, 2018).

Kao uspešan primer primene anonimnih kripto valuta za potrebe transakcija u tamnom vebu, navešćemo Z-Pay, kao platni sistem velikog potencijala sa aktivnim razvojem mehanizma za zaštitu privatnosti. Ključna karakteristika ovog sistema je izdavanje i transfer anonimnih računa odnosno čekova, kojima se vrši plaćanje roba i usluga (Kudlovich, 2018).

I pored svih prednosti i mana načina i informatičkih usluga i alata za obezbeđivanje anonimnosti i privatnosti u delovanju korisnika komunikacionih mreža u nevidljivim slojevima dubokog veba, a posebno u njegovom tamnom delu, dark web-u, činjenica je da pokretački impuls za gotovo sva „crna“ tržišta Darkneta predstavljaju prevashodno kriminalna poslovanja bazirana na nevidljivim transakcijama kripto valuta (Report-CAML-20190812, 2019), koje se vrše i radi „pranja“ virtuelnog novca koji potiče iz ilegalnih aktivnosti.

CITIRANI RADOVI

Bajpai, P. (2019). The 10 Most Important Cryptocurrencies Other Than Bitcoin. *Cryptocurrency*. Dostupno na: https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/, preuzeto 12.08.2019.

Canellis, D. (2018). Here’s how criminals use Bitcoin to launder dirty money. *Hard Fork*. Dostupno na: https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/, preuzeto 04.08.2019.

Cryptocurrency Anti-Money Laundering Report, 2019 Q2. (2019). Report-CAML-20190812, *Cipher Trace Cryptocurrency Intelligence*, July 2019, p. 6.

Greenberg, A. (2014). 'Dark Wallet' is about to make Bitcoin money laundering easier than ever. *Wired*. Dostupno na: https://www.wired.com/2014/04/dark-wallet/, preuzeto 05.08.2019.

Kaminska, I. (2019). Why money laundering risk is very real with crypto cards. *Financial Times*. Dostupno na: https://ftalphaville.ft.com/2019/05/31/1559275247000/Why-money-laundering-risk-is-very-real-with-crypto-cards/, preuzeto 01.08.2019.

Khatwani, S. (2018). Private Key vs Public Key: Understanding The Two & Their Importance In Crypto. *The Money Mongers*. Dostupno na: https://themoneymongers.com/private-key-vs-public-key/, preuzeto 17.08.2019.

Khatwani, S. (2019). Anonymous Bitcoin Wallets To Use In 2019. *The Money Mongers*. Dostupno na: https://themoneymongers.com/anonymous-bitcoin-wallets/, preuzeto 05.08.2019.

Khatwani, S. (2019). Bitcoin Private Key: Noob To Expert Guide. *The Money Mongers*. Dostupno na: https://themoneymongers.com/bitcoin-private-key/, preuzeto 15.08.2019.

Kudlovich, Y. (2018). How Cryptocurrency Mixers and Anonymous Wallets Work. *De Center*. Dostupno na: https://decenter.org/en/how-cryptocurrency-mixers-and-anonymous-wallets-work, preuzeto: 06.08.2018.

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. *Coindesk*. Dostupno na: https://www.coindesk.com/bitcoin-peer-to-peer-electronic-cash-system, preuzeto 14.08.2019.

Reutzel, B. (2016). Report: Bitcoin Wallet Providers Failing to Make Privacy a Priority. *Coindesk*. Dostupno na: https://www.coindesk.com/bitcoin-wallet-providers-failing-privacy-obpp, preuzeto 11.08.2019.

Vladimir C. (2019). The Ultimate Dark Wallet Review. *Blockchain Analyzes & Reviews*. Dostupno na: https://coindoo.com/the-ultimate-dark-wallet-review/, preuzeto 23.08.2019.

Datum prve prijave: 11.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Uljanov, S., & Milošević, Đ. (2019, 10 15). Nevidljive transakcije u dark web-u. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 124-134. doi:10.12709/fbim.07.07.02.14

Style – Chicago Sixteenth Edition:

Uljanov, Sergej, and Đorđe Milošević. 2019. "Nevidljive transakcije u dark web-u." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 124-134. doi:10.12709/fbim.07.07.02.14.

Style – GOST Name Sort:

Uljanov Sergej and Milošević Đorđe Nevidljive transakcije u dark web-u [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 124-134.

Style – Harvard Anglia:

Uljanov, S. & Milošević, Đ., 2019. Nevidljive transakcije u dark web-u. *FBIM Transactions,* 15 10, 7(2), pp. 124-134.

Style – ISO 690 Numerical Reference:

Nevidljive transakcije u dark web-u. **Uljanov, Sergej and Milošević, Đorđe.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 124-134.