STRUČNI RAD (PROFESSIONAL PAPER)
UDK: 343.98:[343.3/.7:004]

mr. sc. Olivije Zimonja,
Ministarstvo unutrašnjih poslova Republike Srpske,
Uprava kriminalističke policije,
olivije.zimonja@mup.vladars.net

mr. sc. Dragana Vujić
Ministarstvo unutrašnjih poslova Republike Srpske,
Uprava kriminalističke policije

KRIPTOVALUTE - IZAZOVI AKTUELNOG GLOBALNOG TRENDA ZA KRIMINALISTIČKU PRAKSU

Kriptovalute predstavljaju oblik digitalne imovine koja se koristi kao sredstvo razmjene, kojom prilikom se upotrebljava kriptografija kao način obezbjeđivanja sigurnosti transakcija, kontrole stvaranja dodatnih novčanih jedinica i radi potvrde transfera valute, a definišu se i kao podskup digitalnih valuta, alternativnih valuta i virtuelnih valuta. Kriptovalute, tačnije njihova upotreba u kriminalne svrhe predstavlja ozbiljan, nedovoljno istražen bezbjednosni izazov u kriminalističkoj teoriji i praksi. Ipak, danas se može govoriti o određenim, do sada uočenim specifičnostima i karakteristikama kriptovaluta i to: neuređena zakonska regulativa, decentralizacija, anonimnost, kriptografija, blockchain tehnologija, zatim činjenica da emisiju kriptovaluta ne kontroliše država, da nije propisan način kreiranja kriptovaluta, globalna rasprostranjenost, te podaci koji govore da se veliki procent kriptovaluta koristi u ilegalne svrhe. Nadalje, krivična djela koja se mogu dovesti u vezu sa upotrebom kriptovaluta su veoma širokog spektra i zahvataju veliki broj inkriminacija kao što su: pranje novca, finansiranje terorizma, malware, ransomware, phishing, poreske prevare, iznude, ucjene, otmice, trgovina putem ilegalnih platformi za trgovinu na internetu različitih vrsta roba kao što su droga, oružje, falsifikovani novac, kreditne kartice, dokumenta, dječija pornografija, mreže zaraženih računara (botnet), te trgovina različitim uslugama i slično.

Cilj ovog rada je da ukaže na specifičnosti koje se javljaju prilikom preduzimanja istrage kod krivičnih djela u kojima su korištene kriptovalute te specifičnostima analize dokaznog materijala i zaplijenje kriptovaluta.

Ključne riječi: *bezbjednost, bezbjednosni izazovi, kriminalistika, kriptovalute, krivična djela, istraga*

CRYPTOCURRENCIES - CHALLENGES OF THE CURRENT GLOBAL TREND FOR CRIMINAL PRACTICE

Cryptocurrencies are a form of digital asset used as a means exchanges, in which cryptography is used as a way to ensure security transactions, controls the creation of additional monetary units and to confirm currency transfers, a they are also defined as a subset of digital currencies, alternative currencies and virtual currencies. Cryptocurrencies, more precisely their use for criminal purposes, represent a serious, insufficiently researched security challenge in criminal theory and practice. However, today we can talk about certain, so far observed specifics and characteristics of cryptocurrencies: unregulated legislation, decentralization, anonymity, cryptography, blockchain technology, the fact that the issuance of cryptocurrencies is not controlled by the state, that there is no prescribed way of creating cryptocurrency, global distribution, and data that speak to a large percentage cryptocurrency used for illegal purposes. Furthermore, the crimes that can be related to the use of cryptocurrencies are very wide and involve a large number of incriminations such as: money laundering, terrorist financing, malware, ransomware, phishing, tax fraud, extortion, blackmail, kidnapping, trafficking through illegal platforms for online trade of various types of goods such as drugs, weapons, counterfeit money, credit cards, documents, child pornography, networks of infected computers (botnets), and trade in various services and the like.

The aim of this paper is to point out the specifics that arise during the investigation of criminal offenses in which cryptocurrencies have been used, as well as the specifics of the analysis of evidence and the seizure of cryptocurrencies.

Keywords: *security, security challenges, criminology, cryptocurrencies, crimes, investigation*

1 UVODNE NAPOMENE

Kriptovalute kao oblik digitalne imovine imaju funkciju koja je na svojevrstan način slična funkciji novca, te ćemo kroz uvodne napomene predstaviti trenutna sredstva koja se pojavljuju na tržišu. Novac je svojevrsna roba za koju se može kupiti svaka druga roba. Novcem se raspoređuju i razmjenjuju svi proizvodi ljudskog rada. Uobičajena definicija novca kaže da novac ima tri osnovne karakteristike i to da je obračunska jedinica, da je spremnik vrijednosti, te da je sredstvo razmjene, iako većina autora smatra da su prva dva svojstva manje važna i da proističu iz trećeg (Novac, 2020). Prema zakonodavstvu Bosne i Hercegovine, gotovina podrazumijeva novčanice i kovani novac koji je u opticaju kao zakonsko sredstvo plaćanja u BiH, kao i ostala sredstva plaćanja (putnički čekovi, lični čekovi, bankovni čekovi, poštanske doznake, te ostala sredstva plaćanja u takvom obliku da se titular mijenja po uručenju) (Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti, 2014). Elektronski novac predstavlja elektronski (digitalni) ekvivalent gotovog novca, čija emisija je takođe centralizovana, pod kontrolom je države i određenih finansijskih institucija, kao što su Paysafecard, Webmoney, Neteller, Western Union, Moneygram i drugi.

Trenutno je na tržištu prisutan virtuelni novac (virtuelna valuta) koji je digitalna predstava vrijednosti kojom se može digitalno trgovati i funkcioniše kao sredstvo razmjene, jedinica računa, skladište vrijednosti, ali nema status pravnog sredstva plaćanja u bilo kojoj nadležnosti. Ne izdaje se, niti garantuje od bilo koje nadležnosti i ispunjava gore navedene funkcije samo ugovorom unutar zajednice koja koristi virtuelnu valutu. Virtuelne valute mogu biti centralizovane i decentralizovane. Centralizovane virtuelne valute se vezuju za jednog administratora koji izdaje valutu, uspostavlja pravila i vodi računovodstvene evidencije. Decentralizovane virtuelne valute nemaju centralni administrativni organ koji reguliše emisiju i nadzor, a kao način obezbjeđivanja sigurnosti transakcija, kontrole stvaranja dodatnih novčanih jedinica i radi potvrde transfera valute koristi se asimetrična kriptografija. Ovakve valute koje se koriste algoritmima i peer to peer sistemom, definisanim i kao blockchain nazivaju se kriptovalute.

U literaturi (Tomašić, 2017) se navodi nekoliko naziva za digitalne valute i to: kriptovalute (eng. cryptocurrencies), virtuelne valute (eng. Virtual currencies), virtuelni novac (eng. Virtual money), digitalni novac (eng. Digital money), digitalne valute (eng. Digital currencies). Evropska centralna banka koristi naziv „Virtual currency schemes", odnosno virtuelne valutne šeme (European central bank, 2012). U nazivu je dodana riječ šema kako bi se naglasilo da se radi o sistemu više komponenti, od kojih je jedna (ključna i karakteristična) komponenta i sam informacioni sistem na kojem se zasnivaju valute, odnosno bez čije pomoći valuta ne bi mogla funkcionisati. Gotovo sve funkcije tog sistema u praksi se moraju obavljati uz upotrebu kompjutera i telekomunikacione tehnologije, pa stoga ima smisla promatrati virtuelne valute na ovaj način, (kao sistem) jer drugačije ne

mogu postojati. Nasuprot tome, klasični novac može ispuniti svoju funkciju i u digitalnom obliku i u klasičnom obliku, pa za njegovu upotrebu teorijski gledano informaciona tehnologija nije presudna (iako je danas nezamisliva isključivo klasična upotreba novca, bez korištenja informacijske tehnologije).

Takođe, Evropska centralna banka je definisala i ostala sredstva plaćanja pa je tako novac sve što se uobičajeno koristi za razmjenu vrijednosti, djeluje kao sredstvo razmjene, skladištenje vrijednosti i obračunska jedinica (Tomašić, 2017). U tom smislu, pojam novca širi je od pojma valute. Valuta je kovani ili štampani 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 dobija svoju vrijednost od povjerenja koje imaju korisnici u izdavaoci valute. Fiat valuta (novac) je uspostavljena od strane vlade ili centralne banke kao jedna vrsta medija za obavljanje transakcija (npr. euro, dolar, kuna). Virtuelna valuta je digitalni prikaz vrijednosti, koji ne izdaje centralna banka, kreditna institucija ili institucija za e-novac, a koja se u nekim okolnostima, može koristiti kao alternativa za novac. Virtuelna valutna šema (eng. Virtual currency scheme) se koristi za opisivanje oba aspekta prenosa vrijednosti, odnosno virtuelnih valuta i izgrađenih tehničkih sistema ili mehanizama koji osiguravaju da ta vrijednost može biti prenesena odnosno korištena. Blockchain je dnevnik ili knjiga zapisa svih transakcija, grupisanih u blokove, napravljenih sa (decentralizovanim) sistemom virtuelne valutne šeme (Tomašić, 2017).

U Bosni i Hercegovini zakoni kojima se regulišu sredstva plaćanja su na nivou entiteta, odnosno Federacije Bosne i Hercegovine i Republike Srpske. Zakon o deviznom poslovanju Republike Srpske (2018) ne predviđa upotrebu virtuelnih valuta kao sredstava plaćanja, već navodi da su sredstva plaćanja konvertibilne marke, domaće hartije od vrijednosti i strana sredstva plaćanja.

Digitalna imovina se predviđa Zakonom o sprečavanju pranja novca i finansiranja terorističkih aktivnosti Bosne i Hercegovine (2014) gdje se kao imovina podrazumijevaju sva sredstva, materijalna ili nematerijalna, bilo da se sastoji u stvarima ili pravima, pokretna ili nepokretna, te isprave ili instrumenti u bilo kom obliku, uključujući elektronski ili digitalni, kojima se dokazuje vlasništvo ili pravo vlasništva nad imovinom uključujući, ali ne i samo, bankarske kredite, putničke čekove, bankarske čekove, novčane naloge, udjele, vrijednosne papire, obveznice, mjenice i kreditna pisma. Takođe, isti zakonski propis određuje da je obveznik dužan naročito obratiti pažnju na rizik od pranja novca i finansiranja terorističkih aktivnosti koji proizilazi iz primjene novih tehnoloških dostignuća koja omogućavaju anonimnost klijenta (npr. elektronsko bankarstvo, upotreba bankomata, telefonsko bankarstvo i dr.), te propisuje da je obveznik dužan uspostaviti procedure i preduzeti dodatne mjere kojima se otklanjaju rizici i sprečava zloupotreba novih tehnoloških dostignuća u svrhu pranja novca i finansiranja terorističkih aktivnosti.

U ovom radu ćemo se koristiti terminom kriptovalute, kojim označavamo oblik digitalne imovine koji se koristi kao sredstvo razmjene koristeći kriptografiju kao način obezbjeđivanja sigurnosti transakcija, kontrole stvaranja dodatnih novčanih jedinica i radi potvrde transfera valute.

2 KRIPTOVALUTE I NJIHOVA UPOTREBA

Iako je trenutno u upotrebi više stotina različitih kriptovaluta kao što su Bitcoin Cash, Litecoin, Ethereum, Monero i slično, u ovom radu ćemo način upotrebe kriptovaluta predstaviti kroz upotrebu najpoznatije među njima Bitcoin-a. Iz same definicije kriptovaluta mogu se uvidjeti karakteristike, način funkcionisanja, te sličnosti i razlike u odnosu na klasični novac. Dakle, i kriptovalute i klasični novac se pojavljuju u elektronskom obliku uz mogućnost prenosa na druge medije i štampanja u papir. Pri tom sam medij za kriptovalute 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 je digitalna, decentralizovana, pseudo anonimna valuta, koja se ne oslanja na vlade ili druge pravne osobe, i čija vrijednost nije garantovana zlatom ili drugim robama. Ona se oslanja na ravnopravnu mrežu računara i održava integritet uz pomoć kriptografije. Bitcoin je složen sistem, a njegova implementacija uključuje kombinaciju kriptografije, distribuiranih algoritama i usaglašenog ponašanja zajednice korisnika. Zagovornici Bitcoin-a tvrde da ima mnoga svojstva koja bi ga mogla učiniti idealnom valutom za trgovinu kao npr. vrlo su 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). Bitcoin kao kriptovaluta oslanja se na kriptografski protokol koji određuje na koji način valuta nastaje, mijenja ili kako se njome trguje. Bitcoin je širom svijeta distribuirana, decentralizovana kripto valuta upravljana samo i isključivo od strane kriptografskog protokola otvorenog koda: nema vlade, kompanije ili banke zadužene za izdavanje ili upravljanje Bitcoinom. Bitcoin je digitalna valuta koja korisnicima omogućuje slanje uplata u decentralizovanoj, ravnopravnoj mreži računara (eng. Peer to peer)[1], te je jedinstven po tome što ne zahtijeva središnju novčanu instituciju za autorizaciju transakcija. Korisnici moraju imati internet vezu i Bitcoin softver za plaćanja prema drugom javnom računu odnosno adresi. Satoši je najmanja jedinica Bitcoina; 1 Bitcoin sadrži 100 miliona Satošija. Prema dizajnu cijelog sistema, ukupna količina svih Bitcoina

1 Engleski izraz *Peer to peer* (isti sa istim ili svaki sa svakim) u tehnologiji podrazumijeva koncept umrežavanja računara bez centralnog računara, gdje je svaki računar inteligentna radna stanica, koja pronalazi druge računare putem emitovanja paketa podataka (poruka), i komunicira s njima direktno, bez potrebe autorizacije na nekom centralnom računaru.

ne može biti veća od 21 milion. Ukupna količina Bitcoin u opticaju se povećava planirano i očekivano, na temelju programskog koda, do postizanja maksimalne količine u 2140. godini (Tomašić, 2017).

Javna istorija 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 istorija ili dnevnik čini knjigu transakcija u kojima se prati svaki Satoši od prvog vlasnika do današnjih vlasnika. Provjerom svih transakcija za određenog kupca, garantuje se da kupac zapravo posjeduje potreban broj Bitcoina za željenu transakciju, te se na taj način sprečavaju prevare. Količina Bitcoin-a u opticaju povećava se sa svakim novim blokom transakcija dodanim u javni dnevnik (tj. Blockchain). Provjerom novih transakcija „rudari" ih pakuju u blokove. Međutim, tu je i kompjuterski zadatak za svaki blok visokog stepena težine, sistemski dizajniran za ograničavanje povećanja novčane mase, bez obzira koliko sporo ili brzo funkcioniše cjelokupna mreža. Bez obzira koliko transakcija sadrži blok, svaki uspješan upis bloka u centralni dnevnik donosi sistemom određeni broj Bitcoin-a rudaru. Prvih nekoliko hiljada 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 špekulativni rizik uspjeha Bitcoina (Tomašić, 2017).

Blockchain je baza podataka u digitalnom obliku, koja sadrži dnevnik svih transakcija učinjenih u sistemu. Decentralizovana je u smislu da svaki učesnik sistema ima mogućnost pohraniti kod sebe vlastitu kopiju. Učesnici ili čvorovi u sistemu (eng. nodes) su ravnopravni svjedoci i kontrolori autentičnosti svake pojedinačne transakcije. Transakcije su grupisane hronološki, 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 neko 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 potiče naziv Blockchain. Ovo je pojednostavljen prikaz funkcionisanja Blockchain tehnologije i tu nisu opisani svi detalji sistema kao ni njegove varijante. Cilj je istaknuti funkcionalnost cijelog sistema baziranog na ravnopravnoj mreži učesnika i tehničkom rješenju, a bez određenog centralizovanog sistema autorizacije, kao što je slučaj kod Internet bankarstva, gdje banka autorizuje i kontroliše transakcije (Tomašić, 2017).

Kriptovalute funkcionišu na principu asimetrične kriptografije koja podrazumijeva posjedovanje javne adrese (eng. Public address). Bitcoin adresa je oznaka ili broj koji možemo uporediti sa brojem klasičnog tekućeg računa u banci. Za svaku postojeću adresu sistem bilježi ulazne i izlazne transakcije, tako da zbir svih transakcija predstavlja stanje na računu. Pri tome se ne čuvaju salda pojedinih

računa nego istorija svih transakcija, iz kojih se može lako izračunati trenutni saldo za svaku adresu. Uz svaku adresu postoji i tzv. privatni ključ (eng. private key). Ukoliko je poznata javna adresa, moguće je imati potpuni uvid u stanje, ali nije moguće trošiti sredstva s računa. Za trošenje je potreban privatni ključ. Javna adresa je niz brojeva i slova, najčešće počinje sa brojem 1 i ima između 30 i 35 karaktera (Tomašić, 2017) (fotografija 1).

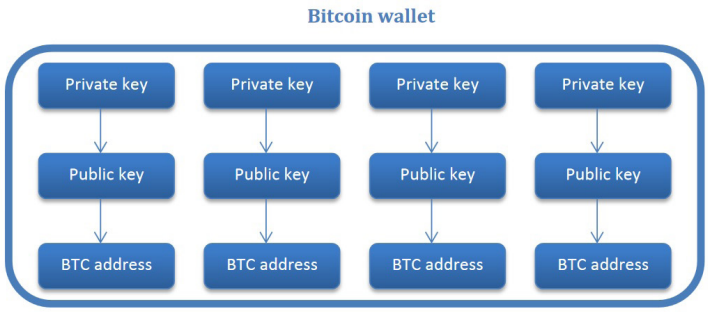
Fotografija 1: Javna adresa (izvor: European cyber crime centre [EC3], 2017)

Takođe, postoje i bitcoin adrese koje počinju sa brojem 3, a koje se najčešće nazivaju i pay-to-script (P2SH) hash adrese. Ovim adresama ne upravlja vlasnik privatnog ključa, već skripta određuje što se događa s transakcijom. Najpopularniji primjer pay-to-script (P2SH) hash adrese je transakcija sa više potpisa gdje više ključeva mora potpisati transakciju kako bi oslobodilo sredstva. Primer takve adrese je 3KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM.

Privatni ključ je znatno duži niz brojeva i slova od javnog ključa i počinje sa slovom K ili L (fotografija 2).

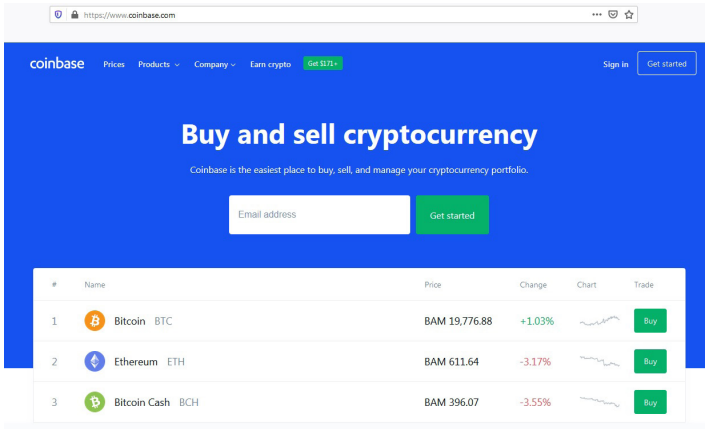
Fotografija 2: Privatni ključ (izvor: EC3, 2017)

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 dostupnim web servisima za pojedinu valutu. Bitcoin novčanik (eng. Bitcoin wallet) se često poistovjećuje sa bitcoin adresom, međutim osnovna razlika je što bitcoin novčanik može da sadrži više bitcoin adresa, odnosno bitcoin novčanik sadrži i javni i privatni i ključ (fotografija 3).



Fotografija 3: Bitcoin novčanik (izvor: EC3, 2017)

Digitalni novčanik, odnosno konkretno bitcoin novčanik je moguće kreirati na nekoj od platformi kao što je npr. coinbase (fotografija 4).



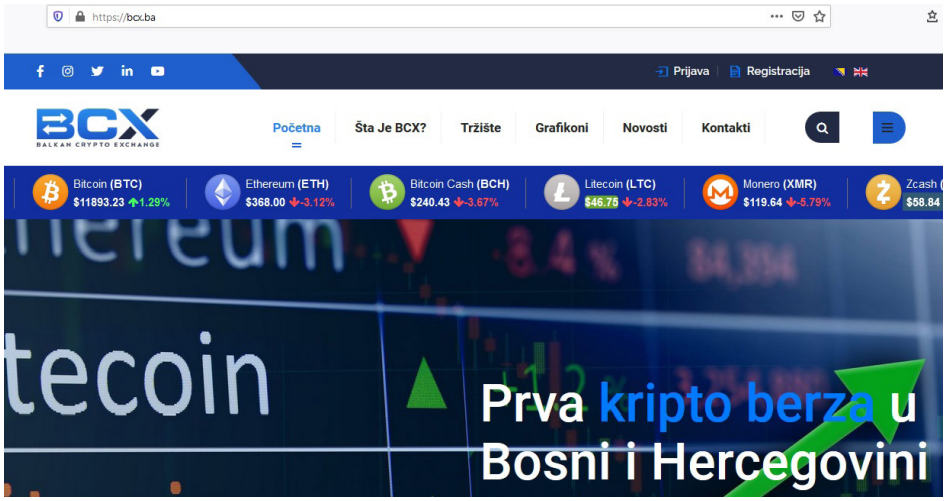
Fotografija 4: Snimak ekrana platforme coinbase (izvor: Coinbase, 2021)

Nakon toga, transakcija se odvija na način što se javni ključ generiše iz privatnog ključa. Na taj način se obezbjeđuje sigurnost transakcije. Prilikom provjere svake transakcije, sistem uz pomoć privatnog ključa provjerava pripada li

odgovarajuća adresa tom ključu, a zatim raspolaže li adresa sa dovoljno novca za izvršenje transakcije. Prilikom prenosa određenog iznosa novčanih jedinica s jednog računa na drugi, kompjuterski program 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 kombinovati traženi iznos iz postojećih adresa. Ukoliko je to kombinovanje moguće, transakcija se šalje svim čvorovima (eng. nodes) na potvrdu ili ovjeru. U slučaju da je nemoguće iskombinovati traženi iznos, uzima se najbliži mogući veći iznos, a ostatak se kroz istu transakciju vraća pošiljaocu na neku od njegovih postojećih adresa.

Digitalni novčanici mogu imati različite oblike pa tako imamo: softver (software) novčanike, hardver (hardware) novčanike, papirne novčanike, mobilne uređaje i web novčanike. Jedini i originalni način za stvaranje novih Bitcoin-a je "kopanje" ili "rudarenje" (eng. Mining). Navedeni termin označava aktivnost kojom se upotrebom kompjuterskih programa dobijaju algoritmi koji čine sastavni dio kriptovaluta. Da bi se obavljala navedena aktivnost potrebno je posjedovanje hardware komponenti i specijalizovanih programa (EC3, 2017). Načini za sticanje bitkoina su različiti, legalni i ilegalni. To može uključivati, pored rudarstva, kupovinu na Internet centrali ili „bankomatu", plaćanje pružene usluge ili prodate robe ili krađu sredstava prethodnim upadom u računar i sl.

Osim navedenog crypto mining-a kriptovalute se mogu kupiti i putem platformi za trgovinu poznatijim kao mjenjačnice za kriptovalute. U Republici Srpskoj je otvorena prva mjenjačnica za kriptovalute u Bosni i Hercegovini pod nazivom BCX (fotografija 5), dok u svijetu postoji veoma veliki broj predmetnih platformi a neke od najpoznatijih su: Poloniex, Binance, Bittrex, Kraken, Localbitcoins (fotografija 6).



Fotografija 5: Snimak ekrana platforme BCX (izvor: BCX, 2020)

Fotografija 6: Najpoznatije svjetske platform za trgovinu kriptovalutama (izvor: EC3, 2017)

Također, konverziju Bitcoin-a u klasični novac, odnosno isplatu novca (eng. cash out) moguće je izvršiti i putem ATM (automated teller machine) uređaja, poznatijih kao bankomati. Na stranici "coinatmradar.com" je moguće vidjeti gdje se u odnosu na našu trenutnu lokaciju nalazi najbliži ATM, kao i lista svih ATM uređaja.

3 ISTRAGA KRIVIČNIH DJELA U KOJIMA SU UPOTREBLJENE KRIPTOVALUTE

Navedene karakteristike kriptovaluta kao što su: neuređena zakonska regulativa, decentralizacija, anonimnost, kriptografija, block chain tehnologija, zatim činjenica da emisiju kriptovaluta ne kontroliše država, da nije propisan način kreiranja kriptovaluta, globalna rasprostranjenost, te podaci (Foley et al., 2019) koji govore da se veliki procenat kriptovaluta koristi u ilegalne svrhe ide u prilog činjenici da upotreba kriptovaluta predstavlja ozbiljan, nedovoljno istražen bezbjednosni izazov, a da se istragama ovih krivičnih djela mora pristupati sveobuhvatno sa kriminalističkog, pravnog i tehničkog aspekta.

Izvršioci krivičnih djela su prednosti šifrovanja osim za prenos poruka prilikom komunikacije, iskoristili i kroz upotrebu kriptovaluta. Tako se danas metode šifrovanja sadržaja određenih poruka i informacija najviše koriste u vojnim, bezbjednosnim, obavještajnom i policijskim poslovima. (Vujić & Zimonja, 2017).

Istraga krivičnih djela u kojima su upotrebljene kriptovalute zahtijeva veoma sveobuhvatan pristup. Ključne karakteristike krivičnih djela u kojima su upotrijebljene kriptovalute a po kojima se ova krivična djela razlikuju od drugih, jesu sljedeće: upotreba kriptovaluta je ograničena na sajber prostor odnosno informacione sisteme; knjige javnih transakcija su dostupne svima u elektronskom

obliku i koriste internet i odgovarajuće uređaje; podaci o transakcijama bilježe se trajno; sve okolnosti transakcija su očigledne, osim vlasništva nad adresom ili novčanikom; Kriptovalutama se obično trguje putem mrežnih tokova; kriptovalute su centralno sredstvo plaćanja na Darknetu; transakcije kriptovalutama u bilo kom iznosu mogu se prenijeti korisnicima širom svijeta u nekoliko sekundi; za sigurno trgovanje kriptovaluta potrebno je napredno znanje o informacionim tehnologijama itd,

Specifičnosti ovih krivičnih djela prate specifičnosti policijskih, istražnih postupaka kao što su odgovarajuća specijalizacija istražitelja, dostupnost odgovarajućih alata (uz naplatu, ili besplatno), efikasan sistem međunarodne policijske saradnje i razmene zvaničnih zahteva i brzina postupka relevantna ovlašćenja istražitelja, na primer za takozvano „patroliranje" Internetom, uključujući Darknet, uspostavljanje adekvatne baze podataka, relevantno zakonodavstvo za čuvanje podataka o korisnicima interneta, posebno na mrežnim tržištima itd.

Počevši od prvih informacija o tome da je krivično djelo izvršeno potrebno je, na samom početku, utvrditi koja vrsta krivičnog djela je izvršena, dokumenovati na pravi način sve potrebne informacije. Nakon toga uslijedile bi mjere i radnje na otkrivanju i rasvjetljavanju predmetnog krivičnog djela kao što su npr. pregled transakcija, foruma, Interneta, Darkneta, međunarodna policijska saradnja ili razmene policijskih podataka, upiti za internet mjenjačnice i druge finansijske institucije i zahtevi za blokiranje sredstava. Sve prethodno bi predstavljalo mjere i radnje u centralnom dijelu istrage koje se preduzimaju sa ciljem pronalaženja imovine i identifikovanja počinioca. Nakon ovog tzv. Centralnog dijela istrage slijedio bi završni postupak koji bi se sastoja od procedura za konačno oduzimanje sredstava, postupaka za hapšenje počinioca i obezbjeđenje dokaza, uglavnom zaplijene i istrage elektronskih uređaja, a sve u vezi sa međunarodnim elementom.

Da bi se došlo do izvršica predmetnih krivičnih djela koje smo ranije nabrojali potrebno je, između ostalog, intenzivno vršiti pretrage na internetu korištenjem komercijalnih alata specijalizovanih za tu namjenu tzv. OSINT (Open Sourse INTelligence) alata. [2]

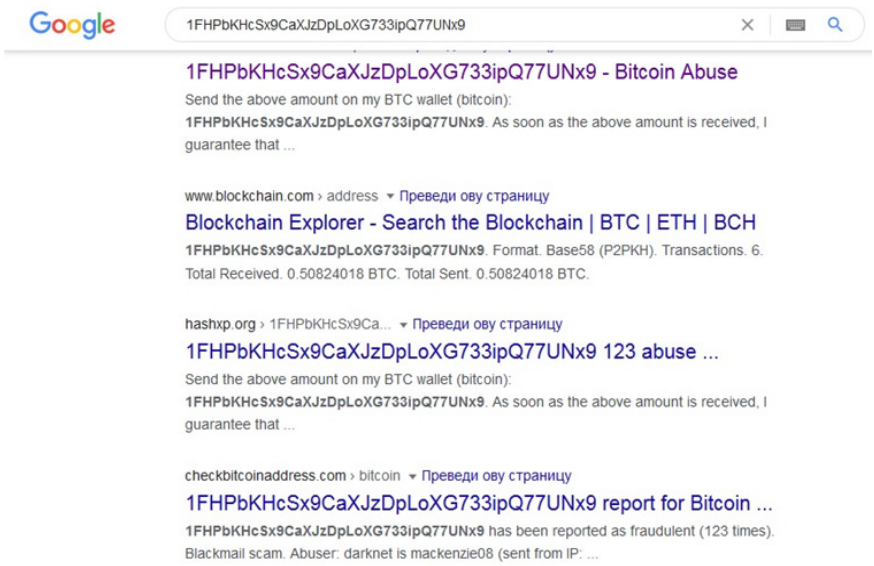
Navedenim je potrebno doći do informacija o transakcijama kriptovaluta, korisničim podacima ostavljenim prilikom kreiranja različitih naloga (IP adresa, email nalog, broj telefona, povezani email nalog, fotografije ličnih dokumenata i slično), foto i video materijal nadzornih kamera, podaci od lica koja su korištena za preuzimanje novca tzv. mule i slično.

Takođe, za razliku od istraga drugih krivičnih djela, kroz istrage ove

2 OSINT metoda je skup procedura za dobijanje podataka iz javnih izvora. OSINT metoda takođe provjerava dobijene podatke o počiniocima i finansijskom toku sredstava. Uglavnom se radi o proveri podataka o IP adresama, korisničkim imenima, pseudonimima, lozinkama, BTC adresama i mikserima. Ovde se postavlja pitanje dokle istražitelj može da pristupi, gde su granice privatnosti.

vrste kriminaliteta neophodno je korištenje posebnih instituta i obrazaca za međunarodnu saradnju (Council of Europe, 2018), propisanih Konvencijom o kompjuterskom kriminalu (Ministarstvo unutrašnjih poslova Republike Srpske, 2018), te neposredna saradnja sa privatnim sektorom kako u zemlji tako i u inostranstvu. Hitnost, pravovremenost, te pravilan način čuvanja i razmjene podatka je ključni element kod ovih istraga. Potom, izuzetno važan element je istovremeno rad na smanjenju ili otklanjanju štete nastale izvršenjem ovih krivičnih djela zajedno sa prikupljanjem informacija i dokaza.

Da bi se izvrsila analiza transakcija kriptovaluta potrebno je krenuti od najosnovnijih pretraga kao što su jednostavno upisivanje predmetne bitcoin adrese u Google pretraživač (fotografija 7).

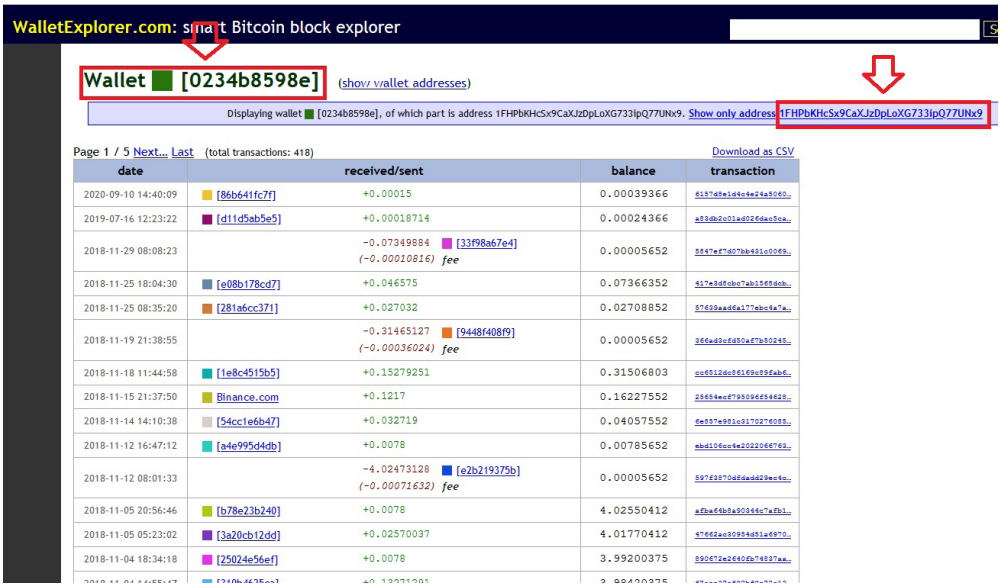


Fotografija 7: Snimak ekrana Google pretrage za BTC adresu: 1FHPbKHcSx9CaX-JzDpLoXG733ipQ77UNx9 (izvor: Google, n. d.)

Na ovaj način je moguće dobiti više informacija o samoj bitcoin adresi te postoji mogućnost da se predmetna adresa poveže sa nekim email nalogom, nalogom na društvenoj mreži, nazivom korisnika na forumu za razmjenu informacija i slično, što će usmjeriti dalji tok istrage. Slijedeći korak, koji se može nazvati i najsloženiji i najvažniji je praćenje transakcija. To se postize upotrebom tzv. internet alata koji se prema kriterijumu besplatne dostupnosti mogu podijeliti na slobodno dostupne i one koji se plaćaju (alati sa više funkcionalnosti se naplaćuju). Čak i besplatni alati, poput walletexplorera (fotografija 8), omogućavaju istražiteljima da detaljno analiziraju transakcije na nivou adrese Bitcoin, kao i na nivou Bitcoin novčanika. Upotreba alata zahteva od istražitelja da imaju posebna znanja o

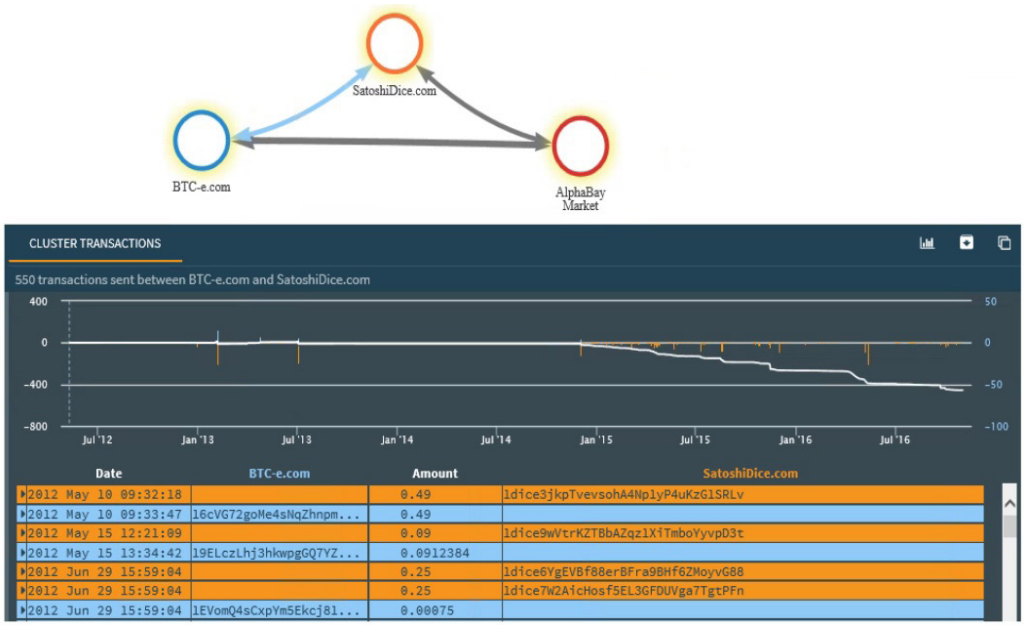
tome kako funkcioniše sistem Bitcoin. Primjeri besplatnih alata su: https://www.blockchain.com/explorer; https://blockchair.com/; https://blockexplorer.com/; https://www.walletexplorer.com/. Pored ovih alata, na internetu postoje i alati koji nude pojednostavljeni uvid na nivou Bitcoin adrese.

Upotrebom alata za praćenje transakcija dobiće se informacije o toku transakcija, odnosno sa koje adrese na koju su prenošena sredstva, kada i u kojem iznosu. Kao što je ranije napomenuto, kod blockchain tehnologije svaka transakcija je vidljiva ali ono što nije vidljivo je ko stoji iza svake pojedinačne adrese, odnosno ko je korisnik. Iz tog razloga je potrebno pratiti svaku pojedinačnu transakciju do trenutka kada će se u lancu pojaviti transakcija putem jedne od poznatih platformi za trgovinu kriptovalutama ili do trenutka isplate (eng. cash out). Tada je moguće od kompanije zahtijevati podatke o korisniku naloga ili sa mjesta gdje je izvršena isplata, npr. ATM uređaj, video materijal, a koji će pomoći u identifikaciji izvršioca.



Fotografija 8: Snimak ekrana upotrebe alata Walletexplorer za pretragu BTC adrese (izvor: Wallet [0234b8598e], 2021)

Osim predstavljenih otvorenih alata za praćenje transakcija moguće je koristiti i komercijalne alate specijalizovano kreirane od strane određenih kompanija. Primjeri komercijalnih alata su: https://www.chainalysis.com/; https://www.elliptic.co/; https://www.blockseer.com/. Prednost komercijalnih alata je što iza njih stoji autoritet određene kompanije, što olakšava dokaznu vrijednost prikupljenih podataka te pruža veći broj podataka koji se dobijaju uz bolju preglednost i vizuelizaciju dobijenih podataka (fotografija 9).



Fotografija 9: Prikaz transakcija koje daje program Chainalysis (izvor: EC3, 2017)

Uzimajući u obzir sve karakteristike bitcoin-a i block chain tehnologije već je moguće konstatovati da praćenje transakcija nije ni malo jednostavna aktivnost, međutim tome treba dodati još jednu veoma važnu otežavajuću okolnost a to je upotreba tzv. "miksera". Mikseri podrazumijevaju servise koje koriste izvršioci krivičnih djela kako bi sakrili transakcije. Odnosno upotrebom predmetnih servisa iznos sredstava sa jedne adrese se nekoliko puta raspodijeli na više različitih adresa čime se maskira izvorna adresa. Primjeri servisa za miksanje su: Bitmixer.io; Bitlaunder.com; Bitcoinfog.com; Coinmixer.net; Helix and Helix Light; Cryptomixer.io; Sharedcoin.com. (EC3, 2017).

Kruna istrage je svakako otkrivanje izvršilaca određenog krivičnog djela i prikupljanje dokaza. Međutim, jedna od specifičnosti istrage kod krivičnih djela u kojima su upotrebljene kriptovalute je identifikacija bitcoin adrese na kojoj se nalazi novac proistekao izvršenjem krivičnog djela i njegova zaplijena.

Da bi se izvršila zaplijena novca sa bitcoin adrese nije dovoljno samo pronaći predmetnu adresu i izvršiti njeno kopiranje, već je potrebno izvršiti transakciju sa bitcoin adrese osumnjičenog na bitcoin adresu kreiranu od strane ovlaštenog lica za tu namjenu. Dakle, potrebno je da ovlašteno lice najprije identifikuje javnu adresu, zatim pronađe privatni ključ osumnjičenog, nakon toga izvrši transakciju i osigura da neovlaštena osoba nije u mogućnosti da dođe u posjed privatnog ključa i izvrši neželjenu transakciju.

Zaplijena medija sa privatnim ključem bila bi dovoljna da se obezbijede sredstva samo pod uslovom da korisnik nema kopiju medija. Istražitelji, međutim,

uglavnom neće imati ove informacije. Zbog toga, za adekvatno osiguranje ili zaplijenu sredstava, obično neće biti dovoljno oduzeti samo privatni ključ, na primer na listu papira. Jedna od posebnosti kriptovaluta je da svako ko ima privatni ključ ima i sredstva.

Prilikom zaplijene novca sa bitcoin adrese neophodno je voditi računa o vrsti novčanika, odnosno da li se radi o: software novčaniku (full client ili light client), hardware novčaniku, papirnom novčaniku, novčaniku za mobilne uređaje ili je u pitanju Web novčanik.

Najpraktičniji način za obavljanje transakcija kada su u pitanju software novčanici u modu full client, je putem platforme Bitcoin Core (https://bitcoincore.org/). Podatke o tome o kojem modu novčanika se u konkretnom slučaju radi moguće je pronaći prilikom forenzičke analize predmetnog računara i to najčešće na sledećem mjestu C:\Users\username\AppData\Roaming\Bitcoin. Nakon što prikupimo podatke o javnom i privatnom ključu potrebno je napraviti transakciju na službeni bitcoin novčanik. (EC3, 2017).

Kada je u pitanju bitcoin novčanik u modu light client, najčešće korišćena platforma za obavljanje transakcija je Electrum (https://electrum.org/#home). Forenzičkom analizom predmetnog računara, moguće je pronaći podatke o bitcoin novčaniku najčešće na sledećoj lokaciji C:\Users\ username\AppData\ Roaming\Electrum. Za razliku od prethodnog moda novčanika u ovom slučaju je umjesto privatnog ključa potrebno pronaći seed code, koji predstavlja zamjenu za privatni ključ prikazan kroz nasumično određen niz riječi (npr. Seed: hurt gloom zebra pool inside time sketch puppy theme belt tackle athlete).

Kada su u pitanju hardware novčanici pristup privatnom ključu koji je pohranjen na hardware-skom novčaniku zahtijeva fizički pristup uređaju. Otežavajuća okolnost je ta što ovaj uređaj može biti dodatno osiguran pin kodom ili nekom drugom autentifikacijom. Razlog zašto osumnjičeni dosta često koriste ovaj vid novčanika je što su sigurni od malware-a i zaštićeni od neželjenih upada jer nisu priključeni na mrežu. Kod papirnih novčanika privatni ključ je potpuno offline. Sve što je potrebno za pristup bitcoinima je privatni ključ koji se može ispisati i pohraniti isključivo na papiru. Privatni ključ je često propraćen javnim ključem i odgovarajućim QR kodovima. Pristup privatnom ključu za novčanike na moblinim uređajima ima nekoliko specifičnosti i zahtijeva otključavanje telefona, otvaranje wallet aplikacije koja može biti zaključana PIN kodom ili otisak verifikacijom. U ovim slučajevima, preporučuje se korištenje specijalizovanih software i hardware uređaja kao što su: Cellebrite, XRY ili sličnih proizvoda. Web novčanik ima karakteristiku da je potpuno online i za pristup web novčaniku potrebno je poznavanje korisničkog imena osumnjičenog ili ID novčanika, lozinke a u velikom broju slučajeva dvofaktorskih kodova za provjeru autentičnosti.

4 ZAKLJUČAK

Istraga krivičnih djela u kojima su upotrebljene kriptovalute obiluje specifičnostima u odnosu na istrage u kojima kriptovalute nisu bile upotrebljene. Uočava se veliki broj izazova koji prate samu upotrebu kriptovaluta kao što su neuređena zakonska regulativa, decentralizacija, anonimnost, kriptografija, block chain tehnologija, zatim karakteristika da emisiju kriptovaluta ne kontroliše država, da nije propisan način kreiranja kriptovaluta, globalna rasprostranjenost, te podaci koji govore da se veliki procenat kriptovaluta koristi u ilegalne svrhe.

Posebno je važna činjenica da je zakonska regulativa koja reguliše kompjuterski kriminalitet u stalnom razvoju i uvijek nedovoljno definisana u skladu sa procesom i brzinom nastanka novih informacionih tehnologija i trendova. Trenutno još ni jedna centralna banka ne posmatra Bitcoin niti ostale virtuelne valute kao novac, što je u koliziji sa stvarnošću u kojoj transakcije sa kriptovalutama naglo rastu i u kojoj se iste polako uvode kao sredstvo plaćanja. Što se njih tiče, poželjno je imati samo jedno sredstvo plaćanja na određenoj teritoriji, jer to daje monetarnoj politici jači efekat. Evropska centralna banka samo konstatuje postojanje ovih valuta i za sada samo posmatra sa strane, bez želje za većim angažovanjem povodom ovog pitanja jer je rizik koji nose sa sobom prisutan, ali je njihov udio u ekonomijama veoma mali, tako da ne predstavljaju prijetnju finansijskom sistemu. Posmatraju ih kao vrstu finansijskih inovacija. Zbog ovakvih stavova, najveći problem u korišćenju predstavljaju nejasne regulacije koje guše sajtove za razmenu virtuelnih valuta. Kao potencijalno rješenje, bitcoin se (npr. u Finskoj) registrovao kao roba. Bitcoin je po svojoj prirodi protokol, isto kao i internet. Program se ne može regulisati (kao što se ne može regulisati slanje e-maila), međutim, mogu se regulisati sajtovi koji se bave razmjenom virtuelnih i konvencionalnih valuta, kao i sajtovi koji služe za kupovinu ili prodaju dobara i usluga za virtuelni novac. Međutim, ako su oni regulisani zakonom na jedan način u jednoj zemlji, postoji mogućnost da su na drugi način regulisani u drugoj. Stoga, postoji način za zaobilaženje državne regulative. S tim u vezi kod istrage predmetnih krivičnih djela svaka istraga predstavlja slučaj za sebe a koji podrazumijeva jedan sveobuhvatan pristup sa kriminalističkog, pravnog i tehničkog aspekta.

Upravo iz tog razloga kroz rad su predstavljena sva tri navedena elementa važna za kvalitetnu istragu u ovim slučajevima a to su pravni, kriminalistički i tehnički a što nas navodi na zaključak da ovakvu istragu nije moguće voditi kao pojedinac već je za sveobuhvatan pristup potrebno djelovanje tima koji sačinjavaju stručna i ovlaštena lica iz oblasti prava, kriminalistike i svakako tehničkih nauka.

Takođe, osim multidisciplinarnog i timskog rada, veoma važan segment predstavlja i saradnja. U ovom kontekstu pod saradnjom podrazumijevamo međuinstitucionalnu saradnju svih institucija za sprovođenje zakona u zemlji i inostranstvu ali kao veoma značajnu specifičnost ovih istraga ističemo važnost saradnje sa privatnim sektorom. Skoro da ni jedna druga istraga ne zahtijeva

toliko brzu razmjenu informacija, poznavanje tehničkih karakteristika podataka, potrebu za brzim čuvanjem, analizom i razmjenom podataka a to je jedino moguće kroz neposrednu saradnju sa privatnim sektorom.
S tim u vezi istrage krivičnih djela u kojima su upotrebljene kriptovalute mogu se predstaviti kao jedan proces koji je potrebno kontinuirano razvijati kroz unapređenje regulative, edukaciju kadrova koji sprovode istrage na svim nivoima (policija, tužilaštvo, sud, druge institucije), razvoj saradnje i svakako preventivne aktivnosti.

5 LITERATURA

BCX. (2020). https://bcx.ba/

Coinbase. (2021). https://www.coinbase.com

Council of Europe [CoE]. (2018). Cybercrime, capacity building. https://www.coe.int/en/web/cybercrime/iproceeds

European central bank. (2012). Virtual currency schemes. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European cyber crime centre [EC3]. (2017). *A guide for bitcoin investigators*. Hague: Europol.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, *32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Google. (n. d.). https://www.google.com/

Ministarstvo unutrašnjih poslova Republike Srpske [MUPRS]. (2018). *Sprečavanje visokotehnološkog kriminaliteta, Regulativa*. https://mup.vladars.net/index.php?vijest=vtk&vrsta=regulativa

Novac. (2020). https://hr.wikipedia.org/wiki/Novac

Tomašić, M. (2017). *Tehnički, ekonomski i pravni aspekti digitalnog novca [Diplomski rad]*. Zadar: Sveučilište u Zadru, Odjel za ekonomiju, Diplomski sveučilišni studij menadžmenta.

Vujić, D., & Zimonja, O. (2017). Dokazna vrijednost šifrovanih poruka iz presretnutih telekomunikacija u krivičnom postupku. *Kriminalistička teorija i praksa, 4*(2), 91–105.

Wallet [0234b8598e]. (2021). https://www.walletexplorer.com/wallet/0234b8598e28750e?from_address=1FHPbKHcSx9CaXJzDpLoXG733ipQ77UNx9)

Zakon o deviznom poslovanju Republike Srpske [ZDPRS]. (2018). S*lužbeni glasnik RS*, (96/03, 123/06, 92/09, 20/14 i 20/18).

Zakon o sprečavanju pranja novca i finansiranja terorističkih aktivnosti [ZSPNFTA]. (2014). *Službeni glasnik BiH*, (53/09, 47/14).