

UNIVERZITET U NIŠU
PRAVNI FAKULTET



Zloupotreba kriptovaluta u izvršenju krivičnih dela

(master rad)

Mentor:

Prof. dr Darko Dimovski

Student:

Luka Jovanović

M011/24-UP

Niš, 2026. godina

SADRŽAJ

1. UVOD	1
1.1. Predmet i značaj istraživanja	2
1.2. Problem istraživanja.....	3
1.3. Ciljevi istraživanja	4
1.4. Hipoteze rada	5
1.5. Metodologija i struktura rada.....	6
2. POJMOVNO ODREĐENJE KRIPTOVALUTA I DIGITALNE IMOVINE	8
2.1. Nastanak i razvoj kriptovaluta	9
2.2. Osnovne karakteristike kriptovaluta	12
2.3. Blockchain, wallet-i, menjačnice i transakcioni tragovi.....	14
2.4. Razlika između kriptovaluta, tokena i druge digitalne imovine	18
3. KRIVIČNOPRAVNI I BEZBEDNOSNI RIZICI POVEZANI SA KRIPTOVALUTAMA	21
3.1. Anonimnost, pseudonimnost i otežana identifikacija učinilaca	22
3.2. Pranje novca, prikrivanje porekla imovine i layering	24
3.3. Darknet tržišta, ransomware, prevare i finansiranje drugih protivpravnih aktivnosti ..	26
3.4. Digitalna imovina kao predmet oduzimanja i dokazivanja.....	27
4. NORMATIVNI OKVIR ZA SUZBIJANJE ZLOUPOTREBE KRIPTOVALUTA	29
4.1. Međunarodni standardi i preporuke: FATF, UNODC, Europol	29
4.2. Regulativa Evropske unije	31
4.3. Pravni okvir Republike Srbije.....	32
4.4. Krivičnopravni odgovor i pitanja sankcionisanja	33
5. ZLOUPOTREBA KRIPTOVALUTA U IZVRŠENJU I PRIKRIVANJU KRIVIČNIH DELA	35
5.1. Modaliteti izvršenja krivičnih dela uz upotrebu kriptovaluta	35
5.2. Kriptovalute kao sredstvo plaćanja, prenosa i prikrivanja protivpravne koristi	36
5.3. Dokazni problemi u otkrivanju, gonjenju i presuđenju	37

5.4. Uloga policije, tužilaštva, sudova i regulatornih organa.....	38
6. STUDIJE SLUČAJA	40
6.1. Silk Road i Ross Ulbricht	40
6.2. Bitfinex hack i pranje ukradenih bitkoina.....	42
7. EMPIRIJSKO ISTRAŽIVANJE.....	44
7.1. Predmet i cilj istraživanja.....	44
7.2. Uzorak i organizacija online ankete (100 ispitanika)	45
7.3. Instrument istraživanja i način prikupljanja podataka	46
7.4. Obrada i analiza rezultata.....	46
7.5. Očekivani doprinos istraživanja.....	56
8. DISKUSIJA	57
9. ZAKLJUČAK	63
10. LITERATURA.....	66
11. SAŽETAK.....	69
12. SUMMARY	70
13. BIOGRAFIJA AUTORA	71
14. PRILOG	72

1. UVOD

Razvoj kriptovaluta i drugih oblika digitalne imovine u poslednjih petnaestak godina značajno je promenio način na koji se razumeju finansijske transakcije, prenos vrednosti i kontrola novčanih tokova. Kriptovalute su prvobitno predstavljene kao decentralizovani oblik elektronskog novca, zasnovan na tehnologiji koja omogućava direktan prenos vrednosti između korisnika, bez nužnog posredovanja banaka i drugih tradicionalnih finansijskih institucija. Takav koncept otvorio je prostor za brojne zakonite upotrebe, naročito u oblasti digitalnih plaćanja, investiranja, tehnoloških inovacija i razvoja novih finansijskih usluga. Međutim, iste osobine koje kriptovalute čine privlačnim za legitimne korisnike mogu predstavljati i značajan izazov za krivično pravo, bezbednosne institucije i organe gonjenja, posebno kada se koriste za izvršenje, finansiranje ili prikrivanje krivičnih dela (Nakamoto, 2008).

Poseban problem javlja se zbog toga što se transakcije kriptovalutama odvijaju u digitalnom prostoru, često brzo, prekogranično i uz upotrebu tehničkih mehanizama koji otežavaju povezivanje određene transakcije sa konkretnim fizičkim licem. Iako blockchain tehnologija ostavlja određeni transakcioni trag, taj trag nije uvek jednostavno povezati sa identitetom učinioca, naročito kada se koriste posredničke platforme, anonimni ili pseudonimni wallet-i, mikseri, decentralizovane menjačnice i druge metode prikrivanja porekla digitalne imovine. Zbog toga kriptovalute sve češće postaju predmet interesovanja u kontekstu pranja novca, poreskih krivičnih dela, prevara, ransomware napada, finansiranja protivpravnih aktivnosti i prikrivanja protivpravne imovinske koristi (Europol, 2024).

Aktuelnost ove teme posebno se ogleda u činjenici da se pravni sistemi, uključujući i pravni sistem Republike Srbije, nalaze pred zadatkom da usklade tehnološke inovacije sa potrebom za efikasnom prevencijom i represijom kriminaliteta. Kriptovalute same po sebi nisu nezakonite, niti se njihova upotreba može svesti samo na kriminalne aktivnosti. Ipak, njihova zloupotreba otvara niz pravnih, procesnih i bezbednosnih pitanja, od identifikacije učinioca i dokazivanja toka novca, preko oduzimanja digitalne imovine, do izricanja i izvršenja krivičnih sankcija. Zbog toga je potrebno analizirati ne samo pojam i funkcionisanje kriptovaluta, već i normativni okvir, institucionalnu praksu i konkretne oblike njihove zloupotrebe u izvršenju i prikrivanju krivičnih dela (FATF, 2024).

1.1. Predmet i značaj istraživanja

Predmet ovog rada jeste analiza zloupotrebe kriptovaluta u izvršenju i prikrivanju krivičnih dela, sa posebnim osvrtom na krivičnopravne, bezbednosne i dokazne izazove koji se javljaju u praksi. Rad se bavi načinima na koje se kriptovalute i druga digitalna imovina mogu koristiti kao sredstvo plaćanja, prenosa, prikrivanja ili čuvanja protivpravno stečene koristi. U tom smislu, predmet istraživanja ne obuhvata samo tehnički aspekt kriptovaluta, već pre svega njihovu pravnu i kriminalističku dimenziju, odnosno pitanje kako se ova vrsta imovine pojavljuje u kontekstu savremenog kriminaliteta. Značaj istraživanja proizlazi iz činjenice da kriptovalute predstavljaju relativno nov, ali sve prisutniji fenomen u krivičnopravnoj praksi. Tradicionalni oblici finansijskog kriminaliteta najčešće su bili povezani sa bankarskim računima, gotovinskim tokovima, privrednim subjektima i formalnim finansijskim institucijama. Kod kriptovaluta, međutim, prenos vrednosti može se odvijati kroz digitalne novčanike, decentralizovane platforme i međunarodne mreže koje nisu uvek lako dostupne domaćim organima. To znači da se pred policiju, tužilaštvo, sudove i regulatorne organe postavljaju novi zahtevi u pogledu stručnosti, tehničkog znanja, međunarodne saradnje i upotrebe specijalizovanih alata za praćenje digitalnih transakcija.

Značaj ove teme ogleda se i u potrebi da se napravi jasna razlika između zakonite upotrebe kriptovaluta i njihove zloupotrebe. U javnosti se kriptovalute često posmatraju jednostrano, ili kao tehnološka inovacija koja donosi finansijsku slobodu, ili kao sredstvo pogodno za kriminalne aktivnosti. Naučni i stručni pristup mora biti uravnoteženiji. Kriptovalute nisu same po sebi kriminalne, ali njihove karakteristike mogu biti iskorišćene za otežavanje otkrivanja protivpravnih radnji. Zbog toga je značajno istražiti koje karakteristike kriptovaluta stvaraju rizike, kako se ti rizici manifestuju u praksi i da li postojeći pravni okvir može da odgovori na takve izazove. Poseban značaj istraživanja odnosi se na Republiku Srbiju, imajući u vidu da je donošenjem Zakona o digitalnoj imovini uspostavljen poseban pravni okvir za ovu oblast. Time je digitalna imovina prepoznata kao pravno relevantna kategorija, ali istovremeno ostaje pitanje koliko su postojeća zakonska rešenja, nadzorni mehanizmi i krivičnopravni instrumenti dovoljni u situacijama kada se kriptovalute koriste za prikrivanje imovine, pranje novca ili druga krivična dela. Upravo zbog toga rad ima teorijski, normativni i praktični značaj, jer povezuje pojam digitalne imovine sa konkretnim problemima krivičnog prava i bezbednosti.

1.2. Problem istraživanja

Osnovni problem istraživanja ogleda se u pitanju kako specifične karakteristike kriptovaluta utiču na izvršenje, prikrivanje, otkrivanje i dokazivanje krivičnih dela. Kriptovalute omogućavaju brz prenos vrednosti, često preko državnih granica, bez neposrednog oslanjanja na tradicionalne finansijske posrednike. Iako se transakcije beleže na blockchainu, identitet korisnika nije uvek neposredno vidljiv, jer se transakcije vezuju za adrese digitalnih novčanika, a ne za ime i prezime konkretnog lica. Takva pseudonimnost ne znači potpunu anonimnost, ali u praksi može značajno otežati rad organa gonjenja.

Problem istraživanja dodatno se usložnjava kada se kriptovalute koriste u kombinaciji sa drugim metodama prikrivanja. Učinioci krivičnih dela mogu koristiti više wallet-a, menjati jednu kriptovalutu za drugu, koristiti platforme sa slabijim pravilima identifikacije korisnika, prebacivati sredstva preko više jurisdikcija ili koristiti servise namenjene otežavanju praćenja transakcionih tragova. Na taj način nastaje složen lanac transakcija koji ima za cilj da se prikrije poreklo imovine, identitet korisnika i veza između izvršenog krivičnog dela i ostvarene koristi.

Istraživački problem se ne odnosi samo na tehničko praćenje transakcija, već i na pravnu kvalifikaciju, dokazivanje i oduzimanje digitalne imovine. U krivičnom postupku potrebno je dokazati ne samo da je određena digitalna imovina postojala, već i da je povezana sa konkretnim krivičnim delom, konkretnim licem i protivpravnom koristi. Pored toga, u praksi se postavlja pitanje kako obezbediti pristup digitalnom novčaniku, kako sprečiti dalje raspolaganje imovinom, kako izvršiti privremeno ili trajno oduzimanje i kako obezbediti da digitalni dokazi budu zakonito pribavljeni i upotrebljivi u postupku.

Još jedan važan problem jeste odnos između brzine tehnološkog razvoja i sporijeg razvoja pravnih normi. Kriminalne zloupotrebe često se prilagođavaju novim tehnologijama brže nego što zakonodavstvo i institucije uspevaju da razviju odgovarajuće mehanizme kontrole. Zbog toga se javlja potreba za stalnim unapređenjem propisa, institucionalnih kapaciteta i stručne obuke. U suprotnom, postoji rizik da se kriptovalute koriste kao sredstvo za izbegavanje tradicionalnih mehanizama finansijskog nadzora i krivičnopravne odgovornosti.

1.3. Ciljevi istraživanja

Opšti cilj ovog rada jeste da se analizira na koji način se kriptovalute mogu zloupotrebljavati u izvršenju i prikrivanju krivičnih dela, kao i da se oceni u kojoj meri postojeći normativni i institucionalni okvir može da odgovori na izazove koje takve zloupotrebe stvaraju. Rad nastoji da poveže teorijsko razumevanje kriptovaluta sa krivičnopravnom analizom i praktičnim problemima organa koji učestvuju u otkrivanju, gonjenju i presuđenju krivičnih dela.

Jedan od posebnih ciljeva rada jeste pojmovno određenje kriptovaluta i digitalne imovine. Da bi se mogla analizirati njihova zloupotreba, neophodno je prethodno objasniti šta su kriptovalute, kako funkcioniše blockchain, šta predstavljaju digitalni novčanici, na koji način se obavljaju transakcije i po čemu se kriptovalute razlikuju od tokena i drugih oblika digitalne imovine. Bez jasnog pojmovnog određenja postoji rizik da se pravna analiza zasniva na nepreciznim ili pogrešnim pretpostavkama.

Drugi poseban cilj jeste identifikovanje najčešćih oblika zloupotrebe kriptovaluta u kriminalnim aktivnostima. U radu će se analizirati upotreba kriptovaluta u pranju novca, prikrivanju porekla imovine, darknet trgovini, ransomware napadima, prevarama i drugim protivpravnim aktivnostima. Posebna pažnja biće posvećena tome da se prikaže kako kriptovalute mogu služiti kao sredstvo plaćanja, prenosa vrednosti ili prikrivanja protivpravne koristi.

Treći poseban cilj jeste analiza međunarodnog, evropskog i domaćeg normativnog okvira. U tom delu rada biće sagledani standardi i preporuke relevantnih međunarodnih organizacija, regulativa Evropske unije i pravni okvir Republike Srbije. Cilj je da se utvrdi da li postojeći propisi pružaju dovoljnu osnovu za nadzor, sprečavanje zloupotreba, dokazivanje i oduzimanje digitalne imovine, kao i gde se mogu uočiti problemi u praktičnoj primeni.

Četvrti poseban cilj jeste ispitivanje dokaznih i institucionalnih izazova. Rad će analizirati ulogu policije, javnog tužilaštva, sudova, regulatornih organa i drugih subjekata u postupcima koji se odnose na zloupotrebu kriptovaluta. Posebno će biti razmotreno pitanje stručne osposobljenosti, međunarodne saradnje, pristupa podacima, čuvanja digitalnih dokaza i saradnje sa pružaocima usluga povezanih sa digitalnom imovinom.

Peti cilj rada jeste da se kroz studije slučaja prikaže kako se zloupotreba kriptovaluta javlja u stvarnim predmetima. Analizom slučajeva Silk Road i Bitfinex hack moguće je pokazati različite modalitete upotrebe kriptovaluta, od plaćanja na darknet tržištima do složenih obrazaca prikrivanja porekla ukradene digitalne imovine. Ove studije slučaja imaju značaj jer omogućavaju povezivanje teorijske, normativne i kriminalističke analize.

Šesti cilj rada jeste sprovođenje empirijskog istraživanja putem online ankete na uzorku od 100 ispitanika. Empirijsko istraživanje treba da pokaže nivo informisanosti ispitanika o kriptovalutama, njihove stavove o rizicima zloupotrebe, percepciju adekvatnosti postojećih propisa i mišljenje o potrebi za strožom kontrolom, boljom međunarodnom saradnjom i specijalizovanom obukom nadležnih organa.

1.4. Hipoteze rada

U skladu sa predmetom, problemom i ciljevima istraživanja, u radu se polazi od nekoliko osnovnih hipoteza. Hipoteze su postavljene tako da omoguće povezivanje teorijskog, normativnog, praktičnog i empirijskog dela rada.

H1: Specifične karakteristike kriptovaluta, kao što su pseudonimnost, brzina transfera, prekogranični karakter transakcija i mogućnost korišćenja različitih tehničkih metoda prikrivanja, značajno olakšavaju prikrivanje porekla protivpravne imovinske koristi i otežavaju identifikaciju učinilaca krivičnih dela.

H2: Važeći normativni okvir predstavlja važnu osnovu za suzbijanje zloupotrebe kriptovaluta, ali u praktičnoj primeni i dalje postoje problemi koji se odnose na dokazivanje, međunarodnu saradnju, tehničko praćenje transakcija i oduzimanje digitalne imovine.

H3: Krivičnopravni odgovor na zloupotrebu kriptovaluta efikasniji je kada je povezan sa razvijenim mehanizmima sprečavanja pranja novca i finansiranja terorizma, regulacijom pružalaca usluga digitalne imovine i specijalizovanom obukom policije, tužilaštva, sudova i regulatornih organa.

H4: Ispitanici u online anketi će u većini oceniti da kriptovalute povećavaju rizik od pranja novca, prevara, ransomware napada i otežanog dokazivanja krivičnih dela.

H5: Studije slučaja Silk Road i Bitfinex potvrdiće da je uspešno otkrivanje i procesuiranje krivičnih dela povezanih sa kriptovalutama moguće, ali da zahteva visok nivo tehničke stručnosti, međunarodne koordinacije i pravilno obezbeđivanje digitalnih dokaza.

Postavljene hipoteze biće proveravane kroz analizu literature, pravnih izvora, međunarodnih standarda, studija slučaja i rezultata empirijskog istraživanja. Na taj način rad neće ostati samo na teorijskom objašnjenju kriptovaluta, već će pokušati da pokaže kako se njihova zloupotreba manifestuje u konkretnom pravnom i bezbednosnom kontekstu.

1.5. Metodologija i struktura rada

U radu će biti primenjen kombinovani metodološki pristup, jer sama tema zahteva povezivanje pravne, bezbednosne, kriminalističke i empirijske analize. Osnovu istraživanja čini normativni metod, koji će se koristiti za analizu međunarodnih, evropskih i domaćih pravnih izvora. Ovaj metod je značajan jer omogućava sagledavanje načina na koji su kriptovalute i digitalna imovina uređene u propisima, kao i procenu da li postojeći pravni okvir pruža adekvatne mehanizme za sprečavanje i sankcionisanje zloupotreba.

Pored normativnog metoda, biće primenjen i dogmatsko-pravni metod, naročito u delu rada koji se odnosi na krivičnopravni odgovor, dokazivanje, oduzimanje imovine i pitanja sankcionisanja. Ovaj metod omogućava tumačenje pravnih normi, njihovo sistemsko povezivanje i razumevanje njihove primene u konkretnim situacijama. Poseban značaj ima analiza odnosa između pravila o digitalnoj imovini, pravila o sprečavanju pranja novca i opštih krivičnopravnih instituta.

Uporednopravni metod koristiće se radi poređenja domaćih rešenja sa standardima Evropske unije i međunarodnim preporukama. Budući da kriptovalute po svojoj prirodi ne poznaju državne granice, uporednopravni pristup je neophodan za razumevanje šireg regulatornog okvira. Zloupotrebe kriptovaluta često imaju transnacionalni karakter, zbog čega se domaći pravni sistem ne može posmatrati izolovano od međunarodnih standarda, evropske regulative i prakse drugih država.

U radu će biti primenjena i analiza sadržaja stručne i naučne literature, izveštaja međunarodnih organizacija i relevantnih normativnih dokumenata. Ova metoda koristiće se za prikupljanje i obradu podataka o najčešćim oblicima zloupotrebe kriptovaluta, trendovima u kriminalitetu, pravnim rizicima i preporukama za unapređenje institucionalnog odgovora. Analiza sadržaja posebno je značajna za razumevanje savremenih oblika finansijskog i visokotehnološkog kriminaliteta.

Metoda studije slučaja biće primenjena u praktičnom delu rada, kroz analizu slučajeva Silk Road i Bitfinex hack. Ovi slučajevi izabrani su zato što jasno pokazuju različite načine zloupotrebe kriptovaluta. Silk Road je značajan za razumevanje upotrebe kriptovaluta kao sredstva plaćanja na darknet tržištu, dok je Bitfinex hack važan za analizu složenih metoda prikrivanja i pranja ukradene digitalne imovine. Studije slučaja omogućiće da se teorijski i normativni nalazi uporede sa stvarnim primerima iz prakse.

Empirijski deo rada zasnivaće se na online anketnom istraživanju na planiranom uzorku od 100 ispitanika. Anketa će biti anonimna i koristiće se za ispitivanje stavova ispitanika o rizicima zloupotrebe kriptovaluta, adekvatnosti propisa, potrebi za strožom kontrolom i značaju specijalizovane obuke nadležnih organa. Podaci će biti obrađeni metodama deskriptivne statistike, kroz prikaz frekvencija, procenata i osnovnih pokazatelja stavova ispitanika.

Struktura rada usklađena je sa postavljenim predmetom i ciljevima istraživanja. Nakon uvodnog dela, drugo poglavlje biće posvećeno pojmovnom određenju kriptovaluta i digitalne imovine. Treće poglavlje obrađivaće krivičnopravne i bezbednosne rizike povezane sa kriptovalutama. Četvrto poglavlje analiziraće normativni okvir za suzbijanje zloupotrebe kriptovaluta, uključujući međunarodne standarde, regulativu Evropske unije i pravni okvir Republike Srbije. Peto poglavlje predstavljaće centralni deo rada, jer će se baviti zloupotrebom kriptovaluta u izvršenju i prikrivanju krivičnih dela. Šesto poglavlje sadržaće studije slučaja, dok će sedmo poglavlje biti posvećeno empirijskom istraživanju. U osmom poglavlju biće izložena diskusija, a u zaključku će biti sumirani najvažniji nalazi, ocenjena potvrđenost hipoteza i date preporuke za unapređenje pravnog i institucionalnog odgovora.

2. POJMOVNO ODREĐENJE KRIPTOVALUTA I DIGITALNE IMOVINE

Kriptovalute i digitalna imovina predstavljaju jednu od najznačajnijih pojava savremenog digitalnog finansijskog sistema, jer su promenile tradicionalno razumevanje novca, vlasništva, plaćanja i prenosa vrednosti. Za razliku od klasičnih oblika novca, koji su vezani za centralne banke, komercijalne banke i državne finansijske sisteme, kriptovalute funkcionišu na osnovu decentralizovane tehnologije, odnosno na mrežama u kojima se evidencija transakcija vodi elektronski, distribuirano i bez potrebe za jednim centralnim autoritetom. Ovakav model omogućava korisnicima da vrše prenos vrednosti direktno, preko digitalnih adresa, uz korišćenje kriptografskih metoda za potvrđivanje autentičnosti transakcija. Zbog toga se kriptovalute ne mogu razumeti samo kao novi oblik novca, već i kao tehnološki, pravni, ekonomski i bezbednosni fenomen koji zahteva pažljivo pojamovno određenje pre svake dalje krivičnopravne analize (Nakamoto, 2008).

Pojmovno određenje kriptovaluta posebno je važno zato što se u praksi često mešaju različiti izrazi, kao što su kriptovaluta, virtuelna valuta, digitalna valuta, token, digitalna imovina, blockchain imovina i kripto-imovina. Iako se ovi pojmovi ponekad koriste kao sinonimi u svakodnevnom govoru, u pravnoj i stručnoj analizi između njih postoje bitne razlike. Kriptovalute se najčešće posmatraju kao digitalni zapisi vrednosti koji koriste kriptografiju i distribuiranu evidenciju transakcija, dok je digitalna imovina širi pojam koji može obuhvatiti ne samo kriptovalute, već i različite vrste tokena, digitalnih prava i drugih oblika imovine izraženih u digitalnom obliku. Upravo zbog toga je neophodno u radu najpre razjasniti osnovne pojmove, jer se tek nakon toga može precizno govoriti o zloupotrebi kriptovaluta u izvršenju i prikrivanju krivičnih dela (Cvetković, 2018).

U pravnom smislu, digitalna imovina je značajna jer se sve češće javlja kao predmet raspolaganja, ulaganja, oporezivanja, kontrole, zaplene i oduzimanja. To znači da ona više nije samo tehnološka novina ili predmet interesovanja užeg kruga korisnika, već postaje pravno relevantna kategorija. Republika Srbija je donošenjem Zakona o digitalnoj imovini prepoznala potrebu da se ova oblast posebno reguliše, čime je digitalna imovina uvedena u domaći pravni okvir kao pojam koji obuhvata virtuelne valute i digitalne tokene. Ovakvo zakonsko određenje važno je za dalju analizu, jer pokazuje da kriptovalute nisu izvan prava, već da se mogu posmatrati kao predmet pravnih odnosa, nadzora i eventualnog krivičnopravnog postupanja (Republika Srbija, 2020).

Sa stanovišta krivičnog prava i bezbednosti, razumevanje kriptovaluta zahteva istovremeno poznavanje njihove tehničke osnove i njihovih praktičnih posledica. Blockchain, digitalni novčanici, javni i privatni ključevi, menjačnice, transakcioni tragovi i decentralizovane mreže nisu samo tehnički pojmovi, već elementi koji mogu imati direktan značaj u otkrivanju i dokazivanju krivičnih dela. Na primer, činjenica da blockchain čuva zapis o transakcijama može pomoći u praćenju toka digitalne imovine, ali činjenica da se transakcije vezuju za adrese, a ne neposredno za identitet fizičkog lica, može otežati identifikaciju učinioca. Zbog toga se u nastavku ovog poglavlja najpre obrađuju nastanak i razvoj kriptovaluta, zatim njihove osnovne karakteristike, tehnička infrastruktura i, na kraju, razlika između kriptovaluta, tokena i drugih oblika digitalne imovine (Narayanan et al., 2016).

2.1. Nastanak i razvoj kriptovaluta

Nastanak kriptovaluta ne može se razumeti bez šireg konteksta razvoja interneta, digitalne ekonomije i dugogodišnjih pokušaja da se stvori elektronski novac koji bi mogao funkcionisati nezavisno od tradicionalnih finansijskih posrednika. Pre pojave Bitcoina postojale su različite ideje o digitalnom novcu, elektronskom plaćanju i kriptografski zaštićenim transakcijama, ali nijedan od tih modela nije uspeo da na trajan način reši problem dvostrukog trošenja, odnosno mogućnosti da isti digitalni zapis bude iskorišćen više puta. Kod fizičkog novca ovaj problem ne postoji na isti način, jer novčanica koja se preda drugom licu više nije kod prethodnog držaoca. Kod digitalnog zapisa, međutim, podaci se mogu kopirati, pa je bilo potrebno pronaći način da se spreči zloupotreba bez oslanjanja na centralnu banku ili drugu instituciju koja bi kontrolisala sve transakcije (Böhme et al., 2015).

Prelomni trenutak u razvoju kriptovaluta predstavlja objavljivanje rada pod nazivom „Bitcoin: A Peer-to-Peer Electronic Cash System”, koji je 2008. godine objavljen pod pseudonimom Satoshi Nakamoto. U tom radu predstavljen je model elektronskog novca koji funkcioniše putem peer-to-peer mreže, odnosno mreže ravnopravnih učesnika, bez potrebe za centralnim posrednikom. Osnovna ideja bila je da se transakcije potvrđuju kroz decentralizovani sistem, pri čemu učesnici mreže zajednički održavaju evidenciju transakcija. Time je stvorena osnova za Bitcoin kao prvu funkcionalnu kriptovalutu koja je uspela da poveže kriptografiju, distribuiranu evidenciju i ekonomski podsticaj učesnika mreže (Nakamoto, 2008).

Bitcoin mreža počela je da funkcioniše 2009. godine, a u početnoj fazi njen značaj bio je uglavnom eksperimentalan i tehnološki. Korisnici su ga posmatrali kao pokušaj stvaranja alternativnog finansijskog sistema, nezavisnog od banaka i državnih monetarnih politika. Vremenom je Bitcoin počeo da dobija tržišnu vrednost, a njegova upotreba se proširila među pojedincima, investitorima, programerima i različitim digitalnim zajednicama. Upravo ta faza razvoja bila je važna jer je pokazala da kriptovaluta može funkcionisati u praksi, da može imati ekonomsku vrednost i da se može prenositi između korisnika bez klasičnog bankarskog sistema (Antonopoulos, 2017).

Razvoj Bitcoina otvorio je prostor za nastanak velikog broja drugih kriptovaluta. Neke od njih nastale su kao izmene postojećeg Bitcoin modela, dok su druge razvijene sa novim tehničkim i funkcionalnim rešenjima. Pojava Etheruma bila je posebno značajna, jer je blockchain tehnologiju proširila izvan jednostavnog prenosa digitalne vrednosti i omogućila razvoj pametnih ugovora, decentralizovanih aplikacija i različitih tokena. Na taj način je kripto-prostor prerastao iz sistema elektronskog novca u mnogo širi ekosistem digitalne imovine, u kome se mogu stvarati različiti oblici digitalnih prava, finansijskih instrumenata i decentralizovanih usluga (Buterin, 2014).

U početku su kriptovalute bile povezane uglavnom sa tehnološkim entuzijastima i korisnicima koji su želeli veću finansijsku autonomiju. Međutim, kako je njihova tržišna vrednost rasla, one su postale predmet interesovanja investitora, kompanija, regulatornih organa, poreskih uprava i organa krivičnog gonjenja. Njihov razvoj više nije mogao da se posmatra samo kao tehnološki eksperiment, već kao pojava sa ozbiljnim ekonomskim i pravnim posledicama. U tom procesu javila se potreba za jasnijim normativnim određenjem, naročito zbog rizika od pranja novca, finansiranja terorizma, poreskih zloupotreba i drugih oblika kriminalne upotrebe (Vandezande, 2017).

Razvoj kriptovaluta pratio je i razvoj tržišne infrastrukture. Pored samih blockchain mreža, nastale su centralizovane i decentralizovane kripto-menjačnice, pružaoci usluga čuvanja digitalne imovine, platforme za trgovinu tokenima, servisi za pozajmljivanje digitalne imovine i drugi oblici poslovanja povezani sa kripto-ekonomijom. Time je stvoren poseban sektor koji funkcioniše na granici finansijskog tržišta, tehnološke inovacije i pravne regulacije. Upravo u tom prostoru nastaju i brojni rizici, jer se korisnici, transakcije i sredstva često kreću između različitih platformi i jurisdikcija, što otežava kontrolu i nadzor (FATF, 2024).

Kriptovalute su se razvijale i u kontekstu globalnog nepoverenja prema tradicionalnim finansijskim institucijama, naročito nakon finansijske krize iz 2008. godine. Ideja decentralizovanog novca bila je privlačna delu javnosti jer je obećavala sistem u kome korisnici ne zavise od banaka, posrednika i državnih intervencija. Ipak, takav sistem je od početka imao dvostruku prirodu. Sa jedne strane, omogućio je inovacije i nove oblike finansijskog poslovanja, dok je sa druge strane otvorio prostor za zloupotrebe, posebno zato što su učinioci krivičnih dela brzo prepoznali mogućnost da digitalnu imovinu koriste za prikrivanje tragova i prenos protivpravne koristi (Yermack, 2015).

Dalji razvoj kriptovaluta doveo je do toga da se one sve više posmatraju ne samo kao sredstvo plaćanja, već i kao investiciona imovina. Mnogi korisnici kupuju kriptovalute ne da bi njima plaćali robu i usluge, već da bi ih čuvali, preprodavali ili koristili u okviru različitih oblika digitalnih finansijskih aktivnosti. Time se promenila i priroda pravnih pitanja koja se postavljaju. Pored pitanja zakonitosti plaćanja, pojavila su se pitanja zaštite investitora, tržišne manipulacije, poreskog tretmana, odgovornosti platformi i pravnog statusa različitih vrsta tokena (Houben & Snyers, 2018).

U domaćem pravu, razvoj kriptovaluta i digitalne imovine dobio je poseban značaj donošenjem Zakona o digitalnoj imovini. Ovaj zakon nastoji da pravno uredi izdavanje digitalne imovine, pružanje usluga povezanih sa digitalnom imovinom, nadzor nad pružaocima usluga i određene aspekte zaštite korisnika. Time je Republika Srbija pokušala da stvori okvir koji istovremeno omogućava razvoj digitalne imovine i smanjenje rizika od zloupotreba. Ipak, samo postojanje zakonskog okvira ne znači da su svi problemi rešeni, jer se u praksi i dalje postavljaju pitanja efikasnog nadzora, međunarodne saradnje, dokazivanja i oduzimanja digitalne imovine (Babović, 2023).

Nastanak i razvoj kriptovaluta zato treba posmatrati kao proces koji je započeo tehnološkom inovacijom, ali se postepeno pretvorio u složen pravni i bezbednosni izazov. Od prvobitne ideje elektronskog novca bez posrednika, kriptovalute su postale deo globalnog finansijskog sistema, predmet investicionih aktivnosti, regulatornih intervencija i krivičnopravnih analiza. Upravo zato je za ovaj rad važno da se kriptovalute ne posmatraju izolovano, već u vezi sa digitalnom imovinom, finansijskim tržištem, pravnim normama i oblicima kriminaliteta koji koriste prednosti savremenih tehnologija (De Filippi & Wright, 2018).

2.2. Osnovne karakteristike kriptovaluta

Jedna od osnovnih karakteristika kriptovaluta jeste njihova digitalna priroda. Kriptovalute nemaju fizički oblik, ne postoje kao novčanice ili kovani novac, već kao digitalni zapisi u okviru određene mreže. Njihovo postojanje, prenos i kontrola zasnivaju se na podacima, kriptografskim ključevima i pravilima mrežnog protokola. To znači da korisnik kriptovalute ne poseduje fizički predmet, već ima mogućnost da putem privatnog ključa raspolaže određenom količinom digitalne vrednosti koja je evidentirana na blockchainu. Ova osobina ima veliki značaj za krivičnopravnu analizu, jer se pitanje posedovanja, kontrole i oduzimanja digitalne imovine razlikuje od klasičnog oduzimanja gotovog novca ili fizičkih predmeta (Antonopoulos, 2017).

Druga važna karakteristika jeste decentralizacija. Kod mnogih kriptovaluta ne postoji centralna institucija koja izdaje valutu, vodi evidenciju svih transakcija i odlučuje o njihovoj validnosti. Umesto toga, mreža funkcioniše kroz veliki broj učesnika koji proveravaju i potvrđuju transakcije prema unapred definisanim pravilima. Decentralizacija je jedna od osobina koja kriptovalutama daje posebnu tehnološku i ideološku vrednost, jer smanjuje zavisnost od tradicionalnih finansijskih posrednika. Ipak, iz perspektive nadzora i krivičnog postupka, decentralizacija može otežati identifikaciju odgovornog subjekta, naročito kada nema jasno određenog operatora ili institucije kojoj se organi mogu obratiti za podatke (Narayanan et al., 2016).

Treća karakteristika kriptovaluta jeste upotreba kriptografije. Kriptografija omogućava zaštitu transakcija, potvrđivanje autentičnosti i kontrolu raspolaganja digitalnom imovinom. Javni ključ ili adresa omogućava primanje sredstava, dok privatni ključ omogućava njihovo slanje i kontrolu. Ukoliko korisnik izgubi privatni ključ, u velikom broju slučajeva gubi i praktičnu mogućnost pristupa svojoj digitalnoj imovini. Sa druge strane, ako privatni ključ dođe u posed drugog lica, to lice može raspolagati digitalnim sredstvima. Ova činjenica je naročito važna kod krađa kriptovaluta, računarskih prevara i postupaka oduzimanja digitalne imovine, jer kontrola nad ključem često znači i faktičku kontrolu nad imovinom (Zohar, 2015).

Jedna od najčešće pominjanih karakteristika kriptovaluta jeste pseudonimnost. To znači da transakcije nisu neposredno vezane za ime, prezime ili druge lične podatke korisnika, već za digitalne adrese.

Pseudonimnost ne znači potpunu anonimnost, jer se transakcije najčešće javno beleže na blockchainu i mogu se analizirati. Međutim, dok se adresa ne poveže sa konkretnim licem, identitet korisnika ostaje prikriven ili nejasan. Upravo ta osobina stvara značajne izazove za policiju, tužilaštvo i druge organe, jer je za dokazivanje potrebno utvrditi ne samo da je neka transakcija izvršena, već i ko je za nju odgovoran (Europol, 2021).

Kriptovalute karakteriše i mogućnost brzog prekograničnog prenosa vrednosti. Tradicionalni međunarodni bankarski transferi često zahtevaju posrednike, vreme obrade, identifikaciju korisnika i određene kontrole. Kod kriptovaluta, transakcija može biti izvršena direktno između korisnika iz različitih država, često bez potrebe da se prolazi kroz bankarski sistem. Ova osobina može biti korisna za zakonite korisnike, ali istovremeno predstavlja rizik kada se koristi za prenos protivpravne imovinske koristi, izbegavanje kontrole ili otežavanje nadležnosti domaćih organa (FATF, 2024).

Još jedna bitna osobina jeste nepovratnost transakcija. Kada se transakcija na blockchainu potvrdi, ona se po pravilu ne može jednostavno poništiti kao što se ponekad može osporiti bankarska transakcija ili platna kartica. Ova osobina doprinosi sigurnosti sistema, jer sprečava naknadne manipulacije potvrđenim zapisima, ali može biti problematična u slučajevima prevare, krađe ili iznude. Ako žrtva pošalje kriptovaluu učiniocu krivičnog dela, povraćaj sredstava zavisi od mogućnosti praćenja, zamrzavanja, zaplene ili dobrovoljnog vraćanja, što u praksi često nije jednostavno (Böhme et al., 2015).

Posebno značajna karakteristika kriptovaluta jeste transparentnost transakcionih zapisa kod javnih blockchain mreža. Na prvi pogled može delovati protivrečno da se kriptovalute povezuju i sa transparentnošću i sa prikrivanjem identiteta. Međutim, ta dva svojstva postoje istovremeno. Transakcije mogu biti javno vidljive, ali korisnici koji stoje iza adresa ne moraju biti odmah poznati. To znači da blockchain može biti koristan izvor dokaza, jer omogućava analizu toka sredstava, ali ne rešava sam po sebi pitanje identiteta učinioca. Upravo zbog toga se u istragama sve više koriste specijalizovani alati za analizu blockchain transakcija i povezivanje adresa sa poznatim platformama ili korisnicima (Meiklejohn et al., 2013).

Kriptovalute se razlikuju i po stepenu stabilnosti vrednosti. Bitcoin i mnoge druge kriptovalute poznate su po velikim promenama tržišne vrednosti, što ih čini rizičnim kao sredstvo čuvanja imovine i kao sredstvo plaćanja. Nasuprot tome, stabilne kriptovalute, odnosno stablecoins, nastoje da održe vrednost vezivanjem za određenu fiat valutu, robu ili drugi oblik imovine.

Ova razlika je značajna zato što stabilne kriptovalute mogu biti pogodnije za plaćanja i transfere, dok volatilne kriptovalute često imaju investicionu funkciju. Sa aspekta krivičnopravnih rizika, obe vrste mogu biti zloupotrebljene, ali na različite načine i u različitim fazama prikrivanja imovine (Arner et al., 2020).

Kriptovalute se takođe odlikuju visokim stepenom tehnološke složenosti. Za prosečnog korisnika, pojmovi kao što su privatni ključ, seed fraza, hash, blok, potvrda transakcije, pametni ugovor ili decentralizovana menjačnica mogu biti teško razumljivi. Ta složenost stvara prostor za prevare, jer učinioci mogu iskoristiti neznanje korisnika nudeći lažne investicije, lažne platforme, phishing poruke ili obmanjujuće projekte. Zbog toga kriptovalute nisu samo pitanje finansijskog nadzora, već i pitanje digitalne pismenosti, zaštite korisnika i prevencije visokotehnološkog kriminaliteta (Europol, 2024).

Važno je istaći da kriptovalute imaju i legitimne funkcije. One se mogu koristiti za brže i jeftinije transakcije, za ulaganje, za razvoj novih tehnoloških rešenja i za finansijske usluge u sredinama gde je pristup bankarskom sistemu ograničen. Međutim, legitimna upotreba ne isključuje potrebu za regulacijom, jer svaka finansijska inovacija može biti zloupotrebljena. Zbog toga pravni sistem mora pronaći ravnotežu između podsticanja inovacija i sprečavanja kriminalne upotrebe digitalne imovine (Houben & Snyers, 2018).

Upravo navedene karakteristike pokazuju zbog čega su kriptovalute posebno važne za ovaj rad. Njihova digitalna priroda, decentralizacija, pseudonimnost, brzina transfera, prekogranični karakter, nepovratnost transakcija i tehnološka složenost stvaraju mogućnosti za zakonitu upotrebu, ali i za različite oblike zloupotrebe. U kontekstu krivičnih dela, ove osobine mogu olakšati prikrivanje porekla imovine, otežati identifikaciju učinioca i komplikovati postupak dokazivanja. Zato se kriptovalute moraju analizirati ne samo kao finansijska inovacija, već i kao pojava koja menja način izvršenja i otkrivanja pojedinih krivičnih dela (UNODC, 2024).

2.3. Blockchain, wallet-i, menjačnice i transakcioni tragovi

Blockchain predstavlja osnovnu tehnologiju na kojoj funkcionišu mnoge kriptovalute. U najjednostavnijem smislu, blockchain se može objasniti kao distribuirana evidencija transakcija koja se sastoji od blokova povezanih u lanac. Svaki blok sadrži određeni broj transakcija, a povezivanje blokova vrši se kriptografskim metodama, tako da naknadna promena ranijih zapisa postaje izuzetno otežana.

Ovakav sistem omogućava da veliki broj učesnika mreže ima uvid u istu evidenciju i da se transakcije potvrđuju bez centralnog posrednika. Za pravnu analizu blockchain je značajan zato što istovremeno pruža trag o kretanju digitalne imovine i stvara nove izazove u pogledu identifikacije korisnika (Nakamoto, 2008).

Kod javnih blockchain mreža, podaci o transakcijama su najčešće dostupni svakome ko koristi odgovarajuće alate za pregled blockchaina. Moguće je videti sa koje adrese je određena količina kriptovalute poslata, na koju adresu je primljena, kada je transakcija izvršena i u kom iznosu. Međutim, takav zapis ne sadrži nužno podatke o stvarnom identitetu lica koje kontroliše adresu. Zbog toga blockchain trag može biti veoma vredan dokazni materijal, ali je za njegovu upotrebu u krivičnom postupku potrebno dodatno povezivanje digitalnih adresa sa konkretnim licima, uređajima, platformama ili drugim dokazima (Meiklejohn et al., 2013).

Digitalni novčanik, odnosno wallet, predstavlja sredstvo putem kog korisnik upravlja svojom kriptovalutom. Važno je naglasiti da wallet najčešće ne čuva kriptovalutu u fizičkom ili klasičnom digitalnom smislu, već čuva ili omogućava pristup privatnim ključevima pomoću kojih korisnik raspolaže sredstvima evidentiranim na blockchainu. Postoje različite vrste wallet-a, među kojima se najčešće razlikuju softverski, hardverski, online i offline novčanici. Sa aspekta bezbednosti, najvažnije pitanje jeste ko kontroliše privatni ključ, jer kontrola nad privatnim ključem u praksi znači mogućnost raspolaganja digitalnom imovinom (Antonopoulos, 2017).

Razlika između custodial i non-custodial wallet-a ima poseban značaj za krivičnopravnu i regulatornu analizu. Kod custodial modela, privatne ključeve u ime korisnika čuva određena platforma ili pružalac usluge, najčešće kripto-menjačnica. U takvim slučajevima postoji subjekt kome se organi mogu obratiti za podatke, zamrzavanje sredstava ili druge oblike saradnje, ukoliko za to postoje zakonski uslovi. Kod non-custodial wallet-a, korisnik sam kontroliše privatni ključ, pa ne postoji posrednik koji može jednostavno ograničiti raspolaganje sredstvima. Ova razlika je važna zato što direktno utiče na mogućnost nadzora, prikupljanja dokaza i oduzimanja digitalne imovine (FATF, 2024).

Kripto-menjačnice predstavljaju platforme preko kojih korisnici mogu kupovati, prodavati ili menjati kriptovalute za tradicionalni novac ili druge oblike digitalne imovine. One imaju centralnu ulogu u povezivanju kripto-ekosistema sa klasičnim finansijskim sistemom, jer omogućavaju ulazak i izlazak sredstava iz digitalnog prostora. Zbog toga su menjačnice posebno važne za regulatorne organe i organe krivičnog gonjenja.

Kada menjačnice primenjuju pravila identifikacije korisnika, čuvanja podataka i prijavljivanja sumnjivih transakcija, one mogu biti značajan izvor informacija u istragama. Kada takva pravila ne postoje ili se ne primenjuju dovoljno, menjačnice mogu postati pogodne za prikrivanje porekla sredstava (Vandezande, 2017).

Pored centralizovanih menjačnica, u praksi sve veći značaj imaju i decentralizovane menjačnice. One omogućavaju korisnicima da međusobno razmenjuju digitalnu imovinu putem pametnih ugovora, često bez klasične registracije naloga i bez centralnog operatora koji direktno upravlja svim transakcijama. Ovakav model može doprineti većoj autonomiji korisnika, ali istovremeno otežava primenu tradicionalnih pravila nadzora. U kontekstu zloupotrebe, decentralizovane menjačnice mogu se koristiti za brzo prebacivanje jedne digitalne imovine u drugu, čime se dodatno komplikuje praćenje porekla sredstava (Schär, 2021).

Transakcioni tragovi predstavljaju jedan od najvažnijih elemenata u analizi kriptovaluta. Za razliku od gotovinskih transakcija, koje često ne ostavljaju lako proverljiv trag, mnoge kripto-transakcije ostaju trajno zabeležene na blockchainu. To znači da istražni organi, uz odgovarajuće znanje i alate, mogu pratiti kretanje sredstava kroz niz adresa. Ipak, taj proces nije jednostavan, jer učinioci mogu koristiti više adresa, više platformi, različite vrste kriptovaluta i tehnike kojima se otežava analiza. Zbog toga se transakcioni tragovi moraju tumačiti pažljivo i u vezi sa drugim dokazima (Europol, 2021).

U praksi je posebno važno pitanje povezivanja blockchain podataka sa podacima iz realnog sveta. Sama činjenica da je određena adresa primila ili poslala sredstva ne znači automatski da je poznato ko je izvršilac. Međutim, ako se ta adresa poveže sa nalogom na menjačnici, IP adresom, elektronskom komunikacijom, uređajem, svedočenjem ili drugim dokazima, tada blockchain trag može dobiti znatno veću dokaznu snagu. Upravo ova kombinacija digitalne forenzike, finansijske istrage i klasičnog kriminalističkog rada predstavlja osnovu uspešnog otkrivanja krivičnih dela povezanih sa kriptovalutama (Casey et al., 2019).

Blockchain analiza može biti korisna i za identifikaciju obrazaca ponašanja. Na primer, ponavljanje određenih transakcija, slanje sredstava na poznate adrese povezane sa nezakonitim aktivnostima, razbijanje većih iznosa na manje transakcije ili brzo prebacivanje sredstava između više adresa mogu ukazivati na pokušaj prikrivanja porekla imovine.

Ipak, takvi obrasci sami po sebi ne moraju biti dovoljan dokaz krivice, već predstavljaju indicije koje moraju biti proverene kroz širi dokazni postupak. U krivičnom pravu je posebno važno da se tehnički podaci ne tumače izolovano, već u vezi sa konkretnim radnjama, namerom i drugim dokazima (Möser et al., 2013).

Poseban problem predstavljaju servisi i tehnike čiji je cilj otežavanje praćenja transakcija. U stručnoj literaturi i izveštajima često se pominju mikseri, tumblers, chain-hopping i korišćenje više platformi ili kriptovaluta radi prikrivanja traga. U ovom radu ovi pojmovi se obrađuju isključivo na analitičkom nivou, jer su važni za razumevanje problema sa kojima se susreću nadležni organi. Njihov značaj je u tome što pokazuju da blockchain trag ne mora uvek biti jednostavan i linearan, već može biti namerno učinjen složenim, što zahteva specijalizovanu obuku i međunarodnu saradnju (FATF, 2024).

Za domaći pravni okvir posebno je važno pitanje pružalaca usluga povezanih sa digitalnom imovinom. Ukoliko se preko određenih platformi vrši kupovina, prodaja, čuvanje ili prenos digitalne imovine, takvi subjekti mogu imati obaveze u pogledu identifikacije korisnika, upravljanja rizicima i saradnje sa nadležnim organima. Time se pokušava smanjiti prostor za zloupotrebe, naročito u oblasti pranja novca i finansiranja terorizma. Ipak, praktični problem ostaje kod platformi koje posluju van domaće jurisdikcije ili kod modela u kojima nema centralnog pružaoca usluge (Republika Srbija, 2020).

Transakcioni tragovi imaju poseban značaj i za pitanje oduzimanja digitalne imovine. Da bi se određena digitalna imovina oduzela, potrebno je utvrditi da ona postoji, da je pod kontrolom određenog lica i da je povezana sa krivičnim delom ili protivpravnom koristi. Kod kriptovaluta se dodatno javlja pitanje pristupa privatnim ključevima, čuvanja oduzete imovine, sprečavanja njenog daljeg prenosa i vrednovanja u uslovima tržišne promenljivosti. Ova pitanja pokazuju da digitalna imovina zahteva posebna procesna i tehnička rešenja, jer se ne može u svemu tretirati isto kao gotov novac, vozilo ili nepokretnost (Europol, 2024).

Blockchain, wallet-i, menjačnice i transakcioni tragovi predstavljaju osnovne elemente za razumevanje funkcionisanja kriptovaluta. Oni istovremeno pokazuju zašto kriptovalute mogu biti korisne za zakonite korisnike i zašto mogu biti privlačne učiniocima krivičnih dela. Za potrebe ovog rada najvažnije je razumeti da blockchain ne omogućava potpunu nevidljivost, ali ni automatsku identifikaciju korisnika. Između ta dva pola nalazi se prostor u kome se odvijaju finansijske istrage, digitalna forenzika, regulatorni nadzor i krivičnopravno dokazivanje (Narayanan et al., 2016).

2.4. Razlika između kriptovaluta, tokena i druge digitalne imovine

Razlikovanje kriptovaluta, tokena i druge digitalne imovine važno je zato što se u praksi ovi pojmovi često koriste neprecizno, iako nemaju isto značenje. Kriptovalute se najčešće definišu kao digitalni oblici vrednosti koji funkcionišu na sopstvenoj blockchain mreži ili u okviru decentralizovanog sistema namenjenog prenosu vrednosti. Bitcoin je najpoznatiji primer kriptovalute jer je zamišljen kao elektronski novac koji se može prenositi neposredno između korisnika. U tom smislu, osnovna funkcija kriptovalute jeste da služi kao sredstvo razmene, čuvanja vrednosti ili obračunska jedinica, iako se u praksi te funkcije ostvaruju u različitom stepenu (Yermack, 2015).

Tokeni su širi i složeniji pojam. Oni najčešće nastaju na već postojećim blockchain mrežama, kao što je Ethereum, i mogu predstavljati različita prava, funkcije ili vrednosti. Za razliku od kriptovaluta koje obično imaju sopstvenu mrežu, tokeni se često izdaju putem pametnih ugovora na postojećoj infrastrukturi. Token može služiti za pristup određenoj usluzi, učešće u projektu, predstavljanje imovinskog prava, glasanje u decentralizovanoj organizaciji ili trgovinu u okviru određenog ekosistema. Zbog takve raznovrsnosti, tokeni zahtevaju pažljiviju pravnu kvalifikaciju od klasičnih kriptovaluta (De Filippi & Wright, 2018).

U stručnoj literaturi često se razlikuju payment tokeni, utility tokeni i security tokeni. Payment tokeni su najbliži kriptovalutama, jer im je osnovna funkcija prenos vrednosti ili plaćanje. Utility tokeni omogućavaju pristup određenoj usluzi, platformi ili digitalnom proizvodu. Security tokeni su najbliži finansijskim instrumentima, jer mogu predstavljati udeo, potraživanje, pravo na prihod ili drugi oblik investicionog prava. Ova podela nije uvek jednostavna, jer jedan token može imati više funkcija, ali je značajna za određivanje pravnog režima, nadzora i odgovornosti izdavalaca (Houben & Snyers, 2018).

Pojam digitalne imovine je širi od pojma kriptovaluta. U domaćem pravu digitalna imovina obuhvata virtuelne valute i digitalne tokene, što znači da zakonodavac pravi razliku između digitalnog zapisa vrednosti koji se može koristiti kao sredstvo razmene i digitalnog zapisa koji može predstavljati određeno pravo. Takvo određenje je važno jer omogućava da se različiti oblici digitalne imovine obuhvate jednim regulatornim okvirom, ali da se istovremeno prepoznaju njihove posebnosti. Za krivičnopravnu analizu to znači da predmet zloupotrebe ne mora biti samo Bitcoin ili slična kriptovaluta, već i drugi oblici digitalne imovine koji imaju ekonomsku vrednost (Republika Srbija, 2020).

Regulativa Evropske unije takođe koristi širi pojam kripto-imovine, nastojeći da obuhvati različite digitalne oblike vrednosti i prava koji se mogu prenositi i čuvati elektronski. Uredba MiCA predstavlja jedan od najvažnijih regulatornih koraka u ovoj oblasti, jer nastoji da uredi tržišta kripto-imovine, izdavanje pojedinih vrsta tokena i pružanje usluga povezanih sa kripto-imovinom. Ovakav pristup pokazuje da se savremena regulacija ne može ograničiti samo na Bitcoin ili tradicionalno shvaćene kriptovalute, već mora obuhvatiti mnogo širi skup digitalnih instrumenata (European Union, 2023).

Razlika između kriptovaluta i tokena ima značaj i za pitanje zloupotrebe. Kriptovalute se često koriste kao sredstvo prenosa ili prikrivanja vrednosti, dok se tokeni mogu zloupotrebiti i kroz lažne investicione projekte, manipulaciju tržištem, obmanjujuće početne ponude i prikrivanje stvarne prirode prava koja se nude korisnicima. Kod pojedinih tokena problem nije samo u tome kako se prenosi vrednost, već i u tome da li je korisnik doveden u zabludu u pogledu stvarne vrednosti, prava ili rizika ulaganja. Zbog toga pravna analiza mora razlikovati situacije u kojima se digitalna imovina koristi kao sredstvo izvršenja krivičnog dela od situacija u kojima je sama digitalna imovina predmet prevare ili manipulacije (Europol, 2024).

Digitalna imovina može imati i oblik nezamenljivih tokena, poznatih kao NFT. NFT predstavlja jedinstveni digitalni zapis koji se može povezati sa digitalnim sadržajem, umetničkim delom, kolekcionarskim predmetom ili drugim oblikom prava. Iako NFT ne funkcioniše isto kao Bitcoin ili druga kriptovaluta, on može imati tržišnu vrednost i može biti predmet kupoprodaje, ulaganja ili zloupotrebe. U kontekstu ovog rada, NFT nije centralni predmet analize, ali je važan kao primer širenja pojma digitalne imovine i potrebe da se pravni sistem prilagodi različitim oblicima digitalnog vlasništva (Fairfield, 2022).

Treba razlikovati i kriptovalute od elektronskog novca i digitalnih oblika tradicionalne valute. Elektronski novac je vezan za zvaničnu valutu i izdavaoca koji je pravno odgovoran za njegovo izdavanje i otkup. Kriptovalute, naročito decentralizovane, ne funkcionišu na isti način, jer njihova vrednost najčešće zavisi od tržišta, poverenja korisnika i pravila mreže. Takođe, centralnobankarske digitalne valute, o kojima se sve više raspravlja u svetu, predstavljaju poseban oblik digitalnog novca koji izdaje centralna banka, pa se ne mogu poistovetiti sa decentralizovanim kriptovalutama (Bank for International Settlements, 2021).

Za krivičnopravnu analizu naročito je važno pitanje da li se određena digitalna imovina može smatrati imovinom, sredstvom plaćanja, predmetom ulaganja ili pravom. Od toga može zavisiti način pravne kvalifikacije, dokazivanja, oduzimanja i zaštite oštećenih lica.

Ako se kriptovaluta koristi kao sredstvo plaćanja za nezakonitu robu ili uslugu, ona ima drugačiju ulogu nego kada je predmet krađe, prevare ili pranja novca. Ako token predstavlja investiciono pravo, tada se mogu otvoriti pitanja lažnog predstavljanja, tržišne manipulacije ili neovlašćenog pružanja finansijskih usluga (Cvetković, 2018).

Razlika između pojedinih oblika digitalne imovine značajna je i za nadležne organe. Policija, tužilaštvo i sudovi moraju razumeti da digitalna imovina nije jedinstvena kategorija u tehničkom i pravnom smislu. Nije isto kada se istražuje transfer Bitcoina, izdavanje tokena, zloupotreba stablecoin-a, krađa pristupnih ključeva ili prevara povezana sa lažnom investicionom platformom. Svaka od ovih situacija može zahtevati drugačije dokaze, drugačiji način praćenja tragova i drugačiji pravni pristup (Casey et al., 2019).

Pojmovno razlikovanje kriptovaluta, tokena i druge digitalne imovine zato predstavlja neophodan osnov za dalju analizu u ovom radu. Bez jasnog razumevanja ovih pojmova nije moguće precizno sagledati krivičnopravne i bezbednosne rizike, normativni okvir, modalitete zloupotrebe i probleme dokazivanja. Kriptovalute predstavljaju samo jedan deo šireg sistema digitalne imovine, ali su zbog svoje rasprostranjenosti, tržišne vrednosti i česte upotrebe u spornim transakcijama posebno značajne za temu zloupotrebe u izvršenju i prikrivanju krivičnih dela (Babović, 2023).

3. KRIVIČNOPRAVNI I BEZBEDNOSNI RIZICI POVEZANI SA KRIPTOVALUTAMA

Kriptovalute predstavljaju složen izazov za krivično pravo i sistem bezbednosti zato što se nalaze na preseku finansijskih tokova, visokih tehnologija, digitalne forenzike i transnacionalnog kriminaliteta. Njihova osnovna funkcija nije kriminalna, jer se mogu koristiti za zakonita plaćanja, ulaganja, prenos vrednosti i razvoj novih oblika digitalne ekonomije. Ipak, iste osobine koje omogućavaju brzinu, decentralizaciju i globalnu dostupnost mogu biti iskorišćene i za prikrivanje identiteta, otežavanje kontrole novčanih tokova i udaljšavanje protivpravne koristi od krivičnog dela iz kog potiče. Zbog toga se kriptovalute u savremenim izveštajima međunarodnih organizacija sve češće pominju u vezi sa pranjem novca, prevarama, ransomware napadima, darknet tržištima i drugim oblicima visokotehnološkog i finansijskog kriminaliteta (Europol, 2024).

Krivičnopravni rizici povezani sa kriptovalutama ne proizlaze samo iz toga što se one mogu koristiti kao sredstvo plaćanja, već i iz toga što omogućavaju drugačiji način čuvanja, prenosa i prikrivanja imovine. Kod tradicionalnog finansijskog kriminaliteta trag novca često se prati preko bankarskih računa, poslovnih knjiga, ugovora, platnih naloga i finansijskih institucija. Kod kriptovaluta se trag nalazi u digitalnim adresama, transakcijama na blockchainu, podacima sa menjačnica, pristupnim ključevima, elektronskim uređajima i komunikaciji korisnika. To znači da se klasična finansijska istraga mora dopuniti digitalnom forenzikom i specijalizovanim znanjima iz oblasti blockchain analitike (Casey et al., 2019).

Bezbednosni rizici posebno se uočavaju u činjenici da kriptovalute omogućavaju prekogranični transfer vrednosti bez fizičkog kretanja novca i bez nužnog oslanjanja na bankarski sistem. Takve transakcije mogu biti zakonite, ali mogu biti iskorišćene i za skrivanje imovine od organa gonjenja, za finansiranje protivpravnih aktivnosti ili za prenos koristi ostvarene krivičnim delom. U takvim okolnostima domaći organi često zavise od saradnje sa stranim platformama, drugim državama i međunarodnim organizacijama, jer učinilac, žrtva, menjačnica, wallet i digitalna imovina mogu biti povezani sa različitim jurisdikcijama. To otežava ne samo otkrivanje i dokazivanje, već i privremeno i trajno oduzimanje imovine (FATF, 2024).

Važno je naglasiti da kriptovalute ne obezbeđuju potpunu nevidljivost. Kod mnogih javnih blockchain mreža transakcije su vidljive i mogu se naknadno analizirati. Međutim, problem nastaje zato što vidljivost transakcije ne znači automatski i vidljivost identiteta korisnika. Organi postupka mogu uočiti određeni tok digitalne imovine, ali moraju dodatno dokazati ko kontroliše adresu, ko je raspolagao privatnim ključem, da li je određena transakcija povezana sa konkretnim krivičnim delom i da li postoji namera prikrivanja ili sticanja protivpravne koristi. Zato se rizici povezani sa kriptovalutama moraju posmatrati kroz više povezanih nivoa: tehnički, dokazni, procesni, regulatorni i krivičnopravni (Meiklejohn et al., 2013).

3.1. Anonimnost, pseudonimnost i otežana identifikacija učinilaca

Jedan od najvažnijih rizika povezanih sa kriptovalutama jeste otežana identifikacija lica koja stoje iza određenih transakcija. U svakodnevnom govoru često se kaže da su kriptovalute anonimne, ali je preciznije govoriti o pseudonimnosti. To znači da se transakcije na blockchainu najčešće ne vezuju neposredno za ime i prezime korisnika, već za digitalne adrese koje funkcionišu kao pseudonimi. Drugim rečima, javno može biti vidljivo da je određena adresa poslala ili primila određenu količinu kriptovalute, ali se iz same adrese ne vidi nužno ko je stvarni korisnik. Upravo ta razlika između vidljivosti transakcije i nevidljivosti identiteta predstavlja jedan od glavnih izazova u krivičnopravnom postupanju (Narayanan et al., 2016).

Pseudonimnost nije isto što i potpuna anonimnost, jer se blockchain tragovi mogu analizirati. Ukoliko se digitalna adresa poveže sa nalogom na menjačnici, IP adresom, uređajem, komunikacijom, dokumentom ili drugim dokazom, moguće je identifikovati lice koje je raspolagalo sredstvima. Međutim, taj proces je složen i zahteva kombinovanje više izvora podataka. Organi postupka ne mogu se osloniti samo na jedan blockchain zapis, već moraju dokazati vezu između digitalne adrese i konkretnog učinioca. To podrazumeva prikupljanje podataka od pružalaca usluga digitalne imovine, analizu uređaja, finansijsko veštačenje i, u mnogim slučajevima, međunarodnu pravnu pomoć (Casey et al., 2019).

Otežana identifikacija učinilaca posebno dolazi do izražaja kada se koriste novčanici nad kojima korisnik samostalno ima kontrolu. Kod platformi koje čuvaju podatke o korisnicima, organi mogu tražiti informacije o identitetu, istoriji transakcija i povezanim računima. Međutim, kada korisnik koristi novčanik bez posrednika, ne postoji centralni subjekt koji raspolaže identifikacionim podacima.

U takvim situacijama dokazivanje se više oslanja na tehničku analizu, podatke iz zaplenjenih uređaja, komunikaciju osumnjičenih i povezivanje više indicija. Zbog toga pseudonimnost ne isključuje mogućnost otkrivanja učinioca, ali postupak čini složenijim, sporijim i skupljim (FATF, 2024).

Sa krivičnog pravnog stanovišta, problem pseudonimnosti posebno je značajan zato što je za odgovornost potrebno utvrditi subjektivnu i objektivnu vezu između lica i radnje izvršenja. Nije dovoljno dokazati da je određena transakcija izvršena, već je potrebno dokazati ko ju je izvršio, sa kojom namerom, u kom kontekstu i u vezi sa kojim krivičnim delom. Kod kriptovaluta se može dogoditi da jedna osoba formalno poseduje nalog, druga kontroliše privatni ključ, treća daje instrukcije, a četvrta koristi sredstva. Takva podela uloga otežava utvrđivanje krivične odgovornosti i zahteva pažljivo razlikovanje izvršioca, pomagača, organizatora i drugih učesnika (Osterburg & Ward, 2019).

Poseban problem predstavlja činjenica da učinioci mogu koristiti više digitalnih adresa i više platformi. Često se ne koristi jedna adresa za sve transakcije, već se sredstva mogu raspoređivati kroz različite novčanike, menjati za druge oblike digitalne imovine ili prebacivati na platforme koje se nalaze u inostranstvu. Takvo ponašanje može imati za cilj prikrivanje toka sredstava, ali u dokaznom smislu mora se pažljivo analizirati, jer sama složenost transakcija ne dokazuje automatski krivičnu nameru. Ona može biti indicija, ali mora biti potkrepljena dodatnim dokazima koji pokazuju poreklo sredstava, znanje učinioca i njegovu nameru da imovinu prikrije ili upotrebi u protivpravne svrhe (Möser et al., 2013).

Pseudonimnost kriptovaluta utiče i na položaj oštećenih lica. Kod prevara, iznuda ili krađa digitalne imovine, žrtva često može videti da su sredstva prebačena na određenu adresu, ali ne zna ko stoji iza te adrese. To kod oštećenih stvara osećaj nemoći, jer za razliku od klasične bankarske transakcije često ne postoji institucija kojoj se može odmah obratiti radi blokade ili poništavanja transakcije. Zbog nepovratnosti blockchain transakcija, brzina reakcije i stručnost nadležnih organa imaju presudan značaj za mogućnost praćenja i eventualnog povraćaja sredstava (Europol, 2021).

U kontekstu Republike Srbije, pitanje identifikacije učinilaca povezano je sa razvojem pravnog okvira za digitalnu imovinu i obavezama pružalaca usluga. Zakon o digitalnoj imovini i propisi iz oblasti sprečavanja pranja novca nastoje da određene subjekte uključe u sistem nadzora, identifikacije korisnika i prijavljivanja sumnjivih aktivnosti. Ipak, domaći propisi imaju ograničen domet kada se transakcije odvijaju preko stranih platformi ili kada korisnici koriste decentralizovane oblike raspolaganja digitalnom imovinom (Republika Srbija, 2020).

3.2. Pranje novca, prikrivanje porekla imovine i layering

Pranje novca predstavlja jedan od najvažnijih krivičnopравnih rizika povezanih sa kriptovalutama. Suština pranja novca jeste da se imovini koja potiče iz krivičnog dela prikrije nezakonito poreklo i da se ona prikaže kao zakonita. Kod tradicionalnog pranja novca najčešće se govori o fazama polaganja, raslojavanja i integracije. U kontekstu kriptovaluta, ove faze mogu izgledati drugačije, ali cilj ostaje isti: udaljavanje imovine od krivičnog dela iz kog potiče i otežavanje dokazivanja veze između učinioca, krivičnog dela i ostvarene koristi (Vandezande, 2017).

Layering, odnosno raslojavanje, posebno je značajan kod kriptovaluta jer se digitalna imovina može brzo prebacivati kroz veći broj adresa i platformi. Učinioci mogu pokušati da stvore složen transakcioni lanac kako bi se otežalo praćenje porekla sredstava. Takve radnje ne moraju uvek biti tehnički sofisticirane, ali mogu biti dovoljno složene da produže istragu, otežaju identifikaciju korisnika i zahtevaju saradnju više subjekata. U praksi se zato analiza pranja novca putem kriptovaluta ne može svesti samo na praćenje jedne transakcije, već zahteva rekonstrukciju celokupnog toka digitalne imovine (FATF, 2024).

Kod pranja novca putem kriptovaluta poseban značaj imaju tačke dodira između digitalnog i tradicionalnog finansijskog sistema. To su najčešće kripto-menjačnice, platforme za trgovinu, pružaoci usluga čuvanja digitalne imovine i bankovni računi koji se koriste za kupovinu ili prodaju kriptovaluta. Ako su ovi subjekti regulisani i ako primenjuju mere identifikacije korisnika, praćenja transakcija i prijavljivanja sumnjivih aktivnosti, mogućnost zloupotrebe se smanjuje. Ako takve kontrole izostanu, rizik se povećava, jer digitalna imovina može biti upotrebljena za prikrivanje porekla sredstava i njihovo vraćanje u zakonite tokove (Houben & Snyers, 2018).

Prikrivanje porekla imovine kod kriptovaluta često je povezano sa namerom da se stvori distanca između krivičnog dela i kasnije upotrebe sredstava. Na primer, protivpravna korist može biti prvo pretvorena u kriptovalutu, zatim prebačena kroz više digitalnih adresa, pa zatim ponovo pretvorena u tradicionalni novac ili korišćena za kupovinu robe, usluga ili druge imovine. U krivičnom pravnom smislu, ključno pitanje jeste dokazivanje da lice zna ili mora znati da imovina potiče iz krivičnog dela, kao i da radnje koje preduzima imaju za cilj prikrivanje ili otežavanje utvrđivanja njenog porekla (Krivični zakonik Republike Srbije).

Kriptovalute mogu biti posebno privlačne za pranje novca zbog brzine transfera i mogućnosti prekograničnog kretanja imovine. Tradicionalni bankarski sistem ima razvijene mehanizme kontrole, dok kripto-ekosistem obuhvata veliki broj različitih platformi, od strogo regulisanih do onih koje posluju u slabije nadziranim jurisdikcijama. Upravo zato FATF insistira na primeni standarda za virtuelnu imovinu i pružaoce usluga virtuelne imovine, uključujući mere poznavanja i praćenja korisnika i razmene podataka relevantnih za transfere digitalne imovine (FATF, 2024).

Sa dokaznog stanovišta, pranje novca putem kriptovaluta zahteva povezivanje blockchain analize sa dokazima o predikatnom krivičnom delu. Nije dovoljno pokazati da je lice koristilo kriptovalute ili da je imalo više transakcija. Potrebno je dokazati da sredstva potiču iz kriminalne aktivnosti i da su radnje raspolaganja imale funkciju prikrivanja, konverzije ili integracije protivpravne koristi. Zbog toga je u praksi veoma važna saradnja između finansijskih istražitelja, digitalnih forenzičara, tužilaštva i organa koji prate sprečavanje pranja novca (Osterburg & Ward, 2019).

Layering u kripto-okruženju može biti komplikovan i zbog upotrebe različitih vrsta digitalne imovine. Sredstva se mogu prebacivati iz jedne kriptovalute u drugu, koristiti na različitim platformama ili kombinovati sa drugim oblicima digitalne imovine. U akademskom i stručnom kontekstu ove pojave se analiziraju kao indikatori rizika, ali se moraju opisivati pažljivo, bez pretvaranja analize u uputstvo za izbegavanje nadzora. Za potrebe ovog rada dovoljno je naglasiti da takve tehnike otežavaju rekonstrukciju toka imovine i zahtevaju specijalizovane istražne sposobnosti (Europol, 2024).

U Republici Srbiji pranje novca je uređeno kroz krivičnopravni okvir i kroz posebne propise o sprečavanju pranja novca i finansiranja terorizma. Uvođenje digitalne imovine u pravni sistem zahteva da se i pružaoци usluga povezanih sa digitalnom imovinom posmatraju kao važan deo preventivnog sistema. To znači da se od njih može očekivati identifikacija korisnika, praćenje poslovnog odnosa, upravljanje rizicima i prijavljivanje sumnjivih aktivnosti. Ipak, efikasnost ovih mera zavisi od praktične primene, nadzora i sposobnosti organa da prikupljene podatke koriste u krivičnom postupku (Republika Srbija, 2017/2019/2020/2023/2024/2025).

3.3. Darknet tržišta, ransomware, prevare i finansiranje drugih protivpravnih aktivnosti

Kriptovalute se u bezbednosnim analizama često povezuju sa darknet tržištima, jer omogućavaju digitalno plaćanje u okruženjima u kojima učesnici nastoje da sakriju identitet. Darknet tržišta funkcionišu kao zatvoreni ili teže dostupni internet prostori u kojima se mogu nuditi nezakonita roba i usluge. Za ovaj rad nije važno tehnički objašnjavati način pristupa takvim tržištima, već ukazati na njihov krivičnopravni značaj: kriptovalute su u pojedinim slučajevima omogućavale da se plaćanje izvrši bez klasičnih bankarskih tragova i bez neposrednog susreta učesnika. Upravo zbog toga darknet tržišta predstavljaju važan primer veze između pseudonimnosti, digitalnog plaćanja i organizovanih protivpravnih aktivnosti (Europol, 2024).

Ransomware napadi predstavljaju jedan od najpoznatijih primera zloupotrebe kriptovaluta u savremenom visokotehnološkom kriminalitetu. U takvim slučajevima učinioци digitalno ugrožavaju dostupnost podataka ili informacionih sistema, a zatim zahtevaju plaćanje u kriptovaluti. Kriptovalute se koriste zato što omogućavaju relativno brz transfer vrednosti i zato što učinioци očekuju da će pseudonimnost otežati njihovu identifikaciju. Ipak, isplate u kriptovalutama takođe ostavljaju transakcione tragove koji se mogu analizirati, što pokazuje da kriptovalute nisu savršeno sredstvo prikrivanja, već sredstvo koje zahteva odgovarajuću forenzičku i finansijsku analizu (Europol, 2024).

Prevare povezane sa kriptovalutama imaju različite oblike, od lažnih investicionih projekata do obmanjujućih platformi i zloupotrebe neznanja korisnika. Poseban problem predstavlja činjenica da mnogi građani ne razumeju dovoljno tehnološku i finansijsku prirodu kriptovaluta, pa mogu poverovati u nerealna obećanja o brzom zaradi, sigurnom profitu ili ekskluzivnim ulaganjima. U takvim slučajevima kriptovalute nisu samo sredstvo plaćanja, već i predmet obmane. Krivičnopravna analiza mora zato razlikovati situacije u kojima se kriptovaluta koristi za transfer protivpravne koristi od situacija u kojima se sam kripto-projekat koristi kao instrument prevare (Europol, 2021).

Kriptovalute se mogu javiti i u finansiranju drugih protivpravnih aktivnosti. Njihova prekogranična priroda, dostupnost i mogućnost korišćenja bez neposrednog kontakta sa bankarskim sistemom čine ih pogodnim za transfere koji mogu biti povezani sa različitim oblicima kriminaliteta. Ipak, treba izbegavati pojednostavljeno zaključivanje da svaka upotreba kriptovaluta ukazuje na nezakonitost.

Krivičnopravno relevantna je konkretna veza između digitalne imovine i protivpravne aktivnosti, a ne sama činjenica da je neko koristio kriptovalutu. Zbog toga je u svakoj istrazi potrebno utvrditi poreklo sredstava, svrhu transakcije, identitet učesnika i postojanje namere (FATF, 2024).

Darknet tržišta, ransomware i kripto-prevare pokazuju da se kriptovalute mogu koristiti u različitim fazama kriminalne aktivnosti. One mogu služiti kao sredstvo plaćanja za nezakonitu robu ili usluge, kao sredstvo iznude, kao način prikupljanja sredstava od oštećenih lica ili kao instrument prikrivanja koristi nakon izvršenog dela. Upravo zbog te različite funkcije kriptovaluta, krivičnopravna kvalifikacija može zavisiti od okolnosti slučaja. U jednom predmetu kriptovaluta može biti sredstvo izvršenja, u drugom predmet krivičnog dela, a u trećem imovina koja se oduzima kao protivpravna korist (Cvetković, 2018).

Sa bezbednosnog stanovišta, najveći problem predstavlja spajanje kriptovaluta sa drugim elementima digitalnog kriminaliteta. Kriptovalute se retko pojavljuju izolovano. One se često kombinuju sa lažnim identitetima, elektronskom komunikacijom, zlonamernim softverom, međunarodnim platformama, podacima na internetu i drugim digitalnim tragovima. Zbog toga odgovor države ne može biti samo normativan, već mora biti i institucionalan. Potrebni su obučeni istražitelji, tužioci i sudije, pristup odgovarajućim alatima, saradnja sa privatnim sektorom i međunarodna razmena informacija (UNODC, 2024).

3.4. Digitalna imovina kao predmet oduzimanja i dokazivanja

Digitalna imovina kao predmet oduzimanja predstavlja jedno od najosetljivijih pitanja u krivičnopravnom postupanju. Kod tradicionalne imovine, kao što su novac, vozila, nepokretnosti ili dragocenosti, organi postupka imaju razvijene modele pronalaženja, popisa, privremenog oduzimanja i čuvanja. Kod kriptovaluta situacija je drugačija, jer se imovina nalazi u digitalnom obliku i može se preneti veoma brzo ako lice zadrži kontrolu nad privatnim ključem. Zbog toga nije dovoljno utvrditi da digitalna imovina postoji, već je potrebno obezbediti faktičku kontrolu nad njom i sprečiti njeno dalje premeštanje (Casey et al., 2019).

Oduzimanje digitalne imovine zahteva razumevanje odnosa između blockchain zapisa, privatnih ključeva i pristupa novčaniku. Ako nadležni organi pronađu adresu na kojoj se nalaze sredstva, to ne znači da automatski mogu raspolagati tom imovinom.

Potreban je pristup privatnom ključu ili saradnja subjekta koji čuva sredstva. Kod custodial platformi moguće je zatražiti zamrzavanje ili prenos sredstava u skladu sa zakonom i međunarodnom saradnjom. Kod samostalnih novčanika, međutim, problem je veći jer lice može odbiti da otkrije pristupne podatke ili sredstva mogu biti prebačena pre nego što organi obezbede kontrolu (FATF, 2024).

Dokazivanje digitalne imovine u krivičnom postupku zahteva očuvanje integriteta digitalnih dokaza. Podaci o transakcijama, pristupnim ključevima, uređajima, elektronskoj komunikaciji i nalogima na platformama moraju biti pribavljeni zakonito i predstavljeni na način koji sud može razumeti. To znači da digitalna forenzika mora biti povezana sa pravilima krivičnog postupka. Ako se dokaz pribavi nezakonito, postoji rizik da ne bude upotrebljiv. Ako se pribavi zakonito, ali se ne objasni dovoljno jasno, postoji rizik da sud ne razume njegov značaj ili vezu sa konkretnim krivičnim delom (Osterburg & Ward, 2019).

Poseban problem jeste vrednovanje digitalne imovine. Kriptovalute mogu imati izrazito promenljivu tržišnu vrednost, pa se postavlja pitanje po kojoj vrednosti se procenjuju u trenutku izvršenja krivičnog dela, u trenutku oduzimanja ili u trenutku donošenja sudske odluke. Ta promenljivost može imati značaj za visinu protivpravne koristi, imovinskopравни zahtev oštećenog, visinu štete i srazmernost mera. Zato postupanje sa digitalnom imovinom zahteva ne samo tehničko znanje, već i finansijsko, računovodstveno i pravno razumevanje tržišta kriptovaluta (Houben & Snyers, 2018).

Digitalna imovina kao dokaz ima dvostruku prirodu. Sa jedne strane, ona može biti predmet krivičnog dela ili protivpravna korist. Sa druge strane, sama evidencija transakcija može biti dokaz o kretanju imovine, kontaktima između učesnika i pokušaju prikrivanja. Blockchain zapis može pokazati tok sredstava, ali ne može samostalno odgovoriti na sva pravna pitanja. Zato se mora kombinovati sa drugim dokazima, kao što su izveštaji menjačnica, podaci sa uređaja, izveštaji veštaka, komunikacija osumnjičenih i finansijska dokumentacija (Meiklejohn et al., 2013).

Uspesi u pojedinim međunarodnim predmetima pokazuju da digitalna imovina nije nedostižna za organe gonjenja. Američko Ministarstvo pravde je, na primer, u predmetima povezanim sa Silk Road i Bitfinex pokazalo da se i veoma složeni tokovi kriptovaluta mogu pratiti, dokazivati i povezivati sa konkretnim licima kada postoji kombinacija tehničke analize, finansijske istrage i međunarodne saradnje. Međutim, takvi predmeti istovremeno pokazuju da se radi o postupcima koji zahtevaju vreme, stručnost i institucionalne kapacitete (U.S. Department of Justice, 2022).

4. NORMATIVNI OKVIR ZA SUZBIJANJE ZLOUPOTREBE KRIPTOVALUTA

Normativni okvir za suzbijanje zloupotrebe kriptovaluta razvija se postepeno, jer pravo često kasni za tehnološkim inovacijama. U početnoj fazi razvoja kriptovaluta mnoge države nisu imale jasna pravila o njihovom statusu, oporezivanju, nadzoru i upotrebi. Vremenom, kako su kriptovalute postale tržišno značajne i kako su se sve češće pojavljivale u krivičnim istragama, države i međunarodne organizacije počele su da razvijaju posebne standarde. Ti standardi ne polaze od zabrane kriptovaluta, već od potrebe da se njihova upotreba uvede u pravni okvir, naročito u oblasti sprečavanja pranja novca, finansiranja terorizma, zaštite korisnika i krivičnogopravnog oduzimanja imovine (FATF, 2024).

Regulacija kriptovaluta mora da pomiri dva cilja. Prvi cilj je omogućavanje tehnoloških i finansijskih inovacija, jer digitalna imovina može doprineti razvoju tržišta, novih usluga i konkurencije. Drugi cilj je zaštita finansijskog sistema i društva od zloupotreba. Ukoliko je regulacija previše slaba, postoji rizik od pranja novca, prevara i izbegavanja nadzora. Ukoliko je previše restriktivna, može usporiti inovacije i prebaciti aktivnosti u neregulisane ili strane prostore. Zbog toga se savremeni normativni okvir zasniva na proceni rizika, identifikaciji korisnika, nadzoru pružalaca usluga i međunarodnoj saradnji (Houben & Snyers, 2018).

Za temu ovog rada posebno je važno razlikovati regulatorni i krivičnopravni odgovor. Regulatorni odgovor odnosi se na pravila koja uređuju tržište digitalne imovine, rad pružalaca usluga, obaveze identifikacije korisnika i sprečavanje sumnjivih transakcija. Krivičnopravni odgovor odnosi se na sankcionisanje konkretnih krivičnih dela, oduzimanje protivpravne koristi, dokazivanje i odgovornost učinilaca. Ova dva nivoa moraju biti povezana, jer dobar preventivni sistem može olakšati krivične istrage, dok efikasan krivičnopravni odgovor ima preventivni efekat na buduće zloupotrebe (Vandezande, 2017).

4.1. Međunarodni standardi i preporuke: FATF, UNODC, Europol

FATF ima centralnu ulogu u razvoju međunarodnih standarda za sprečavanje pranja novca i finansiranja terorizma u vezi sa virtuelnom imovinom. Preporuka 15 i prateća tumačenja proširili su AML/CFT standarde na virtuelnu imovinu i pružaoce usluga virtuelne imovine.

Suština ovog pristupa jeste da se subjekti koji omogućavaju kupovinu, prodaju, razmenu, prenos ili čuvanje virtuelne imovine uključe u sistem procene rizika, identifikacije korisnika, čuvanja podataka i prijavljivanja sumnjivih aktivnosti. FATF u izveštaju iz 2024. godine posebno ističe da primena standarda i dalje nije ujednačena u svim jurisdikcijama, što stvara prostor za regulatorne praznine i prekogranične zloupotrebe (FATF, 2024).

Jedan od važnih elemenata FATF pristupa jeste takozvano „travel rule” pravilo, odnosno zahtev da relevantne informacije o pošiljaocu i primaocu prate transfer virtuelne imovine kada učestvuju regulisani pružaoci usluga. Cilj ovog pravila jeste da se smanji anonimnost transfera u delovima kripto-ekosistema koji su povezani sa profesionalnim pružaocima usluga. Ipak, primena ovog pravila u praksi nije jednostavna, jer postoje tehnički, pravni i organizacioni izazovi, naročito kada se transakcije odvijaju preko više država ili kada jedna strana koristi neregulisani novčanik (FATF, 2024).

UNODC posmatra kriptovalute u širem kontekstu transnacionalnog organizovanog kriminala, sajber kriminala i spajanja tradicionalnih i digitalnih oblika kriminaliteta. Značaj UNODC pristupa ogleda se u tome što se problem kriptovaluta ne posmatra samo kao finansijsko-tehničko pitanje, već kao deo šire kriminalne infrastrukture. Kriptovalute mogu biti povezane sa online prevarama, iznudama, pranjem novca i drugim oblicima kriminaliteta koji prelaze državne granice. Zbog toga UNODC naglašava potrebu za međunarodnom saradnjom, jačanjem kapaciteta institucija i povezivanjem pravnog, tehničkog i operativnog odgovora (UNODC, 2024).

Europol ima značajnu ulogu u analizi trendova i podršci državama članicama u borbi protiv sajber kriminaliteta i organizovanog kriminala. U izveštaju IOCTA 2024. Europol ukazuje da se kriptovalute sve češće javljaju u predmetima investicionih prevara, pranja novca, ransomware napada i drugih oblika digitalnog kriminaliteta. Posebno se naglašava da kriminalci koriste sve složenije načine za prikrivanje tokova sredstava, dok organi gonjenja moraju razvijati kapacitete za praćenje i analizu takvih tokova (Europol, 2024).

Međunarodni standardi imaju poseban značaj zato što se kriptovalute koriste globalno. Ako jedna država ima stroga pravila, a druga nema efikasan nadzor, učinioci mogu pokušati da iskoriste slabiju jurisdikciju. Zbog toga je međunarodna usklađenost važna za sprečavanje takozvanog regulatornog arbitriranja, odnosno premeštanja aktivnosti u države sa slabijim pravilima. U oblasti digitalne imovine ovo pitanje je još izraženije nego kod tradicionalnih finansija, jer se transakcije mogu odvijati brzo, digitalno i bez fizičkog prisustva korisnika (FATF, 2024).

4.2. Regulatorika Evropske unije

Evropska unija je poslednjih godina razvila sveobuhvatniji pristup regulisanju kripto-imovine. Jedan od najvažnijih propisa jeste Uredba 2023/1114 o tržištima kripto-imovine, poznata kao MiCA. Cilj ove uredbe jeste stvaranje jedinstvenog pravnog okvira za izdavanje i trgovinu određenim oblicima kripto-imovine, kao i za pružaoce usluga povezanih sa kripto-imovinom. MiCA nastoji da obezbedi pravnu sigurnost, zaštitu korisnika i stabilnije tržište, ali i da smanji prostor za zloupotrebe u neregulisanom kripto-sektoru (European Union, 2023).

MiCA je značajna zato što uvodi obaveze za pružaoce usluga kripto-imovine, uključujući pravila o organizaciji poslovanja, transparentnosti, zaštiti korisnika i nadzoru. Time se kripto-tržište približava tradicionalnijim oblicima finansijske regulacije, ali uz uvažavanje posebnosti digitalne imovine. Za krivičnopravnu temu ovog rada MiCA je važna jer bolja regulacija tržišta može pomoći u smanjenju zloupotreba, očuvanju podataka i identifikaciji subjekata koji učestvuju u transakcijama (European Union, 2023).

Pored MiCA uredbe, izuzetno je važna i Uredba 2023/1113 o informacijama koje prate transfere sredstava i određene transfere kripto-imovine. Ova uredba predstavlja deo evropskog AML/CFT okvira i proširuje pravila o informacijama koje prate transfere i na određene transfere kripto-imovine. Njena suština je da se poveća sledljivost transakcija i smanji mogućnost da se kripto-imovina koristi za pranje novca ili finansiranje terorizma bez dovoljno podataka o učesnicima transfera (European Union, 2023).

Regulatorika Evropske unije važna je i za Srbiju, iako Srbija nije članica EU. Kao država kandidat i kao država čiji se finansijski i pravni sistem razvija u pravcu evropskih standarda, Srbija ima interes da prati evropska rešenja u oblasti digitalne imovine, sprečavanja pranja novca i visokotehnološkog kriminaliteta. Pored toga, transakcije digitalnom imovinom često uključuju platforme i korisnike iz EU, pa domaći organi u praksi mogu zavisiti od saradnje sa evropskim institucijama i subjektima (Babović, 2023).

Evropski pristup pokazuje da se problem kriptoimaluta ne rešava samo krivičnim sankcijama. Naprotiv, naglasak je na preventivnom i nadzornom okviru koji treba da smanji rizik pre nego što dođe do krivičnog dela. Kada su pružaoци usluga regulisani, kada se korisnici identifikuju i kada postoje podaci o transferima, organima gonjenja je lakše da kasnije rekonstruišu tok sredstava. Zbog toga je regulatorika EU značajna i kao preventivni i kao dokazni okvir (Vandezande, 2017).

4.3. Pravni okvir Republike Srbije

Republika Srbija je donošenjem Zakona o digitalnoj imovini napravila važan korak u pravnom prepoznavanju kriptovaluta i drugih oblika digitalne imovine. Ovaj zakon uređuje izdavanje digitalne imovine, sekundarno trgovanje, pružanje usluga povezanih sa digitalnom imovinom, založno i fiducijarno pravo na digitalnoj imovini, kao i nadležnosti Narodne banke Srbije i Komisije za hartije od vrednosti. Time je digitalna imovina dobila poseban pravni okvir, što je značajno za pravnu sigurnost, nadzor i mogućnost institucionalnog postupanja (Republika Srbija, 2020).

Prema objašnjenjima nadležnih institucija, domaći zakon prepoznaje dve osnovne forme digitalne imovine: virtuelne valute i digitalne tokene. Virtuelne valute nemaju status novca ili valute, ali ih fizička ili pravna lica mogu prihvatati kao sredstvo razmene. Digitalni tokeni predstavljaju nematerijalno imovinsko pravo koje u digitalnom obliku može predstavljati jedno ili više drugih imovinskih prava. Ova razlika je važna jer pokazuje da domaće pravo ne posmatra svu digitalnu imovinu jednako, već razlikuje njene oblike i funkcije (Komisija za hartije od vrednosti Republike Srbije, 2020).

Pravni okvir Republike Srbije relevantan je i kroz propise o sprečavanju pranja novca i finansiranja terorizma. Ovi propisi imaju poseban značaj zato što se zloupotreba kriptovaluta često javlja upravo u kontekstu prikrivanja porekla imovine i transfera protivpravne koristi. Uključivanje pružalaca usluga povezanih sa digitalnom imovinom u sistem obveznika može doprineti boljoj identifikaciji korisnika, praćenju sumnjivih aktivnosti i saradnji sa nadležnim organima. Ipak, efikasnost ovakvih rešenja zavisi od njihove praktične primene i od toga da li nadzorni i istražni organi imaju dovoljno stručnih kapaciteta (Republika Srbija, 2017/2019/2020/2023/2024/2025).

Krivični zakonik Republike Srbije značajan je zato što zloupotrebe kriptovaluta najčešće neće predstavljati potpuno nova krivična dela, već će se uklapati u postojeće krivičnopravne institute. Kriptovalute se mogu pojaviti u okviru pranja novca, prevare, iznude, neovlašćenog pristupa računarskim sistemima, poreskih krivičnih dela, finansiranja protivpravnih aktivnosti ili drugih dela, u zavisnosti od konkretnih okolnosti. To znači da kriptovaluta najčešće nije poseban osnov odgovornosti, već sredstvo izvršenja, predmet dela, protivpravna korist ili dokaz (Krivični zakonik Republike Srbije).

Domaći pravni okvir ima prednost u tome što je digitalna imovina zakonski prepoznata, ali postoje i izazovi. Jedan od izazova jeste transnacionalni karakter kripto-transakcija. Čak i kada domaće pravo ima jasna pravila, učinilac može koristiti stranu platformu ili novčanik koji nije neposredno dostupan domaćim organima. Drugi izazov jeste tehnička složenost dokazivanja. Treći izazov odnosi se na brzinu razvoja novih oblika digitalne imovine, zbog čega zakonodavstvo i praksa moraju stalno da se prilagođavaju (Babović, 2023).

4.4. Krivičnopravni odgovor i pitanja sankcionisanja

Krivičnopravni odgovor na zloupotrebu kriptovaluta zasniva se na primeni postojećih krivičnih dela na nove oblike izvršenja. To znači da se kriptovalute u krivičnom pravu najčešće ne posmatraju kao poseban kriminalni fenomen izolovan od drugih dela, već kao instrument ili predmet koji može biti uključen u različite kriminalne radnje. Na primer, ako se kriptovaluta koristi za prikrivanje porekla imovine, pravna analiza se može kretati u pravcu pranja novca. Ako se koristi za obmanu oštećenih lica, može biti relevantna prevara. Ako se traži kao uplata nakon digitalne iznude, može biti povezana sa visokotehnološkim kriminalitetom i iznudom (Krivični zakonik Republike Srbije).

Pitanje sankcionisanja posebno je važno zato što krivična sankcija ne sme biti samo formalna reakcija na izvršeno delo, već mora imati i preventivni efekat. Kod zloupotrebe kriptovaluta preventivni efekat sankcije zavisi od toga da li se učiniocu zaista oduzima protivpravna korist. Ako lice zadrži digitalnu imovinu ili uspe da prikrije njen tok, sama kazna može imati manji efekat. Zbog toga su finansijska istraga i oduzimanje imovine posebno važni delovi krivičnog odgovora (Osterburg & Ward, 2019).

Efikasan krivičnopravni odgovor zahteva i specijalizaciju nadležnih organa. Policija mora imati znanja iz digitalne forenzike i blockchain analize, tužilaštvo mora umeti da usmeri istragu i predloži odgovarajuće dokaze, a sud mora razumeti prirodu digitalne imovine i značaj tehničkih dokaza. Bez toga postoji rizik da se predmet formalno procesuirá, ali da dokazivanje bude slabo, nerazumljivo ili nedovoljno povezano sa elementima krivičnog dela. Zbog toga obuka nadležnih organa predstavlja jedan od najvažnijih uslova efikasnog sankcionisanja (UNODC, 2024).

Sankcionisanje zloupotreba kriptovaluta mora biti povezano i sa međunarodnom saradnjom. Kripto-transakcije se često odvijaju preko više država, a podaci potrebni za dokazivanje mogu se nalaziti kod stranih platformi. Ako međunarodna saradnja nije brza i efikasna, postoji rizik da sredstva budu premeštena ili da se izgube važni dokazi. Zbog toga se savremeni krivičnopravni odgovor ne može zasnivati samo na domaćim normama, već mora uključivati međunarodne mehanizme pravne pomoći, policijsku saradnju i saradnju sa privatnim sektorom (FATF, 2024).

Krivičnopravni odgovor ne treba posmatrati samo represivno, već i preventivno. Pored kažnjavanja učinilaca, važno je jačati nadzor nad pružaocima usluga digitalne imovine, edukovati građane o rizicima, razvijati kapacitete za rano prepoznavanje sumnjivih transakcija i unapređivati saradnju između regulatornih i pravosudnih organa. Samo kombinacija prevencije, regulacije, istrage, dokazivanja i sankcionisanja može dati potpun odgovor na zloupotrebe kriptovaluta (Europol, 2024).

5. ZLOUPOTREBA KRIPTOVALUTA U IZVRŠENJU I PRIKRIVANJU KRIVIČNIH DELA

Zloupotreba kriptovaluta u izvršenju i prikrivanju krivičnih dela predstavlja centralno pitanje ovog rada. Do sada je objašnjeno šta su kriptovalute, koje su njihove osnovne karakteristike, kakve rizike stvaraju i koji normativni okvir nastoji da te rizike kontroliše. U ovom poglavlju naglasak se premešta na konkretne načine na koje kriptovalute mogu biti uključene u kriminalnu aktivnost. One se mogu koristiti kao sredstvo plaćanja, kao način prenosa protivpravne koristi, kao sredstvo prikrivanja imovine, kao predmet krađe ili prevare, ali i kao dokaz koji ukazuje na tok kriminalne aktivnosti (Europol, 2021).

Važno je naglasiti da upotreba kriptovaluta ne menja nužno suštinu krivičnog dela, ali može promeniti način njegovog izvršenja i dokazivanja. Prevara ostaje prevara i kada se isplata traži u kriptovaluti. Pranje novca ostaje pranje novca i kada se protivpravna korist prebacuje kroz digitalne adrese. Iznuda ostaje iznuda i kada se traži digitalna imovina. Međutim, kriptovalute uvode nove tehničke i procesne okolnosti koje mogu otežati identifikaciju učinioca, praćenje koristi i dokazivanje namere (Cvetković, 2018).

Zloupotreba kriptovaluta naročito je problematična zato što može omogućiti udaljšavanje učinioca od žrtve i od mesta posledice. Kod klasičnih krivičnih dela često postoji fizički kontakt, lokalni finansijski trag ili poznata institucija preko koje je izvršeno plaćanje. Kod kriptovaluta učinilac može biti u jednoj državi, žrtva u drugoj, platforma u trećoj, a digitalna imovina može biti premeštena kroz više mreža. To stvara ozbiljne izazove za nadležnost, međunarodnu saradnju i brzinu postupanja (FATF, 2024).

5.1. Modaliteti izvršenja krivičnih dela uz upotrebu kriptovaluta

Kriptovalute se mogu koristiti u izvršenju krivičnih dela na više načina. Prvi modalitet jeste njihova upotreba kao sredstva plaćanja za nezakonu robu ili usluge. U takvim slučajevima kriptovaluta omogućava digitalnu razmenu vrednosti između učesnika koji nastoje da izbegnu tradicionalne finansijske tokove. Ovakav modalitet posebno je poznat iz predmeta povezanih sa darknet tržištima, gde je digitalno plaćanje imalo značajnu ulogu u funkcionisanju protivpravnih platformi (Europol, 2024).

Drugi modalitet jeste upotreba kriptovaluta kao sredstva iznude. Kod ransomware napada ili drugih oblika digitalne ucene, učinilac može zahtevati da žrtva uplati određenu vrednost u kriptovaluti. Razlog za takav zahtev jeste očekivanje da će se lakše prikriti identitet primaoca i otežati povraćaj sredstava. Međutim, transakcija i dalje ostavlja trag, što može biti značajno za istragu ako organi blagovremeno reaguju i ako imaju pristup odgovarajućim alatima i međunarodnoj saradnji (Europol, 2024).

Treći modalitet jeste upotreba kriptovaluta u investicionim i drugim finansijskim prevarama. U takvim slučajevima oštećeni se mogu navesti da uplate novac ili digitalnu imovinu u lažni projekat, lažnu platformu ili navodno sigurnu investiciju. Kriptovalute se koriste jer veliki broj građana nema dovoljno znanja o njihovom funkcionisanju, a istovremeno je privučen mogućnošću brze zarade. Takve prevare pokazuju da kriptovalute nisu samo sredstvo transfera, već i tema oko koje se može izgraditi obmanjujući narativ (Europol, 2021). Četvrti modalitet odnosi se na krađu digitalne imovine. Kriptovalute mogu biti predmet krivičnog dela kada učinilac neovlašćeno pribavi pristup privatnom ključu, nalogu na menjačnici ili digitalnom novčaniku. U takvim slučajevima ključni dokazni problemi odnose se na način pribavljanja pristupa, identifikaciju lica koje je prenelo sredstva i dokazivanje da je raspolaganje bilo neovlašćeno. Budući da se transakcije ne mogu jednostavno poništiti, pravovremeno otkrivanje i blokiranje daljeg kretanja sredstava ima veliki značaj (Casey et al., 2019).

Peti modalitet jeste upotreba kriptovaluta u prikrivanju već ostvarene protivpravne koristi. Nakon izvršenog krivičnog dela, učinilac može pokušati da imovinu pretvori u kriptovalutu, prebaci je kroz više adresa ili je kasnije ponovo konvertuje u tradicionalni novac. Ovaj modalitet je posebno značajan u kontekstu pranja novca, jer se kriptovalute koriste kao sredstvo udaljavanja imovine od njenog kriminalnog izvora (FATF, 2024).

5.2. Kriptovalute kao sredstvo plaćanja, prenosa i prikrivanja protivpravne koristi

Kriptovalute kao sredstvo plaćanja imaju poseban krivičnopravni značaj onda kada se koriste za plaćanje nezakonite robe, usluga ili aktivnosti. U takvim slučajevima one funkcionišu slično gotovini, ali sa važnim razlikama. Plaćanje se ne obavlja fizički, već digitalno; učesnici ne moraju biti na istom mestu; a trag nije u bankarskom sistemu, već na blockchainu i platformama koje su eventualno korišćene.

Ova kombinacija čini kriptovalute pogodnim sredstvom za digitalna protivpravna tržišta, ali i predmetom forenzičke analize (Meiklejohn et al., 2013).

Kao sredstvo prenosa, kriptovalute omogućavaju brzo premeštanje vrednosti između različitih adresa i država. To može biti zakonito, ali u kriminalnom kontekstu služi udaljavanju imovine od mesta izvršenja dela ili od lica koje je neposredno pribavilo korist. Prekogranični karakter posebno otežava postupanje, jer domaći organi možda nemaju direktan pristup podacima ili imovini. Zato se u istragama često mora koristiti međunarodna pravna pomoć i saradnja sa platformama koje posluju u drugim državama (FATF, 2024).

Kao sredstvo prikrivanja protivpravne koristi, kriptovalute se koriste kada učinilac želi da oteža dokazivanje porekla sredstava. Prikrivanje se može odnositi na poreklo imovine, identitet korisnika, stvarnog vlasnika digitalnog novčanika ili krajnju namenu sredstava. U krivičnopravnom smislu, posebno je važno dokazati da takvo prikrivanje nije slučajno ili tehnički neutralno, već da postoji svest o kriminalnom poreklu imovine i namera da se ta veza prikrije (Krivični zakonik Republike Srbije).

Kriptovalute su posebno značajne i zato što omogućavaju čuvanje vrednosti izvan klasičnog bankarskog sistema. Lice koje poseduje privatni ključ može imati faktičku kontrolu nad značajnom imovinom bez računa u banci i bez fizičkog predmeta koji se lako pronalazi. To otežava imovinske istrage, naročito ako organi ne znaju da digitalna imovina postoji ili ako ne uspeju da pronađu pristupne podatke. Zato istraživanje imovine u savremenim predmetima mora obuhvatiti i digitalne tragove, uređaje, naloge i moguće veze sa kripto-platformama (Casey et al., 2019).

5.3. Dokazni problemi u otkrivanju, gonjenju i presuđenju

Dokazni problemi kod kriptovaluta počinju već u fazi otkrivanja krivičnog dela. Žrtva može prijaviti da je prevarena ili da su joj sredstva prebačena na nepoznatu adresu, ali organi moraju utvrditi gde su sredstva otišla, ko kontroliše adresu i da li se sredstva mogu dalje pratiti. Ukoliko se reaguje kasno, digitalna imovina može biti premeštena kroz više adresa ili konvertovana u drugi oblik imovine. Zato je brzina postupanja važna, ali ona mora biti usklađena sa zakonitim pribavljanjem dokaza (Europol, 2021).

U fazi gonjenja, tužilaštvo mora povezati tehničke podatke sa pravnim elementima krivičnog dela. Blockchain analiza može pokazati tok sredstava, ali tužilac mora dokazati ko je preduzeo radnju, da li je imao nameru, da li je znao za kriminalno poreklo imovine i kakva je veza između digitalne transakcije i krivičnog dela. To znači da tehnički dokaz mora biti preveden u pravno relevantne činjenice. Bez tog povezivanja postoji rizik da postupak ostane na nivou složene tehničke analize koju sud ne može dovoljno jasno da primeni (Osterburg & Ward, 2019).

U fazi suđenja, poseban izazov predstavlja razumevanje digitalnih dokaza. Sud mora razumeti šta znači blockchain adresa, šta je privatni ključ, kako se potvrđuje transakcija, šta pokazuje izveštaj blockchain analize i koja su ograničenja takvog dokaza. Zbog toga je uloga veštaka veoma važna. Veštak ne treba samo da predstavi tehničke podatke, već da objasni njihovo značenje na način razumljiv sudu, tužilaštvu, odbrani i drugim učesnicima postupka (Casey et al., 2019).

Dokazni problemi se dodatno povećavaju kada se koriste strane platforme. Podaci o korisniku, nalogu, IP adresama, transferima ili konverzijama mogu se nalaziti kod subjekta koji posluje izvan Republike Srbije. U takvim slučajevima domaći organi moraju koristiti mehanizme međunarodne saradnje, što može trajati i zavisiti od pravnog režima druge države. Ako saradnja kasni, postoji rizik da se dokazi izgube ili da digitalna imovina bude premeštena (FATF, 2024). Još jedan problem jeste dokazivanje stvarne kontrole nad digitalnom imovinom. Lice može tvrditi da ne kontroliše adresu, da je izgubilo pristup, da je neko drugi koristio njegov uređaj ili da nije znalo za poreklo sredstava. Zbog toga se moraju prikupljati dodatni dokazi: komunikacija, pristupni podaci, ponašanje nakon transakcije, veze sa menjačnicama, podaci sa uređaja i svedočki iskazi. Sam blockchain trag je važan, ali najjači dokazni značaj ima kada se poveže sa drugim dokazima (Meiklejohn et al., 2013).

5.4. Uloga policije, tužilaštva, sudova i regulatornih organa

Policija ima ključnu ulogu u početnoj fazi otkrivanja i prikupljanja dokaza. Kod krivičnih dela povezanih sa kriptovalutama policija mora brzo identifikovati relevantne digitalne tragove, obezbediti uređaje, prikupiti podatke od oštećenih lica, analizirati transakcije i proceniti da li postoji mogućnost hitnog sprečavanja daljeg prenosa imovine. To zahteva specijalizovana znanja, jer postupanje sa digitalnim dokazima mora biti precizno i zakonito (Casey et al., 2019).

Tužilaštvo usmerava istragu i ima zadatak da tehničke nalaze poveže sa pravnim elementima krivičnog dela. Uloga tužioca posebno je važna kod određivanja pravca istrage, predlaganja dokaznih radnji, traženja međunarodne pravne pomoći i odlučivanja o imovinskim merama. Ako tužilaštvo nema dovoljno razumevanja digitalne imovine, postoji rizik da se ne preduzmu sve potrebne mere ili da se dokazi ne predstavljaju na pravno relevantan način (Osterburg & Ward, 2019).

Sudovi imaju ulogu da obezbede zakonitost postupka, ocene dokaze i donesu odluku o krivici, sankciji i oduzimanju imovine. Kod kriptovaluta sud mora razumeti i pravnu i tehničku prirodu dokaza. Posebno je važno da sud pravilno oceni veštačenja, blockchain analize i dokaze o kontroli nad digitalnom imovinom. Ukoliko sud ne razume dovoljno prirodu digitalnih tragova, može doći do pogrešne ocene dokaza ili do nedovoljnog obrazloženja odluke (Casey et al., 2019).

Regulatorni organi imaju preventivnu i nadzornu ulogu. Njihov zadatak nije samo reagovanje nakon izvršenog krivičnog dela, već uspostavljanje pravila koja smanjuju rizik od zloupotreba. To uključuje nadzor nad pružaocima usluga digitalne imovine, praćenje primene pravila o identifikaciji korisnika, kontrolu tržišnog ponašanja i saradnju sa drugim institucijama. U Republici Srbiji posebno su značajne nadležnosti Narodne banke Srbije i Komisije za hartije od vrednosti u okviru Zakona o digitalnoj imovini (Republika Srbija, 2020).

Efikasan odgovor na zloupotrebu kriptovaluta moguć je samo ako policija, tužilaštvo, sudovi i regulatorni organi deluju povezano. Ako regulator prikupi podatke, ali ih organi gonjenja ne koriste, efekat je ograničen. Ako policija otkrije transakcioni trag, ali tužilaštvo ne usmeri istragu pravilno, dokazivanje može biti slabo. Ako sud ne razume tehničke dokaze, presuđenje može biti otežano. Zbog toga je institucionalna koordinacija jednako važna kao i sam normativni okvir (UNODC, 2024).

6. STUDIJE SLUČAJA

Studije slučaja imaju poseban značaj u ovom radu jer omogućavaju da se teorijska i normativna analiza poveže sa konkretnim primerima iz prakse. Kriptovalute se često opisuju apstraktno, kroz pojmove kao što su pseudonimnost, blockchain, digitalna imovina, pranje novca i transakcioni tragovi. Međutim, stvarni predmeti pokazuju kako se ti pojmovi pojavljuju u konkretnim istragama, optuženjima, presudama, zaplenama i oduzimanju imovine. Zato se kroz studije slučaja može jasnije sagledati kako kriptovalute funkcionišu kao sredstvo plaćanja, prenosa, prikrivanja i dokazivanja (Casey et al., 2019).

Za potrebe ovog rada izabrana su dva slučaja: Silk Road i Ross Ulbricht, kao primer ranog i uticajnog darknet tržišta u kome je Bitcoin imao važnu ulogu, i Bitfinex hack, kao primer krađe velike količine kriptovalute i složenog pokušaja pranja digitalne imovine. Ova dva slučaja nisu izabrana zato što su jedini, već zato što jasno pokazuju dve različite dimenzije problema. Silk Road pokazuje upotrebu kriptovaluta kao sredstva plaćanja u nezakonitom digitalnom tržištu, dok Bitfinex pokazuje probleme praćenja, dokazivanja i oduzimanja digitalne imovine nakon velikog kripto-incidenta (U.S. Department of Justice, 2022).

6.1. Silk Road i Ross Ulbricht

Silk Road je jedno od najpoznatijih darknet tržišta i jedan od prvih velikih slučajeva u kojima je Bitcoin imao značajnu ulogu u izvršenju i prikrivanju protivpravnih aktivnosti. Platforma je funkcionisala kao online tržište na kome su korisnici mogli da kupuju i prodaju nezakonitu robu i usluge, dok je Bitcoin korišćen kao sredstvo plaćanja. Za ovaj rad nije presudan tehnički način funkcionisanja platforme, već činjenica da je slučaj pokazao kako se digitalna infrastruktura, pseudonimnost i kriptovalute mogu spojiti u model kriminalnog poslovanja (U.S. Department of Justice, 2015).

Ross Ulbricht je u američkom postupku označen kao osnivač i operator Silk Road platforme. Njegov slučaj je postao simbol ranog perioda kriminalne upotrebe kriptovaluta, jer je pokazao da Bitcoin može imati praktičnu ulogu u digitalnom kriminalnom tržištu. U postupku su značajni bili digitalni dokazi, podaci o poslovanju platforme, komunikacija, tragovi transakcija i zaplene bitkoina.

Slučaj je istovremeno pokazao da pseudonimnost i upotreba dark web tehnologija ne znače potpunu zaštitu od istrage i krivičnog gonjenja (U.S. Department of Justice, 2015).

Silk Road je značajan jer pokazuje kriptovalutu kao sredstvo plaćanja u nezakonitom ekosistemu. Bitcoin se koristio zato što je omogućavao digitalno plaćanje između korisnika koji nisu morali da se poznaju i koji su nastojali da izbegnu tradicionalne finansijske tragove. Međutim, Bitcoin transakcije nisu bile potpuno nevidljive. Upravo postojanje blockchain tragova i mogućnost njihove analize doprineli su razumevanju finansijskih tokova povezanih sa platformom. Time je ovaj slučaj pokazao dvostruku prirodu kriptovaluta: one mogu olakšati protivpravne aktivnosti, ali istovremeno mogu ostaviti tragove korisne za istragu (Meiklejohn et al., 2013).

U ovom slučaju važno je i pitanje oduzimanja digitalne imovine. Američki organi su u predmetima povezanim sa Silk Road zaplenili značajne količine bitcoina, što je pokazalo da digitalna imovina može biti predmet zaplene i oduzimanja ukoliko se obezbedi pristup i dokaže veza sa krivičnim delom. Jedna od kasnijih zaplena povezanih sa Silk Road slučajem odnosila se na bitcoine velike vrednosti, što dodatno pokazuje da digitalna imovina može ostati relevantna i godinama nakon izvršenja krivičnih dela (U.S. Department of Justice, 2022).

Ross Ulbricht je 2015. godine osuđen na kaznu doživotnog zatvora u vezi sa vođenjem Silk Road platforme, a slučaj je ostao jedan od najpoznatijih primera američkog krivičnog gonjenja povezanog sa darknet tržištima i Bitcoinom. Kasnije, u januaru 2025. godine, Ulbricht je pomilovan od strane predsednika SAD Donalda Trumpa, ali ta kasnija odluka ne menja značaj samog slučaja za pravnu i kriminalističku analizu zloupotrebe kriptovaluta. Za ovaj rad najvažnije je to što predmet Silk Road pokazuje kako se kriptovalute mogu koristiti u kriminalnom poslovnom modelu, ali i kako digitalni tragovi mogu postati ključni deo dokazivanja (Reuters, 2025).

Analitički značaj slučaja Silk Road ogleda se u nekoliko elemenata. Prvo, pokazuje da kriptovalute mogu biti funkcionalno sredstvo plaćanja na nezakonitim tržištima. Drugo, pokazuje da pseudonimnost ne sprečava nužno identifikaciju učinilaca. Treće, pokazuje da digitalna imovina može biti predmet zaplene i oduzimanja. Četvrto, pokazuje da uspešna istraga zahteva kombinaciju klasičnog kriminalističkog rada, digitalne forenzike, finansijske analize i međunarodne saradnje. Zbog toga je ovaj slučaj nezaobilazan u radu koji se bavi zloupotrebom kriptovaluta u izvršenju i prikrivanju krivičnih dela (Europol, 2021).

6.2. Bitfinex hack i pranje ukradenih bitcoina

Bitfinex hack predstavlja jednu od najznačajnijih studija slučaja kada je reč o krađi i pranju velike količine kriptovalute. Prema podacima američkog Ministarstva pravde, 2016. godine je iz kripto-menjačnice Bitfinex ukradeno približno 120.000 bitcoina. Ovaj slučaj je posebno važan zato što ne pokazuje samo krađu digitalne imovine, već i višegodišnji pokušaj njenog prikrivanja i pranja kroz složene transakcione obrasce (U.S. Department of Justice, 2024).

U predmetu Bitfinex, ključni problem nije bio samo utvrđivanje da je digitalna imovina ukradena, već praćenje njenog daljeg kretanja. Ukradeni bitcoini su tokom vremena prebacivani kroz različite tokove, uz pokušaje da se oteža povezivanje sredstava sa izvornom krađom. Američko Ministarstvo pravde navodi da je plan pranja uključivao opsežno raslojavanje transakcija, korišćenje različitih platformi i pokušaje prikrivanja porekla sredstava. Za ovaj rad je važno naglasiti da se ovakvi podaci iznose u analitičkom smislu, kao prikaz izazova za organe gonjenja, a ne kao opis radnji koje bi se mogle praktično oponašati (U.S. Department of Justice, 2024).

Slučaj Bitfinex pokazuje da blockchain može biti i prepreka i pomoć u istrazi. Sa jedne strane, veliki broj transakcija i pokušaja prikrivanja otežava praćenje sredstava. Sa druge strane, činjenica da javni blockchain čuva transakcione zapise omogućava istražiteljima da godinama kasnije analiziraju tokove digitalne imovine. Upravo ova osobina kriptovaluta razlikuje ih od gotovinskog kriminaliteta: tragovi mogu biti prikriveni, raslojeni i komplikovani, ali često ne nestaju potpuno (Meiklejohn et al., 2013).

U ovom predmetu značajno je i to što su američki organi uspeli da povežu određena lica sa pranjem ukradene kriptovalute. Ilya Lichtenstein je 2024. godine osuđen na pet godina zatvora zbog uloge u zaveri pranja novca povezanoj sa Bitfinex krađom, dok je slučaj privukao pažnju javnosti zbog velike vrednosti ukradene i zaplenjene digitalne imovine. Ovaj predmet pokazuje da dokazivanje može trajati godinama, ali da kombinacija blockchain analize, digitalnih dokaza i finansijske istrage može dovesti do procesuiranja (U.S. Department of Justice, 2024).

Bitfinex slučaj je posebno pogodan za analizu pojma layering. Ukradena digitalna imovina nije jednostavno zadržana na jednoj adresi, već je pokušavano njeno prikrivanje kroz složene tokove. To pokazuje zašto je u kripto-istragama neophodno posmatrati širu sliku, a ne samo pojedinačnu transakciju.

Istražitelji moraju analizirati kretanje sredstava kroz vreme, povezivati adrese, utvrđivati tačke ulaska i izlaska iz kripto-ekosistema i tražiti veze sa konkretnim licima. Ovakav rad zahteva stručnost i institucionalnu istrajnost (Casey et al., 2019).

Za pravnu analizu posebno je važno pitanje oduzimanja imovine. Bitfinex predmet pokazuje da digitalna imovina velike vrednosti može biti predmet zaplene, ali samo ako organi uspeju da utvrde gde se nalazi i ko nad njom ima kontrolu. To je važno i za zaštitu oštećenih, jer krivični postupak ne treba da se završi samo sankcionisanjem učinioca, već i rešavanjem pitanja protivpravne koristi i eventualnog povraćaja sredstava. U predmetima digitalne imovine, upravo imovinski aspekt često ima centralni značaj (U.S. Department of Justice, 2024).

Analitički posmatrano, Bitfinex slučaj potvrđuje više hipoteza ovog rada. Prvo, kriptovalute mogu biti predmet krivičnog dela i protivpravne koristi. Drugo, njihovo prikrivanje može trajati dugo i uključivati složene digitalne tragove. Treće, blockchain analiza može biti ključna za dokazivanje, ali mora biti povezana sa drugim dokazima. Četvrto, međunarodna saradnja i tehnička stručnost predstavljaju uslov za efikasno procesuiranje. Zbog toga Bitfinex predstavlja dobar primer savremenog problema u kome se ukrštaju visokotehnološki kriminalitet, pranje novca, digitalna forenzika i krivičnopravno oduzimanje imovine (Europol, 2024).

7. EMPIRIJSKO ISTRAŽIVANJE

Empirijsko istraživanje predstavlja važan deo rada jer omogućava da se teorijska i normativna analiza dopuni stavovima ispitanika o zloupotrebi kriptovaluta u izvršenju i prikrivanju krivičnih dela. Tema kriptovaluta nije značajna samo za pravnike, ekonomiste, policijske službenike i stručnjake za bezbednost, već i za širu javnost, jer sve veći broj građana dolazi u dodir sa digitalnom imovinom, bilo kroz ulaganje, informisanje, online plaćanja ili medijske sadržaje o kripto-tržištu. Zbog toga je bilo korisno ispitati kako ispitanici razumeju osnovne rizike, da li kriptovalute povezuju sa pranjem novca, prevarama i ransomware napadima, kao i da li smatraju da su postojeći propisi i institucionalni kapaciteti dovoljni.

Istraživanje je koncipirano kao online anketa na uzorku od 100 ispitanika. Takav oblik istraživanja izabran je zato što omogućava brzo prikupljanje odgovora, lakšu distribuciju upitnika i uključivanje ispitanika različitog pola, starosti i obrazovnog nivoa. Iako ovakav uzorak ne omogućava potpuno generalizovanje rezultata na celokupnu populaciju, on je pogodan za akademski rad jer daje pregled dominantnih stavova i ukazuje na pravce u kojima se mogu razvijati buduća istraživanja.

U ovom poglavlju najpre se određuju predmet i cilj istraživanja, zatim se objašnjava uzorak i način organizacije online ankete, opisuje se instrument istraživanja i način prikupljanja podataka, a potom se prikazuju i analiziraju rezultati za svako pitanje iz upitnika. Na kraju se ukazuje na očekivani doprinos istraživanja za razumevanje krivičnopravnih i bezbednosnih rizika povezanih sa kriptovalutama.

7.1. Predmet i cilj istraživanja

Predmet empirijskog istraživanja jesu stavovi ispitanika o zloupotrebi kriptovaluta u izvršenju i prikrivanju krivičnih dela. Istraživanje je usmereno na nekoliko povezanih pitanja: koliko ispitanici poznaju pojam kriptovaluta, da li su ih ranije koristili, koje rizike najčešće povezuju sa njihovom upotrebom, kako ocenjuju postojeće propise i da li podržavaju strožu kontrolu kripto-platформи i specijalizovanu obuku nadležnih organa. Na taj način empirijski deo rada dopunjuje prethodna poglavlja u kojima su kriptovalute obrađene sa pojmovnog, krivičnopravnog, bezbednosnog i normativnog aspekta.

Osnovni cilj istraživanja jeste da se utvrdi kako ispitanici percipiraju kriptovalute kao mogući instrument kriminalnih aktivnosti. Posebna pažnja posvećena je stavovima o prikriivanju identiteta učinioca, pranju novca, ransomware napadima, dokazivanju krivičnih dela, međunarodnoj saradnji i oduzimanju digitalne imovine. Ovi elementi su izabrani zato što predstavljaju ključne izazove u praksi organa koji se bave otkrivanjem, gonjenjem i presuđenjem krivičnih dela povezanih sa digitalnom imovinom.

Poseban cilj istraživanja jeste da se utvrdi da li ispitanici prepoznaju potrebu za unapređenjem institucionalnog odgovora. To se odnosi na strožu kontrolu pružalaca usluga digitalne imovine, obaveznu identifikaciju korisnika na kripto-plattformama, specijalizovanu obuku policije, tužilaštva i sudova, kao i efikasnije oduzimanje digitalne imovine. Time se empirijsko istraživanje povezuje sa praktičnim preporukama koje mogu biti značajne za završni deo rada.

7.2. Uzorak i organizacija online ankete (100 ispitanika)

Istraživanje je sprovedeno na uzorku od 100 ispitanika. Uzorak je prigodnog karaktera, što znači da su u istraživanju učestvovala lica koja su bila dostupna istraživaču i spremna da popune online upitnik. Ovakav uzorak je čest u studentskim i akademskim istraživanjima manjeg obima, naročito kada je cilj da se dobiju indikativni podaci o stavovima, a ne da se izvrši reprezentativno ispitivanje celokupne populacije.

Online anketa je organizovana tako da ispitanici mogu samostalno popuniti upitnik, bez prisustva istraživača. Takav način prikupljanja podataka ima nekoliko prednosti. Pre svega, ispitanici mogu odgovoriti u trenutku koji im odgovara, što povećava verovatnoću učešća. Pored toga, online format omogućava anonimnost, što je posebno važno kod tema koje se odnose na kriminalitet, digitalnu imovinu i stavove o efikasnosti državnih organa. Anonimnost smanjuje mogućnost da ispitanici daju društveno poželjne odgovore i podstiče iskrenije izjašnjavanje.

U uzorku su obuhvaćeni ispitanici različitog pola, starosti i stepena obrazovanja. Time se dobija širi uvid u percepciju kriptovaluta među licima koja imaju različito životno iskustvo, nivo obrazovanja i potencijalno različit stepen digitalne pismenosti. Ipak, treba naglasiti da rezultati ne predstavljaju stav celokupne populacije, već stavove konkretnog uzorka od 100 ispitanika. Zbog toga se zaključci iz ankete tumače kao indikativni i dopunski u odnosu na teorijsku i pravnu analizu.

7.3. Instrument istraživanja i način prikupljanja podataka

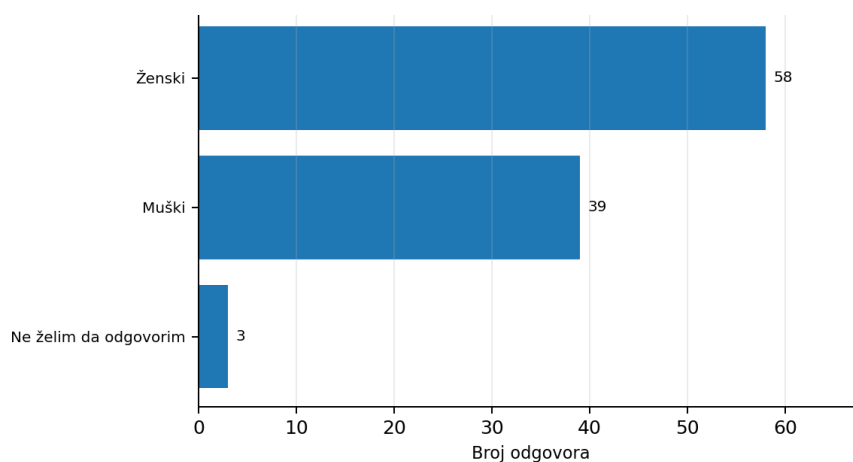
Instrument istraživanja bio je strukturisani anketni upitnik koji se sastojao od 18 pitanja. Prva pitanja odnosila su se na osnovne sociodemografske karakteristike ispitanika, kao što su pol, starosna grupa i stepen obrazovanja. Nakon toga ispitivano je prethodno iskustvo sa kriptovalutama i samoprocena poznavanja pojma kriptovaluta. Ovaj deo upitnika bio je važan jer omogućava da se rezultati kasnije tumače u odnosu na nivo informisanosti i iskustva ispitanika. Drugi deo upitnika odnosio se na percepciju rizika. Ispitanici su ocenjivali da li kriptovalute olakšavaju prikrivanje identiteta učinioca, pranje novca, ransomware napade, dokazivanje krivičnih dela i druge oblike zloupotrebe. U ovom delu korišćena je Likertova skala od 1 do 5, pri čemu niža ocena označava neslaganje, srednja ocena delimičan ili neodlučan stav, a viša ocena veći stepen slaganja sa tvrdnjom. Likertova skala je pogodna jer omogućava kvantitativno prikazivanje stavova i lakše poređenje odgovora. Treći deo upitnika odnosio se na normativne i institucionalne aspekte. Ispitanici su se izjašnjavali o dovoljnosti domaćih propisa, potrebi za strožom kontrolom pružalaca usluga digitalne imovine, značaju međunarodne saradnje, obaveznoj identifikaciji korisnika na kripto-plattformama, specijalizovanoj obuci nadležnih organa i unapređenju oduzimanja digitalne imovine. Poslednje pitanje bilo je otvorenog tipa i omogućilo je ispitanicima da sami navedu šta smatraju najvećim problemom u suzbijanju zloupotreba kriptovaluta.

Podaci su prikupljeni elektronskim putem, a odgovori su nakon toga razvrstani i obrađeni deskriptivnom analizom. Za pitanja zatvorenog tipa prikazan je broj odgovora po ponuđenim kategorijama, dok su kod otvorenog pitanja odgovori grupisani u tematske kategorije prema značenju. Rezultati su predstavljeni grafički, a ispod svakog grafikona dato je kratko tumačenje koje objašnjava dominantne stavove i njihov značaj za predmet rada.

7.4. Obrada i analiza rezultata

Obrada rezultata izvršena je metodom deskriptivne statistike. Za svako pitanje prikazan je broj ispitanika koji su izabrali određeni odgovor, a rezultati su predstavljeni grafikonima radi preglednijeg tumačenja. Budući da je uzorak obuhvatio 100 ispitanika, broj odgovora ujedno se može posmatrati i kao procenat uzorka. Kod pitanja višestrukog izbora ukupan broj označenih odgovora veći je od broja ispitanika, jer je svaki ispitanik mogao označiti više od jednog odgovora.

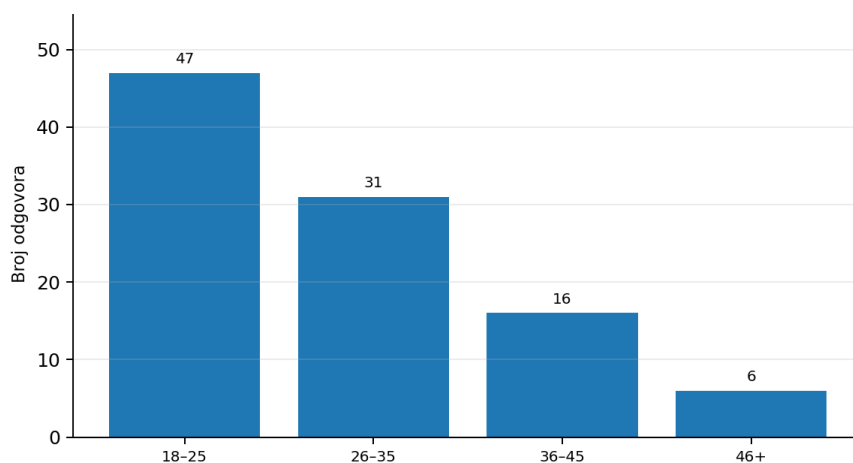
1. Pol ispitanika



Grafikon 1. Pol ispitanika

Rezultati su pokazali da su u anketi učestvovala 58 osobe ženskog pola, 39 osoba muškog pola, dok su 3 ispitanika izabrala odgovor da ne žele da se izjasne. Ovakva struktura pokazuje da je u uzorku nešto veće učešće ispitanica, ali da su oba pola dovoljno zastupljena da se mogu sagledati osnovni stavovi različitih grupa. Manji broj ispitanika koji nije želeo da odgovori ukazuje da pitanje pola nije predstavljalo prepreku za popunjavanje ankete.

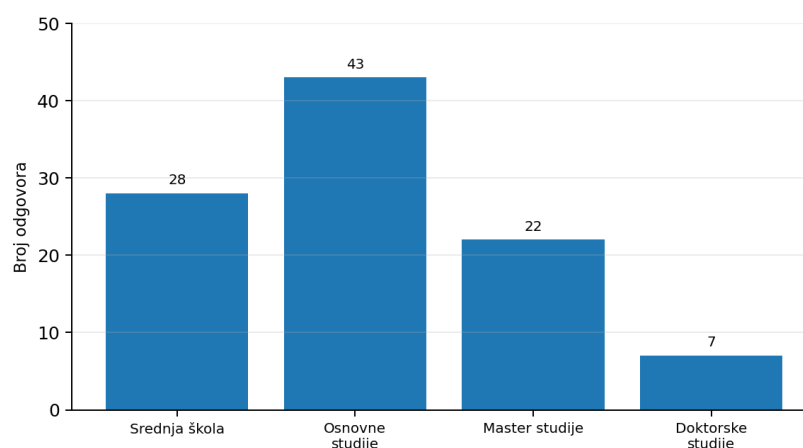
2. Starosna grupa



Grafikon 2. Starosna struktura ispitanika

Najveći deo uzorka čine ispitanici starosti od 18 do 25 godina, kojih je bilo 47, dok je 31 ispitanik pripadao grupi od 26 do 35 godina. U starosnoj grupi od 36 do 45 godina bilo je 16 ispitanika, a najmanje je bilo ispitanika starijih od 46 godina, ukupno 6. Ovakva struktura pokazuje da su u istraživanju najviše učestvovali mlađi ispitanici, što je očekivano kod online ankete o digitalnoj imovini, jer mlađa populacija češće prati tehnološke i finansijske novine.

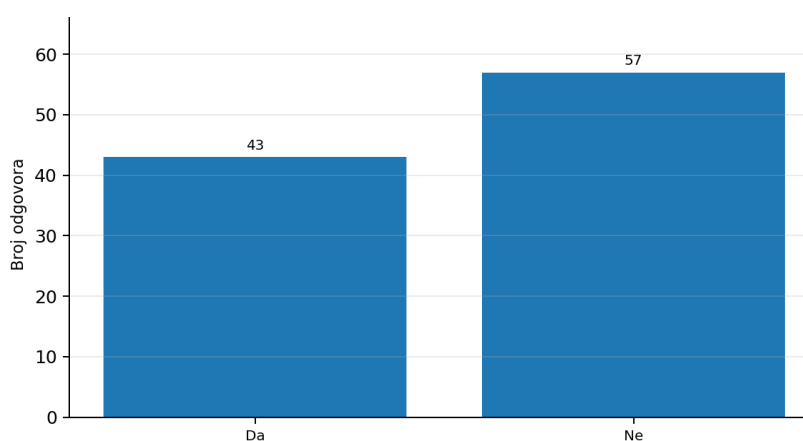
3. Stepen obrazovanja



Grafikon 3. Stepen obrazovanja ispitanika

Prema stepenu obrazovanja, najveći broj ispitanika ima završene osnovne studije, ukupno 43. Srednju školu kao najviši stepen obrazovanja navelo je 28 ispitanika, master studije 22 ispitanika, dok je 7 ispitanika navelo doktorske studije. Ovakva obrazovna struktura je pogodna za temu istraživanja, jer obuhvata ispitanike različitog obrazovnog profila, ali sa izraženim učešćem visokoobrazovanih lica koja mogu imati razvijenije stavove o pravnim, ekonomskim i bezbednosnim pitanjima.

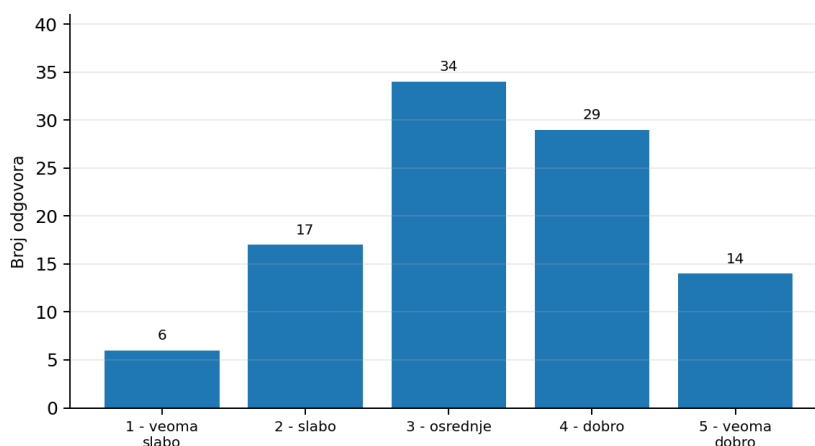
4. Da li ste ranije koristili kriptovalute?



Grafikon 4. Prethodno korišćenje kriptovaluta

Na pitanje da li su ranije koristili kriptovalute, 43 ispitanika odgovorila su potvrdno, dok je 57 ispitanika navelo da ih nije koristilo. Rezultati pokazuju da većina ispitanika nema lično iskustvo u korišćenju kriptovaluta, ali da je značajan deo uzorka ipak imao dodira sa ovom vrstom digitalne imovine. Ovaj nalaz je važan jer pokazuje da stavovi ispitanika ne potiču isključivo iz neposrednog iskustva, već i iz informisanja putem medija, obrazovanja, okruženja i opšteg razumevanja digitalnih finansija.

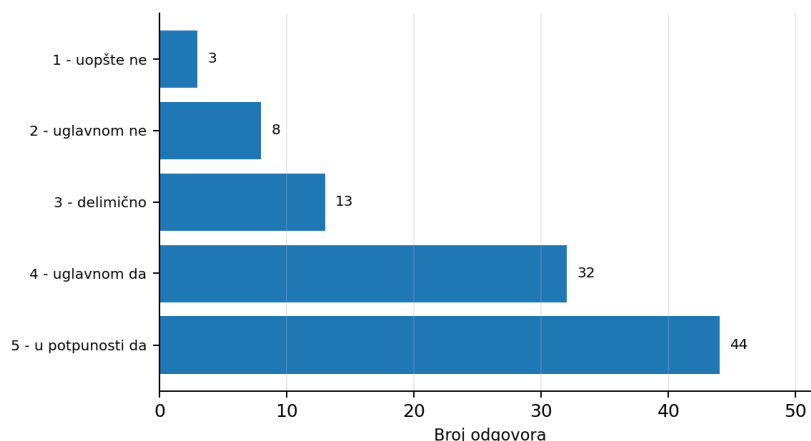
5. Koliko dobro poznajete pojam kriptovaluta?



Grafikon 5. Samoprocena poznavanja pojma kriptovaluta

Rezultati pokazuju da najveći broj ispitanika, njih 34, svoje poznavanje kriptovaluta ocenjuje srednjom ocenom. Dobro poznavanje navelo je 29 ispitanika, dok je veoma dobro poznavanje navelo 14 ispitanika. Slabo poznavanje navelo je 17 ispitanika, a veoma slabo 6 ispitanika. Ovakva raspodela ukazuje da većina ispitanika ima bar osnovno ili srednje razumevanje kriptovaluta, ali da postoji prostor za dodatnu edukaciju, naročito kada se kriptovalute posmatraju iz ugla pravnih rizika i mogućih zloupotreba.

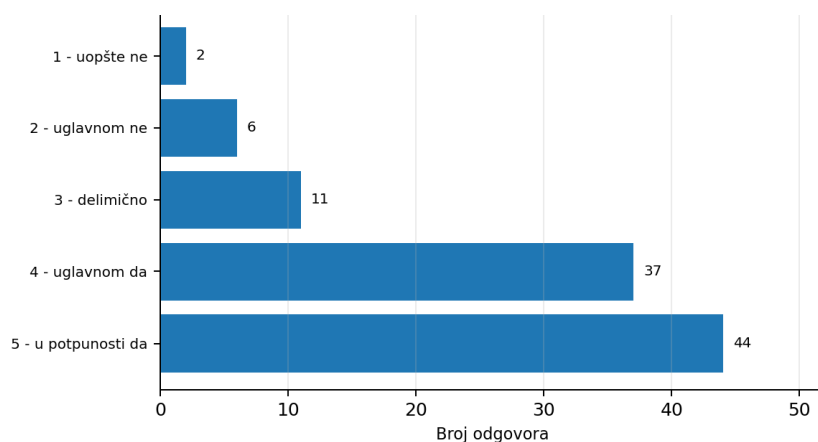
6. Da li smatrate da kriptovalute olakšavaju prikrivanje identiteta učinioca?



Grafikon 6. Stav o prikrivanju identiteta učinioca

Većina ispitanika smatra da kriptovalute olakšavaju prikrivanje identiteta učinioca. Od ukupnog broja, 44 ispitanika u potpunosti se složilo sa ovom tvrdnjom, a 32 ispitanika uglavnom se složilo. Delimično slaganje iskazalo je 13 ispitanika, dok je manji broj, odnosno 8 i 3 ispitanika, smatrao da kriptovalute uglavnom ili uopšte ne olakšavaju prikrivanje identiteta. Ovakvi rezultati ukazuju da se u percepciji ispitanika pseudonimnost i otežana identifikacija korisnika vide kao jedan od glavnih rizika kriptovaluta.

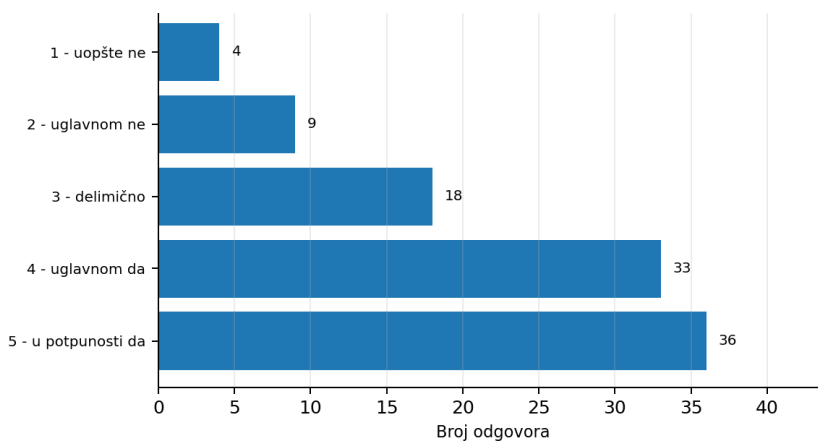
7. Da li kriptovalute olakšavaju pranje novca?



Grafikon 7. Stav o kriptovalutama i pranju novca

Na pitanje da li kriptovalute olakšavaju pranje novca, 44 ispitanika u potpunosti se složilo, dok je 37 ispitanika navelo da se uglavnom slaže. Delimično slaganje iskazalo je 11 ispitanika, a samo 6 ispitanika uglavnom se nije složilo, dok su 2 ispitanika odgovorila da se uopšte ne slažu. Rezultat pokazuje veoma izraženu percepciju rizika od pranja novca, što je povezano sa uverenjem da se digitalna imovina može koristiti za prikrivanje porekla sredstava, brzo prebacivanje vrednosti i otežavanje kontrole finansijskih tokova.

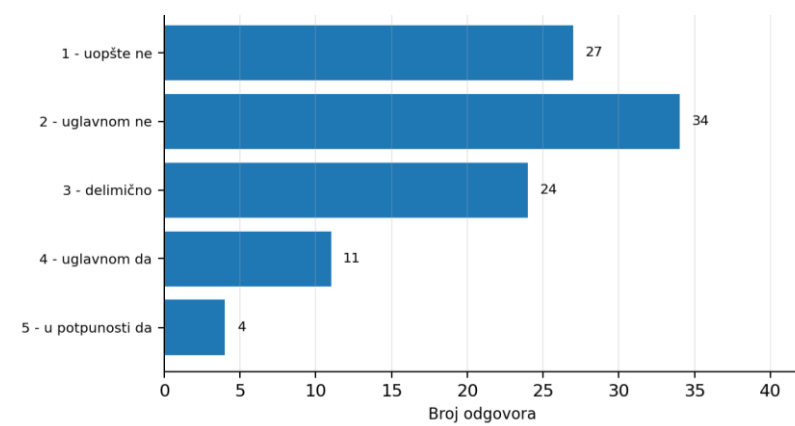
8. Da li se kriptovalute često povezuju sa ransomware napadima?



Grafikon 8. Povezanost kriptovaluta sa ransomware napadima

Rezultati pokazuju da 36 ispitanika u potpunosti smatra da se kriptovalute često povezuju sa ransomware napadima, dok je 33 ispitanika uglavnom saglasno sa tom tvrdnjom. Delimično slaganje iskazalo je 18 ispitanika, dok je 9 ispitanika uglavnom negiralo ovu povezanost, a 4 ispitanika je uopšte nije prepoznalo. Ovakva raspodela pokazuje da većina ispitanika prepoznaje ulogu kriptovaluta u savremenim oblicima digitalne iznude, posebno zbog načina na koji se zahtevi za plaćanje često formulišu u virtuelnoj imovini.

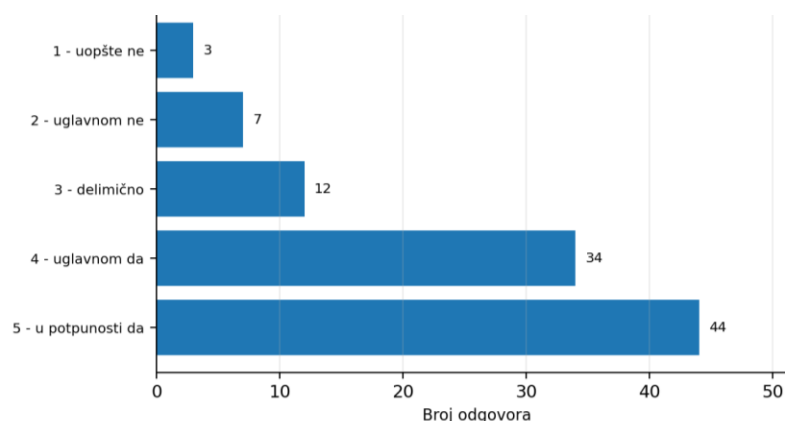
9. Da li su domaći propisi dovoljni za suzbijanje zloupotreba?



Grafikon 9. Stav o dovoljnosti domaćih propisa

Kada je reč o dovoljnosti domaćih propisa za suzbijanje zloupotreba, najveći broj ispitanika nije iskazao poverenje u postojeći normativni okvir. Ukupno 34 ispitanika smatra da domaći propisi uglavnom nisu dovoljni, dok 27 ispitanika smatra da uopšte nisu dovoljni. Delimičnu dovoljnost propisa prepoznala su 24 ispitanika, dok je 11 ispitanika navelo da su propisi uglavnom dovoljni, a 4 ispitanika da su u potpunosti dovoljni. Rezultati ukazuju na izraženu potrebu za unapređenjem propisa, ali i za boljom praktičnom primenom postojećih normi.

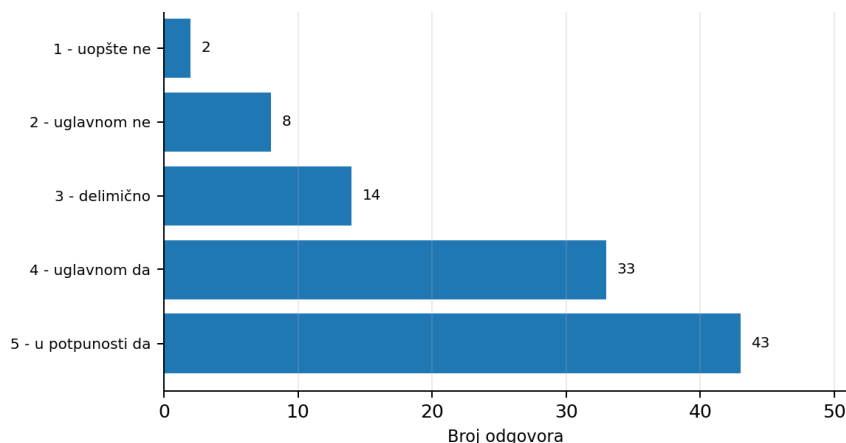
10. Da li je potrebna stroža kontrola pružalaca usluga digitalne imovine?



Grafikon 10. Potreba za strožom kontrolom pružalaca usluga digitalne imovine

Većina ispitanika podržava strožu kontrolu pružalaca usluga digitalne imovine. Najviše ispitanika, njih 44, u potpunosti smatra da je takva kontrola potrebna, dok 34 ispitanika uglavnom podržava ovu meru. Delimično slaganje iskazalo je 12 ispitanika, dok je 7 ispitanika uglavnom protiv, a 3 ispitanika uopšte ne vidi potrebu za strožom kontrolom. Ovi rezultati ukazuju na to da ispitanici pružaoce usluga, kao što su menjačnice i platforme, vide kao ključne tačke nadzora u sprečavanju zloupotreba digitalne imovine.

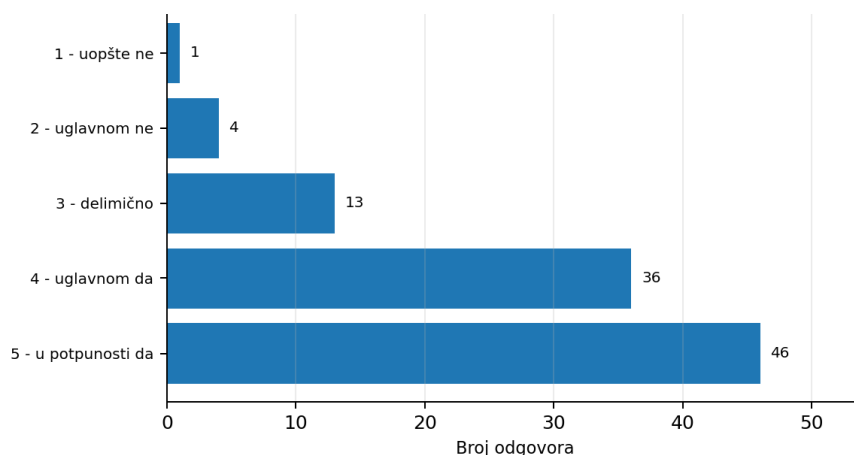
11. Da li anonimni novčanici i mikseri otežavaju dokazivanje krivičnih dela?



Grafikon 11. Uticaj anonimnih novčanika i miksera na dokazivanje

Prema rezultatima, 43 ispitanika u potpunosti smatraju da anonimni novčanici i mikseri otežavaju dokazivanje krivičnih dela, dok 33 ispitanika uglavnom deli taj stav. Delimično slaganje iskazalo je 14 ispitanika, dok je 8 ispitanika uglavnom negiralo, a 2 ispitanika potpuno negiralo ovu tvrdnju. Ovakav rezultat pokazuje da ispitanici prepoznaju tehničke mehanizme prikrivanja digitalnih tragova kao ozbiljan dokazni problem, posebno u predmetima koji se odnose na pranje novca i prikrivanje protivpravne koristi.

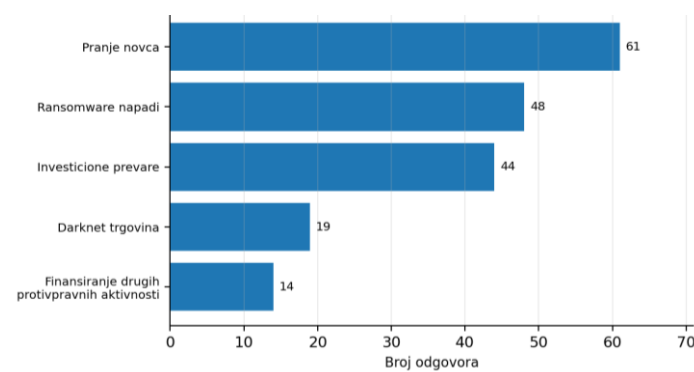
12. Da li međunarodna saradnja ima presudan značaj u ovom području?



Grafikon 12. Značaj međunarodne saradnje

Međunarodnu saradnju kao presudno važnu u potpunosti prepoznaje 46 ispitanika, dok 36 ispitanika smatra da ona uglavnom ima presudan značaj. Delimično slaganje iskazalo je 13 ispitanika, dok je samo 4 ispitanika uglavnom negiralo, a 1 ispitanik potpuno negirao značaj međunarodne saradnje. Ovakvi rezultati su očekivani imajući u vidu transnacionalni karakter kripto-transakcija, činjenicu da se platforme često nalaze u drugim državama i da je za prikupljanje dokaza neretko potrebna saradnja više jurisdikcija.

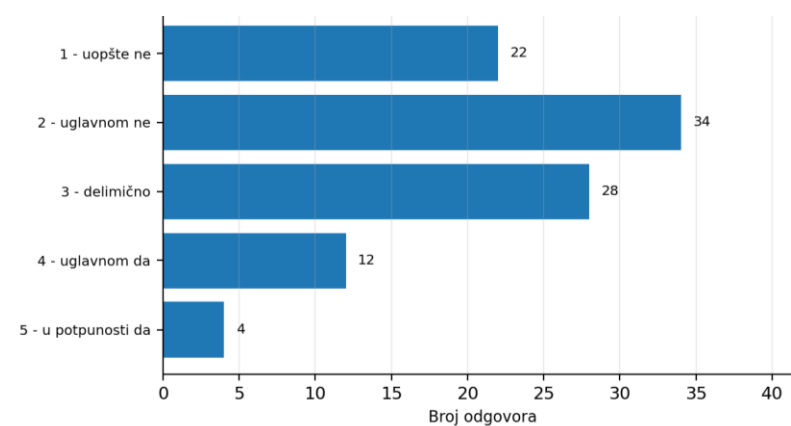
13. Koji oblik zloupotrebe smatrate najopasnijim?



Grafikon 13. Najopasniji oblici zloupotrebe kriptovaluta

Kod pitanja o najopasnijim oblicima zloupotrebe ispitanici su mogli označiti više odgovora, pa je ukupno evidentirano 186 izbora. Najčešće je označeno pranje novca, sa 61 izborom, zatim ransomware napadi sa 48 izbora i investicione prevare sa 44 izbora. Darknet trgovinu označilo je 19 ispitanika, dok je finansiranje drugih protivpravnih aktivnosti izabrano 14 puta. Rezultati pokazuju da ispitanici najveći rizik vide u finansijskom prikrivanju i digitalnoj iznudi, dok darknet tržišta i finansiranje drugih aktivnosti prepoznaju kao važne, ali nešto manje dominantne oblike zloupotrebe.

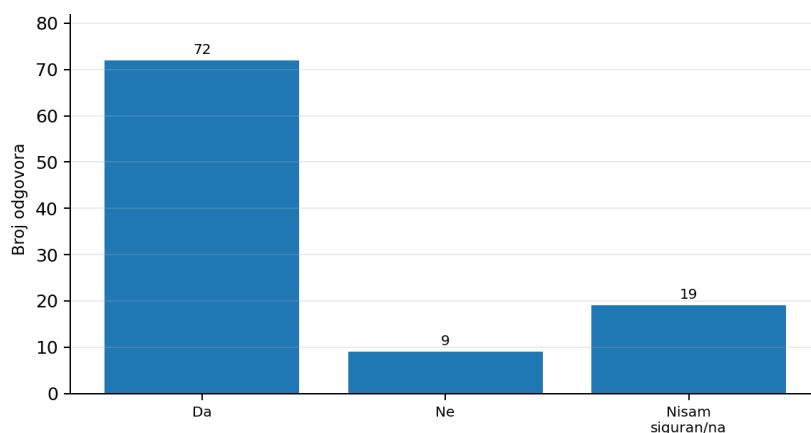
14. Da li krivične sankcije imaju dovoljan preventivni efekat?



Grafikon 14. Preventivni efekat krivičnih sankcija

Rezultati pokazuju da ispitanici uglavnom nemaju visok stepen poverenja u preventivni efekat postojećih krivičnih sankcija. Ukupno 34 ispitanika smatra da sankcije uglavnom nemaju dovoljan preventivni efekat, dok 22 ispitanika smatra da ga uopšte nemaju. Delimičan efekat prepoznalo je 28 ispitanika, dok 12 ispitanika smatra da sankcije uglavnom imaju preventivni efekat, a 4 ispitanika da ga imaju u potpunosti. Ovakvi rezultati ukazuju da ispitanici smatraju da sama kazna nije dovoljna ukoliko nije praćena efikasnim otkrivanjem, dokazivanjem i oduzimanjem protivpravne koristi.

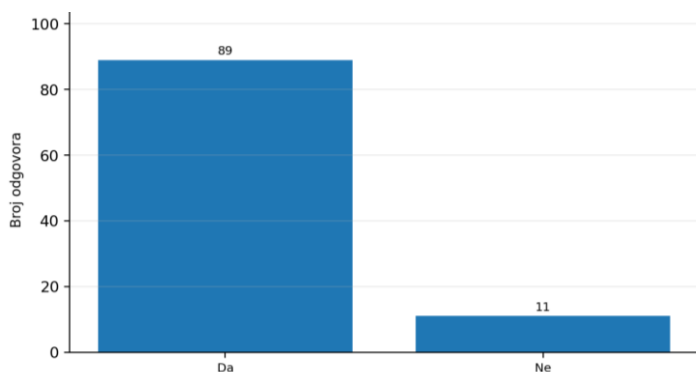
15. Da li biste podržali obaveznu identifikaciju korisnika na svim kripto-platformama?



Grafikon 15. Podrška obaveznoj identifikaciji korisnika

Obaveznu identifikaciju korisnika na svim kripto-platformama podržala su 72 ispitanika. Protiv ove mere bilo je 9 ispitanika, dok 19 ispitanika nije bilo sigurno. Ovakav rezultat pokazuje da većina ispitanika daje prednost bezbednosnom i regulatornom aspektu u odnosu na potpunu anonimnost korisnika. Istovremeno, broj nesigurnih ispitanika pokazuje da deo javnosti verovatno prepoznaje i pitanje privatnosti, pa bi svako strože pravilo moralo biti jasno obrazloženo i usklađeno sa zaštitom podataka o ličnosti.

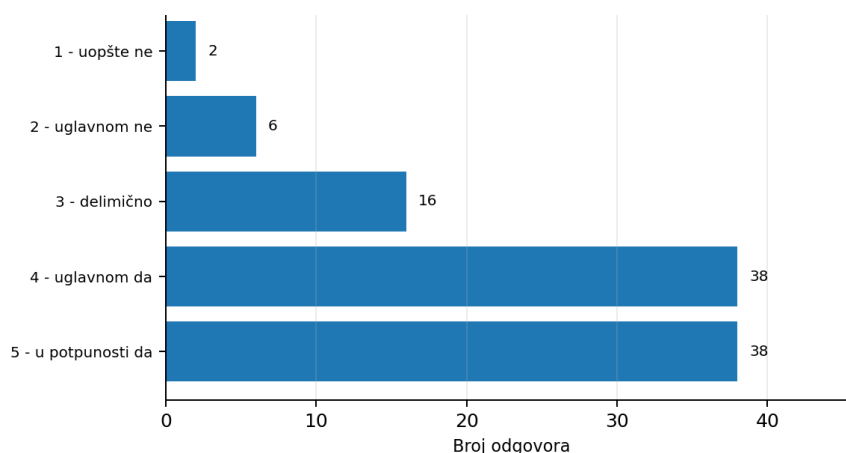
16. Da li biste podržali specijalizovanu obuku policije, tužilaštva i sudova?



Grafikon 16. Podrška specijalizovanoj obuci nadležnih organa

Specijalizovanu obuku policije, tužilaštva i sudova podržalo je 89 ispitanika, dok je 11 ispitanika navelo da ne podržava ovu meru. Rezultati veoma jasno ukazuju da ispitanici smatraju da se zloupotrebe kriptovaluta ne mogu efikasno suzbijati bez stručnog znanja nadležnih organa. Ovaj nalaz je posebno važan zato što se kriptovalute ne mogu razumeti samo kroz opšta pravna pravila, već zahtevaju poznavanje digitalne forenzike, blockchain analize i finansijskih istraga.

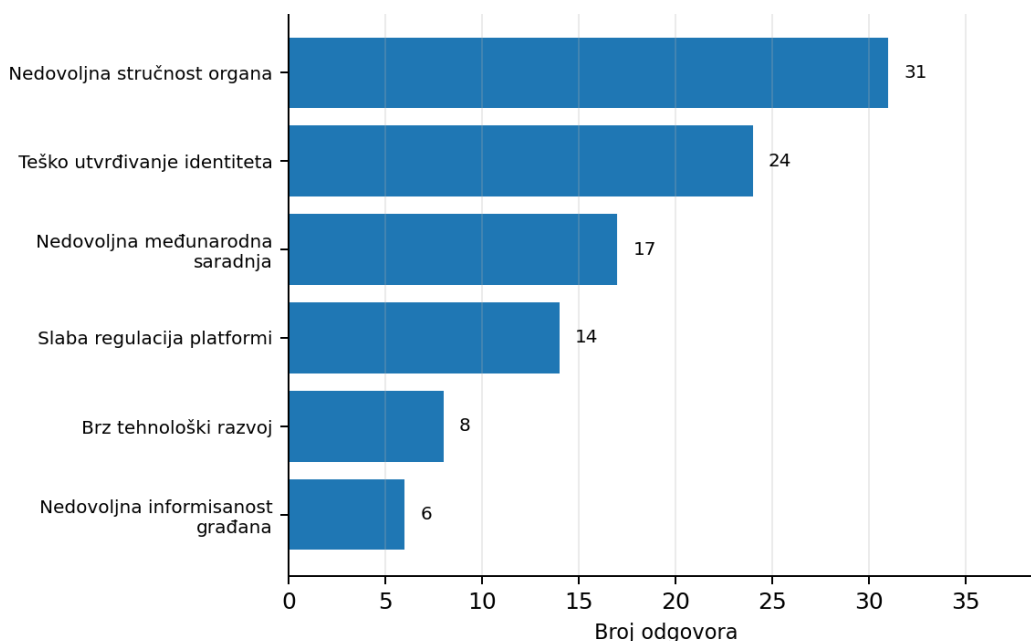
17. Da li smatrate da je potrebno unaprediti oduzimanje digitalne imovine?



Grafikon 17. Potreba za unapređenjem oduzimanja digitalne imovine

Potrebu za unapređenjem oduzimanja digitalne imovine u potpunosti prepoznaje 38 ispitanika, dok još 38 ispitanika uglavnom podržava takvo unapređenje. Delimično slaganje iskazalo je 16 ispitanika, dok je 6 ispitanika uglavnom protiv, a 2 ispitanika uopšte ne smatra da je unapređenje potrebno. Rezultati pokazuju da ispitanici razumeju značaj imovinskog aspekta krivičnog postupka, jer efikasno sankcionisanje zloupotreba kriptovaluta nema pun efekat ako protivpravna korist ostane dostupna učiniocu.

18. Po vašem mišljenju, koji je najveći problem u suzbijanju zloupotreba kriptovaluta?



Grafikon 18. Najveći problemi u suzbijanju zloupotreba kriptovaluta

Otvoreni odgovori ispitanika naknadno su razvrstani u tematske kategorije. Najveći broj ispitanika, njih 31, kao glavni problem naveo je nedovoljnu stručnost nadležnih organa. Teško utvrđivanje identiteta učinilaca istakla su 24 ispitanika, dok je 17 ispitanika naglasilo nedovoljnu međunarodnu saradnju. Slabu regulaciju platformi navelo je 14 ispitanika, brz tehnološki razvoj 8 ispitanika, a nedovoljnu informisanost građana 6 ispitanika. Ovakav nalaz pokazuje da ispitanici problem ne vide samo u propisima, već i u praktičnoj sposobnosti institucija da prate tehnološke promene i efikasno postupaju u konkretnim predmetima.

7.5. Očekivani doprinos istraživanja

Očekivani doprinos empirijskog istraživanja ogleda se u tome što se teorijska i pravna analiza dopunjuje stavovima ispitanika. Rezultati ankete pokazuju kako ispitanici razumeju kriptovalute, koje rizike najviše prepoznaju i u kojoj meri smatraju da je potreban snažniji institucionalni odgovor. Time se dobija potpunija slika o društvenoj percepciji problema, što je važno jer su zloupotrebe kriptovaluta povezane ne samo sa propisima i tehnologijom, već i sa nivoom informisanosti građana.

Istraživanje doprinosi radu i time što potvrđuje da ispitanici najčešće prepoznaju pranje novca, prikrivanje identiteta, ransomware napade i otežano dokazivanje kao ključne rizike. Ovi nalazi su u skladu sa osnovnim problemom rada, jer ukazuju da kriptovalute u javnoj percepciji nisu sporne samo kao finansijska novina, već kao instrument koji može otežati rad organa gonjenja i omogućiti prikrivanje protivpravne koristi.

Poseban doprinos istraživanja odnosi se na stavove o unapređenju institucionalnog odgovora. Većina ispitanika podržava strožu kontrolu pružalaca usluga digitalne imovine, obaveznu identifikaciju korisnika, specijalizovanu obuku policije, tužilaštva i sudova, kao i unapređenje oduzimanja digitalne imovine. Ovi rezultati mogu biti korisni za formulisanje preporuka u završnom delu rada, naročito u pravcu jačanja stručnih kapaciteta, bolje međunarodne saradnje i praktičnije primene propisa.

Na kraju, istraživanje ima i ograničenja. Uzorak je prigodan i obuhvata 100 ispitanika, pa se rezultati ne mogu u potpunosti generalizovati na celokupnu populaciju. Ipak, oni imaju vrednost kao dopunski empirijski pokazatelj i mogu poslužiti kao osnova za šire istraživanje u budućnosti. U okviru ovog rada, rezultati ankete imaju funkciju da povežu teorijski, normativni i praktični deo analize i da pokažu kako se rizici zloupotrebe kriptovaluta prepoznaju iz perspektive ispitanika.

8. DISKUSIJA

Diskusija rezultata pokazuje da se teorijski, normativni i empirijski deo rada međusobno dopunjuju. U prethodnim poglavljima objašnjeno je da kriptovalute i digitalna imovina nisu same po sebi nezakonite, ali da njihove tehničke i funkcionalne karakteristike mogu biti zloupotrebene u izvršenju i prikrivanju krivičnih dela. Posebno su istaknuti pseudonimnost, brzina prenosa, prekogranični karakter transakcija, decentralizovana struktura i mogućnost otežanog povezivanja digitalne adrese sa stvarnim identitetom korisnika. Rezultati ankete potvrđuju da ispitanici u velikoj meri prepoznaju upravo ove rizike, jer većina smatra da kriptovalute olakšavaju prikrivanje identiteta učinioca, pranje novca i otežano dokazivanje krivičnih dela. Time se pokazuje da empirijski nalazi prate osnovne teorijske pretpostavke rada i ukazuju da se rizici kriptovaluta ne prepoznaju samo u stručnoj literaturi, već i u stavovima ispitanika.

U teorijskom delu rada kriptovalute su objašnjene kao digitalni zapisi vrednosti koji funkcionišu na osnovu blockchain tehnologije, kriptografskih metoda i decentralizovane mreže. Takva struktura omogućava da se transakcije odvijaju bez centralnog posrednika, što može biti prednost u zakonitoj upotrebi, ali istovremeno predstavlja izazov za nadzor i krivičnopravno postupanje. Rezultati ankete pokazuju da 43 ispitanika ima prethodno iskustvo sa korišćenjem kriptovaluta, dok 57 ispitanika nije ranije koristilo kriptovalute. Ovaj podatak je značajan jer pokazuje da stavovi o rizicima ne dolaze samo od korisnika koji imaju neposredno iskustvo, već i od ispitanika koji kriptovalute poznaju posredno, kroz informacije iz medija, obrazovanja, društvenog okruženja ili opšteg interesovanja za digitalne finansije. To potvrđuje da je tema kriptovaluta postala društveno prepoznatljiva, čak i među licima koja ih neposredno ne koriste (Nakamoto, 2008).

Posebno je važno što su ispitanici svoje poznavanje pojma kriptovaluta najčešće ocenili srednjom ili dobrom ocenom. Najveći broj ispitanika, njih 34, naveo je srednji nivo poznavanja, 29 ispitanika ocenilo je svoje poznavanje kao dobro, a 14 kao veoma dobro. Sa druge strane, 17 ispitanika navelo je slabo, a 6 veoma slabo poznavanje. Ovakva raspodela ukazuje da većina ispitanika ima osnovnu svest o tome šta su kriptovalute, ali da se ne može govoriti o potpunom i stručnom razumevanju. To je važno za tumačenje rezultata, jer ispitanici uglavnom prepoznaju rizike, ali njihovi stavovi mogu biti zasnovani više na opštoj percepciji nego na detaljnom poznavanju pravnih i tehničkih mehanizama.

U ranijem delu rada istaknuto je da je pseudonimnost jedna od najvažnijih karakteristika kriptovaluta sa stanovišta krivičnog prava. Blockchain transakcije mogu biti javno vidljive, ali se one najčešće vezuju za digitalne adrese, a ne neposredno za ime i prezime korisnika. Upravo zbog toga postoji razlika između vidljivosti transakcionog traga i identifikacije stvarnog učinioca. Rezultati ankete potvrđuju da ispitanici ovu okolnost prepoznaju kao značajan problem. Čak 44 ispitanika u potpunosti se složilo sa tvrdnjom da kriptovalute olakšavaju prikrivanje identiteta učinioca, dok se 32 ispitanika uglavnom složilo. To znači da je 76 ispitanika iskazalo jasan stav da kriptovalute mogu otežati identifikaciju lica koja učestvuju u protivpravnim transakcijama. Ovaj rezultat je u skladu sa teorijskom analizom pseudonimnosti i dokaznih izazova u povezivanju digitalne adrese sa konkretnim fizičkim licem (Meiklejohn et al., 2013).

Empirijski nalazi potvrđuju i teorijsku pretpostavku da kriptovalute mogu biti naročito značajne u kontekstu pranja novca i prikrivanja porekla imovine. U prethodnim poglavljima objašnjeno je da digitalna imovina može biti korišćena za prebacivanje vrednosti kroz više adresa, platformi i jurisdikcija, čime se otežava utvrđivanje veze između krivičnog dela, učinioca i protivpravne koristi. U anketi je 44 ispitanika u potpunosti ocenilo da kriptovalute olakšavaju pranje novca, dok se 37 ispitanika uglavnom složilo sa tom tvrdnjom. To znači da ukupno 81 ispitanik prepoznaje kriptovalute kao faktor koji može doprineti pranju novca. Ovakav rezultat je posebno značajan jer pokazuje da ispitanici najviše prepoznaju upravo finansijsko-kriminalističku dimenziju problema, odnosno mogućnost da digitalna imovina bude upotrebljena za prikrivanje porekla sredstava (FATF, 2024).

Pitanje pranja novca povezano je i sa rezultatima koji se odnose na najopasnije oblike zloupotrebe kriptovaluta. Kod pitanja višestrukog izbora, pranje novca je označeno 61 put, što ga čini najčešće prepoznatim oblikom zloupotrebe. Nakon toga slede ransomware napadi sa 48 izbora i investicione prevare sa 44 izbora. Ovi rezultati pokazuju da ispitanici kriptovalute ne posmatraju samo kao tehničko sredstvo plaćanja, već pre svega kao instrument koji može omogućiti prikrivanje, iznudu i obmanu. U tom smislu, rezultati ankete se dobro uklapaju u teorijski deo rada, gde je istaknuto da kriptovalute mogu imati različite uloge: mogu biti sredstvo plaćanja, predmet krivičnog dela, sredstvo prikrivanja protivpravne koristi ili dokaz u krivičnom postupku.

Ransomware napadi su u teorijskom delu rada obrađeni kao jedan od najpoznatijih savremenih oblika zloupotrebe kriptovaluta. U takvim slučajevima učinioci zahtevaju plaćanje u digitalnoj imovini, računajući na brzinu transfera i otežanu identifikaciju primaoca.

Rezultati ankete pokazuju da ispitanici u velikoj meri prepoznaju ovu vezu: 36 ispitanika u potpunosti smatra da se kriptovalute često povezuju sa ransomware napadima, dok se 33 ispitanika uglavnom slaže. Dakle, 69 ispitanika vidi jasnu povezanost kriptovaluta i digitalne iznude. Ovaj nalaz pokazuje da ransomware nije samo stručni ili policijsko-bezbednosni problem, već i fenomen koji je prepoznat u široj javnosti kao važan oblik digitalnog kriminaliteta (Europol, 2024).

Kada se posmatraju stavovi o domaćim propisima, rezultati pokazuju određeno nepoverenje ispitanika u postojeći normativni okvir. Ukupno 34 ispitanika smatra da domaći propisi uglavnom nisu dovoljni, dok 27 ispitanika smatra da uopšte nisu dovoljni. Samo 11 ispitanika smatra da su uglavnom dovoljni, a 4 ispitanika da su u potpunosti dovoljni. Ovakvi rezultati ukazuju da većina ispitanika prepoznaje potrebu za dodatnim unapređenjem propisa ili njihove praktične primene. To se može povezati sa teorijskom analizom prema kojoj samo formalno postojanje zakona nije dovoljno ako institucije nemaju kapacitete da prate digitalne transakcije, sarađuju sa stranim platformama i efikasno obezbede digitalne dokaze. U Republici Srbiji digitalna imovina jeste zakonski prepoznata, ali praksa i institucionalna primena ostaju posebno važni za ocenu stvarne efikasnosti sistema (Republika Srbija, 2020).

Sličan zaključak proizlazi i iz odgovora na pitanje o strožoj kontroli pružalaca usluga digitalne imovine. Većina ispitanika podržava jačanje kontrole, jer je 44 ispitanika u potpunosti saglasno sa potrebom za strožom kontrolom, dok se 34 ispitanika uglavnom slaže. To znači da 78 ispitanika vidi menjačnice, platforme i druge pružaoce usluga digitalne imovine kao važne tačke nadzora. Ovakav nalaz je u skladu sa savremenim međunarodnim pristupom, prema kome se regulacija ne usmerava na zabranu kriptovaluta, već na nadzor nad subjektima koji omogućavaju ulazak i izlazak sredstava iz kripto-ekosistema. Posebno se insistira na identifikaciji korisnika, praćenju transakcija i prijavljivanju sumnjivih aktivnosti, jer upravo ti mehanizmi mogu olakšati kasnije krivično gonjenje (Vandezande, 2017).

Rezultati ankete jasno potvrđuju i značaj dokaznih problema koji su obrađeni u teorijskom delu rada. Na pitanje da li anonimni novčanici i mikseri otežavaju dokazivanje krivičnih dela, 43 ispitanika u potpunosti se složilo, dok se 33 ispitanika uglavnom složilo. To znači da 76 ispitanika prepoznaje tehničke mehanizme prikrivanja kao ozbiljan dokazni izazov. Ovaj rezultat je važan jer pokazuje da ispitanici ne posmatraju problem samo kroz pitanje propisa, već i kroz praktičnu sposobnost organa da rekonstruišu tokove digitalne imovine. U teorijskom delu rada objašnjeno je da blockchain može ostaviti transakcioni trag, ali da taj trag ne mora biti jednostavan za tumačenje ako se koriste različite adrese, platforme ili sredstva za otežavanje praćenja (Casey et al., 2019).

Međunarodna saradnja se pokazala kao jedna od najjače podržanih kategorija u rezultatima ankete. Ukupno 46 ispitanika u potpunosti smatra da međunarodna saradnja ima presudan značaj, dok se 36 ispitanika uglavnom slaže. To znači da 82 ispitanika jasno prepoznaje transnacionalnu prirodu problema. Ovaj rezultat je u potpunosti usklađen sa teorijskim delom rada, jer su kripto-transakcije često povezane sa više država: korisnik može biti u jednoj državi, menjačnica u drugoj, serveri u trećoj, a oštećeni u četvrtoj. Bez međunarodne saradnje teško je pribaviti podatke, zamrznuti sredstva, izvršiti zaplenu ili obezbediti dokaze koji se nalaze van domaće nadležnosti (UNODC, 2024).

Posebno značajan nalaz odnosi se na stavove ispitanika o preventivnom efektu krivičnih sankcija. Rezultati pokazuju da ispitanici uglavnom nemaju visok stepen poverenja u same sankcije kao dovoljan mehanizam odvraćanja. Ukupno 34 ispitanika smatra da krivične sankcije uglavnom nemaju dovoljan preventivni efekat, dok 22 ispitanika smatra da ga uopšte nemaju. Delimičan efekat prepoznalo je 28 ispitanika, a samo manji broj smatra da sankcije uglavnom ili u potpunosti ostvaruju preventivnu funkciju. Ovaj nalaz je važan jer pokazuje da ispitanici razumeju da kažnjavanje nije dovoljno ako nije praćeno efikasnim otkrivanjem, dokazivanjem i oduzimanjem protivpravne koristi. Time se potvrđuje jedna od važnih pretpostavki rada: kod krivičnih dela povezanih sa kriptovalutama nije presudna samo visina kazne, već sposobnost sistema da pronađe učinioca, dokaže delo i oduzme digitalnu imovinu.

Podrška obaveznoj identifikaciji korisnika na kripto-platformama takođe je veoma izražena. Čak 72 ispitanika podržala su ovu meru, 9 je bilo protiv, dok 19 nije bilo sigurno. Ovaj rezultat pokazuje da većina ispitanika daje prednost bezbednosnom i regulatornom aspektu u odnosu na potpunu anonimnost korisnika. Ipak, broj nesigurnih ispitanika nije zanemarljiv i ukazuje da deo javnosti verovatno prepoznaje i pitanje privatnosti, zaštite podataka i prava zakonitih korisnika. Zbog toga se u praksi mora tražiti ravnoteža između potrebe za identifikacijom korisnika i zaštite legitimne privatnosti. Teorijski deo rada je pokazao da kriptovalute ne treba posmatrati isključivo kao kriminalni instrument, već kao digitalnu imovinu koja ima i zakonite funkcije, zbog čega regulacija mora biti srazmerna i pažljivo oblikovana (Houben & Snyers, 2018).

Najizraženija podrška u anketi odnosi se na specijalizovanu obuku policije, tužilaštva i sudova. Ovu meru podržalo je 89 ispitanika, dok je samo 11 bilo protiv. Ovaj nalaz je posebno važan jer ukazuje da ispitanici jasno prepoznaju da se zloupotrebe kriptovaluta ne mogu efikasno suzbijati samo opštim pravnim znanjem.

Potrebna su specijalizovana znanja iz oblasti digitalne forenzike, blockchain analize, finansijskih istraga, međunarodne saradnje i oduzimanja digitalne imovine. To je u potpunosti u skladu sa teorijskim delom rada, u kome je naglašeno da policija, tužilaštvo i sudovi moraju razumeti kako funkcionišu digitalni novčanici, transakcioni tragovi, menjačnice i privatni ključevi kako bi mogli pravilno da postupaju u predmetima ove vrste (Casey et al., 2019).

Rezultati koji se odnose na oduzimanje digitalne imovine dodatno potvrđuju značaj imovinskog aspekta krivičnog postupka. Ukupno 38 ispitanika u potpunosti smatra da je potrebno unaprediti oduzimanje digitalne imovine, dok još 38 ispitanika uglavnom podržava takvo unapređenje. To znači da 76 ispitanika prepoznaje da borba protiv zloupotrebe kriptovaluta nije potpuna ako se učiniocu ne oduzme protivpravna korist. Ovaj nalaz je u skladu sa teorijskim razmatranjem prema kome digitalna imovina može biti i predmet krivičnog dela i protivpravna korist i dokaz. Kod kriptovaluta oduzimanje je posebno složeno zato što se imovina može brzo preneti, jer pristup zavisi od privatnih ključeva, a vrednost imovine može značajno varirati (FATF, 2024).

Otvoreno pitanje dodatno je produbilo nalaze ankete. Najveći broj ispitanika, njih 31, kao glavni problem naveo je nedovoljnu stručnost nadležnih organa. Teško utvrđivanje identiteta učinilaca navela su 24 ispitanika, dok je 17 ispitanika istaklo nedovoljnu međunarodnu saradnju. Slabu regulaciju platformi navelo je 14 ispitanika, brz tehnološki razvoj 8 ispitanika, a nedovoljnu informisanost građana 6 ispitanika. Ovi odgovori su značajni jer pokazuju da ispitanici problem zloupotrebe kriptovaluta ne vide samo u nedostatku propisa, već pre svega u praktičnim teškoćama primene prava. Drugim rečima, ispitanici smatraju da je ključni problem sposobnost institucija da prate tehnološke promene i da na njih odgovore efikasno.

Kada se uporede teorijski deo rada i rezultati ankete, može se zaključiti da između njih postoji visok stepen podudarnosti. Teorija naglašava pseudonimnost, pranje novca, transnacionalnost, dokazne teškoće, potrebu za regulacijom pružalaca usluga i značaj stručne obuke. Anketa pokazuje da ispitanici upravo ove elemente najčešće prepoznaju kao ključne rizike. Posebno se izdvajaju pranje novca, prikrivanje identiteta, ransomware napadi, potreba za međunarodnom saradnjom i potreba za specijalizovanom obukom nadležnih organa. Time empirijski deo potvrđuje osnovne pravce teorijske analize i pokazuje da se problem zloupotrebe kriptovaluta ne može svesti samo na tehničko pitanje, već obuhvata pravo, bezbednost, finansije, institucije i obrazovanje.

Rezultati ankete mogu se povezati i sa postavljenim hipotezama rada. Prva hipoteza, prema kojoj specifične karakteristike kriptovaluta olakšavaju prikrivanje porekla protivpravne imovinske koristi i otežavaju otkrivanje učinilaca, nalazi potvrdu u odgovorima ispitanika o prikrivanju identiteta, pranju novca i otežanom dokazivanju. Druga hipoteza, koja polazi od toga da postojeći normativni okvir predstavlja osnovu, ali da u praksi postoje problemi, potvrđena je kroz nepoverenje ispitanika u dovoljnost domaćih propisa i kroz naglašavanje nedovoljne stručnosti institucija. Treća hipoteza, prema kojoj je krivičnopravni odgovor efikasniji uz AML/CFT mehanizme, regulaciju pružalaca usluga i obuku organa, podržana je rezultatima o strožoj kontroli platformi, međunarodnoj saradnji i specijalizovanoj obuci. Četvrta hipoteza potvrđena je time što većina ispitanika kriptovalute povezuje sa pranjem novca, prevarama, ransomware napadima i dokaznim problemima. Peta hipoteza biće dodatno potvrđena kroz studije slučaja, jer one pokazuju da je procesuiranje moguće, ali uz visok nivo tehničke i institucionalne koordinacije.

Studije slučaja Silk Road i Bitfinex posebno pomažu u tumačenju rezultata ankete. Ispitanici su kao najopasnije oblike zloupotrebe najčešće navodili pranje novca, ransomware i investicione prevare, dok su darknet tržišta označena ređe. Ipak, slučaj Silk Road pokazuje da darknet tržišta imaju veliki analitički značaj, jer pokazuju kako kriptovalute mogu služiti kao sredstvo plaćanja u organizovanom digitalnom kriminalnom okruženju. Sa druge strane, Bitfinex slučaj pokazuje zašto ispitanici opravdano prepoznaju pranje novca i prikrivanje imovine kao centralne probleme. Taj slučaj ilustruje koliko dugo i složeno može trajati praćenje ukradene digitalne imovine i koliko su značajni blockchain analiza, međunarodna saradnja i oduzimanje imovine (U.S. Department of Justice, 2024).

U diskusiji treba naglasiti i određena ograničenja empirijskog istraživanja. Uzorak je obuhvatio 100 ispitanika i ima prigodan karakter, što znači da se rezultati ne mogu u potpunosti generalizovati na celokupnu populaciju. Pored toga, znatan deo ispitanika nije ranije koristio kriptovalute, pa se njihovi stavovi mogu zasnivati na opštoj informisanosti, a ne na neposrednom iskustvu. Ipak, to ne umanjuje značaj istraživanja, jer je cilj bio da se ispita percepcija rizika, a ne tehničko znanje profesionalnih korisnika. Dobijeni rezultati imaju vrednost kao dopunski empirijski pokazatelj i kao osnova za povezivanje teorijskog, normativnog i praktičnog dela rada.

9. ZAKLJUČAK

Kriptovalute i digitalna imovina predstavljaju jedan od najznačajnijih izazova savremenog krivičnog prava, kriminalistike i sistema bezbednosti. Njihov razvoj pokazuje da tehnološke inovacije mogu imati dvostruku prirodu. Sa jedne strane, kriptovalute omogućavaju brži prenos vrednosti, nove oblike finansijskog poslovanja, digitalna ulaganja i razvoj decentralizovanih sistema. Sa druge strane, iste karakteristike koje ih čine korisnim u zakonitim transakcijama mogu biti iskorišćene za izvršenje, prikrivanje i otežano dokazivanje krivičnih dela. Zbog toga kriptovalute ne treba posmatrati kao pojavu koja je sama po sebi nezakonita, već kao sredstvo koje, u zavisnosti od načina upotrebe, može imati i zakonitu i protivpravnu funkciju.

U radu je najpre ukazano na pojmovno određenje kriptovaluta i digitalne imovine, jer je pravilno razumevanje osnovnih pojmova neophodno za svaku dalju pravnu analizu. Kriptovalute se razlikuju od tradicionalnog novca, ali i od drugih oblika digitalne imovine, kao što su tokeni i različiti digitalni zapisi prava. Posebno je značajno to što se njihovo funkcionisanje zasniva na blockchain tehnologiji, digitalnim novčanicima, privatnim i javnim ključevima, menjačnicama i transakcionim tragovima. Upravo ovi elementi imaju veliki značaj u krivičnom postupku, jer mogu istovremeno olakšati praćenje toka imovine, ali i otežati identifikaciju lica koje zaista stoji iza određene transakcije.

Analiza krivičnopravnih i bezbednosnih rizika pokazala je da su pseudonimnost, brzina prenosa, prekogranični karakter transakcija i mogućnost korišćenja više digitalnih adresa među najvažnijim faktorima koji otežavaju rad nadležnih organa. Iako blockchain često ostavlja trag, taj trag sam po sebi nije dovoljan za utvrđivanje krivične odgovornosti. Potrebno je dokazati ko kontroliše određenu adresu, na koji način je digitalna imovina pribavljena, da li postoji veza sa konkretnim krivičnim delom i da li je postojala namera prikrivanja porekla imovine. Zbog toga se u predmetima povezanim sa kriptovalutama klasična krivična istraga mora dopuniti digitalnom forenzikom, finansijskom analizom i međunarodnom saradnjom.

Posebno mesto u radu zauzima pitanje pranja novca i prikrivanja porekla protivpravne imovinske koristi. Kriptovalute se mogu koristiti za brzo prebacivanje vrednosti, za raslojavanje transakcija i za udaljavanje imovine od njenog kriminalnog izvora. Međutim, rad je pokazao da kriptovalute ne obezbeđuju potpunu nevidljivost, već stvaraju složeniji oblik transakcionog traga.

To znači da uspeh istrage zavisi od stručnosti organa, dostupnosti podataka, saradnje sa pružaoциma usluga digitalne imovine i mogućnosti da se digitalni tragovi povežu sa stvarnim licima i konkretnim radnjama izvršenja.

Normativni okvir ima ključnu ulogu u suzbijanju zloupotreba kriptovaluta, ali sam po sebi nije dovoljan ako se ne primenjuje efikasno. Međunarodni standardi, regulativa Evropske unije i pravni okvir Republike Srbije pokazuju da se oblast digitalne imovine sve više uvodi u pravni sistem. Posebno su važna pravila koja se odnose na identifikaciju korisnika, nadzor pružalaca usluga digitalne imovine, sprečavanje pranja novca, prijavljivanje sumnjivih aktivnosti i oduzimanje protivpravne koristi. Ipak, u praksi ostaju izazovi koji se odnose na transnacionalni karakter kripto-transakcija, brze tehnološke promene i potrebu za specijalizovanim znanjima kod policije, tužilaštva i sudova.

U radu je potvrđeno da se kriptovalute mogu pojaviti u različitim ulogama u vezi sa krivičnim delima. One mogu biti sredstvo plaćanja, sredstvo prenosa vrednosti, način prikrivanja protivpravne koristi, predmet krađe ili prevare, ali i dokaz koji ukazuje na tok kriminalne aktivnosti. To znači da se kriptovalute ne mogu posmatrati jednostrano. U jednom slučaju one mogu biti instrument izvršenja krivičnog dela, u drugom predmet krivičnog dela, a u trećem imovina koju je potrebno oduzeti. Upravo zbog toga je neophodno da organi postupka razumeju njihovu tehničku, ekonomsku i pravnu prirodu.

Studije slučaja Silk Road i Bitfinex pokazale su praktičnu potvrdu teorijskih stavova iz rada. Slučaj Silk Road ukazuje na upotrebu kriptovaluta kao sredstva plaćanja u okviru nezakonitog digitalnog tržišta, dok slučaj Bitfinex pokazuje složenost praćenja ukradene digitalne imovine i pokušaja njenog prikrivanja kroz različite transakcione tokove. Ovi slučajevi potvrđuju da je uspešno otkrivanje i procesuiranje zloupotreba kriptovaluta moguće, ali da zahteva visok nivo tehničke stručnosti, međunarodnu koordinaciju, upotrebu digitalnih dokaza i sposobnost nadležnih organa da prate tokove digitalne imovine kroz duži vremenski period.

Empirijsko istraživanje sprovedeno putem online ankete dodatno je potvrdilo osnovne nalaze rada. Rezultati su pokazali da ispitanici u velikoj meri prepoznaju kriptovalute kao mogući faktor rizika u pranju novca, prikrivanju identiteta učinilaca, ransomware napadima, prevarama i otežanom dokazivanju krivičnih dela. Većina ispitanika podržala je strožu kontrolu pružalaca usluga digitalne imovine, obaveznu identifikaciju korisnika na kripto-platformama, unapređenje međunarodne saradnje i specijalizovanu obuku policije, tužilaštva i sudova.

Ovi rezultati ukazuju da problem zloupotrebe kriptovaluta nije samo teorijsko ili normativno pitanje, već i pitanje društvene percepcije rizika i poverenja u sposobnost institucija da na te rizike odgovore.

Na osnovu sprovedene analize može se zaključiti da su postavljene hipoteze u velikoj meri potvrđene. Specifične karakteristike kriptovaluta zaista mogu olakšati prikrivanje porekla protivpravne koristi i otežati identifikaciju učinilaca. Postojeći normativni okvir predstavlja važnu osnovu za suzbijanje zloupotreba, ali u praksi i dalje postoje problemi u dokazivanju, međunarodnoj saradnji i oduzimanju digitalne imovine. Krivičnopravni odgovor je efikasniji kada je povezan sa preventivnim mehanizmima, regulacijom pružalaca usluga, AML/CFT sistemom i stručnom obukom nadležnih organa. Rezultati ankete potvrđuju da ispitanici prepoznaju kriptovalute kao rizik za pranje novca, prevare i otežano dokazivanje, dok studije slučaja pokazuju da je uspešno procesuiranje moguće, ali samo uz visok stepen institucionalne i tehničke pripremljenosti.

Najvažniji zaključak rada jeste da borba protiv zloupotrebe kriptovaluta ne može biti zasnovana samo na krivičnim sankcijama. Sankcionisanje je neophodno, ali ono mora biti praćeno efikasnim otkrivanjem, dokazivanjem i oduzimanjem protivpravne imovine. Ukoliko učinilac zadrži digitalnu imovinu ili uspe da prikrije njen tok, preventivni efekat krivičnog sistema biće slabiji. Zbog toga je potrebno razvijati finansijske istrage, digitalnu forenziku, blockchain analitiku, institucionalnu saradnju i praktične procedure za hitno postupanje u slučajevima kada postoji rizik od premeštanja digitalne imovine.

U budućem periodu posebnu pažnju treba posvetiti jačanju kapaciteta policije, tužilaštva i sudova. Potrebna je specijalizovana obuka iz oblasti digitalne imovine, načina funkcionisanja blockchaina, postupanja sa digitalnim dokazima, praćenja transakcija i oduzimanja kriptovaluta. Takođe je neophodno unaprediti saradnju sa regulatornim organima, finansijsko-obaveštajnim jedinicama, pružaocima usluga digitalne imovine i međunarodnim institucijama. Samo povezan i stručan institucionalni odgovor može biti efikasan u oblasti u kojoj se tehnologija brzo menja, a učinioci krivičnih dela stalno prilagođavaju svoje metode.

Kriptovalute predstavljaju trajan izazov za savremeno krivično pravo, ali i oblast u kojoj pravo ne sme ostati pasivno. Njihova zloupotreba zahteva pravovremenu reakciju, ali i razumevanje činjenice da zabrana ili pojednostavljeno posmatranje nisu dovoljni. Potrebno je razviti uravnotežen pristup koji istovremeno omogućava zakonitu upotrebu digitalne imovine, štiti korisnike i finansijski sistem, a nadležnim organima daje stvarne mogućnosti da otkriju, dokažu i sankcionišu krivična dela povezana sa kriptovalutama.

10. LITERATURA

1. Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain* (2nd ed.). O'Reilly Media.
2. Arner, D. W., Auer, R., & Frost, J. (2020). Stablecoins: Risks, potential and regulation. *Bank for International Settlements Working Papers*.
3. Babović, M. G. (2023). Uporednopravni regulatorni odgovori na izazove digitalne imovine. *Strani pravni život*, 67(3), 447–469. https://doi.org/10.56461/SPZ_23305KJ
4. Bank for International Settlements. (2021). *Central bank digital currencies: Foundational principles and core features*. Bank for International Settlements.
5. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238. <https://doi.org/10.1257/jep.29.2.213>
6. Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Ethereum White Paper.
7. Casey, E., Katz, G., & Lewthwaite, J. (2019). Honing digital forensic processes. *Digital Investigation*, 28, 138–146.
8. Cvetković, M. (2018). Novčane obaveze i kriptovalute. *Zbornik radova Pravnog fakulteta u Nišu*, 57(81), 119–138.
9. De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
10. European Union. (2015). *Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. Official Journal of the European Union.
11. European Union. (2018). *Directive (EU) 2018/1673 on combating money laundering by criminal law*. Official Journal of the European Union.
12. European Union. (2023). *Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets*. Official Journal of the European Union.
13. European Union. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets*. Official Journal of the European Union.
14. Europol. (2021). *Cryptocurrencies: Tracing the evolution of criminal finances*. Europol Spotlight.
15. Europol. (2024). *Internet organised crime threat assessment (IOCTA) 2024*. Europol.

16. Fairfield, J. (2022). *Runaway technology: Can law keep up?* Cambridge University Press.
17. Financial Action Task Force. (2024). *Virtual assets: Targeted update on implementation of the FATF standards on VAs and VASPs*. FATF.
18. Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament.
19. Komisija za hartije od vrednosti Republike Srbije. (2020). *Zakon o digitalnoj imovini*. Komisija za hartije od vrednosti Republike Srbije.
20. Krivični zakonik Republike Srbije. *Službeni glasnik RS*, br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.
21. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. *Proceedings of the 2013 Internet Measurement Conference*, 127–140.
22. Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *2013 APWG eCrime Researchers Summit*, 1–14.
23. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.
24. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.
25. Osterburg, J. W., & Ward, R. H. (2019). *Criminal investigation: A method for reconstructing the past* (8th ed.). Routledge.
26. Republika Srbija. (2020). *Zakon o digitalnoj imovini*. *Službeni glasnik RS*, br. 153/2020.
27. Republika Srbija. (2017/2019/2020/2023/2024/2025). *Zakon o sprečavanju pranja novca i finansiranja terorizma*. *Službeni glasnik RS*, br. 113/2017, 91/2019, 153/2020, 92/2023, 94/2024 i 19/2025.
28. Reuters. (2025, January 22). *Trump pardons Silk Road founder Ross Ulbricht*. Reuters.
29. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, 103(2), 153–174.
30. UNODC. (2024). *Transnational organized crime and the convergence of cyber- and traditional crime: Risks and opportunities of response*. United Nations Office on Drugs and Crime.
31. U.S. Department of Justice. (2015). *Ross Ulbricht, a/k/a “Dread Pirate Roberts,” sentenced in Manhattan federal court to life in prison*. U.S. Department of Justice.
32. U.S. Department of Justice. (2022). *U.S. Attorney announces historic \$3.36 billion cryptocurrency seizure and conviction in connection with Silk Road fraud*. U.S. Department of Justice.

33. U.S. Department of Justice. (2024). *2016 Bitfinex hack*. U.S. Department of Justice.
34. U.S. Department of Justice. (2024). *Bitfinex hacker sentenced for money laundering conspiracy involving billions in stolen cryptocurrency*. U.S. Department of Justice.
35. Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review*, 33(3), 341–353. <https://doi.org/10.1016/j.clsr.2017.03.011>
36. Yermack, D. (2015). Is Bitcoin a real currency? An economic appraisal. In D. L. K. Chuen (Ed.), *Handbook of digital currency* (pp. 31–43). Academic Press.
37. Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM*, 58(9), 104–113. <https://doi.org/10.1145/2701411>

11. SAŽETAK

Rad se bavi zloupotrebom kriptovaluta u izvršenju i prikrivanju krivičnih dela, sa posebnim osvrtom na krivičnopravne, bezbednosne i dokazne izazove koje digitalna imovina stvara u savremenom društvu. U radu se najpre objašnjava pojam kriptovaluta i digitalne imovine, njihov nastanak, osnovne karakteristike, kao i značaj blockchain tehnologije, digitalnih novčanika, menjačnica i transakcionih tragova. Posebna pažnja posvećena je rizicima koji se odnose na pseudonimnost korisnika, otežanu identifikaciju učinilaca, pranje novca, prikrivanje porekla imovine, ransomware napade, prevare i korišćenje kriptovaluta na darknet tržištima. Analiziran je međunarodni, evropski i domaći normativni okvir, kao i uloga policije, tužilaštva, sudova i regulatornih organa u otkrivanju i dokazivanju ovih krivičnih dela. Kroz studije slučaja Silk Road i Bitfinex prikazani su konkretni primeri zloupotrebe kriptovaluta. Empirijski deo rada zasniva se na online anketi sprovedenoj na uzorku od 100 ispitanika, čiji rezultati pokazuju da većina ispitanika prepoznaje kriptovalute kao značajan rizik za pranje novca, prevare i otežano dokazivanje. Zaključuje se da je efikasan odgovor moguć samo uz bolju regulaciju, međunarodnu saradnju, specijalizovanu obuku nadležnih organa i unapređene mehanizme oduzimanja digitalne imovine.

Ključne reči: kriptovalute, digitalna imovina, pranje novca, krivična dela, dokazivanje.

12. SUMMARY

THE MISUSE OF CRYPTOCURRENCIES IN THE COMMISSION AND CONCEALMENT OF CRIMINAL OFFENCES

This paper examines the misuse of cryptocurrencies in the commission and concealment of criminal offences, with special emphasis on criminal law, security and evidentiary challenges created by digital assets in contemporary society. The paper first explains the concept of cryptocurrencies and digital assets, their origin, main characteristics, and the importance of blockchain technology, digital wallets, exchanges and transaction traces. Particular attention is paid to risks related to user pseudonymity, difficult identification of offenders, money laundering, concealment of the origin of assets, ransomware attacks, fraud and the use of cryptocurrencies on darknet markets. The international, European and national regulatory framework is analysed, as well as the role of the police, prosecution, courts and regulatory authorities in detecting and proving these criminal offences. Through the case studies of Silk Road and Bitfinex, the paper presents concrete examples of cryptocurrency misuse. The empirical part of the paper is based on an online survey conducted on a sample of 100 respondents, whose results show that most respondents recognise cryptocurrencies as a significant risk for money laundering, fraud and difficult evidence gathering. The paper concludes that an effective response is possible only through better regulation, international cooperation, specialised training of competent authorities and improved mechanisms for confiscating digital assets.

Keywords: cryptocurrencies, digital assets, money laundering, criminal offences, evidence.

13. BIOGRAFIJA AUTORA

Luka Jovanović rođen je 19.11.1996. godine u Nišu. Završio je Osnovnu školu “Vuk Karadžić” Doljevac, izdvojeno odeljenje u Pukovcu sa odličnim uspehom i kao nosilac diplome “Vuk Karadžić”. U Nišu je nastavio svoje dalje školovanje, gde je završio gimnaziju “Svetozar Marković”. Po završetku srednje škole, školske 2015/2016. godine, upisao je Pravni fakultet Univerziteta u Nišu. Diplomirao je dana 17.10.2022. godine na Pravnom fakultetu Univerziteta u Nišu sa prosečnom ocenom 7,77 i time stekao zvanje diplomirani pravnik.

Nakon diplomiranja, u periodu od 15.11.2022. godine do 31.08.2024. godine bio je zaposlen na određeno vreme u Turističkoj organizaciji opštine Doljevac, gde je obavljao poslove pravnika. Od 01.09.2024. godine zaposlen je u OŠ “Vuk Karadžić” Doljevac na poslovima sekretara ustanove, gde i trenutno radi.

Master akademske studije na Pravnom fakultetu Univerziteta u Nišu, smer unutrašnjih poslova, upisao je školske 2024/2025. godine. Sve ispite predviđene studijskim program položio je sa prosečnom ocenom 9,40. Studijski istraživački rad na temu “Informisanost o kriptovalutama i rizicima povezanim sa njihovom upotrebom” ocenjen je ocenom 10. Stručnu praksu obavio je u OŠ “Vuk Karadžić”.

14. PRILOG

ANKETA

Stavovi o zloupotrebi kriptovaluta u izvršenju i prikrivanju krivičnih dela

Uputstvo za ispitanike: Anketa je anonimna i koristi se isključivo u svrhu akademskog istraživanja. Molimo Vas da na pitanja odgovarate iskreno. Popunjavanje upitnika traje približno 5–7 minuta.

Rb.	Pitanje	Tip odgovora
1	Pol ispitanika	Muški / Ženski / Ne želim da odgovorim
2	Starosna grupa	18–25 / 26–35 / 36–45 / 46+
3	Stepen obrazovanja	Srednja škola / Osnovne / Master / Doktorske
4	Da li ste ranije koristili kriptovalute?	Da / Ne
5	Koliko dobro poznajete pojam kriptovaluta?	Likert 1–5
6	Da li smatrate da kriptovalute olakšavaju prikrivanje identiteta učinioca?	Likert 1–5
7	Da li kriptovalute olakšavaju pranje novca?	Likert 1–5
8	Da li se kriptovalute često povezuju sa ransomware napadima?	Likert 1–5
9	Da li su domaći propisi dovoljni za suzbijanje zloupotreba?	Likert 1–5
10	Da li je potrebna stroža kontrola pružalaca usluga digitalne imovine?	Likert 1–5
11	Da li anonimni novčanici i mikseri otežavaju dokazivanje krivičnih dela?	Likert 1–5
12	Da li međunarodna saradnja ima presudan značaj u ovom području?	Likert 1–5
13	Koji oblik zloupotrebe smatrate najopasnijim?	Višestruki izbor
14	Da li krivične sankcije imaju dovoljan preventivni efekat?	Likert 1–5
15	Da li biste podržali obaveznu identifikaciju korisnika na svim kripto-plattformama?	Da / Ne / Nisam siguran/na
16	Da li biste podržali specijalizovanu obuku policije, tužilaštva i sudova?	Da / Ne
17	Da li smatrate da je potrebno unaprediti oduzimanje digitalne imovine?	Likert 1–5
18	Po vašem mišljenju, koji je najveći problem u suzbijanju zloupotreba kriptovaluta?	Otvoreno pitanje

Hvala na učešću!