UDC: 351.817:343.983 Info M str. 36-42

FORENZIKA BLOKČEJNA KRIPTOVALUTE BITKOIN: PREGLED TEHNIKA I ALATA
BITCOIN BLOCKCHAIN FORENSICS: A SURVEY OF TECHNICS AND TOOLS

Milica Matijević Gostojić, Goran Sladić, Željko Vuković, Slaviša Đukanović

REZIME: Forenzička praksa u digitalnom domenu pokazala je da je kriptonovac u središtu velikog broja sudskih procesa koji uključuju digitalne dokaze. Kako je transakcije kriptonovca teško pratiti i deanonimizovati, s obzirom na tehnologiju blokčejn, veliki značaj imaju tehnike i alati kreirani sa ciljem da istražiteljima u tome pomognu. U ovom radu izloženo je trenutno stanje u polju forenzike blokčejna sa fokusom na tehnike i alate koji se koriste prilikom forenzičkih istraga transakcija u kriptovaluti bitkoin. U obzir su uzete tehnike i alati koji su besplatni i/ili otvorenog koda.

KLJUČNE REČI: digitalna forenzika, blokčejn, kriptovaluta, bitkoin

ABSTRACT: Digital forensics practice shows that a digital currency widely appears in legal cases that involve digital evidence. As blockchain makes cryptocurrency transactions hardly traceable and de-anonymizable, there are a lot of tools and techniques that are created to help digital forensic investigators. In this paper, we study the current state of the blockchain forensics field focusing on tools and techniques that are used in digital forensic investigations of bitcoin transactions. We considered techniques and free and/or open-source tools.

KEY WORDS: digital forensics, blockchain, cryptocurrency, bitcoin

1 UVOD

Organizovane kriminalne grupe svoje aktivnosti sve više baziraju na kriptonovcu [1], te se kriptonovac, izuzimajući njegovu legitimnu upotrebu, više ne vezuje samo za kriminalne aktivnosti u digitalnom prostoru, već za kriminalne aktivnosti uopšte [2]. Otuda podstrek za istraživanje i razvoj forenzičkih tehnika i alata kojima je u određenoj meri moguće proniknuti u sled događaja od interesa u koji se sudovi mogu pouzdati. To znači da je istragu potrebno izvršiti pouzdanim alatom koji će istragu učiniti efikasnom, pa i pomoću više alata da bi se potvrdila podudarnost rezultata i učvrstila njihova validnost [3]. Takođe, u operativnom radu policijskih službenika, koji forenzičkim istražiteljima obezbeđuju materijal za istragu, neophodni su softverski alati za pravovremeno prikupljanje informacija [4]. Međutim, pravna branša u Republici Srbiji ne krije veće poverenje u upotrebu komercijalnih alata u odnosu na besplatne alate, što naročito finansijski neopskrbljenim laboratorijama za digitalnu forenziku, koje se late besplatnih alata ili alata otvorenog koda, može otvoriti put ka osporavanju nalaza i mišljenja. Iz tog razloga je neophodno razumevanje načina funkcionisanja alata koji se koriste od strane istražitelja da bi se na sudu mogla dokazati validnost rezultata proizvedenih takvim alatima, kao i svesnost o postojanju velikog broja alata kroz čiju upotrebu treba dati potporu istrazi.

Nakon što je predstavljena kriptovaluta bitkoin 2009. godine [5], varijacijama u algoritmima heširanja i tehnikama anonimizacije nastale su i mnoge druge kriptovalute [6]. Međutim, bitkoin je do danas najpopularnija kriptovaluta [2, 7], stoga se za nju vezuje enormna količina podataka među kojima se mogu sakriti tragovi neregularnih transakcija i uopšte, tragovi aktivnosti zlonamernih korisnika, koje je sve teže pronaći. Da bi istraga nelegalnih aktivnosti koje uključuju kriptonovac bila uspešna, neretko je potrebna saradnja između veštaka iz oblasti informacionih tehnologija koji poznaje digitalnu forenziku kao nauku, pravnih tela i menjačnica koje obezbeđuju konverziju u virtuelne valute [8]. Pri tome je obaveza veštaka da poznaje tehnike i alate koji se u konkretnom slučaju mogu iskoristiti.

U ovom radu je dat prikaz tehnika koje su do trenutka pisanja aktuelne u forenzici blokčejna kriptovalute bitkoin kao i tabelarni prikaz besplatnih alata i/ili alata otvorenog koda kako bi se veštaku olakšalo upoznavanje sa trenutnim stanjem u oblasti forenzičke analize bitkoin blokčejna. Sa tradicionalnih tehnika za analizu podataka blokčejna vođenih heuristikama, većina metoda istrage je prešla na shvatanje blokčejna kao acikličnog usmerenog grafa, kod koga je do informacija moguće doći uz pomoć algoritama iz teorije grafova. Međutim, tehnike mašinskog učenja takođe su u poletu s ozbirom na potencijalno šablonske manevre u okviru bitkoin blokčejna i veliku količinu podataka, koje je ručno nemoguće analizirati. Nažalost, poneki od besplatnih alata/alata otvorenog koda, koji su uzeti u obzir u ovome radu sadrže referencu ka komercijalnim alatima i komentar o njihovoj većoj efikasnoti.

U odeljku 2 ovog rada obrađene su teorijske osnove protokola blokčejn vezanog za kriptovalutu bitkoin i digitalne forenzike sa fokusom na forenziku bitkoin blokčejna. Zatim je u odeljku 3 dat pregled relevantne literature. U odeljku 4 predstavljene su tehnike analize bitkoin blokčejna, dok su u odeljku 5 tabelarno prikazani alati kojima su neke od pomenutih tehnika implementirane. Odeljak 6 bavi se studijom slučaja forenzike bitkoin blokčejna i odeljak 7 sadrži zaključak.

2 TEORIJSKE OSNOVE

Za razumevanje tehnika i načina funkcionisanja alata koji se koriste u forenzičkoj analizi blokčejna, neophodno je upoznavanje sa pojmom blokčejna koji se u ovom radu vezuje za kriptovalutu bitkoin, kao i sa pojmom digitalne forenzike i forenzike blokčejna.

2.1 *Blokčejn kriptovalute bitkoin*

Tehnologije na kojima se zasniva funkcionisanje kriptovaluta su blokčejn i „tačka-tačka“ mreža [9]. Blokčejn predstavlja bazu podataka o transakcijama kriptonovca, koja se može

svesti na termin „glavne knjige“. Međutim, blokčejn je decentralizovan sistem, jer jedne te iste podatke blokčejna održava i kontroliše distribuirana mreža servera, odnosno, čvorova, koji komuniciraju po tačka-tačka principu [10]. Kako je blokčejn decentralizovan, ne postoji centralni autoritet, a informacije su zaštićene enkripcijom [11].

Informacije o transakcijama izvršenim između čvorova mreže ne mogu biti izmenjene niti obrisane. Transakcije blokčejna smeštene su u blokove sa uputstvima za verifikaciju validnosti transakacija i informacijama o prethodnom bloku. Mehanizam funkcionisanja blokčejna sastoji se u dodavanju pomenutih blokova po sledećem principu: korisnik koji uspostavi konsenzus za dodavanje novog bloka, inicira transakciju, odnosno transfer kriptonovca iz jednog digitalnog novčanika u drugi. Ovaj zahtev za transakcije biva razaslan svima u tačka-tačka mreži nakon čega čvorovi vrše verifikaciju zahtevanih transakcija u bloku. Ako je verifikacija uspešna, u blokčejn se dodaje blok sa transakcijama koje sadrže informacije o uplatiocu, primaocu, sumi i datumu transfera kriptonovca, a u digitalni novčanik primaoca dospeva data količina kriptonovca [11]. Pri tome, uplatilac i primalac kriptonovca reprezentovani su adresama, dugačkim nizovima karaktera koji se mogu kriptografski potpisati i koji kriju identitet uplatioca i primaoca. Uz to je uobičajeno da se ove adrese menjaju s vremena na vreme sa ciljem dodatnog obezbeđivanja anonimnosti [7].

U slučaju kriptovalute bitkoin, protokol kojim se postiže konsenzus za dodavanje novog bloka u blokčejn, naziva se rudarenje (eng. *mining, proof-of-work*), a korisnici koji su u trci za postizanje konsenzusa nazivaju se rudarima (eng. *miners*). *Rudarenje podrazumeva rešavanje računski izuzetno komplikovanog problema, koji zahteva veliku računsku moć hardverske opreme. Što je veća računska moć, veća je verovatnoća postizanja konsenzusa. Tako rudari, za stavljanje na raspolaganje svoje hardverske moći funkcionisanju blokčejna i korisnicima koji koriste kriptonovac, dobijaju određenu nadoknadu u kriptonovcu (eng. block reward) i proviziju od svake transakcije novododatog bloka (eng. transaction fee) [7].*

2.2 *Digitalna forenzika*

Digitalna forenzika se definiše kao primena naučnih metoda na proces koji obuhvata identifikaciju, prikupljanje, pregledanje, analizu i prezentaciju digitalnih tragova u cilju rekonstrukcije događaja okarakterisanih kao kriminalne. Tokom faze identifikacije u okviru forenzičkog procesa, istražitelj određuje koje digitalne uređaje sa mesta zločina će istražiti. Identifikovanim digitalnim uređajima istražitelj pristupa radi prikupljanja sirovih podataka, nad kojima potom vrši pregledanje čime sirovi podaci istražitelju postaju razumljivi. Digitalni tragovi, koji na sudu mogu postati dokazi, proističu analizom pregledanih podataka. Na kraju, pronađeni tragovi se prezentuju, najčešće u vidu Nalaza i mišljenja veštaka, kako bi bili adekvatno predstavljeni na sudu [12].

U zavisnosti od digitalnog uređaja ili skladišta podataka, oblast digitalne forenzike deli se na podoblasti kao što su forenzika masovne memorije, forenzika radne memorije, forenzika računarskih mreža, forenzika multimedijalnih zapisa, forenzika aplikacija, forenzika mobilnih uređaja, ali i usko specijalizovane oblasti kao što je forenzika blokčejna, koja se najčešće vezuje za kriptonovac.

Forenziku bitkoin blokčejna posmatraćemo u užem smislu, što podrazumeva onlajn praćenje transakcija u blokčejnu bez zadiranja u podatke skladištene na čvrstom disku ili u radnoj memoriji konkretnog računara. Cilj forenzičke istrage bitkoin blokčejna je najčešće deanonimizacija korisnika, što se postiže praćenjem transakcija do transakcije koja sadrži poznatu adresu, odnosno, adresu menjačnice koja je izvršila konverziju stvarnog novca u digitalni ili obrnuto. Međutim, ovde treba napomenuti da postoje menjačnice koje od svojih klijenata ne zahtevaju registraciju, odnosno, otkrivanje identiteta. Ipak, u slučajevima u kojima nije moguća deanonimizacija, tragovi koji se dobiju klasterovanjem adresa ili očitavanjem metapodataka transakcija, mogu biti korisni u pojedinim procesima.

Zlonamernim korisnicima bitkoin blokčejna na raspolaganju su servisi i metode koji omogućuju dodatnu privatnost. Razume se da takvi servisi i metode otežavaju istragu forenzičarima. Neki od njih su kripto-mikseri (eng. *crypto-mixers*), slojevite transakcije (eng. *layering transactions*) i „oguljeni“ lanci (eng. *peel chain*). Kripto-mikseri su servisi kojima je moguće prikriti izvor novca tako što se izvrši uplata u tzv. bazen iz koga potom novac može biti povučen ali u različitim svotama. Princip slojevitih transakcija uključuje više transakcija za potrebe jednog transfera novca, čime se zatire trag novca koji se uplaćuje na krajnju adresu. Na kraju, princip „oguljenog“ lanca podrazumeva lanac transakcija u kome se od svake transakcije odbija po mala količina novca, koji se povrati [13].

3 PREGLED LITERATURE

U ovom odeljku predstavljeni su pregledni radovi koji se bave tehnikama i/ili alatima forenzike blokčejna bilo da je u pitanju bitkoin ili druga kriptovaluta.

Tehnike analize strukture podataka blokčejn vezane za sistem kriptovalute bitkoin opisane su u [8]. U radu je dat detaljan opis aktuelnih tehnika, kako onih koje su se pokazale uspešne, tako i onih neuspešnih.

Istraživanjem na temu analize transakcija vezanih za kriptovalute tehnikom analize podataka (eng. *data mining*) bave se autori rada [14]. Takođe, pružaju uvid u alate koji se koriste za analizu pomenutih transakcija, kao i alate za vizualizaciju podataka pohranjenih u blokčejnu. Alati su grupisani u tri grupe: alati za dobavljanje, transformisanje podataka, alati za vizualizaciju podataka i onlajn platforme za analizu transakcija u realnom vremenu. Aspekti digitalne forenzike koji su obrađeni u ovom radu su praćenje transakcija i protivmere praćenja transakcija, kao i analiza korisničkog ponašanja kao individue i grupno. Na kraju, autori su diskutovali tehnike i alate koje su uzeli u obzir iznevši njihove prednosti i mane. Našim radom upotpunjujemo prikaz tehnika i njima pridružujemo opsežniji prikaz alata.

Za razliku od prethodnog rada, autori rada [7] tehnici analize podataka dodaju tehniku baziranu na teoriji igara (eng.

game theory) i tehniku koja se bazira na analizi grafova. Kroz mali skup alata, rad se dotiče istrage malicioznih aktivnosti blokčejna digitalne valute. Ovi alati pomažu pri praćenju transfera digitalnog novca kroz transakcije, pri analizi mreže korisnika u potrazi za malicioznim ponašanjem, kao i pri analizi aktivnosti u toku kojih je došlo do konverzije stvarne valute u digitalnu i obrnuto. Međutim, za digitalnu forenziku umnogome najznačajniji aspekt digitalnog novca – deanonimizacija blokčejn korisnika, u radu je kratko komentarisan.

Diskusiju o efikasnosti alata koji se koriste pri analizi kriminalnih aktivnosti u okviru blokčejna kriptovaluta beleže autori rada [15]. Alati su sagledani sa četiri aspekta: deanonimizacija korisnika, istraga ekonomske prirode blokčejna kriptovalute, istraga tržišta kriptovaluta i programski jezik kojim su implementirani protokoli za razmenu digitalnih valuta. Pored ova četiri aspekta, autori daju taksonomiju analitičkih pristupa koji karakterišu pojedine alate: analiza veza, analiza metapodataka, analiza toka novca, analiza korisničkog ponašanja, analiza transakcionih provizija i analiza digitalnog tržišta, odnosno, digitalnih novčanika. Potencijlna mana ovog istraživanja je siromašan skup diskutovanih alata, te je intencija našeg rada obogaćivanje ovoga skupa.

4 TEHNIKE ANALIZE BLOKČEJNA KRIPTOVALUTE BITKOIN

U ovom poglavlju dat je pregled tehnika koje se uspešno primenjuju u analizi blokčejna kriptovalute bitkoin. Pregled je nastao sjedinjavanjem najnovijih istraživanja na ovu temu i konciznim organizovanjem suštinskih zapažanja.

4.1 *Analiza blokčejna vođena heuristikama*

Tehniku koja se bazira na heuristikama su predstavili autori u radu [16] tvrdivši da ona može dovesti do otkrivanja identiteta korisnika kriptovalute bitkoin. To se potencijalno postiže grupisanjem sličnih transakcija i njihovim povezivanjem sa vlasnicima adresa koje se u transakcijama pominju. Ove grupe, ili klasteri, otkrivaju šablone, strukturu i veze, što daje predstavu o hronološkom toku transakcija [17]. Neke od heuristika su višestruke uplate (eng. *multiple inputs*), heuristika kusura (eng. *coin change*) i vremenske heuristike (eng. *temporal heuristics*) [14].

Heuristika višestruke uplate jedna je od najšire upotrebljenih heuristika pri analizi blokčejna. Sastoji se u rezonu da sve adrese vezane za uplatioca u okviru transakcije pripadaju istom korisniku, s obzirom na činjenicu da je nakon inicijacije transakcije, korisnik u obavezi da digitalno potpiše transakciju pomoću privatnih ključeva svih adresa kojima se kriptonovac uplaćuje.

Heuristika kusura nalaže da u okviru jedne transakcije, vrednost koja se uplaćuje mora biti jednaka vrednosti koja je uplaćena. U slučaju da se ove vrednosti razlikuju, razlika, odnosno, kusur, mora biti vraćena inicijatoru transakcije, odnosno, uplatiocu. Vrednost kusura u transakciji sa bar dve adrese pošiljaoca mora biti manja od obe vrednosti pri adresama pošiljaoca. Takođe, uobičajeno je da kusur karakteriše više decimalnih mesta u odnosu na vrednost koja se uplaćuje.

Vremenske heuristike vezane su za specijalne servise koje nudi blokčejn kriptovalute, zvane servisi mešanja (eng. *mixing services*). Ove heuristike iskorišćavaju vremenske atribute depozitnih transakcija i transakcija kusura.

Klasterovanje adresa svrstava se u tradicionalne pristupe analizi blokčejna kriptovalute, koje nisu efikasne u slučaju upotrebe više adresa po transakciji [9].

Pored navedenih heuristika, treba spomenuti i heuristiku ponovnog korišćenja (eng. *reuse*) i heuristiku tipa adrese (eng. *address type*). Prema prvoj, ako je jedna od dve adrese primaoca nova u blokčejnu, a druga nije, onda je nova adresa najverovatnije adresa na koju se uplaćuje kusur. Prema drugoj, ako su adrese pošiljaoca istog tipa (ili sve počinju sa 1 ili sve počinju sa 3 ili sve počinju sa bc1) i samo jedna adresa primaoca je tog tipa, onda je ta adresa, adresa na koju se uplaćuje kusur.

4.2 *Primena teorije grafova pri analizi blokčejna*

Kako se blokčejn može posmatrati kao usmereni aciklični graf čiji su čvorovi i ivice različiti koncepti bitkoin sistema, to su se javili pristupi rešavanju problema pseudoanonimnosti u okviru blokčejna koji se baziraju na analizi grafa. Postoji nekoliko pristupa baziranih na strukturi grafa. Graf čiji čvorovi predstavljaju transakcije, a ivice su izlazne sume digitalnog novca koje povezuju transakcije. Zatim, graf čiji su čvorovi adrese, odnosno javni ključevi, a ivice predstavljaju transakcije usmerene od izvorne ka odredišnoj adresi. Na kraju, sreću se klaster-grafovi, koji se od prethodnih razlikuju po tome što čvorove čine klasteri adresa, a ne adrese pojedinačno [18].

Pomenute vrste grafa smatraju se grafovima sa karakteristikama (eng. *property-graphs*), s obzirom na to da za svaki čvor i ivicu može biti vezano više karakteristika kao što su stepen grafa, temporalne karakteristike transakcija, pripadnost određenom klasteru itd. Iteracijom kroz graf i kalkulacijama sa ovim karakteristikama, moguće je doći do zaključaka o toku digitalnog novca kao i o vezama između adresa [18].

Pored prolaska kroz graf radi kalkulacija sa karakteristikama čvorova i ivica, pristup analizi može biti i potraga za podgrafom koji odgovara određenom šablonu [18]. Neke od varijacija ovog pristupa su „razbijanje“ grafa na dva manja [17] ili više podgrafova [19]. Rezultat ove analize može biti identifikovanje bihevioralnih karakteristika toka transakcija.

Automatska analiza blokčejna bazirana na analizi grafova obuhvata programe koji vrše parsiranje podataka blokčejna kako bi se izdvojili podaci o transakcijama i adresama. Parsirani podaci se potom kontekstualizuju i vizualizuju uz pomoć dodatnih informacija nastalih kao rezultat automatske pretrage veba [8].

Kao i u slučaju automatske analize blokčejna, analiza upotrebom algoritama rezultuje kontekstualizacijom podataka blokčejna dolaskom do informacija iz različitih eksternih izvora kao što su veb-forumi, društvene mreže, veb-sajtovi itd. Jedan primer algoritamske analize blokčejna uključuje algoritam Page Rank [20], dok drugi koristi algoritam Bread First Search. Međutim, tehnika pronalaženja kritičnih čvorova grafa [21] najzastupljenija je u otkrivanju neregularnih transakcija [8].

4.3 *Primena tehnika mašinskog učenja pri analizi blokčejna*

Među tehnikama mašinskog učenja koje se koriste za analizu podataka blokčejna izdvajaju se duboko učenje (eng. *deep learning*), grafovske neuronske mreže (eng. *graph neural networks*) i grafovske konvolutivne mreže (eng. *graph convolutional network*) [8]. Tehnika dubokog učenja bazira se na algoritmu struc2vec i pomaže u otkrivanju sumnjivih veza između čvorova [22]. Dizajn grafovskih neuronskih mreža služi učenju niskodimenzionalnih grafovskih struktura koje se koriste za identifikovanje zlonamernih korisnika ili skrivenih „rudara“ [9]. Grafovske konvolutivne mreže koriste se za skupljanje informacija o vezama između čvorova, što predstavlja pripremu za upotrebu drugih tehnika mašinskog učenja [23].

Pored navedenog, autori rada [24] svedoče o upotrebi tehnika nadgledanog mašinskog učenja za etiketiranje transakcija kao neregularnih. Među ovim tehnikama se izdvajaju logistička regresija (eng. *logistic regression*), višenivovski binarni klasifikator (eng. *multilayer perceptron*), klasifikator *Naive Bayes, algoritam za poboljšanje performansi binarnih klasifikatora AdaBoost (Adaptive Boosting), stablo odlučivanja (eng. Decision Tree), metoda potpornih vektora (eng. Support Vector Machine, SVM), klasifikator Random Forest i neuronske mreže (eng. Neural Networks). Navedeni algoritmi imaju različit učinak u otkrivanju neregularnih transakcija, što prikazuje* Tabela 1.

Algoritam	Tačnost
Logistička regresija	0,96
Višenivovski binarni klasifikator	0,91
Klasifikator Naive Bayes	0,89
AdaBoost	0,97
Stablo odlučivanja	0,96
Metoda potpornih vektora	0,97
Klasifikator Random Forest	0,97
Neuronske mreže	0,94

Tabela 1 *Tačnost algoritama nadgledanog mašinskog učenja u otkrivanju neregularnih transakcija*

4.4 *Rezime tehnika analize bitkoin blokčejna*

Radi komparacije tehnika analize blokčejna opisanih u prethodna tri odeljka, u ćelijama Tabele 2 prikazani su ciljevi koje pristupi pomenutih tehnika treba da postignu pri analizi blokčejna.

Pristup tehnike analize blokčejna	Cilj
Heuristika višestruke uplate	Grupisanje adresa po pripadnosti istom novčaniku
Heuristika kusura	Određivanje adrese kusura, odnosno, adrese koja pripada novčaniku uplatioca
Vremenske heuristike	Otkrivanje šablona u ponašanju korisnika koji koriste servise mešanja
Heuristika ponovnog korišćenja	Određivanje adrese kusura
Heuristika tipa adrese	Određivanje adrese kusura
G(transakcije, izlazne sume)	Zaključivanje o toku digitalnog novca i vezama između adresa
G(adrese, transakcije)	
G(klaster adresa, transakcije)	
Razbijanje grafa na dva podgrafa	Identifikovanje bihevioralnih karakteristika toka transakcija
Razbijanje grafa na više grafova	
Parseri podataka blokčejna bazirani na analizi grafova	Kontekstualizacija podataka blokčejna
Page Rank algoritamska analiza blokčejna	
Bread First Search algoritamska analiza blokčejna	
Tehnika pronalaženja kritičnih čvorova grafa	
Duboko učenje	Otkrivanje sumnjivih veza između čvorova
Grafovske neuronske mreže	Identifikovanje zlonamernih korisnika ili skrivenih „rudara“
Grafovske konvolutivne mreže	Skupljanje informacija o vezama između čvorova
Nadgledano mašinsko učenje	Etiketiranje transakcija kao neregularnih

Tabela 2: *Rezime tehnika analize blokčejna*

5 ALATI ZA ANALIZU BLOKČEJNA KRIPTOVALUTE BITKOIN

Neke od navedenih tehnika, koje se koriste u forenzičkoj analizi podataka finansijskog blokčejna implementirane su u okviru alata koji se potencijalno mogu koristiti prilikom forenzičke istrage. U ovom odeljku dat je tabelarni pregled pomenutih alata i njihova veza sa tehnikama koje primenjuju. Takođe, zabeleženi su komentari u vezi sa održavanjem alata i operativnim sistemom/sistemima za koje postoje izvršne datoteke alata.

Naziv	Godina revizije	Operativni sistem	Opis/Tehnika
Bitiodine[1]	2013	Linux	Automatska analiza bazirana na analizi grafa; Ekstrakcija, transformacija i skladištenje blokčejn podataka
Numisight[2]	2015	Windows Mac	Automatska analiza bazirana na analizi grafa
Maltego[3]	2023	Linux Windows Mac	Automatska analiza bazirana na analizi grafa
Learnmeabitcoin.com[4]	neažurna baza podataka	onlajn	Automatska analiza bazirana na analizi grafa
Blockchain.info[5]	2023	onlajn	Sadrži informacije kao što su poznate adrese korisnika
Blockchair[6]	2023	onlajn	Prikaz blokčejn podataka i procena sigurnosti transakcija
WalletExplorer[7]	2023	onlajn	Sadrži informacije kao što su poznate adrese korisnika
Blockchain2graph[8]	2020	Linux Windows	Ekstrakcija, transformacija i skladištenje blokčejn podataka
BlockSci[9]	2020	Potrebno je kompajlirati	Ekstrakcija, transformacija i skladištenje blokčejn podataka
BTCSpark[10]	Ne održava se	Potrebno je kompajlirati	Ekstrakcija, transformacija i skladištenje blokčejn podataka
bitcoin-etl[11]	2021	Potrebno je kompajlirati	Ekstrakcija, transformacija i skladištenje blokčejn podataka
rusty-blockparser[12]	2023	Potrebno je kompajlirati	Ekstrakcija, transformacija i skladištenje blokčejn podataka
btctrackr[13]	2018	Potrebno je kompajlirati	Ekstrakcija, transformacija i skladištenje blokčejn podataka
BlockchainVis[14]	2020	Linux Windows Mac	Vizualizacija
Blockchain 3D Explorer[15]	2022	onlajn	Vizualizacija
OXT[16]	2023	onlajn	Vizualizacija
KYCP[17]	2023	onlajn	Automatska analiza bazirana na podacima alata OXT
Bitcoin Big Bang[18]	2023	onlajn	Vizualizacija
BitInfoCharts[19]	2023	onlajn	Vizualizacija
BitNodes[20]	2023	onlajn	Vizualizacija

1 https://github.com/tzarskyz/bitiodine
2 https://bitbucket.org/numisight/explorer/downloads/
3 https://www.maltego.com/
4 https://learnmeabitcoin.com/
5 https://www.blockchain.com/explorer

6 SLUČAJ UPOTREBE

Pranje novca (eng. *money laundering*) je najčešći vid zloupotrebe tehnologije blokčejn [1], stoga je reprezentativan slučaj za istragu pomoću nekih od pomenutih alata, krađa bitkoina iz digitalnog novčanika britanske menjačnice Cashaa 11. jula 2020. godine[21]. Stoga je u ovom odeljku predstavljen put kojim bi jedan forenzičar mogao ići rešavajući ovaj slučaj.

Na adresu digitalnog novčanika 14RYUUaMW1shoxCav4znEh64xnTtL3a2Ek nelegalno je uplaćeno 335,91312085 bitkoina. Zadatak istražitelja je da uđe u trag vlasniku ove adrese.

Ako se izvrši uvid u detalje adrese 14RYUUaMW1shoxCav4znEh64xnTtL3a2Ek pomoću alata blockchain.com, primećuje se da je ova adresa učestvovala kao pošiljalac u dve transakcije, a kao primalac, u tri transakcije, računajući i transakciju u kojoj je na ovu adresu uplaćeno 335,91312085 bitkoina. Najpre je na ovu adresu sa adrese 1Jt9mebBwqCk8ijrVDoT5aySu2q9zpeKde uplaćeno 1.05977049 bitkoina, a zatim je ista suma novca isplaćena na adresu 3GsH7DpsL38RqxXwKMhpPXN7EtBQtkMufS. Kako transakcija u kojoj je izvršena isplata poseduje još tri adrese sa kojih je novac isplaćen, rezon istražitelja bi trebalo da bude hipoteza da pomenute tri adrese pripadaju istom virtuelnom novčaniku kao i adresa 14RYUUaMW1shoxCav4znEh64xnTtL3a2Ek, odnosno, istom korisniku. Većina alata za analizu bitkoin blokčejna poseduje funkciju klasterovanja adresa. Na primer, onlajn alat WalletExplorer se može iskoristiti za potvrđivanje istražiteljeve hipoteze. Dakle, u ovom koraku, istražitelj zna koje još adrese potencijalno pripadaju zlonamernom korisniku i može dalje da ih prati.

Praćenje toka kriptonovca dalje je najlakše pomoću alata koji omogućava vizuelni uvid. Alat OXT služi ovoj svrsi ako se pođe od transakcije koja sadrži spornu adresu na koju je uplaćena enormna količina kriptonovca sa adresa menjačnice Cashaa (abb197c3dbdec3a0884da38098bc0ef2412b801d55e7287298b0f0082cf86a7e). Kako se proširuje lanac transakcija, tako se uviđa šablon po kome se kriptonovac kreće – šablon „oguljenog“ lanca (eng. *peel chain*). Na Slici 1 prikazane su pomenute transakcije. Transakcije koje imaju jednu adresu uplatioca i dve (ponegde i tri) adrese primaoca, račvaju se dok istražitelj ne dođe do transakcija u kojima učestvuju adrese menjačnica, koje je alat prethodno indeksirao. Nazivi menjačnica su ispisani na Slici 1.

6 https://blockchair.com/
7 https://www.walletexplorer.com/
8 https://github.com/straumat/blockchain2graph
9 https://github.com/citp/BlockSci
10 https://github.com/JeremyRubin/BTCSpark
11 https://github.com/blockchain-etl/bitcoin-etl
12 https://github.com/gcarq/rusty-blockparser
13 https://github.com/qshuai/btctracker
14 https://github.com/csuvis/BlockchainVis
15 https://blockchain3d.info/
16 https://oxt.me/
17 https://kycp.org/#/
18 https://info.elliptic.co/hubfs/big-bang/bigbang-v1.html
19 https://bitinfocharts.com/
20 https://bitnodes.io/
21 https://help.cashaa.com/knowledgebase/cashaa-india-otc-bitcoin-hack-update/?source=post_page-----96351bcbff76

Dolaskom do adresa za koje alat tvrdi da pripadaju određenim menjačnicama, istražitelj je učinio veliki korak, s obzirom na to da menjačnice potencijalno sadrže registrovane korisnike adresa na koje je kriptonovac uplaćen sa adresa menjačnice, odnosno, sadrže identitet korisnika. Dakle, uz pravno obraćanje datim menjačnicama potencijalno je moguće deanonimizovati zlonamerne korisnike.

7 ZAKLJUČAK

Postoji opsežno istraživanje u oblasti analize bitkoin blokčejna sa fokusom kako na tehnikama, tako i na alatima. Međutim, sa aspekta pravosuđa, upotreba mnogih alata i predlaganih tehnika od strane istraživača nije dovoljno održavana niti testirana, a samim tim nije ni pouzdana u misiji produkovanja dokaza u sudskom postupku. U ovome radu su izložene tehnike analize bitkoin blokčejna od kojih su neke implementirane u okviru navedenih alata. Alati su besplatni ili otvorenog koda, što znači da su potpuno transparentni za oko istražitelja koji traži opravdanje za pouzdanje u njihovu upotrebu.

Mnogi alati za analizu bitkoin blokčejna implementiraju heuristike na osnovu kojih vode kroz istragu. Ipak, istražitelji nikako ne bi trebalo u potpunosti da se pouzdaju u rezultate alata prilikom sastavljanja Nalaza i mišljenja, već da u Nalazu iznesu objašnjenje postupka koji je upotrebom alata doveo do određenih rezultata. Naročitu opreznost bi istražitelj trebalo da pokloni alatima koji implementiraju neku od tehnika mašinskog učenja ili veštačke inteligencije uopšte.

Da bi istraga, odnosno, analiza bitkoin blokčejna bila uspešna, potreban je, ne samo pouzdan alat, već i ekspert-istražitelj. Bez poznavanja šablona koje karakterišu anomalije u toku transakcija, istražitelju ni jedan alat za vizualizaciju ne može pomoći. Takođe, istražitelj mora da ima u vidu sve heuristike koje mu mogu pomoći u rezonu, kako bi mogao razumeti rezultate alata koji se na heuristikama baziraju. Na kraju, dobro razumevanje implementacije tehnika za analizu bitkoin blokčejna ključno je za transfer znanja ka pravnoj branši koja odlučuje o prihvatanju, odnosno, odbacivanju tragova pronađenih od strane digitalnog istražitelja.

Posmatrajući sa aspekta tradicionalnog finansijskog sistema, u kome postoji centralni autoritet, pojava kriptovaluta predstavlja anomaliju, koja sa rastom svojih pristalica sve više problema zadaje državnim težnjama ka regulaciji. Stoga je za očekivati da upotreba kriptovaluta u skorijoj budućnosti bude regulisana u toj meri da je, bez obzira na konkretnu kriptovalutu, moguće doći do tragova koji vode do deanonimizacije korisnika.

8 LITERATURA

[1] Elsayed, S. (2023). Cryptocurrencies,corruption and organised crime, U4 Helpdesk Answer 2023.

[2] Europol, (2022). Cryptocurrencies: Tracing the evolution of criminal finances, Europol.

[3] 27037, 2015. ISO/IEC 27037:2012 – Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Institute for Standardization of Serbia.

[4] Milunović, M., Đukanović, S., Košanin, I., Pejčić, B., Kolavčić, I., & Marinković1, V. (2022) Primena savremenih softverskih alata u mapiranju bezbedonosno interesantnih objekata i pojava. YUINFO 2022.

[5] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. Pdf, 4(2), 15.

[6] Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. Forensic Science International: Digital Investigation, 46, 301576.

[7] Tovanich, N. (2022). Visual Analytics for Monitoring and Exploration of Bitcoin Blockchain Data (Doctoral dissertation, Université Paris-Saclay).

[8] Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Analysis techniques for illicit bitcoin transactions. Frontiers in Computer Science, 2, 600596.

[9] Li, Z., & He, E. (2023). Graph Neural Network-Based Bitcoin Transaction Tracking Model. IEEE Access.

[10] European Parliament, (2018). Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion.

[11] Reddy, N. (2019). Practical cyber forensics. Apress.

[12] Årnes, A. (Ed.). (2017). Digital forensics. John Wiley & Sons.

[13] Salisu, S., & Filipov, V. (2023, February). Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 338-347).

[14] Liu, X. F., Jiang, X. J., Liu, S. H., & Tse, C. K. (2021). Knowledge discovery in cryptocurrency transactions: A survey. Ieee access, 9, 37229-37254.

[15] Balaskas, A., & Franqueira, V. N. (2018, June). Analytical tools for blockchain: Review, taxonomy and open challenges. In 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-8). IEEE.

[16] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., et al. (2013). "A fistful of bitcoins: characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (New York, NY), 127–140. doi: 10.1145/2504730.2504747.

[17] Reid, F., and Harrigan, M. (2011). "An analysis of anonymity in the bitcoinsystem," in 2011 International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing (Boston, MA). doi: 10.1109/PASSAT/SocialCom.2011.79

[18] Sharma, A., Agrawal, A., Bhatia, A., & Tiwari, K. (2022, March). Bitcoin's blockchain data analytics: A graph theoretic perspective. In International Conference on Advanced Information Networking and Applications (pp. 459-470). Cham: Springer International Publishing.

[19] Ron, D., and Shamir, A. (2012). Quantitative Analysis of the Full Bitcoin Transaction Graph. The International Association for Cryptologic Research (IACR) Cryptology ePrint Archive, 584.

[20] Fleder, M., Kester, M. S., and Pillai, S. (2015). Bitcoin transaction graph analysis. arXiv. preprint arXiv:1502.01657.

[21] Maesa, D. D. F., Marino, A., and Ricci, L. (2018). Data-driven analysis of Bitcoin properties: exploiting the users graph. Int. J. Data Sci. Anal. 6, 63–80. doi: 10.1007/s41060-017-0074-x

[22] Steenfatt, N., Nikolentzos, G., Vazirgiannis, M., and Zhao, Q. (2018). "Learning structural node representations on directed graphs," in International Conference on Complex Networks and their Applications (Cham: Springer), 132–144. doi: 10.1007/978-3-030-05414-4_11

[23] Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., et al. (2019). "Anti-money laundering in bitcoin: experimenting with graph convolutional networks for financial forensics," in Tutorial in the Anomaly Detection in Finance Workshop at the 25th SIGKDD Conference on Knowledge Discovery and Data Mining (Anchorage, AK).
[24] Bhowmik, M., Chandana, T. S. S., & Rudra, B. (2021, April). Comparative study of machine learning algorithms for fraud detection in blockchain. In 2021 5th international conference on computing methodologies and communication (ICCMC) (pp. 539-541). IEEE.

mast. inž. Milica Matijević Gostojić, asistent-master na Katedri za informatiku
Kontakt: matijevicmilica@uns.ac.rs
Oblasti interesovanja: informaciona bezbednost, digitalna forenzika, računarske mreže

prof. dr Goran Sladić, redovni profesor, šef Katedre za informatiku
Kontakt: sladicg@uns.ac.rs
Oblasti interesovanja: bezbednost informacionih sistema, bezbednost IoT sistema, bezbedan razvoj softvera, cloud tehnologije, upravljanje dokumentima i elektronsko poslovanje

doc. dr Željko Vuković, docent na Katedri za informatiku
Kontakt: zeljkov@uns.ac.rs
Oblasti interesovanja: softversko inženjerstvo vođeno modelima, integracija, bezbednost računarskih mreža

mr Slaviša Đukanović, pomoćnik načelnika Sektora za analitiku, telekomunikacione i informacione tehnologije u Sektoru za analitiku, telekomunikacione i informacione tehnologije
Kontakt: slavisa.djukanovic@mup.gov.rs
Oblasti interesovanja: telekomunikacije, informacione tehnologije, informaciona bezbednost

CIP – Каталогизација у публикацији Народна библиотека Србије, Београд 659.25:004
INFO M : časopis za informacione tehnologije i multimedijalne sisteme = journal of Information technology and multimedia systems / glavni i odgovorni urednik Miroslav Minović. - [Štampano izd.]. - God. 1, br. 1 (2002)- . - Beograd : Fakultet organizacionih nauka, 2002- (Smederevo : Newpress). - 30 cm
Dva puta godišnje. - Je nastavak: Info Science = ISSN 1450-6254. - Drugo izdanje na drugom medijumu: Info M (Online) = ISSN 2683-3646
ISSN 1451-4397 = Info M (Štampano izd.)
COBISS.SR-ID 105690636