Daniela Gavurová, Andrej Lipták

Podvodné konanie realizované prostredníctvom virtuálnych mien

Anotácia: Autori sa vo vedeckej práci venujú problematike, pre ktorú je typické využívanie virtuálnych mien ako alternatívneho digitálneho platobného prostriedku so zameraním na podvodné konanie. Neporušiteľnosť právom chránených záujmov je potrebné zaistiť aj v špecifickom prostredí virtuálnych mien. Špecifické prostredie so sebou prináša aj špecifické metódy a formy páchania trestnej činnosti, ktoré je potrebné efektívne poznávať aj vzhľadom na neustálu dynamiku skúmanej oblasti. V článku sa skúma podstata podvodného konania v sfére virtuálnych mien s cieľom vytvoriť logický rámec opierajúci sa o štatistické výstupy analýz transakcií s virtuálnou menou a o vybranú kazuistiku.

Kľúčové slová: virtuálne meny, podvodné konanie, decentralizované financie, trestná činnosť

Úvod

Riziká súvisiace s používaním virtuálnych mien sú v spoločnosti čoraz viac aktuálnejšie a ich závažnosť a relevancia rastie úmerne s nárastom používania virtuálnych mien. Virtuálne meny fungujú na špecifických technológiách, ich funkčnosť je zabezpečená kryptografickými riešeniami a mechanizmami, zahŕňajú decentralizované, distribuované systémy, sú udržiavané a zveľaďované odborne zdatnými osobami, teda predstavujú špecifický priestor, ktorý je potrebné poznávať aj najmä preto, že v rámci tohto priestoru môže a dochádza k rozmanitej trestnej činnosti.

Primárnym cieľom článku je s využitím prvkov kvalitatívneho výskumu poskytnúť odbornej a laickej verejnosti hlbší prienik do problematiky nelegálnych aktivít (podvodného konania), ich znakov a špecifík, priblíženie metód, foriem a techník, ktoré sa v priestore virtuálnych mien využívajú na páchanie tejto vybranej trestnej činnosti. Výstupy štatisticky zhrnutých dát vyplývajúcich z blockchain analýzy preukazujú skutočnosť, že v roku 2022 bol evidovaný nárast podvodných konaní súvisiacich s virtuálnymi menami. Je preto na mieste skúmať túto problematiku, analyzovať jej špecifiká a znaky a uceleným spôsobom poukázať na podvodné konania realizované prostredníctvom virtuálnych mien za účelom ochrany majetku potenciálnych poškodených a minimalizovania takýchto nezákonných aktivít.

1. VYMEDZENIE POJMOV

- Virtuálna mena - digitálny nositeľ hodnoty, ktorý nie je vydaný ani garantovaný centrálnou bankou, ani orgánom verejnej moci, nie je nevyhnutne naviazaný na zákonné platidlo a ktorý nemá právny status meny ani peňazí, ale je akceptovaný niektorými osobami ako nástroj výmeny, ktorý možno elektronicky prevádzať, uchovávať alebo s ním elektronicky obchodovať.[1]
- Transakcia s virtuálnou menou – kryptograficky založená reprezentácia elektronického prevádzania virtuálnej meny v distribuovanej sieti s využitím blockchain technológie.
- Kryptoaktívum - digitálne vyjadrenie hodnoty alebo práv, ktoré možno prenášať a elektronicky uchovávať s použitím technológie distribuovanej databázy transakcií alebo podobnej technológie.[2]

[1] § 131, ods. 7 – zákon č. 300/2005 Z.z. Trestný zákon.
[2] článok 3, bod 2. - Návrh nariadenia EURÓPSKEHO PARLAMENTU A RADY o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937.

- Peňaženka virtuálnej meny – technické zariadenie zaisťujúce ochranu súkromných kryptografických kľúčov v mene jej klientov, na držbu, uchovávanie a prevod virtuálnej meny.[3]
- Zmenáreň virtuálnej meny - obchodovanie s virtuálnou menou, ktorého predmetom je nákup virtuálnej meny za eurá alebo cudziu menu alebo predaj virtuálnej meny za eurá alebo cudziu menu.[4]
- Token - typ kryptoaktíva, ktorého účelom je zachovávať stabilnú hodnotu naviazaním na hodnotu viacerých fiat mien, ktoré sú zákonným platidlom, jednu alebo viaceré komodity alebo jedno či viacero kryptoaktív, alebo na hodnotu kombinácie takýchto aktív alebo je typ kryptoaktíva, ktoré sa má používať hlavne ako prostriedok výmeny a ktorého účelom je zachovávať stabilnú hodnotu naviazaním na hodnotu fiat meny, ktorá je zákonným platidlom alebo je typ kryptoaktíva, ktoré je určené na poskytovanie digitálneho prístupu k tovaru alebo službe.[5]

2. PODVODNÉ KONANIE

Pojem *podvod* je z právneho hľadiska definovaný ako konanie, pri ktorom dochádza k uvedeniu do omylu alebo využitiu omylu poškodenej osoby. Týmto konaním dochádza k obohateniu o majetok prípadne pokusu o obohatenie sa o majetok poškodenej osoby páchateľom.[6]

Základný znak podvodného konania môžeme charakterizovať ako uvedenie poškodenej osoby do omylu alebo prípadne využitie jej omylu. O omyle hovoríme vtedy, ak sa páchateľ snaží vylákať od poškodenej osoby peniaze na základe nepravdivých skutočností alebo využije nevedomosť poškodenej osoby. Sekundárnym znakom podvodu je dobrovoľné konanie poškodenej osoby. Ide o prípady, kedy osoba dá páchateľovi peniaze v dobrej viere, že dostane za ne určitý tovar, službu, či prospech.

Virtuálna mena sa stala populárnou vo svetle digitálnej ekonomiky a decentralizovanej finančnej sústavy. Spolu s jej popularitou sa však objavujú aj rôzne formy podvodov a zneužívania.

Virtuálne meny sa v praxi často označujú ako kryptomeny, tokeny či coiny. Vo všeobecnosti môžeme virtuálnu menu charakterizovať ako kryptomenu, ktorú nevydáva žiadna štátna autorita. Získava sa tzv. „ťažením“ digitálnych mincí nazývaných aj tokenov, za pomoci výpočtovej techniky. Jej využitie môžeme nájsť predovšetkým v investovaní na burzách ale aj na on-line platby. Vyťažené „mince“ je možné nakúpiť a zároveň aj spätne predávať za reálne peniaze. Medzi najznámejšie kryptomeny patria Bitcoiny, Litecoiny, Ripple a mnohé ďalšie.[7]

3. TYPOLÓGIA PODVODNÝCH KONANÍ REALIZOVANÝCH PROSTREDNÍCTVOM VIRTUÁLNYCH MIEN

- Rug Pull podvodné konania,

---

[3] § 9, písm. n) – zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[4] § 9, písm. o) – zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[5] článok 3, bod 3.,4.,5. - Návrh nariadenia E EURÓPSKEHO PARLAMENTU A RADY o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937.

[6] Prevencia kriminality.sk. [online] [cit. 14.04.2023]. Dostupné na internete:
< https://prevenciakriminality.sk/>.

[7] Finifo. sk.[online] [cit. 14.04.2023]. Dostupné na internete:
< https://www.fininfo.sk/fininfo/inovacie/kryptomeny/kryptomeny.html>.

    - Podvodné predaje tokenov,
    - Podvodné konanie v liquidity poole,
    - Maximum Extractable Value (MEV) bot podvodné konanie.
- Podvodné konania založené na budovaní vzťahov,
    - Podvodné konania založené na budovaní romantických vzťahov (ďalej aj „romániky“),
    - Podvodné konania založené na budovaní dlhodobých vzťahov.
- Phishingové útoky.
- Falošné ICO (Initial Coin Offering).
- Cryptojacking.

4. METÓDY VYKONÁVANIA PODVODVODNÝCH KONANÍ V PROSTREDÍ VIRTUÁLNYCH MIEN

- Vyčkávacia metóda.
- Wash-trading metóda.
- Pump metóda.
- Hedge metóda.

5. PODVODNÉ KONANIE VYKONÁVANÉ PROSTREDNÍCTVOM VIRTUÁLNYCH MIEN

Objektom skúmania tejto práce sú aj podvodné konania, teda konania, ktorých podstatou je obohatenie sa páchateľa na škodu cudzieho majetku tým, že využije niečí omyl, respektíve niekoho do omylu uvedie, páchané prostredníctvom virtuálnych mien. Abstrahujeme od podvodných konaní, ktoré súvisia s virtuálnymi menami len okrajovo, kde samotné podvodné konanie nepozostáva z fundamentu virtuálnych mien. Môžeme hovoriť napríklad o podvode, keď poškodený poskytne citlivé údaje k vlastnému bankovému účtu, resp. k debetnej alebo platobnej karte páchateľovi, ktorý poškodeného uvedie do omylu tak, že mu oznámi, že fiktívnym obchodovaním s virtuálnou menou dosiahol nárok na vyplatenie zisku z tejto činnosti, a že predmetné citlivé údaje potrebuje. Aj keď v tomto prípade sa virtuálne meny spomínajú, z fundamentálneho hľadiska virtuálne meny s týmto podvodným konaním špecifický súvis nemajú. Významným bolo uvedenie do omylu ľsťou, ktorú páchateľ spomenutím virtuálnych mien dosiahol, virtuálne meny však neboli použité ako špecifický nástroj páchania tohto podvodného konania.[8] Predmetom skúmania budú teda tie špecifické podvodné konania, pre ktoré je typické prostredie virtuálnych mien, resp. tie, ktoré by bez vykonania transakcie s virtuálnou menou nebolo možné vykonať. Páchateľom týchto podvodných konaní je osoba s patričným vzdelaním a erudíciou v oblasti virtuálnych mien, disponuje hardvérovým a softvérovým rozhraním a na realizovanie podvodných konaní využíva špecifické metódy, formy a techniky súvisiace s fundamentom virtuálnych mien.

Predmet skúmania zahŕňa:

5.1. Phishing

[8] Žene povedali, že vďaka bitcoinu zarobila tisíce eur. [online] [cit. 14.12.2022]. Dostupné na internete: < https://spravy.rtvs.sk/2022/12/zene-povedali-ze-vdaka-bitcoinu-zarobila-tisice-eur-islo-vsak-o-podvod/>.

Vo všeobecnosti môžeme phishing definovať ako druh kybernetického útoku, pri ktorom sa podvodníci snažia získať citlivé informácie od používateľov, akými sú heslá alebo súkromné kľúče k virtuálnym peňaženkám. Títo podvodníci sa často predstavujú ako oficiálni zástupcovia virtuálnych menových búrz alebo peňaženiek a vyzývajú používateľov na kliknutie na zavádzajúce odkazy alebo na poskytovanie svojich citlivých informácií. Obeťou phishingového útoku môže byť v podstate ktokoľvek, ktorákoľvek osoba s e-mailovým kontom.

Phishing sa často vyskytuje v súvislosti s virtuálnymi menami, pretože tieto sú často používané v transakciách na internete a môžu byť ľahko prevedené bez nutnosti fyzického prítomnosti používateľa. Podvodníci môžu používať rôzne spôsoby na získanie dôvery od používateľov, ako sú napríklad vydávanie sa za oficiálnych zástupcov kryptomenových búrz alebo projektov, ktoré používateľom ponúkajú zaujímavé príležitosti na investovanie, alebo vydávanie sa za známe osobnosti, ktoré majú veľký vplyv v kryptomenovej komunite. Phishing môže byť veľmi sofistikovaný a dôveryhodný. Podvodníci môžu používať techniky, ako sú napríklad úprava URL adries, aby sa zdali byť oficiálnymi, alebo napodobňovanie dizajnu a loga oficiálnych webových stránok. Útočníci môžu používať aj taktiky sociálneho inžinierstva, akými sú vytváranie falošných príbehov alebo zdôrazňovanie rizík, aby sa používatelia cítili ohrození a boli ochotní poskytnúť svoje citlivé informácie. Preto je dôležité, aby používatelia boli opatrní a starostlivo skúmali každú e-mailovú správu alebo webovú stránku, ktorú dostanú od neznámych zdrojov. Mali by sa vyhýbať klikaniu na odkazy alebo sťahovaniu súborov, ktoré sú neznáme alebo nevyžiadané a mali by sa uistiť, že webová stránka alebo e-mailová správa, ktorú dostali, je skutočne oficiálna a spoľahlivá. Používatelia by mali byť opatrní aj pri zadávaní svojich citlivých informácií a mali by sa uistiť, že sú na stránke, ktorá je overená a bezpečná. Kryptomeny sú často terčom phishingu, pretože ich hodnota je často vysoká a prenosy sú rýchle a anonymné. Používatelia by mali byť opatrní pri posielaní kryptomien a mali by si overiť adresu, na ktorú posielajú kryptomeny. Mali by sa uistiť, že adresa patrí skutočnému príjemcovi a nie podvodníkovi, ktorý sa vydáva za príjemcu. Používatelia by si tiež mali zvoliť dôveryhodnú a bezpečnú kryptomenovú burzu alebo peňaženku a vyhýbať sa neznámym a neoverenýmplatformám. Pre podniky a organizácie je tiež dôležité, aby mali dobré bezpečnostné opatrenia a využívali technológie, ktoré im pomôžu chrániť sa pred phishingom a inými druhmi podvodov. Medzi tieto opatrenia patria napríklad filter na spam, firewall, ochrana pred vírusmi a škodlivým softvérom a tréning zamestnancov na rozpoznávanie phishingu a ďalších druhov podvodov.[9]

5.2. ICO (Initial Coin Offering)

Ďalšou formou podvodu s virtuálnou menou sú falošné ICO (Initial Coin Offering). ICO sa stal populárnym spôsobom, ako financovať nové projekty a startupy v oblasti blockchainu a kryptomeny. Pri ICO vydáva projekt novú kryptomenu alebo token a predáva ju investorom za iné kryptomeny alebo fiat meny, ako napríklad doláre alebo eurá. Títo investori veria, že táto nová kryptomena alebo token bude mať v budúcnosti hodnotu a že investícia bude zisková. ICO môže byť veľmi ziskové pre projekt, pretože môže získať veľké množstvo finančných prostriedkov od investorov, ktorí veria v jeho úspech. Ale ako aj v prípade akéhokoľvek investovania, existuje riziko. ICO nemajú žiadnu reguláciu a nie sú chránené žiadnymi bezpečnostnými opatreniami alebo poistením. To znamená, že investori môžu stratiť svoje peniaze, ak projekt zlyhá alebo ak sa ukáže, že bol podvod. Ďalším problémom ICO sú rizikové projekty, ktoré môžu byť založené na nerealizovateľných ideách alebo nepreukázateľných

[9] Co je to phishing.sk. [online] [cit. 14.04.2023]. Dostupné na internete:
< https://www.flexi.sk/clanok/co-to-je-phishing >.

technológiách. Falošné ICO sa často predstavujú ako reálne projekty, ktoré však nemajú žiadnu reálnu hodnotu a ich jedným cieľom je získať finančné prostriedky od používateľov.[10]

5.3. Cryptojacking

Cryptojacking je druh kybernetickej hrozby, pri ktorej sa zneužíva výpočtová sila používateľov na ťaženie kryptomien bez ich súhlasu alebo vedomia. V podstate ide o to, že zlodeji využívajú výkon počítača alebo mobilného zariadenia na ťaženie kryptomeny pre seba. Tento spôsob podvodu sa môže vyskytnúť na niekoľkých miestach. Jedným z najbežnejších miest, kde sa cryptojacking vyskytuje, sú webové stránky, ktoré obsahujú skrytý kód na ťaženie kryptomeny. Pri návšteve týchto stránok váš počítač začne ťažiť kryptomenu, pričom vy neviete, že sa to deje. Tento kód môže byť veľmi ťažko zistiť, pretože sa skrýva v pozadí a beží na vašom počítači s minimálnym vplyvom na jeho výkon. Ďalším miestom, kde sa môže vyskytnúť cryptojacking, sú infikované aplikácie. Niektoré aplikácie môžu obsahovať kód na ťaženie kryptomeny a využívať výkon vášho mobilného zariadenia na ťaženie bez vášho súhlasu. Znepokojivou skutočnosťou je, že tento typ útoku môže mať vážne následky pre používateľov. Zvýšené používanie procesoru môže spôsobiť zvýšenú spotrebu energie a tepla, čo môže viesť k rýchlemu opotrebeniu hardvéru a zníženiu jeho životnosti. Okrem toho môže byť váš počítač alebo mobilné zariadenie pomalé a neefektívne, čo môže viesť k neuspokojivému používateľskému zážitku.[11]

5.4. Rug Pull podvodné konania

Dosiahli rozmach v roku 2021. Až 37 % zo všetkých podvodných konaní súvisiacich s virtuálnymi menami, ktoré vyplývajú z blockchain analýzy, boli druhom tohto podvodného konania. Hodnota všetkých transakcií s virtuálnou menou, teda celková škoda spôsobená týmto podvodným konaním dosiahla výšku približne 2,6 miliárd Eur.[12] Vo všeobecnosti je podstatou uvedeného podvodného konania uvedenie do omylu a následné spôsobenie škody páchateľom tak, že naláka investorov, aby podporili určitý projekt s virtuálnou menou a následne tento projekt s vloženým finančným kapitálom páchateľ zlikviduje bez akejkoľvek spätnej návratnosti, aj keď bola často predom prisľúbená.[13] Je samozrejmé, že závažnosť takéhoto činu sa odvíja od výšky spôsobenej škody, v našom záujme je však rozobrať formy Rug Pull podvodných konaní v závislosti od ich sofistikovanosti. Za menej sofistikovanú a najbežnejšiu formu Rug Pull podvodov môžeme považovať podvodné predaje tokenov. Obvyklosť tejto formy je prezentovaná jej početnosťou, a jej príčinou sú relatívne nízke nároky na erudíciu a technické rozhranie, ktoré je potrebné na realizovanie transakcie s virtuálnou menou. Z technickej stránky osobe páchateľa v podstate stačí, ak je poškodený držiteľom akejkoľvek peňaženky virtuálnej meny, ktorá podporuje uchovávanie súkromného kľúča ponúkaného tokenu a má finančné zdroje na vykonanie transakcie s virtuálnou menou. Buď je táto transakcia s páchateľom realizovaná priamo, alebo prostredníctvom poskytovateľa zmenárne alebo burzy virtuálnej meny. V tomto ohľade sa vyskytuje otázka, či takýto poskytovateľ vykonal naozaj

---

[10] Nbs.sk. [online] [cit. 10.04.2023]. Dostupné na internete:
< https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/ >.

[11] Interpol.int. [online] [cit. 10.04.2023]. Dostupné na internete:
< https://www.interpol.int/Crimes/Cybercrime/Cryptojacking >.

[12] *The 2022 Crypto Crime Report*. [online] [cit. 14.12.2022]. Dostupné na internete:
<https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>

[13] ŠANTA, J., 2022. *Virtuálne meny a trestná činnosť*. In: KURILOVSKÁ, L., MARKOVÁ, V., ed., 2022. *Aktuálne otázky trestného práva v teórii a praxi 10. ročník,* s. 99 - 114.

všetky opatrenia odbornej starostlivosti voči klientovi (poškodenému) a či konal v súlade so smernicou Európskeho parlamentu a Rady (EÚ) predchádzaní využívaniu finančného systému na účely legalizovania výnosov z trestnej činnosti alebo financovania terorizmu [14], resp. či konal v súlade s inými právnymi predpismi zakotvujúcimi obchodovanie s virtuálnymi menami alebo kryptoaktívami a či tento poskytovateľ zmenárne alebo burzy virtuálnej meny nemá na podvodnom konaní *culpa levis* určitý podiel viny. Páchateľ potom vytvorí token na blockchaine, ktorý takéto vytvorenie podľa určitých kryptografických pravidiel umožňuje, napríklad v rámci virtuálnej meny Ethereum ako ERC20 token alebo napríklad v rámci virtuálnej meny Binance Coin ako BEP20 token. Následná časť podvodného konania, uvádzanie do omylu, už závisí od daného páchateľa. Niektorí využívajú formu ICO[15] modelu podvodného konania, pričom predávajú tokeny pod zámienkou podpory určitého projektu s virtuálnou menou s tým, že investorom sľúbia, že všetky virtuálne meny alebo fiat meny, za ktoré si poškodený nakúpi podvodné tokeny, použijú na financovanie projektu, respektíve spoločnosti, ktorá projekt realizuje. Virtuálne alebo fiat meny majú slúžiť teda na prenájom nehnuteľností, vyplácanie miezd zamestnancom a na iné operatívne výdavky. Páchateľ predaj tokenov často prezentuje ako vynikajúcu investičnú príležitosť s výnosmi tak veľkými, ako sú nastavené ciele projektu. Poškodeného uvedie do omylu, keďže ten po obdržaní virtuálnej meny – tokenu často až s veľkou časovou odchýlkou zistí, že spoločnosť realizujúca projekt bola zrušená alebo je v likvidácii, že projekt stagnuje, finančné prostriedky smerujúce projektu sú prevedené na inú adresu virtuálnej meny a že hodnota vlastnených tokenov, ktorá bola na krátku dobu ekvivalentom hodnoty vstupných finančných prostriedkov, výrazne klesá, respektíve sa blíži nule. Páchateľ v tomto ohľade môže stále komunikovať s poškodeným, môže verejne preukazovať pokračovanie projektu, dávať poškodenému nádej, ale to iba v záujme udržania latencie podvodného konania. Niektorí páchatelia využívajú formu tokenizácie, keď k predávaným tokenom pripájajú zdanlivé práva k vlastníctvu tokenizovaného majetku, resp. rozhodovacie právomoci, ktoré sú opäť len zdanlivo, fiktívne kauzálne spojené s množstvom vlastnených tokenov. V praxi to vyzerá tak, že páchateľ vytvorí určité množstvo tokenov, ktoré reprezentujú podiely v spoločnosti a určí, že ak bude projekt, alebo spoločnosť realizujúca projekt potrebovať vykonať kľúčovú zmenu, právo rozhodovať o tejto zmene budú mať držitelia uvedených tokenov pomerne podľa počtu držaných tokenov. Takáto lesť motivuje poškodených vykonávať transakcie s virtuálnou menou na účel držby čo najväčšieho počtu tokenov. Prípadne páchateľ vytvorí určité množstvo tokenov, ktoré charakterizujú podiel na tokenizovanej hnuteľnej alebo nehnuteľnej veci, pričom tokeny prvotne ocení v závislosti od reálnej hodnoty nehnuteľnosti a počas predaja tokenov tvrdí, že sú tieto tokeny kryté predmetnou vecou. Osobitným prípadom sú virtuálne meny, ktorých účelom je kopírovať cenu fiat meny, kde sa hodnota tejto virtuálnej meny odvíja od krytia fiat menou, prípadne inými virtuálnymi menami. Situácia pri týchto podvodných konaniach môže byť veľmi zložitá, najmä, ak doba od investície poškodeného až po následne spôsobenú škodu páchateľom môže trvať aj niekoľko rokov.[16]

---

[14] Smernica Európskeho parlamentu a Rady (EÚ) z 30.mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ - Ú. v. ES L 156 30.5.2018 v aktuálnom znení.

[15] *What Is an ICO (Initial Coin Offering)?* [online] [cit. 15.12.2022]. Dostupné na internete: <https://academy.binance.com/en/articles/what-is-an-ico>.

[16] *The difference between Initial Coin Offerings and Token Sales*. [online] [cit. 15.12.2022]. Dostupné na internete: <https://www.linkedin.com/pulse/difference-between-initial-coin-offerings-token-sales-westerheide>.

Viac sofistikovanou formou Rug Pull podvodov sú podvody v liquidity pooloch. Liquidity pooly [17] sú veľmi významným prvkom zaisťujúcim fungovanie systému decentralizovaných financií. Ich ideou je zabezpečenie spôsobilosti na realizáciu transakcií s virtuálnou menou, keďže jednoduché párovanie dopytu a ponuky by predlžovalo čas na vykonanie transakcie. Do liquidity poolov môžu účastníci siete uzamknúť svoje voľné virtuálne meny, poskytnúť ich na vykonávanie decentralizovaných financií, ako sú výmeny virtuálnej meny za inú virtuálnu menu, decentralizované obchodovanie, požičiavanie a pod., za určitú odmenu, ktorá vyplýva z podmienok daného liquidity poolu, ktoré sú určené kryptograficky.[18] Na rozdiel od predchádzajúcej formy sa tieto podvody dejú v krátkom časovom slede, vytvára sa množstvo tokenov s krátkou dobou životnosti. Tokeny majú totožné alebo veľmi podobné názvy a od vytvorenia až po ich zánik neuplynie v priemere viac ako 45 minút. Prvotne páchateľ kryptograficky vytvorí takýto token, zadá množstvo vytvorených tokenov spolu s označením loga a názvu tokenu. Neskôr kryptograficky vytvorí liquidity pool[19], ktorý pozostáva z páru virtuálnych mien. Väčšinou sa jedná o pár virtuálnej meny, na ktorej blockchaine sa liquidity pool vytvoril a zároveň predom vytvorený token. Páchateľ potom pridá do liquidity poolu virtuálne meny podľa určeného páru a ostáva mu len čakať na užívateľov siete, ktorí budú ochotní vykonať transakciu s virtuálnou menou a uzamknú svoje virtuálne meny v liquidity poole. Motiváciou poškodeného je špekulácia na raste ceny podvodného tokenu, ktorý si podľa podmienok „kurzu“ nastaveného liquidity poolom má právo z poolu vziať a ďalej nimi disponovať, prípadne sa môže jednať o situáciu, kedy liquidity pool poskytne podvodný token ako kolaterál za uzamknutie virtuálnej meny v liquidity poole, a to pomerne podľa nastavených kryptografických pravidiel liquidity poolu.[20] V poslednom období sa eviduje nárast transakcií s virtuálnou menou v priestore decentralizovaných financií. Ruka v ruke sa eviduje aj nárast transakcií s virtuálnou menou, ktoré sa dajú označiť ako nelegálne, sú poznačené určitým druhom trestnej činnosti, ktorá bola ohlásená a identifikovaná a takisto bola označená aj verejná adresa páchateľa, ktorá v tejto transakcii s virtuálnou menou vystupovala. Dáta vyplývajú z blockchainov, pri ktorých je možné tieto transakcie s virtuálnou menou spolu so súvisiacimi prvkami, akým je spomínaná verejná adresa páchateľa, identifikovať. Od roku 2020 do roku 2021 bol v rámci decentralizovaných financií štatisticky zistený viac ako 1 964 % -ný nárast týchto nelegálnych transakcií s virtuálnou menou.[21] Tento nárast v spojení s potrebou likvidity poolov v sfére decentralizovaných financií vytvára príležitosť pre páchateľov sofistikovanejších Rug Pull podvodných konaní, a preto nie je prekvapením, keď sa v prípade liquidity poolov krátko po ich vzniku vykonajú viaceré transakcie s virtuálnou menou, ktoré by pri dodržaní etiky slúžili na agregovanie potrebnej likvidity na chod decentralizovaných financií. Prvé transakcie s virtuálnou menou v rámci novovytvoreného liquidity poolu sa vykonajú už do niekoľkých sekúnd. Po nazbieraní dostatočného objemu uzamknutých virtuálnych mien v páre, páchateľ vyberie z liquidity poolu všetky virtuálne meny, a tým

---

[17] *Liquidity Pool, The concept eplained*. [online] [cit. 16.04.2023]. Dostupné na internete: <https://www.edsx.ch/blognews/liquidity-pool>.

[18] *What are Liquidity pools in DeFi and How Do They Work?* [online] [cit. 17.12.2022]. Dostupné na internete: <https://academy.binance.com/en/articles/what-are-liquidity-pools-in-defi>.

[19] *How to Create Pool on PancakeSwap: BEP20 Pair Creation*. [online] [cit. 17.12.2022]. Dostupné na internete: <https://tokpie.io/blog/how-create-pool-pancakeswap-bep20-pair/>.

[20] CERNERA, F., LA MORGIA, M., SASSI, F., MEI, A., 2022. *Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB).* [online] [cit. 17.12.2022]. Dostupné na internete: < https://www.researchgate.net/publication/361359291_Token_Spammers_Rug_Pulls_and_SniperBots_An_Analysis_of_the_Ecosystem_of_Tokens_in_Ethereum_and_the_Binance_Smart_Chain_BNB>.

[21] *The 2022 Crypto Crime Report.* [online] [cit. 14.12.2022]. Dostupné na internete: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>.

zamedzí akýkoľvek prístup k spätnej zámene tokenu za virtuálnu menu v páre, respektíve zamedzí prístup k poskytnutému kolaterálu. Takéto podvodné konanie v liquidity poole môže páchateľ vykonávať *vyčkávacou metódou*, teda počká na transakcie s virtuálnou menou bez svojho ďalšieho pričinenia. Páchateľ však namiesto vyčkávania, môže poškodených aktívne uvádzať do omylu tým, že metódou *wash-trading* zdanlivo zvýši dôveryhodnosť liquidity poolu. Wash-trading sa okrem iného často používa pri páchaní podvodného konania s predajom NFT – jedinečných tokenov, keď sa cena NFT umelo navyšuje. Páchateľ kúpi NFT za 1 jednotku virtuálnej meny, umiestni ju na NFT trhovisko za 2 jednotky virtuálnej meny. Ak po určitom čase nedôjde k nákupu NFT od inej osoby, páchateľ si ju kúpi sám prostredníctvom inej adresy a to isté NFT umiestni na trhovisko už za vyššiu cenu, napr. za 3 jednotky virtuálnej meny. Páchateľ v takomto prípade umelo zvyšuje cenu NFT, pokým jeho ponuku nespáruje dopyt poškodeného, ktorý môže po nákupe takéhoto NFT buď pokračovať v podvodnej schéme ďalej, alebo postupne znižovať cenu NFT, ktorá sa s najväčšou pravdepodobnosťou po čase dostane veľmi blízko k nule.[22] V prípade liquidity poolu je však páchateľovým cieľom pri použití wash-trading metódy skôr zvýšiť objem transakcií s virtuálnou menou než cenu podvodných tokenov. Na zvýšenie ceny páchatelia používajú *pump metódu*. Páchatelia na rôznych sociálnych sieťach (Telegram, Discord, Reddit, Twitter...) zverejňujú informácie o predpokladanom zvýšení ceny tokenu, prezentujú svoje podvodné tokeny ako jedinečnú investičnú príležitosť, posielajú záznamy trhových analýz tokenov s predpokladmi, že do pár hodín nastane obrovské zvýšenie ceny tokenov a vytvárajú na užívateľov siete tlak, známy aj ako FOMO - strach z premeškania. Poškodení potom pomáhajú svojím dopytom zvýšiť cenu uvedeného tokenu.[23]Umelé nafúknutie ceny podvodného tokenu na jednej strane priláka nových poškodených, na druhej strane motivuje poškodených, ktorí už vykonali operáciu v rámci liquidity poolu, investovať do poolu ešte viac virtuálnej meny. Typická pre páchateľov vykonávajúcich podvodné konanie v liquidity poole je *metóda hedge*, ktorou si páchateľ zaisťuje nezrealizovaný zisk. Tým, že páchateľ nemá trhový mechanizmus úplne pod kontrolou, môže nastať situácia, kedy poškodený po alokovaní podvodného tokenu, ešte počas riadneho fungovania liquidity poolu, tento token vymení naspäť za vložené virtuálne meny. Alokovaním tokenu z liquidity poolu sa cena tokenu zvýši. Znalý páchateľ chce využiť aj tento moment, preto si pri vytváraní liquidity poolu rezervuje určité množstvo podvodného tokenu, ktorý neuzamkne v liquidity poole. Po zdvihnutí ceny začne páchateľ mimo liquidity poolu podvodné tokeny predávať, napr. iným užívateľom, liquidity poolom, smart kontraktom alebo burzám a zmenárňam virtuálnej meny. Takýmto spôsobom si páchateľ poistí zisk aj počas aktívneho prevádzkovania liquidity poolu. Páchatelia takéhoto Rug Pull podvodu majú vysokú znalosť prostredia a ekosystému virtuálnych mien a využívajú rôzne metódy a techniky na nelegálne obohatenie sa. Z blockchain analýzy vykonanej v štúdii, ktorá hodnotí a analyzuje transakcie s virtuálnou menou v rámci blockchainu Binance coin (BSC) a blockchainu Etherea [24] vyplýva, že viac ako polovica z analyzovaných 414 936 liquidity poolov na BSC vykazuje známky

---

[22] *What is NFT Wash Trading?* [online] [cit. 14.12.2022]. Dostupné na internete: <https://www.coindesk.com/learn/what-is-nft-wash-trading/>.

[23] HAMRICK, JT., ROUHI, F., MUKHERJEE, A., FEDER, A., GANDAL, N., MOORE, T., VASEK, M., 2021. *An examination of the cryptocurrency pump-and-dump ecosystem.* [online] [cit. 16.12.2022]. Dostupné na internete: < https://bfi.uchicago.edu/wp-content/uploads/Gandal-Neil-etal-An-examination-of-the-cryptocurrency-pump-and-dump-ecosystem.pdf>.

[24] CERNERA, F., LA MORGIA, M., SASSI, F., MEI, A., 2022. *Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB)*. [online] [cit. 17.12.2022]. Dostupné na internete: < https://www.researchgate.net/publication/361359291_Token_Spammers_Rug_Pulls_and_SniperBots_An_Analysis_of_the_Ecosystem_of_Tokens_in_Ethereum_and_the_Binance_Smart_Chain_BNB>.

podvodných liquidity poolov. Podvodné Rug Pull liquidity pooly sú aj v blockchaine Etherea, z analyzovaných 26 817 je podvodných viac ako 80 %. Vo väčšine prípadov sa jedná o vytvorenie liquidity poolov a vytvorenie tokenov, ktoré nemajú životnosť dlhšiu ako jeden deň. Tieto pooly spravuje viac ako 116 500 rozdielnych adries v BSC a viac ako 16 500 rozdielnych adries na Ethereum blockchaine. Z uvedených adries, ktoré je možné spárovať s identitou reálnej osoby pri ideálnej súčinnosti zmenární a búrz virtuálnych mien s KYC (požiadavkami na identifikovanie totožnosti osoby zakladajúcej si napr. peňaženku virtuálnej meny)[25] bolo zistené, že 75 % adries v BSC zodpovedných za vytváranie veľkého množstva tokenov v rámci krátkeho času vykonali aspoň jeden Rug Pull podvod s liquidity poolom. Na druhej strane v Ethereum blockchaine sa Rug Pull podvodu dopustilo „len" 7,6 % týchto spamovacích adries. Z porovnania týchto výsledkov môžeme vyvodiť záver, že aj napriek tomu, že v blockchaine Etherea dochádza k častejším Rug Pull podvodom s liquidity poolmi, sú adresy, ktoré vytvoria za krátky čas mnoho tokenov zodpovednejšie, teda predstavujú väčšiu istotu etického prevádzkovania liquidity poolu, ako je to v prípade Binance coin blockchainu. Za zmienku stojí aj skutočnosť, že ak páchateľ použije niektorú z vyššie spomínaných manipulačných metód (wash-trading metóda, pump metóda alebo hedge metóda), jeho zisk sa zvýši v priemere z 0,11 BNB v rámci Binance coin blockchainu a z 1,34 ETH v rámci Ethereum blockchainu na 0,25 BNC a na 12 ETH. To však nemá vplyv na percentuálnu úspešnosť vykonania Rug Pull podvodného konania s liquidity poolom, ktorá je bez použitia uvedených metód a s použitím uvedených metód bez významnej odchýlky skoro rovnaká, a to 39,1 % v Binance coin blockchaine a 61,9% v Ethereum blockchaine. [26]

Za obzvlášť špecifické Rug Pull podvodné konanie možno považovať podvod s MEV (Maximum Extractable Value) botmi. Tento podvod súvisí s fundamentom transakcie s virtuálnou menou. Predtým, než je určitá transakcia zaradená do bloku transakcií s virtuálnou menou, je nutné, aby táto bola transakcia overená a potvrdená. Overenie, potvrdenie a zaradenie transakcie s virtuálnou menou do bloku transakcií podlieha kryptografickým mechanizmom, ktoré sú typické pre tú danú virtuálnu menu. Predtým, je však potrebné transakciu skonštruovať a zverejniť ju sieti do tzv. mempoolu.[27] Mempool zahŕňa všetky transakcie, ktoré chcú používatelia siete zaradiť do blockchainu. Na účely tohto článku uvádzame, že zaradenie transakcie do blockchainu, a teda uskutočnenie transakcie je podmienené profitabilitou, teda hodnotou virtuálnej meny, ktorú určí používateľ siete pri skonštruovaní transakcie určenej pre ťažiarov, čo je typické najmä pre proof of work algoritmus konsenzu, aj keď algoritmov konsenzu je v oblasti virtuálnych mien väčšie množstvo.[28] MEV bot teda skenuje mempool a transakcie zverejnené a čakajúce na zaradenie do bloku transakcií, detekuje ich a automaticky vytvára nové transakcie s virtuálnou menou na báze pôvodných transakcií (umiestnených v mempoole) podľa želania osoby, ktorá MEV bot používa a znevýhodňuje ostatných používateľov, ktorí skonštruovali transakciu s virtuánou menou skôr, a to napríklad tým, že za vykonanie novej transakcie dostane ťažiar väčšiu odmenu (aj keď reálne bezvýznamnú). Ťažiar

---

[25] *The importance of KYC for crypto exchanges.* [online] [cit. 18.12.2022]. Dostupné na internete: <https://withpersona.com/blog/kyc-crypto>

[26] CERNERA, F., LA MORGIA, M., SASSI, F., MEI, A., 2022. *Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB).* [online] [cit. 17.12.2022]. Dostupné na internete: https://www.researchgate.net/publication/361359291_Token_Spammers_Rug_Pulls_and_SniperBots_An_Analysis_of_the_Ecosystem_of_Tokens_in_Ethereum_and_the_Binance_Smart_Chain_BNB.

[27] *What is mempool? Pre-chain process may attract regulatory scrutiny*. [online] [cit. 18.12.2022]. Dostupné na internete: <https://currency.com/what-is-mempool>.

[28] Mining explained: *A detailed guide on how cryptocurrency mining works.* [online] [cit. 18.12.2022]. Dostupné na internete: <https://freemanlaw.com/mining-explained-a-detailed-guide-on-how-cryptocurrency-mining-works/>.

teda uprednostní novú transakciu s virtuálnu menou, pretože sa riadi profitabilitou. [29] Toto samotné konanie nie je predmetom skúmania, aj keď môže vykazovať znaky neférového zaobchádzania v oblasti virtuálnych mien. Čo však za Rug Pull podvodné konanie považujeme, je vytvorenie smart kontraktu, akým je napríklad Salmonella, ktorý cieli na MEV boty tak, že vytvorí kryptograficky prispôsobený token a liquidity pool tak, aby bolo možné token kúpiť, no nebolo možné ho spätne uzamknúť v liquidity poole, resp. spätne predať. Tento smart kontrakt zároveň skonštruuje transakcie s virtuálnou menou, zverejní ich mempoolu na zaradenie do blockchainu pričom transakcie upraví (dá im nízku odmenu pre ťažiarov – zníži profitabilitu), aby ich MEV bot detekoval, zhodnotil a vytvoril nové transakcie, ktoré sú pre ťažiarov profitabilnejšie. Tie sa zaradia do bloku transakcií s virtuálnou menou. Ťažiari teda následne namiesto predstieranej transakcie zaradia do blockchainu transakciu MEV bota, ktorý vytvoril požiadavku na nákup podvodného tokenu v liquidity poole. Po vykonaní transakcie nie možné spätne liquidity poolu podvodný token predať. Tým, že niektoré MEV boty fungujú na princípe nákup tokenu – nárast ceny tokenu – predaj tokenu, stávajú sa ideálnym prostredníkom na vykonanie práve tohto druhu MEV bot Rug Pull podvodného konania. Takto spustený a nekontrolovaný MEV bot, nemusí byť kontrolovaný poškodeným aj niekoľko dní, čím sa zvyšuje spôsobená škoda. [30]

5.5. Podvodné konania založené na budovaní vzťahu medzi poškodeným a páchateľom

Podvodné konania založené na budovaní vzťahov súvisiace s priestorom virtuálnych mien sú typické tým, že páchateľ predstiera budovanie vzťahu na účel vytvorenia osobného puta s poškodeným. Po získaní dôvery poškodeného začne páchateľ vykonávať aktivitu súvisiacu so žiadaním o zaslanie virtuálnych mien na jeho verejnú adresu. Podvodné konania založené na budovaní romantického vzťahu (ďalej aj „romániky“) s poškodeným útočia na citovú stránku poškodeného, keďže páchateľ svoje podvodné konanie skrýva za poskytnutie pomoci v neľahkej životnej situácii, za podporu jeho blízkych, za prejav lásky a dôvery voči páchateľovi. Využitím blockchain analýzy je možné v priestore virtuálnych mien vyčísliť a v čase určiť množstvo virtuálnych mien v prepočte na vybranú fiat menu, ktorými sa páchateľ využitím takejto formy páchanie podvodného konania obohatil. Od obdobia marca 2022 do decembra 2022 sa prostredníctvom románikov vedeli páchatelia obohatiť v priemere aj o viac ako 300 000 Eur za 30 dní. Priemerný depozit za rok 2022, ktorý vo virtuálnych menách skladali poškodení na účet páchateľov predstavoval čiastku približne 15 000 Eur. Príčinou toho je unikátna povaha tejto formy podvodného konania, ktorá cieli na emočnú, personálnu stránku poškodených. [31] Ako príklad môže slúžiť kazuistika z nedávnej praxe, kedy poškodená osoba zasielala virtuálne meny vojakovi, ktorý poškodenej sľuboval láskyplné stretnutia. [32]

Podvodné konania založené na budovaní dlhodobého vzťahu, ktorý páchateľ s poškodeným pestuje len na účel realizácie neoprávneného prospechu v budúcnosti, sú veľmi nebezpečným

---

[29] *Guide to an MEV Bot: Creating an Arbitrage Bot on Ethereum Mainnet*. [online] [cit. 18.12.2022]. Dostupné na internete: <https://www.blocknative.com/blog/mev-and-creating-a-basic-arbitrage-bot-on-ethereum-mainnet>.

[30] ADAN, V., DAZA, V., MAZORRA, B., 2022. *Do not rug on me: Zero-dimensional Scam Detection*. [online] cit. 18.12.2022]. Dostupné na internete: < https://www.researchgate.net/publication/357953042_Do_not_rug_on_me_Zero-dimensional_Scam_Detection>,

[31] *Crypto Crime Report, 2023*. [online] [cit. 16.04.2023]. Dostupné na internete: <https://go.chainalysis.com/2023-crypto-crime-report.html>.

[32] *Ako odhaliť a chrániť sa pred romantickými podvodmi*. [online] [cit. 16.04.2023]. Dostupné na internete: <https://www.binance.com/sk/blog/community/poznajte-podvody-ako-odhali%C5%A5-a%C2%A0chr%C3%A1ni%C5%A5-sa-pred-romantick%C3%BDmi-podvodmi-1518637594616558934>.

fenoménom v tejto oblasti. Páchatelia si vytipujú cieľové osoby, s ktorými si vytvárajú dlhodobý vzťah, pričom na umocnenie dôvery využívajú prvky sociálneho inžinierstva. Vytvárajú si falošné profily na sociálnych médiách, dlhodobo prezentujú svoj životný štýl s cieľom dôveryhodného pôsobenia. Veľmi častým je využívanie aplikácií, akými sú WhatsApp, LinkedIn, WeChat, Signal, Reddit alebo Telegram. Počas budovania vzťahu páchatelia často vykonávajú aj prieskum a profiláciu bonity a naivity poškodených. Vysoká bonita a vysoká naivity u poškodených predstavuje ideálny potenciálny cieľ pre páchateľa, ktorý po určitom čase, keď už uzná za vhodné, že je medzi ním a poškodeným dostatočne vysoký stupeň dôvery, začne spomínať investície, transakcie alebo možnosti zbohatnutia prostredníctvom virtuálnych mien. Páchatelia neraz dokážu presvedčiť poškodeného, aby si vytvoril peňaženku virtuálnej meny, aby na svoje meno nakúpil virtuálne meny a posielal ich páchateľovi na verejnú adresu. Ak už páchateľ vyčerpá finančný potenciál poškodeného, snaží sa presvedčiť poškodeného, aby si finančné prostriedky vo fiat mene požičal od inštitúcií alebo od známych a za tieto následne nakúpil virtuálne meny. Typicky si páchatelia vytipujú na tento typ podvodného konania staršie osoby, osoby, ktoré sú citlivé, zraniteľné a ktoré na sociálnych sieťach prejavujú dobromyseľnosť. [33]

Záver

Virtuálna mena je využívaná na páchanie podvodnej aktivity veľmi rozmanitým spôsobom. Páchatelia neprávom profitujú z nedostatočnej vzdelanosti účastníkov spoločnosti v oblasti virtuálnych mien a s nimi súvisiacimi technológiami. Laická verejnosť dostatočne nepozná fundamentálnu stránku virtuálnych mien, nie je dostatočne informovaná o tejto technickej oblasti a pod rúškom tajomného a rýchleho zbohatnutia sa dopúšťa konania, ktoré zneužívajú páchatelia podvodných konaní a premieňajú nevedomosť poškodených na vlastný nelegálny prospech. Foriem podvodných konaní je viacero. V článku sa venujeme postupnosti od tej najjednoduchšej až po tu najzložitejšiu formu podvodného konania vo vzťahu k technickosti prostredia virtuálnej meny. Abstrahovali sme avšak od skúmania tých podvodných konaní, pri ktorých nevystupuje virtuálna mena z hľadiska svojho technologického fundamentu. Výsledkom je to, že v prostredí virtuálnej meny často dochádza k tzv. Rug Pull podvodným konaniam na úrovni podvodných predajov tokenov, tokenizácie, podvodov v liquidity pooloch alebo podvodov s MEV botmi, k phishingovým útokom, falošným ICO a cryptojackingu. Do akej úrovne sofistikovanosti takýchto podvodných konaní sa poškodený dostane, vyplýva z jeho erudície v oblasti virtuálnych mien. Spomenúť treba skutočnosť, že sofistikované podvodné konania sú vykonávané vo veľmi malom časovom rámci, zasahujú do veľmi špecifických oblastí ekosystému virtuálnych mien, preto je ich odhaľovanie, objasňovanie, vyšetrovanie a dokazovanie spojené s potrebou vysokej odbornej znalosti a erudície oprávnených subjektov. Ďalšou formou páchania podvodných konaní vo sfére virtuálnych mien sú konania súvisiace s vytváraním vzťahu medzi páchateľom a poškodeným. Takýto vzťah neskôr páchateľ zneužije vo svoj prospech a s určitým stupňom manipulácie dokáže pôsobiť na poškodeného a dosiahnuť svoj nezákonný cieľ.

Používatelia virtuálnych mien by preto mali byť opatrní, mali by dodržiavať bezpečnostné opatrenia, používať silné heslá, vyberať si dôveryhodné a známe zmenárne virtuálnej meny, mali by udržiavať svoj súkromný kľúč v externých peňaženkách virtuálnej meny a mali by využívať dvojfaktorovú autentifikáciu. Nezastupiteľné miesto v prevencii má aj istá miera informovanosti, erudícia o nových spôsoboch, metódach, formách a technikách

[33] *Crypto Crime Report, 2023*. Dostupné na internete: <https://go.chainalysis.com/2023-crypto-crime-report.html> .

podvodov. Táto práca má význam najmä v tejto oblasti preventívneho pôsobenia poskytnutím najaktuálnejších informácií ohľadom podvodných konaní vo sfére virtuálnych mien.

Zoznam bibliografických odkazov

ADAN, V., DAZA, V., MAZORRA, B., 2022. *Do not rug on me: Zero-dimensional Scam Detection*. [online] cit. 18.12.2022]. Dostupné na internete: < https://www.researchgate.net/publication/357953042_Do_not_rug_on_me_Zero-dimensional_Scam_Detection>.

CERNERA, F., LA MORGIA, M., SASSI, F., MEI, A., 2022. *Token Spammers, Rug Pulls, and Sniper Bots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB)*. [online] [cit. 17.12.2022]. DOI: 10.48550/arXiv.2206.08202 Dostupné na internete: < https://www.researchgate.net/publication/361359291_Token_Spammers_Rug_Pulls_and_SniperBots_An_Analysis_of_the_Ecosystem_of_Tokens_in_Ethereum_and_the_Binance_Smart_Chain_BNB>.

Co je to phishing.sk. [online] [cit. 14.04.2023] Dostupné na internete: < https://www.flexi.sk/clanok/co-to-je-phishing >.

Crypto Crime Report, 2023. [online] [cit. 16.04.2023] Dostupné na internete: https://go.chainalysis.com/2023-crypto-crime-report.html.

Finifo. sk. [online] [cit. 14.04.2023] Dostupné na internete: < https://www.fininfo.sk/fininfo/inovacie/kryptomeny/kryptomeny.html>.

HAMRICK, JT., ROUHI, F., MUKHERJEE, A., FEDER, A., GANDAL, N., MOORE, T., VASEK, M., 2021. *An examination of the cryptocurrency pump-and-dump ecosystem.* [online] [cit. 16.12.2022]. DOI: 10.1016/j.ipm.2021.102506. Dostupné na internete: < https://bfi.uchicago.edu/wp-content/uploads/Gandal-Neil-etal-An-examination-of-the-cryptocurrency-pump-and-dump-ecosystem.pdf>.

Interpol.int. [online] [cit. 10.04.2023] Dostupné na internete: < https://www.interpol.int/Crimes/Cybercrime/Cryptojacking >.

Návrh nariadenia EURÓPSKEHO PARLAMENTU A RADY o trhoch s kryptoaktívami a o zmene smernice (EÚ) 2019/1937.

Nbs.sk. [online] [cit. 10.04.2023] Dostupné na internete: < https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/ >.

Prevencia kriminality.sk. [online] [cit. 14.04.2023] Dostupné na internete: < https://prevenciakriminality.sk >.

ŠANTA, J., 2022. *Virtuálne meny a trestná činnosť*. In: KURILOVSKÁ, L., MARKOVÁ, V., ed., 2022. *Aktuálne otázky trestného práva v teórii a praxi 10. ročník*. Zborník príspevkov z 10. ročníka interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou. Bratislava: Akadémia Policajného zboru v Bratislave, s. 99 - 114.

ŠANTA, J. a I. ŠANTA., 2022. *Procesnoprávne aspekty trestnej činnosti spojenej s virtuálnymi menami*. In: *Justičná revue – roč. 2022*, vydanie 10/2022, s. 1146 - 1164.

ŠANTA, J., ŠANTA, I., SZABOVÁ, E., 2022. *Manipulácia s trhom – niektoré medzinárodné a trestnoprávne aspekty*. In:. *Justičná revue – roč. 2022*, vydanie 11/2022, s. 1296 - 1311.

ŠANTA, J., ŠANTA, I., ŠIROKÝ, T.. 2022. *K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami.* In: *Justičná revue – roč. 2022*, vydanie 4/2022, s.484 – 499.

ŠANTA, J. a I. ŠANTA, 2022. *K niektorým legislatívnym a ekonomickým aspektom virtuálnych mien v legislatíve Európskej únie a Slovenskej republiky*. In: *Justičná revue – roč. 2022*, vydanie 2/2022, s. 164 – 179.

ŠANTA, J. a I. ŠANTA, 2022. *Riziká investovania do virtuálnych mien z ekonomického a trestnoprávneho hľadiska.* In: *Justičná revue – roč. 2022*, vydanie 3/2022, s. 365 – 378.

The 2022 Crypto Crime Report. [online] [cit. 14.12.2022] Dostupné na internete: <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>.

Zákon č. 297/2008 Z.z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov .

Zákon č. 300/2005 Z.z. Trestný zákon.

Keywords: virtual currency, fraud, terrorism financing, decentralized finance, criminal activity

Summary

Virtual currency is used to commit fraudulent activities in various ways. Perpetrators take advantage of the lack of education among members of society regarding virtual currencies and related technologies. The general public is not sufficiently informed about the fundamental aspects of virtual currencies, and under the guise of mysterious and quick enrichment, they engage in activities exploited by perpetrators of fraudulent activities who transform the ignorance of victims into their own illegal profit. There are several forms of fraudulent activities, and this contribution focuses on the sequence - from the simplest form to the most complex form of fraudulent conduct in relation to the technical environment of virtual currency.

Therefore, virtual currency users should be careful, adhere to security measures, use strong passwords, choose reliable and well-known virtual currency exchanges, keep their private keys in external virtual currency wallets, and use two-factor authentication. A certain level of information and erudition about new ways, methods, forms, and techniques of fraud are irreplaceable in prevention. This contribution is particularly important as regards the area of preventive actions by providing the most up-to-date information on fraudulent activities in the sphere of virtual currencies.

por. Mgr. Daniela Gavurová
odbor Bratislava
Národná kriminálna agentúra Prezídia PZ
Pribinova 2, 812 72 Bratislava
e-mail: daniela.gavurova@minv.sk

Mgr. Andrej Lipták
odbor finančného vyšetrovania
Národná centrála osobitných druhov kriminality PPZ
Pribinova 2, 812 72 Bratislava
e-mail: andrej.liptak@minv.sk

Recenzent: mjr. doc. Ing. Mária Sabayová, PhD.