Sektorová analýza VA / VASP

Obsah

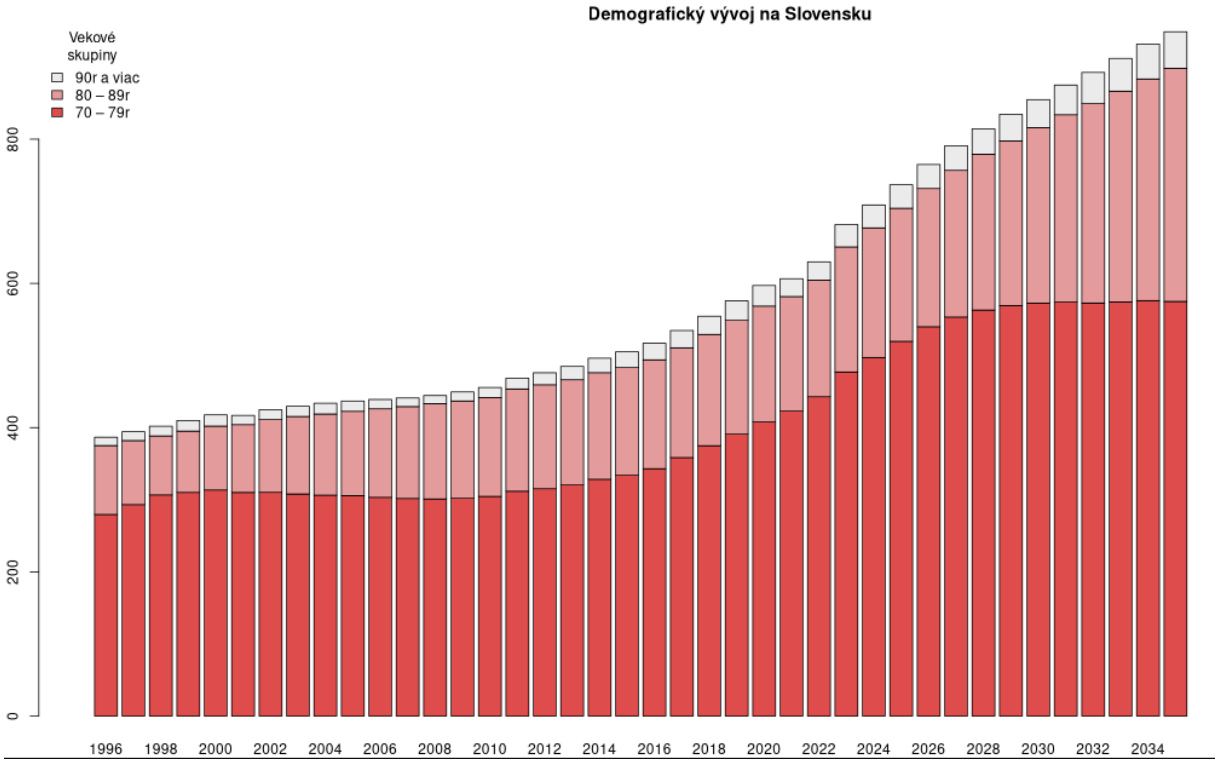
1. Slovenská republika – základné informácie

Slovenská republika sa konštituovala ako právny nástupca po rozpustení Česko-Slovenskej federácie dňa 1. januára 1993. S rozlohou 49 036 km² a geografickým umiestnením v strednej Európe je pre štát kľúčové angažovať sa v medzinárodných štruktúrach a alianciách. Toto zahrnutie je zásadné na viacerých úrovniach: lokálnej, ako je napríklad Visegrádska skupina (V4), regionálnej – Európska únia (EU) a Severoatlantická aliancia (NATO), ako aj na globálnej úrovni, reprezentovanej Organizáciou Spojených národov (OSN).

- od 19.01.1993 je Slovenská republika členom Organizácie Spojených národov.
- od 29.03.2004 je členom Severoatlantickej aliancie (NATO).
- od 01.05.2004 patrí medzi členské štáty Európskej únie.
- od 21.12.2007 je súčasťou Schengenského priestoru.
- od 01.01.2009 je členom Európskej menovej únie, známej ako Eurozóna, kde sa stala šestnástou členskou krajinou.

Počet obyvateľov Slovenskej republiky je 5 426 857 (stav k 31.03.2023).[1]

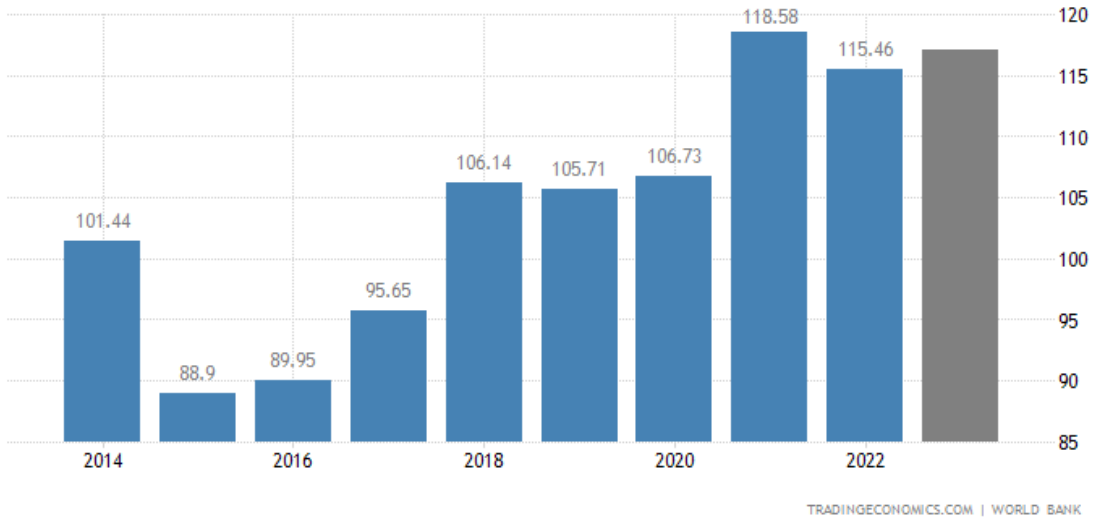
Demografická štruktúra obyvateľstva je nasledovná:
Obrázok č.1



Zdroj: https://www.iz.sk/30-grafov-o-zdravotnictve/demograficky-vyvoj-na-slovensku

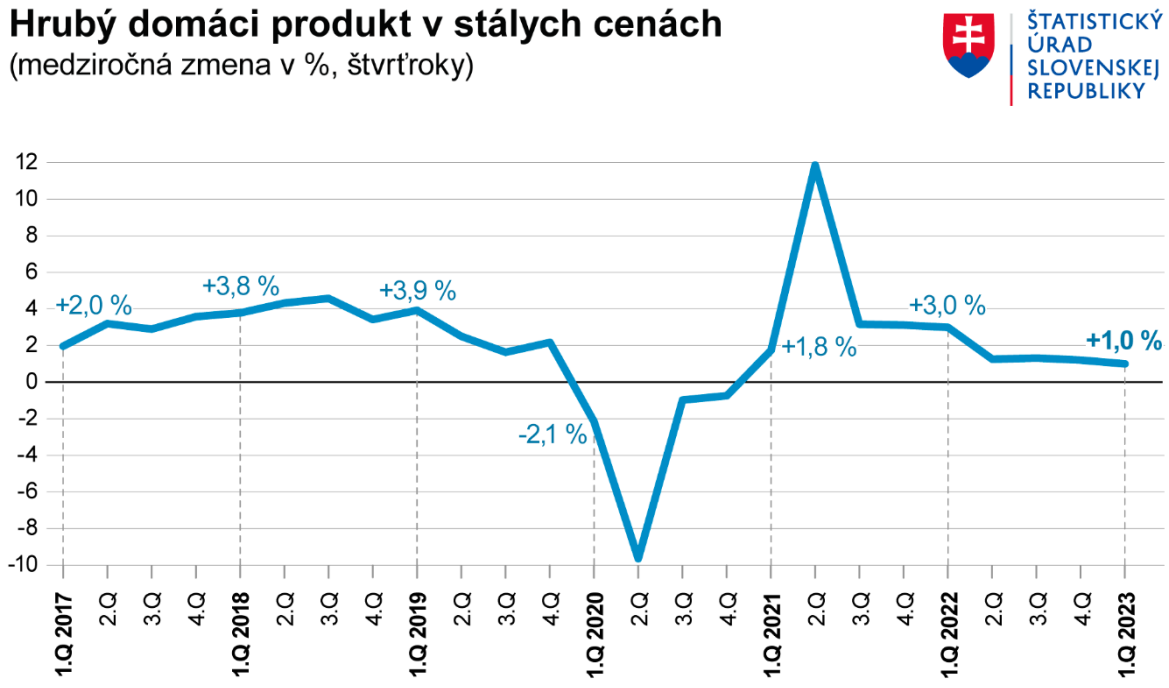
V medzinárodnom porovnaní výšky HDP patrí Slovenskej republike 61 priečka. [2]

HDP Slovenskej republiky v absolútnych číslach (v mld. USD):
Obrázok č.2



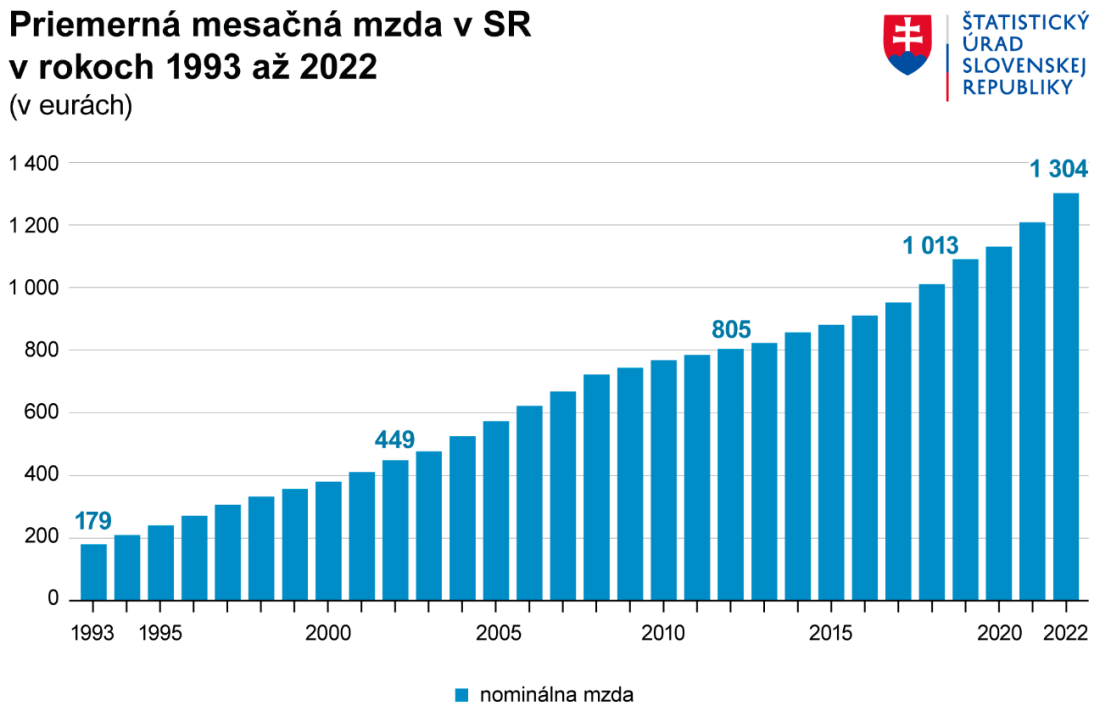
Zdroj: https://tradingeconomics.com/slovakia/gdp

Obrázok č.3



Zdroj: Štatistický úrad Slovenskej republiky

Obrázok č.4



Zdroj: Štatistický úrad Slovenskej republiky

Okrem ekonomických ukazovateľov poukazujúcich na stabilitu a rast ekonomiky je v kontexte VA / VASP sektoru veľmi dôležité vnímať aj zlepšujúca sa dostupnosť internetu a rast počtu používateľov internetu na Slovensku.

Počet používateľov internetu:
Obrázok č.5

Zdroj:
https://data.worldbank.org/indicator/IT.NET.USER.ZS?contextual=default&end=2022&locations=SK-EU-1W&start=2009

2. Kryptoadopcia

V poslednej dekáde sa sektor virtuálnych aktív (VA) vyvinul z marginálneho trhu, ktorý v období od roku 2009 (založenie Bitcoinu) do roku 2011 (jeho expanzia medzi užívateľmi, najmä z IT komunity), charakterizoval len limitovaný záujem, do významného ekonomického odvetvia s hodnotou v miliardách, resp. biliónoch dolárov. Dnes tento sektor preniká do mnohých iných oblastí, vrátane bankovníctva, financií a informačných technológií, čím sa stáva neoddeliteľnou súčasťou globálnej ekonomiky.

Nasledujúci graf ukazuje celkovú tržnú kapitalizáciu VA – kryptoaktív od roku 2013.
Obrázok č.6

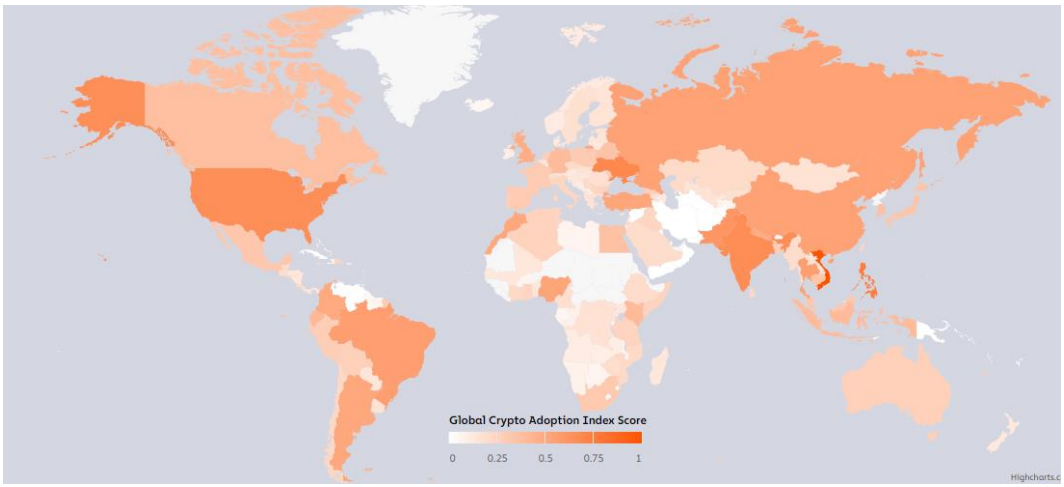
Zdroj: https://coinmarketcap.com/charts/ , dátum: 04.04.2023

Dve najvýznamnejšie obdobia trhového rastu, známe ako „bull runy“, keď došlo k nárastu trhovej kapitalizácie v dôsledku prílivu nových investorov a kapitálu, sa odohrali v rokoch 2018 a 2021.

Spoločnosť Chainalysis na svojom webovom sídle zverejnila Chainalysis' 2022 Global Crypto Adoption Index, ktorý sleduje adopciu kryptomien v jednotlivých štátoch. Zo 146 hodnotených krajín sa Slovenská republika umiestnila na 80. mieste s celkovým indexom adopcie kryptomien hodnoteným skóre 0,168. Najvyšší stupeň adopcie kryptomien zaznamenal Vietnam, ktorý s indexom 1,000 obsadil prvé miesto v rebríčku.
Z mapy nižšie je jasne vidieť, že krajiny v našom okolí ako Ukrajina (3 miesto), Poľsko (33 miesto) a Česká republika (62 miesto) majú vyššiu mieru kryptoadopcie medzi občanmi a inštitúciami, a naopak Maďarsko (91 miesto) a Rakúsko (107 miesto) nižšiu mieru adopcie.

Nasledujúci obrázok popisuje globálnu kryptoadapciu v roku 2022

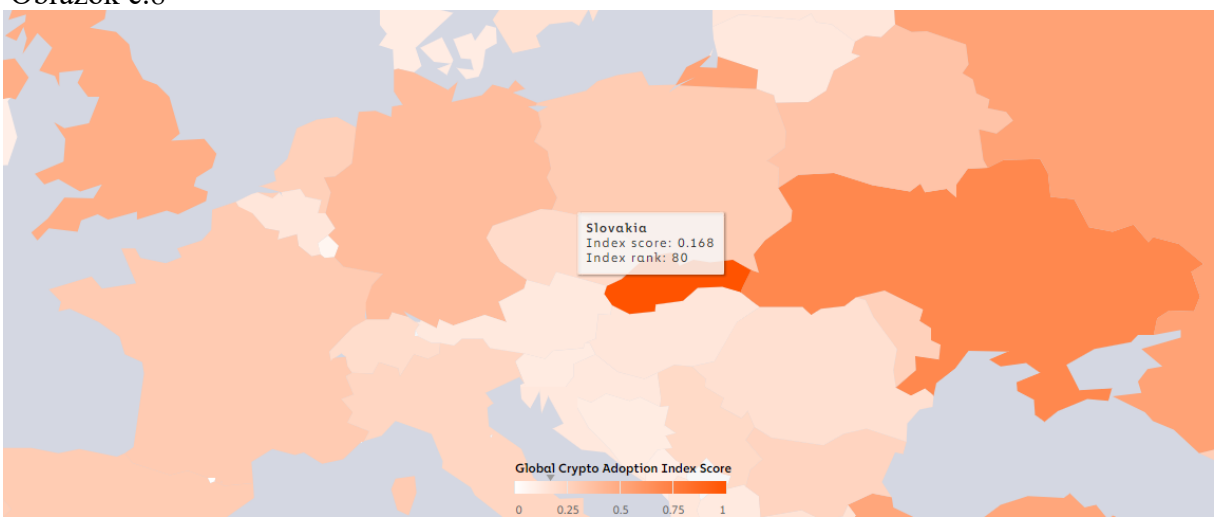
Obrázok č.7



Zdroj: https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

Porovnanie okolitých krajín so Slovenskom:

Obrázok č.8



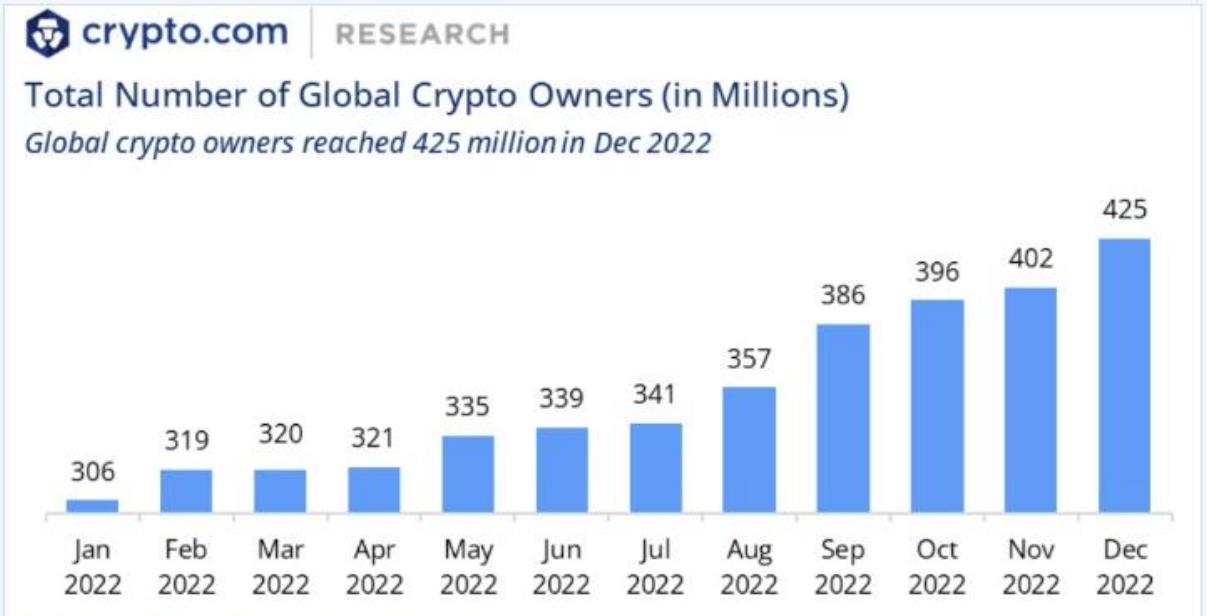
Zdroj: https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

Z mapy je jasne vidieť, že krajiny v našom okolí ako Ukrajina (v rebríčku 3), Poľsko (v rebríčku 33) a Česká republika (v rebríčku 62) majú vyššiu mieru kryptoadopcie medzi občanmi a inštitúciami, a naopak Maďarsko (rank 91) a Rakúsko (v rebríčku 107) nižšiu mieru adopcie.

V globálnom meradle má adopcia kryptomien kontinuálne rastúcu tendenciu a podľa prieskumu Crypto.com od 01/2022 do 12/2022 sa celkový počet používateľov zvýšil na celkových 425 milónov.

Nasledujúci obrázok popisuje vývoj vzrastu počtu držiteľov krypto aktív za rok 2022.

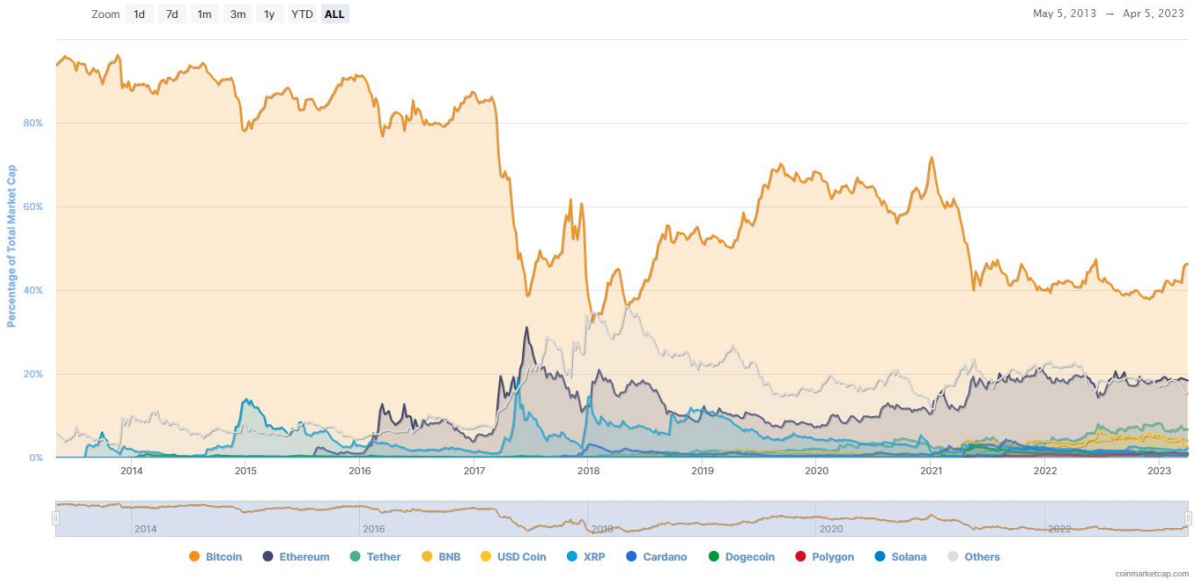
Obrázok č.9



Zdroj: Crypto.com

V súvislosti s rastom adopcie kryptomien je dôležité pozrieť sa aj na štruktúru takzvaného „Grafu dominancie Bitcoinu“, ktorý udáva percentuálne zastúpenie Bitcoinu na celkovej tržnej kapitalizácií celého krypta. Nasledujúci graf to graficky znázorňuje:

Obrázok č.10



Zdroj: https://coinmarketcap.com/charts/#dominance-percentage, dátum: 05.04.2023

Ku dňu 05.04.2023 webová stránka Coinmarketcap.com, ako kľúčový bod kumulujúci dáta o tržných kapitalizáciách jednotlivých kryptomien a tokenov uvádzala dáta o 23 199[1]

[1] https://coinmarketcap.com/charts/

kryptomien a tokenov. Toto enormné množstvo kryptomien a tokenov je takmer nemožné komplexne sledovať a vyhodnocovať v reálnom čase.

Množstvo potencionálnych hrozieb spojených s rizikom AML/CFT exponenciálne rastie oproti bežným kryptomenám a tokenom, pri kryptomenách, ktoré sa nazývajú tzv. „privacy coins“ taktiež nazývané anonymné meny.

Samostatná kapitola tejto sektorovej analýzy bude venovaná anonymným kryptomenám. Dôležité je ale poukázať na reštriktívny postup niektorých krajín voči týmto anonymným menám. Príkladom môže byť napríklad Južná Kórea, ktorá zakázala obchodovanie anonymných mien Monero a Zcash pre veľkú hrozbu spojenú s AML / CFT[2]. Dubaj v roku 2023 rovnako pristúpil na základe prijatia novej regulácie k zákazu anonymných kryptomien. Dubaj definuje anonymné kryptomeny ako: „typ virtuálneho aktíva, ktorý bráni vysledovaniu transakcií alebo záznamu o vlastníctve prostredníctvom distribuovaných verejných účtovných kníh a pre ktorý „poskytovateľ služieb virtuálneho aktíva“ (VASP) nemá žiadne zmierňujúce technológie alebo mechanizmy umožňujúce vysledovateľnosť alebo identifikáciu vlastníctva.“[3]

3. Vývoj sektora virtuálnych mien v Slovenskej republike do 31.12.2022

Virtuálne meny (napr. Bitcoin, Litecoin, Ethereum a ďalšie) nie sú v Slovenskej republike uznané ako oficiálna tuzemská či zahraničná mena, nepredstavujú elektronické peniaze v zmysle zákona o platobných službách[4] a nemajú fyzickú protihodnotu vo forme zákonného platidla. Napriek tomu je možné v tejto oblasti aj u nás sledovať permanentný dynamický vývoj, a to tak v smere technologickom, ako aj v oblasti stále pribúdajúcich subjektov pôsobiacich na trhu virtuálnych mien a služieb, ktorých ponuka priamo koreluje s primerane sa zväčšujúcim dopytom po virtuálnych menách u bežnej populácie. Pre takéto obchodovanie nie sú v súčasnosti zavedené žiadne osobitné požiadavky (v zmysle: akýkoľvek regulačný proces) a na podnikanie donedávna postačovalo len všeobecné živnostenské oprávnenie vo forme voľnej živnosti, pričom tieto subjekty nepodliehali ani AML dohľadu/kontrole.

Definícia:

Metodické usmernenie Ministerstva financií Slovenskej republiky č. MF/10386/2018-721 k postupu zdaňovania virtuálnych mien (ďalej len „metodické usmernenie“) uvádza aj definíciu virtuálnej meny, pod ktorou sa rozumie digitálny nositeľ hodnoty, ktorý nie je vydaný ani garantovaný centrálnou bankou ani orgánom verejnej moci, ani nie je nevyhnutne naviazaný na zákonné platidlo, nemá právny status meny alebo peňazí, ale je akceptovaný

[2] https://www.cpomagazine.com/data-privacy/south-koreas-new-crypto-aml-law-bans-trading-of-privacy-coins-monero-zcash/
[3] https://www.coindesk.com/policy/2023/02/08/dubai-prohibits-privacy-coins-under-new-crypto-rules/
[4] Zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v z. n. p.

niektorými fyzickými alebo právnickými osobami ako platobný prostriedok a ktorý možno prevádzať, uchovávať alebo s ním elektronicky obchodovať.

Novelou zákona 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 v znení neskorších predpisov (ďalej len „zákon“) účinnou od 01.11.2020, došlo k rozšíreniu taxatívne vymedzeného okruhu povinných osôb aj o právnické a fyzické osoby poskytujúce služby peňaženky virtuálnej meny a zmenárne virtuálnej meny (ďalej len „poskytovatelia služieb v oblasti virtuálnych mien“) - VASP. Uvedená novela bola v tejto časti implementáciou smernice európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa menila smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, do právneho poriadku Slovenskej republiky.

Práve neustály a rýchly technologický vývoj na jednej strane, v spojení s dĺžkou legislatívnych procesov na európskej aj vnútroštátnej úrovni na strane druhej, predstavuje jeden z najväčších limitov v nastavovaní optimálneho právneho rámca regulácie a kontroly v tejto oblasti.

Základy právneho rámca pre virtuálne meny sa začali postupne včleňovať do slovenského právneho poriadku od roku 2018.

1. októbra 2018 nadobudol účinnosť zákon o dani z poistenia[5] a zákon o účtovníctve[6] v rozsahu zadefinovania pojmov týkajúcich sa virtuálnych mien a ich zdaňovania.

Uvedeným novelám predchádzalo Metodické usmernenie Ministerstva financií Slovenskej republiky č. MF/10386/2018-721 k postupu zdaňovania virtuálnych mien (ďalej len „metodické usmernenie“), ktorým sa zabezpečuje jednotný výklad pri zdaňovaní príjmu plynúceho z predaja virtuálnej meny podľa zákona o dani z príjmov[7]. Podľa tohto metodického usmernenia sa príjem plynúci z predaja virtuálnej meny aj podľa zákona o dani z príjmov považuje za zdaniteľný príjem.

Detailné rozpracovanie zdanenia a identifikovaných trendov v tejto oblasti bude podrobne predstavené v neskorších sekciách tejto sektorovej analýzy. Dňa 01.11.2020 nadobudla účinnosť novela zákona o legalizácii[8], ktorou sa medzi povinné osoby v AML oblasti zaradili subjekty poskytujúce služby spojené s virtuálnymi menami, a to konkrétne poskytovatelia služieb peňaženky virtuálnej meny a poskytovatelia služieb zmenárne virtuálnej meny, ktorí sa profesionálne zaoberajú zmenárenskými službami medzi virtuálnou menou a fiat menami[9].

[5] Zákon č. 213/2018 Z. z. o dani z poistenia, ktorým bol okrem iného novelizovaný zákon č. 595/2003 Z. z. o dani z príjmov v z. n. p.
[6] Zákon č. 431/2002 Z. z. o účtovníctve v z. n. p.
[7] Zákon č. 595/2003 Z. z. o dani z príjmov v z. n. p.
[8] zákon č. 279/2020 Z. z., ktorým sa mení a dopĺňa zákon 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 v z. n. p. a ktorým sa menia a dopĺňajú niektoré zákony.
[9] t. j. mince a bankovky, ktoré sú označené ako zákonné platidlo a elektronické peniaze krajiny, prijímané ako prostriedok výmeny vo vydávajúcej krajine

Zároveň novelou zákona o legalizácii bol s účinnosťou od 01.11.2020 novelizovaný aj živnostenský zákon[10], na základe čoho boli poskytovatelia služieb zmenárne virtuálnej meny a poskytovatelia služieb peňaženky virtuálnej meny zaradení medzi viazané živnosti.

Práve novela zákona o legalizácií zo dňa 01.11.2020 sa stala kľúčovou pri smerovaní a monitorovaní ďalšieho vývoja sektora virtuálnych mien v Slovenskej republike. Všetky subjekty, ktoré do toho času podnikali v oblasti poskytovania služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny, si povinne museli na príslušnom živnostenskom úrade registrovať živnosť uvedenú v bode 82a (poskytovanie služieb zmenárne virtuálnej meny) a/alebo v bode 82b (poskytovanie služieb peňaženky virtuálnej meny) prílohy č. 2 živnostenského zákona.

Nasledovalo prechodné obdobie od 01.11.2020 do 28.02.2021, počas ktorého si subjekty poskytujúce služby zmenárne virtuálnej meny a/alebo služby peňaženky virtuálnej meny boli povinné tieto živnosti registrovať, nakoľko živnostenské oprávnenie vydané na živnosť, ktorá svojím obsahom spĺňala znaky poskytovania služieb zmenárne virtuálnej meny alebo poskytovania služieb peňaženky virtuálnej meny vydané do 31. októbra 2020 dňa 28. februára 2021 zaniklo.

Prechodné obdobie bolo zavedené aj pre zmeny prijaté zákonom o legalizácií. V období od 01. 11.2020 do 31.01.2021 bola poskytovateľom služieb zmenárne virtuálnej meny a poskytovateľom služieb peňaženky virtuálnej meny uložená povinnosť vypracovať program vlastnej činnosti podľa §20 zákona o legalizácii. V období do 31.05.2021 boli poskytovatelia služieb zmenárne virtuálnej meny a poskytovateľom služieb peňaženky virtuálnej meny zaviazaní povinnosťou dodatočne vykonať starostlivosť podľa ustanoví zákona o legalizácií ku všetkým existujúcim klientom.

Po ukončení prechodného obdobia v októbri 2021 FSJ zorganizovala úvodné (on-line) stretnutie pre povinné osoby. Školenie prebehlo on-line formou prostredníctvom WEBEX a bolo zamerané na zdôraznenie povinnosti poskytovateľov služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny, ktoré im vyplývajú zo zákona o legalizácií ako povinným osobám a aplikovanie ustanovení zákona v procese prevencie a odhaľovania legalizácie a financovania terorizmu pri činnosti povinnej osoby.

Už pri doručovaní pozvánok na školenie bola spozorovaná veľká diverzita subjektov, ktoré si predmetné činnosti registrovali s pomerne vysokým percentuálnym zastúpením takých, ktoré činnosť reálne nevykonávajú. Sekundárnym problémom, ktorý bol pri organizovaní školenia zaznamenaný bol nedostatočne nastavený komunikačný kanál medzi Finančnou spravodajskou jednotkou ako orgánom dohľadu v AML oblasti a poskytovateľmi služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny ako povinnými osobami v zmysle zákona o legalizácií. Doručovanie pozvánok na školenie prostredníctvom elektronického doručovacieho systému „slovensko.sk“ do elektronických schránok sa ukázalo ako neefektívne, nakoľko väčší počet subjektov pozvánku o plánovanom školení nedostal. Situácia bola operatívne riešená pracovníkmi Finančnej spravodajskej jednotky

[10] zákon č. 455/1991 Z. z. o živnostenskom podnikaní v z. n. p.

a komunikovaná ad hoc. Školenia sa následne zúčastnilo 24 osôb (z 92 subjektov, ktorým boli zaslané pozvánky cez Fabasoft), pričom len 19 osôb sa identifikovalo.

4. Súčasný licenčný proces na Slovensku

I) Všeobecnými podmienkami prevádzkovania viazanej živnosti sú:
- dosiahnutie veku 18 rokov
- spôsobilosť na právne úkony
- bezúhonnosť (preukazuje sa výpisom z registra trestov)

II) Podmienkou prevádzkovania živnosti je splnenie podmienky odbornej spôsobilosti, a to nasledovným spôsobom:
- doklad o ukončení úplného stredného všeobecného vzdelania alebo úplného stredného odborného vzdelania.

Registrované subjekty ktoré vykonávajú činnosť podľa § 5 ods. 2, písm. o) poskytovateľ služieb peňaženky virtuálnej meny a p) poskytovateľ služieb zmenárne virtuálnej meny, voči tretím stranám sa stávajú povinnými osobami a musia plniť všetky povinnosti stanovené zákonom 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 (ďalej len „AML zákon“).
Na Slovensku však absentuje špecializovaná právna úprava v predmetnom segmente. Pre porovnanie v iných finančných segmentoch ide napríklad o zákon 483/2011 Z.z o bankách, konkrétne § 7 (bankové povolenia), zákon 492/2009 Z.z. o platobných službách, konkrétne § 63, § 64, § 79a. Zákon č. 566/2001 Z.z. o cenných papieroch a investičných službách, konkrétne § 54, § 55, § 70 (povolenie, podmienky na udelenie povolenia), zákon č. 202/1995 Z.z. Devízový zákon, konkrétne § 6 (devízová licencia), zákon č.171/2005 Z.z. o hazardných hrách, konkrétne § 16 (podmienky licencie).

AML zákon stanovuje povinnosti subjektu podnikajúceho v segmente VA/VASP a určuje mu aj jeho povinnosti. Z hľadiska prevencie legalizácie je zvolená logická súslednosť, začínajúca určením vykonania povinnej starostlivosti ku klientovi.

Základnú starostlivosť ku klientovi je vždy potrebné vykonať v celom rozsahu § 10 ods. 1 AML zákona. Samotný AML zákon s prihliadnutím na teleologický výklad ustanovenia § 10 AML zákona nepripúšťa vykonanie základnej starostlivosti vo vzťahu ku klientovi odložiť až do momentu výberu finančných prostriedkov z účtu klienta. Povinnosť vykonať základnú starostlivosť vo vzťahu ku klientovi už pri uzatváraní obchodného vzťahu platí bez ohľadu na výšku obchodu.

Podľa § 10 ods. 1 AML zákona základná starostlivosť povinnej osoby vo vzťahu ku klientovi zahŕňa:

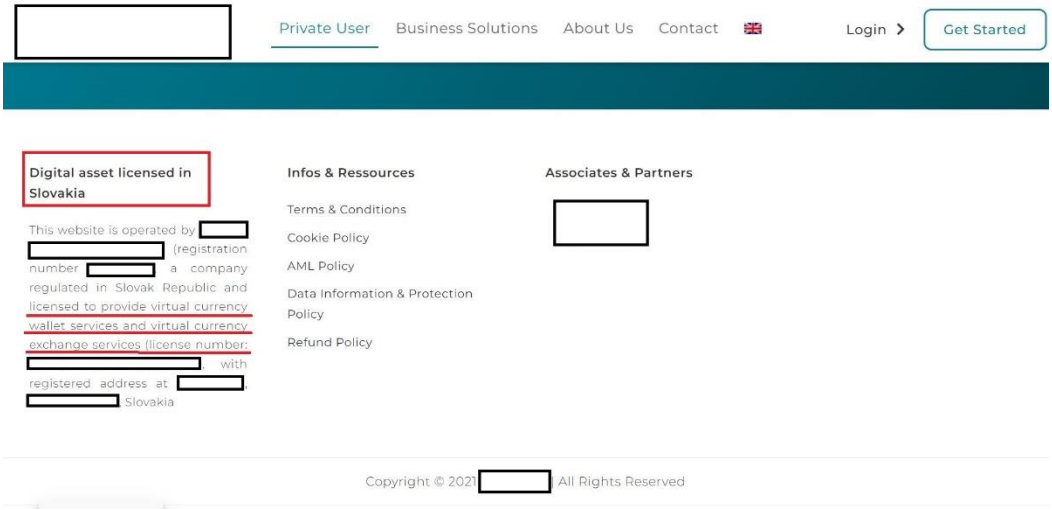
a) identifikáciu klienta a overenie jeho identifikácie,
b) identifikáciu konečného užívateľa výhod a prijatie primeraných opatrení na overenie informácií týkajúcich sa identifikácie konečného užívateľa výhod vrátane opatrení na zistenie vlastníckej štruktúry a riadiacej štruktúry klienta, ktorý je právnickou osobou alebo združením majetku; pri identifikácii konečného užívateľa výhod sa povinná osoba nesmie spoliehať výlučne na údaje získané z registra právnických osôb, podnikateľov a orgánov verejnej moci, ak na základe hodnotenia rizík podľa § 20a existuje vyššie riziko legalizácie alebo financovania terorizmu a je povinná overiť informácie týkajúce sa identifikácie konečného užívateľa výhod ešte z ďalšieho dôveryhodného zdroja,
c) získanie a vyhodnotenie informácií o účele a plánovanej povahe obchodu alebo obchodného vzťahu a informácií o povahe podnikania klienta,
d) zistenie, či klient alebo konečný užívateľ výhod klienta je politicky exponovanou osobou alebo sankcionovanou osobou,
e) v závislosti od rizika legalizácie alebo financovania terorizmu zistenie pôvodu finančných prostriedkov alebo majetku pri obchode alebo obchodnom vzťahu,
f) zistenie, či klient koná vo vlastnom mene,
g) vykonávanie priebežného monitorovania obchodného vzťahu vrátane preskúmania konkrétnych obchodov vykonaných počas trvania obchodného vzťahu na účel zistenia, či vykonávané obchody sú v súlade s poznatkami povinnej osoby o klientovi, jeho obchodnom profile, prehľade možných rizík spojených s klientom a so zdrojom finančných prostriedkov a majetku použitých pri obchodnom vzťahu alebo obchode, a zabezpečenie aktualizácie dokumentov, údajov alebo informácií, ktoré má povinná osoba k dispozícii o klientovi.

FSJ vykonáva priebežne kontroly u VASP-ov, vzhľadom na ich náročnosť a personálne možnosti je ale množstvo skontrolovaných subjektov v rádoch jednotiek z celkového množstva VASP-ov. FSJ na základe 3 vykonaných kontrol uložila 2 subjektom pokutu a sankciu zverejnenia rozhodnutia, ktoré zatiaľ nenadobudli právoplatnosť. Pri ďalšom subjekte je začaté správne konanie pre porušenie ustanovení AML zákona a zároveň pri jednom subjekte kontrola prebieha.

Subjekty podnikajúce v sektore virtuálnych aktív na základe živnostenského oprávnenia a so sídlom na Slovensku často využívajú princíp európskej pasportizácie. Na svojich webových stránkach potom uvádzajú, že sú „regulované a licencované“ na Slovensku. Toto tvrdenie, hoci je čiastočne pravdivé, môže byť v zmysle regulácie zavádzajúce, , kedže vzhľadom na nulové požiadavky zo strany regulátorov resp. neexistenciu regulátora je to zavádzajúce tvrdenie.

Príklad VASP-a registrovaného na Slovensku, deklarujúceho tvrdenia, že je licencovaný na poskytovanie služieb peňaženky virtuálnej meny a služby zmenárne virtuálnej meny, v súlade so zákonom. Ako číslo licencie uvádza iný identifikačný údaj a toto môže viesť k zmäteniu potencionálnych klientov a vzniku domnienky, že činnosť subjektu je plnohodnotne dohliadaná a regulovaná zo strany slovenských regulačných a dozorných orgánov.

Obrázok č.11



Zdroj: webová stránka VASP, 12/2022, monitoring FSJ

V praxi živnostenskému úradu bola daná len registračná povinnosť pre VASP-ov bez akéhokoľvek licenčného konania. Pre vydanie živnostenského oprávnenia je treba splniť nasledujúce základné podmienky:

Riziká spojené s absenciou procesov zameraných na preverenie pôvodu majetku a pozadia osôb zakladajúcich a riadiacich VASP-ov na Slovensku:

Za mimoriadne riziko možno považovať aj absenciu akéhokoľvek preverovania osôb a pôvodu počiatočného majetku spoločnosti, ktorá podniká ako:

I) Poskytovateľ služieb peňaženky virtuálnej meny - poskytovateľom služieb peňaženky virtuálnej meny osoba sa rozumie osoba, ktorá poskytuje služby na ochranu súkromných kryptografických kľúčov v mene jej klientov, na držbu, uchovávanie a prevod virtuálnej meny

a / alebo

II) Poskytovateľom služieb zmenárne virtuálnej meny - poskytovateľom služieb zmenárne virtuálnej meny osoba sa rozumie osoba, ktorá v rámci svojej podnikateľskej činnosti ponúka alebo vykonáva obchody s virtuálnou menou, ktorých predmetom je nákup virtuálnej meny za eurá alebo cudziu menu alebo predaj virtuálnej meny za eurá alebo cudziu menu.

V mnohých štátoch, vrátane členských krajín Európskej únie ale aj mimo nej, je proces udelenia licencie na podnikanie v oblasti kryptoaktív zo strany regulátora často spojený s dôkladným preverovaním pôvodu finančných prostriedkov, ktoré boli použité na založenie a prevádzku spoločnosti žiadajúcej o licenciu. Regulačné orgány spolu s inými príslušnými

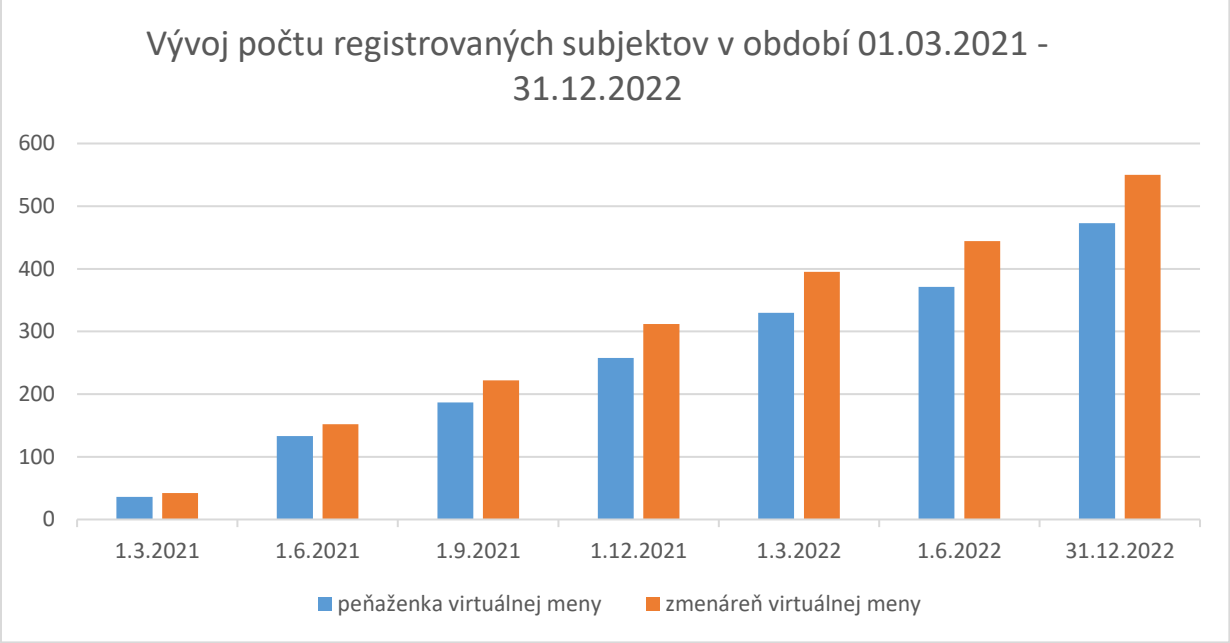
úradmi sa sústredia na overenie identity osôb stojacich za daným projektom, konečných užívateľov výhod a tiež personálne obsadenie spoločnosti, najmä na vrcholových pozíciách – v riadení a obzvlášť v oblasti compliance. Niektoré regulačné úrady dokonca explicitne vyžadujú, aby bol riaditeľ compliance alebo hlavný pracovník pre compliance miestny občan, teda z danej krajiny.

Jedným z významných rizík je pritom aj možnosť, aby VASP-ovia mali svoje sídlo na tzv. virtuálnych adresách. Tieto adresy môžu uľahčiť obchádzanie regulačných požiadaviek a skutočné fyzické umiestnenie spoločnosti zostáva často nejasné, čo komplikuje regulátorom možnosť vykonávať efektívny dohľad a kontroly.

5. Situácia na Slovensku

Priebežným preverovaním prostredníctvom odboru živnostenského podnikania sekcie verejnej správy Ministerstva vnútra Slovenskej republiky bol vzhľadom na veľkosť Slovenskej republiky zistený neprimerane vysoký počet subjektov, ktoré majú registrovaný predmet činnosti poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny (viď. graf č. 1).

Graf č.1



Vysoký nárast počtu subjektov, ktoré si registrovali ako predmet podnikania poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny ako aj informácie, ktoré FSJ získala počas organizovania školenia povinných osôb na jeseň 2021 viedol k vydaniu

usmernenia Finančnej spravodajskej jednotky k plneniu povinností podľa zákona č. 297/2008 Z. z. pre právnické osoby a fyzické osoby - podnikateľov, ktoré poskytujú služby peňaženky virtuálnej meny a zmenárne virtuálnej meny, ktoré sú zaradené medzi povinné osoby podľa § 5 ods. 1 písm. o) a p) zákona č. 297/2008 Z. z., z ktorého vyplýva nasledovné:

V súčasnosti poskytovateľ služieb v oblasti virtuálnych mien môže podľa platnej právnej úpravy danú činnosť vykonávať iba za predpokladu, že má príslušné živnostenské oprávnenie. Podrobnosti o ohlasovaní, druhoch a rozsahu živností Živnostenský zákon a príloha č. 2 (Viazané živnosti) Živnostenského zákona. Zápis Živnostenským zákonom určených údajov vykonávajú okresné úrady, odbor živnostenského podnikania.

Na základe príslušného živnostenského oprávnenia osoba v rámci svojej podnikateľskej činnosti poskytuje služby klientom (tretím osobám). Poskytovaním služieb v oblasti virtuálnych mien sa rozumie najmä prevádzkovanie webových sídiel či mobilných aplikácií umožňujúcich vykonávanie obchodov s virtuálnou menou (nákup virtuálnej meny za fiat menu a naopak), či prevádzkovanie/poskytovanie aplikácií alebo iných mechanizmov na držanie, ukladanie a prevod virtuálnej meny v mene ich klientov.

Poskytovateľ služieb v oblasti virtuálnych mien musí disponovať jednak príslušným živnostenským oprávnením v zmysle Živnostenského zákona a zároveň musí danú činnosť aj reálne vykonávať, t. j. svoje služby poskytovať klientom (tretím osobám). Ak osoba spĺňa uvedené predpoklady, možno ju zaradiť medzi povinné osoby podľa § 5 ods. 1 písm. o) a p) zákona o legalizácii. Uvedený právny názor vychádza z logického výkladu zákona, že osoba, ktorá reálne neposkytuje svoje služby v uvedenej oblasti nemá žiadnych klientov, nevykonáva obchody a neuzatvára obchodné vzťahy podľa § 9 písm. d), f) a g) zákona o legalizácii.

Podmienkami naplnenia definície povinnej osoby podľa § 5 ods. 1 písm. o) a p) zákona o legalizácii sú teda príslušné živnostenské oprávnenie v zmysle Živnostenského zákona a zároveň poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny klientom, ako predmet podnikateľskej činnosti.

Na základe uvedeného, slovenská právnická osoba alebo fyzická osoba - podnikateľ, ktorá má predmetné živnostenské oprávnenie na poskytovanie služieb peňaženky virtuálnej meny a/alebo zmenárne virtuálnej meny, avšak túto službu žiadnym klientom reálne neposkytuje, nie je povinnou osobou v zmysle § 5 ods. 1 písm. o) a p) zákona o legalizácii. Povinnou osobou je osoba iba v prípade, keď v rámci svojej podnikateľskej činnosti poskytuje služby v oblasti virtuálnych mien. Za výkon podnikateľskej činnosti nie je možné považovať správu vlastného majetku, ak pri nej nedochádza k výkonu určitej podnikateľskej činnosti. Za výkon podnikateľskej činnosti v oblasti virtuálnych mien teda nemožno považovať nákup a predaj virtuálnej meny za fiat menu na burzách, držbu virtuálnej meny v peňaženke virtuálnej meny a podobne, ak daná osoba koná vo vlastnom mene (na vlastný účet) a s vlastným majetkom, t. j. využíva služby iných subjektov, ale sama žiadne služby tretím osobám neposkytuje.

Slovenské právnické alebo fyzické osoby - podnikatelia poskytujúce služby v oblasti virtuálnych mien sú pri poskytovaní takýchto služieb zaradené medzi povinné osoby v zmysle § 5 ods. 1 písm. o) a p) zákona o legalizácii len, ak túto činnosť majú uvedenú v predmete podnikania, čiže majú na to živnostenské oprávnenie. V opačnom prípade pôjde o protiprávne

konanie, ktoré porušuje Živnostenským zákonom stanovenú povinnosť vykonávať určitú podnikateľskú činnosť na základe živnostenského oprávnenia, a zároveň bude zakladať deliktuálnu resp. trestnoprávnu zodpovednosť osoby za takéto konanie (neoprávnené podnikanie).

6. Výsledky prieskumu sektora poskytovateľov služieb virtuálnej meny v Slovenskej republike spracovaného za obdobie do 30.06.2022 dotazníkovou formou.

V priebehu júla 2022 bolo zo strany Finančnej spravodajskej jednotky distribuovaných spolu 451 dotazníkov, ktoré boli zaslané všetkým subjektom s registrovaným predmetom činnosti poskytovanie služieb zmenárne virtuálnej meny a/alebo poskytovanie služieb peňaženky virtuálnej meny registrovaným do 30.06.2022. Vzhľadom na predchádzajúce skúsenosti s doručovaním prostredníctvom slovensko.sk, nakoľko bolo potrebné dôslednejšie odsledovať reálnu doručiteľnosť dotazníkov subjektom, bola tentokrát zvolená zo strany Finančnej spravodajskej jednotky forma poštového doručenia. Výsledky, ktoré sa tým dosiahli, boli relevantnejšie a poskytli zaujímavý pohľad do sektora poskytovateľov služieb virtuálnej meny v Slovenskej republike.

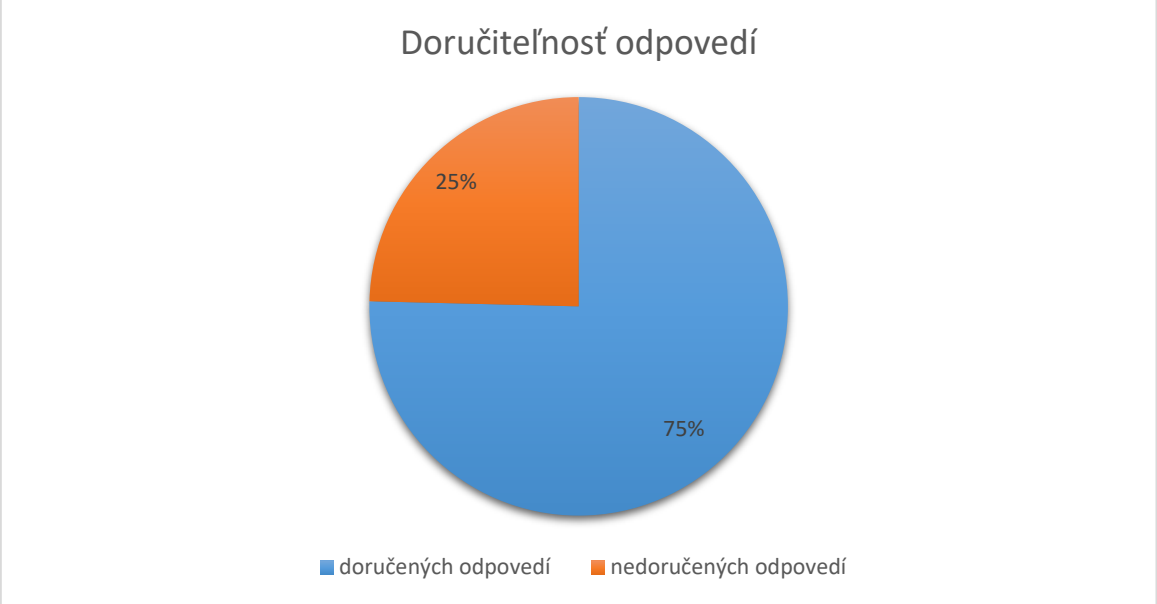
Súčasťou zasielaných dotazníkov bolo aj metodické usmernenie Finančnej spravodajskej jednotky k plneniu povinností podľa zákona č. 297/2008 Z. z. pre právnické osoby a fyzické osoby - podnikateľov, ktoré poskytujú služby peňaženky virtuálnej meny a zmenárne virtuálnej meny, ktoré sú zaradené medzi povinné osoby podľa § 5 ods. 1 písm. o) a p) zákona o legalizácií a Indikátory rizikovosti pre poskytovateľov služieb zmenárne virtuálnej meny a poskytovateľov služieb peňaženky virtuálnej meny, spracované Finančnou spravodajskou jednotkou. Zaslanie uvedených dokumentov, ktoré sú síce zverejnené na webovom sídle Finančnej spravodajskej jednotke, ale mnohé subjekty o nich nemali vedomosť malo pozitívny obojstranný edukačný efekt. Mnohé subjekty na základe doručeného dotazníka kontaktovali Finančnú spravodajskú jednotku telefonicky alebo mailom a prejavili ochotu spolupracovať pri sektorovom hodnotení rizík. Z nemenej veľkého počtu kontaktov však vyplynuli otázky a nedorozumenia, ktoré v sektore virtuálnych mien súčasná legislatívna úprava vyvoláva.

Podrobnou analýzou a vyhodnotením doručených a neprevzatých zásielok bolo zistené, že z celkového počtu zaslaných dotazníkov (spolu 451) bolo približne 82% úspešne doručených adresátom. Zásielky si z rôznych dôvodov neprevzalo 80 subjektov (cca 18%). Finančnej spravodajskej jednotke boli doručené odpovede od spolu 340 subjektov, čo predstavuje cca 74%. V tomto bode treba poznamenať, že niektoré subjekty, ktoré si dotazník prebrali odpoveď nezaslali, iné aj napriek tomu, že zásielku prevziať nestihli, vyplnený dotazník Finančnej spravodajskej jednotke doručili.

Tento aspekt naznačuje, že subjekty pôsobiace v infraštruktúre virtuálnych aktív na Slovensku sú vzájomne prepojené a disponujú medzi sebou dobre nastavenými komunikačnými kanálmi. Tieto prepojenia a komunikačné štruktúry by v budúcnosti mohli byť efektívne využité na zlepšenie spolupráce s dozornými a regulačnými orgánmi. Rozšírenie a optimalizácia týchto komunikačných kanálov by mohla podstatne prispieť k transparentnosti, lepšiemu monitoringu a efektívnejšej regulácii celého sektora, čím by sa zvýšila jeho bezpečnosť a dôveryhodnosť. Táto synergia by zároveň poskytla regulátorom lepšie nástroje pre prevenciu a riešenie potenciálnych rizík v oblasti virtuálnych aktív.

Graf č.2

Graf č.3



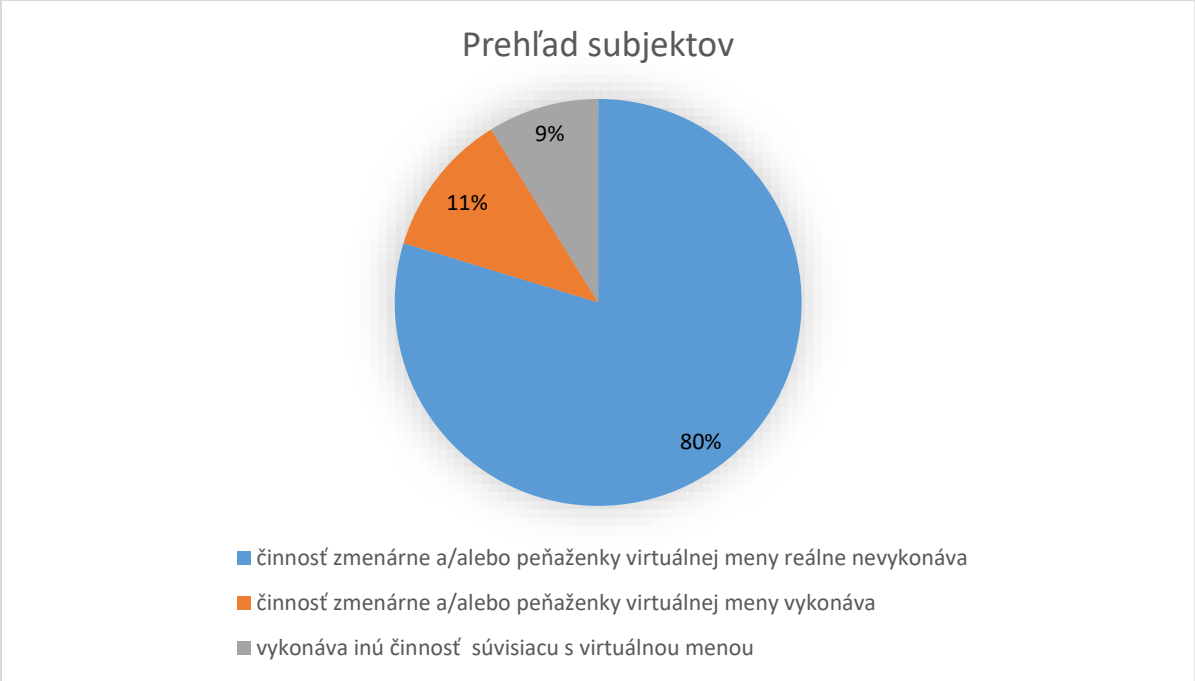
Ďalšou analýzou a vyhodnocovaním došlých odpovedí bolo zistené, že z 340 odpovedí doručených Finančnej spravodajskej jednotke až 271 subjektov (cca 80 %) uvádza, že činnosť nevykonáva. Takmer polovica z týchto respondentov uviedla, že si predmet činnosti poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny registrovala v presvedčení, že ide o obligatórnu povinnosť v prípade ak chce svoje prostriedky či už osobné alebo z podnikania investovať do virtuálnej meny. Tieto subjekty majú reálne skúsenosti s nákupom a držbou virtuálnej meny pre vlastnú potrebu a považujú ju za veľmi bezpečný a dôveryhodný prostriedok na zhodnotenie investícií alebo formu sporenia. Obchodujú výlučne s vlastnými prostriedkami a služby pre tretie osoby neposkytujú.

Zvyšné subjekty, ktoré mali ako predmet činnosti registrované poskytovanie služieb zmenárne virtuálnej meny a/alebo poskytovanie služieb peňaženky virtuálnej meny a uviedli, že činnosť nevykonávajú, s virtuálnou menou vôbec neprichádzajú do kontaktu a dôvody, pre ktoré požiadali o živnostenské oprávnenie v tejto oblasti je možné zhrnúť ako laický záujem, podporovaný pozitívnymi mediálnymi informáciami o atraktívnych ziskoch, kombinovaný s jednoduchým procesom registrácie, absenciou komplikovanejších požiadaviek na vydanie oprávnenia pre poskytovanie služieb zmenárne a/alebo peňaženky virtuálnej meny (rovnaké ako pri iných), ktorý nie je spoplatnený (je jedno koľko živností si subjekt zapíše, poplatok platí stále rovnaký). Väčšina týchto subjektov nemala ani minimálnu vedomosť o tom, že zápisom živnosti poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny zároveň spĺňajú predpoklad pre povinnú osobu v zmysle zákona o legalizácií, z ktorého im vyplývajú konkrétne povinnosti.

Vyhodnocovaním odpovedí bola zároveň identifikovaná samostatná skupina subjektov, ktoré služby zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny neposkytujú, avšak sú aktívne podnikateľský činné na trhu s virtuálnou menou ako takou resp. sa na činnosti spojenej s virtuálnou menou aktívne pripravujú. Do tejto skupiny sú zahrnuté subjekty, ktoré deklarujú činnosti ako ťažba kryptomeny, vývoj nových softvérových riešení, staking či poskytovanie marketingových a vzdelávacích služieb.

Medzi subjektami, ktoré uvádzajú, že vykonávajú iné služby sa objavil aj kryptomenový fond, ktorý na Slovensku vznikol a na svojom webovom sídle uvádza, že je registrovaný pod Národnou bankou Slovenska (https://www.cveu.eu/).

Graf č.4

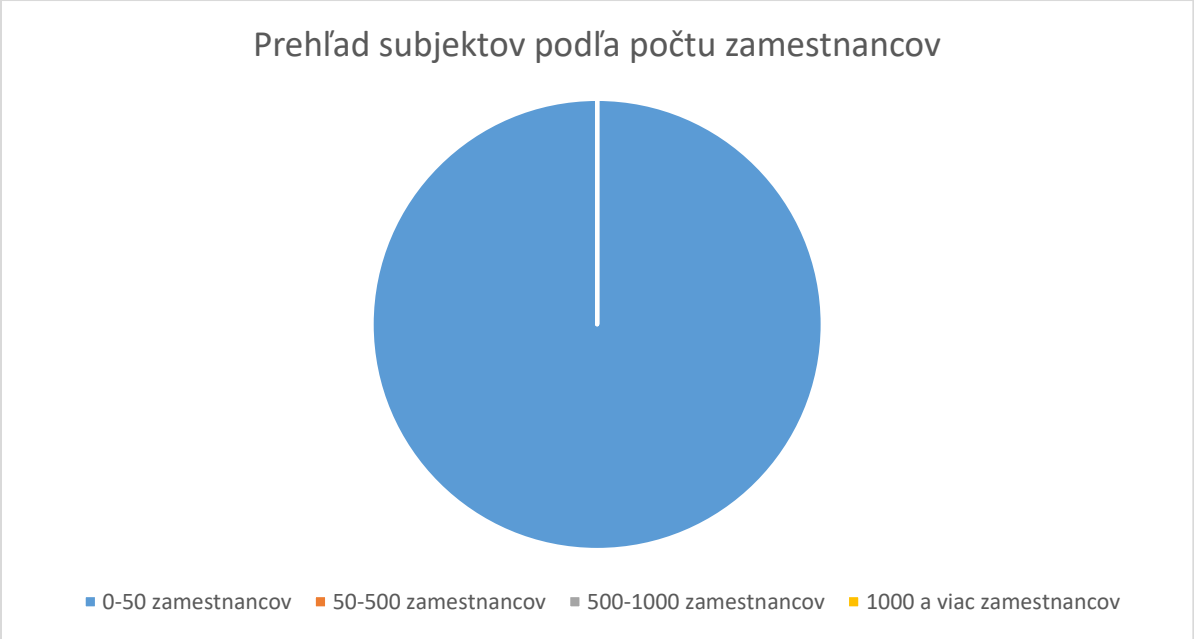


Ďalšie vyhodnocovanie dotazníkov bolo primárne zamerané na informácie od subjektov, ktoré mali ku dňu 30.06.2022 platné živnostenské oprávnenie pre poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny a zároveň aj reálne túto činnosť vykonávali pre tretie osoby (klientov).

6.1. Geografické kritéria

Takýmto spôsobom bolo zistené, že 100% subjektov vykonávajúcich činnosti zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny v Slovenskej republiky sú menšieho rozsahu a uvádzajú počet zamestnancov do 50. Značná časť subjektov dokonca uvádzala, že nemá žiadnych zamestnancov.

Graf č.5

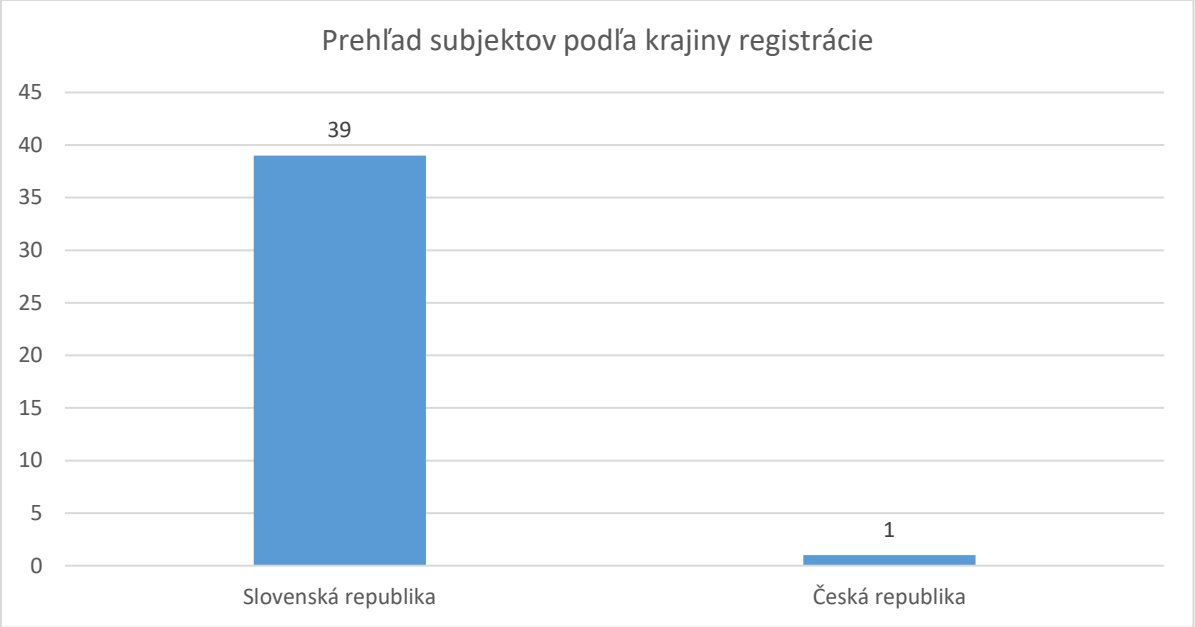


Analýzou kritérií geografickej lokalizácie subjektov bolo zistené, že drvivá väčšina je ako VASP registrovaná len v Slovenskej republike. Iba jeden subjekt uviedol, že je registrovaný v Slovenskej republike aj v Českej republike.

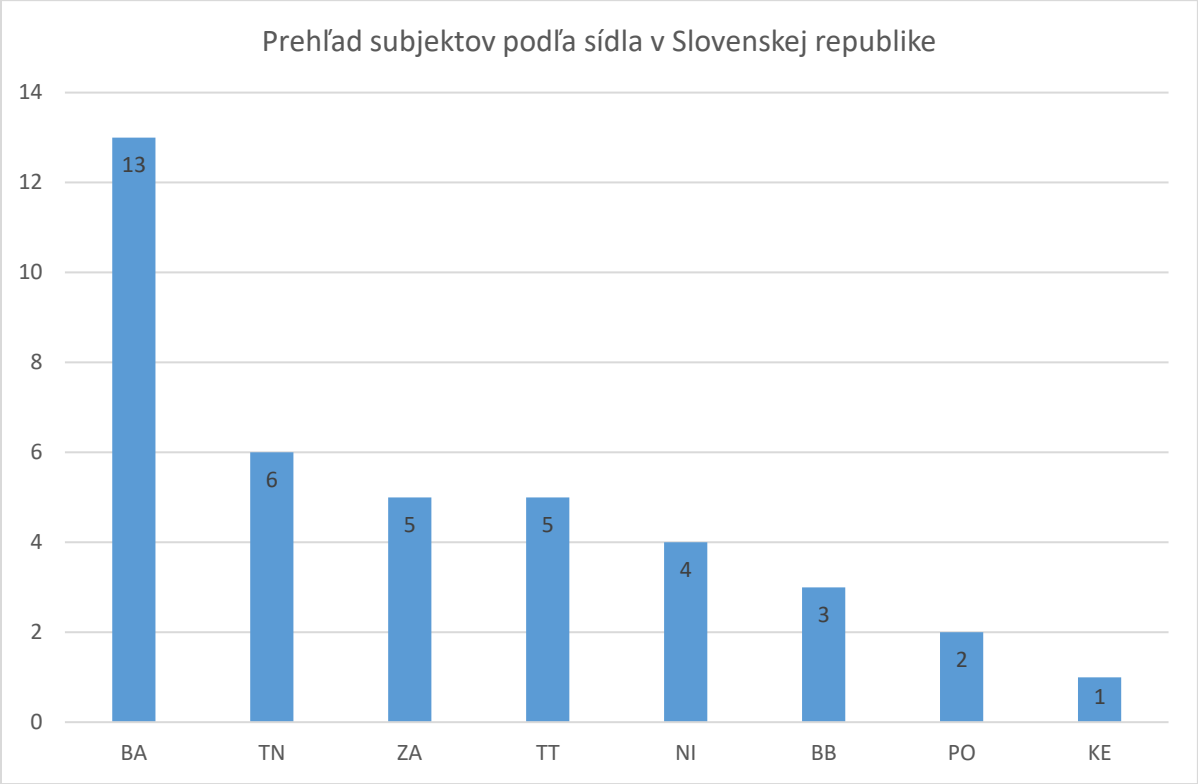
Porovnaním adries sídiel spoločností bolo zistené, že jednotlivé subjekty sú rozvrstvené v rámci celého územia Slovenskej republike s výraznejšou dominanciou bratislavského kraja. Pre bližšie informácie viď graf č. 7.

Zaujímavým geografickým kritériom, ktoré bolo vyhodnotené nad rámec otázok z dotazníka sa týka majetkového pozadia jednotlivých spoločností registrovaných a podnikajúcich ako poskytovatelia služieb virtuálnej meny v Slovenskej republike. Pri vyhodnotení tejto oblasti boli využité zdroje z Obchodného registra Slovenskej republiky k subjektom figurujúcim ako štatutár, majiteľ či akcionár spoločnosti. Z uvedeného bolo zistené, že vyhodnocované subjekty, ktoré v Slovenskej republike podnikajú s virtuálnou menou má rovnako aj majetkové pozadie v Slovenskej republike, avšak časť subjektov vykazuje znaky zložitejšej majetkovoprávnej štruktúry s prepojením na zahraničné právnické a/alebo fyzické osoby bez preukázaného vzťahu k Slovenskej republike. Tieto skutočnosti bližšie reflektuje graf č. 8.

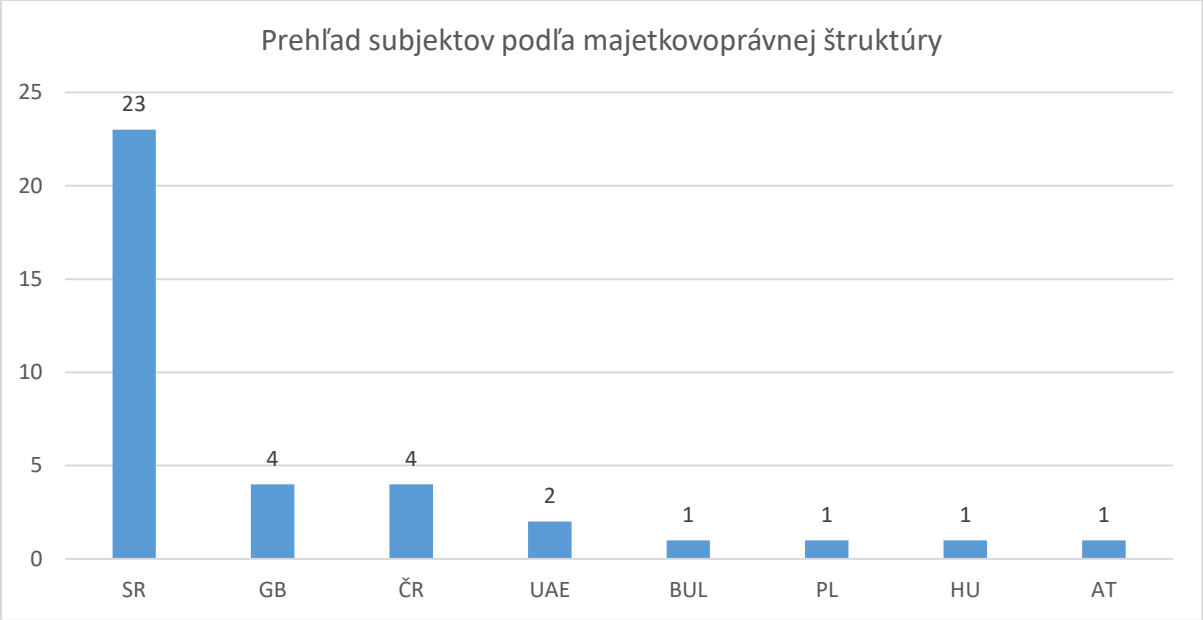
Graf č.6



Graf č.7

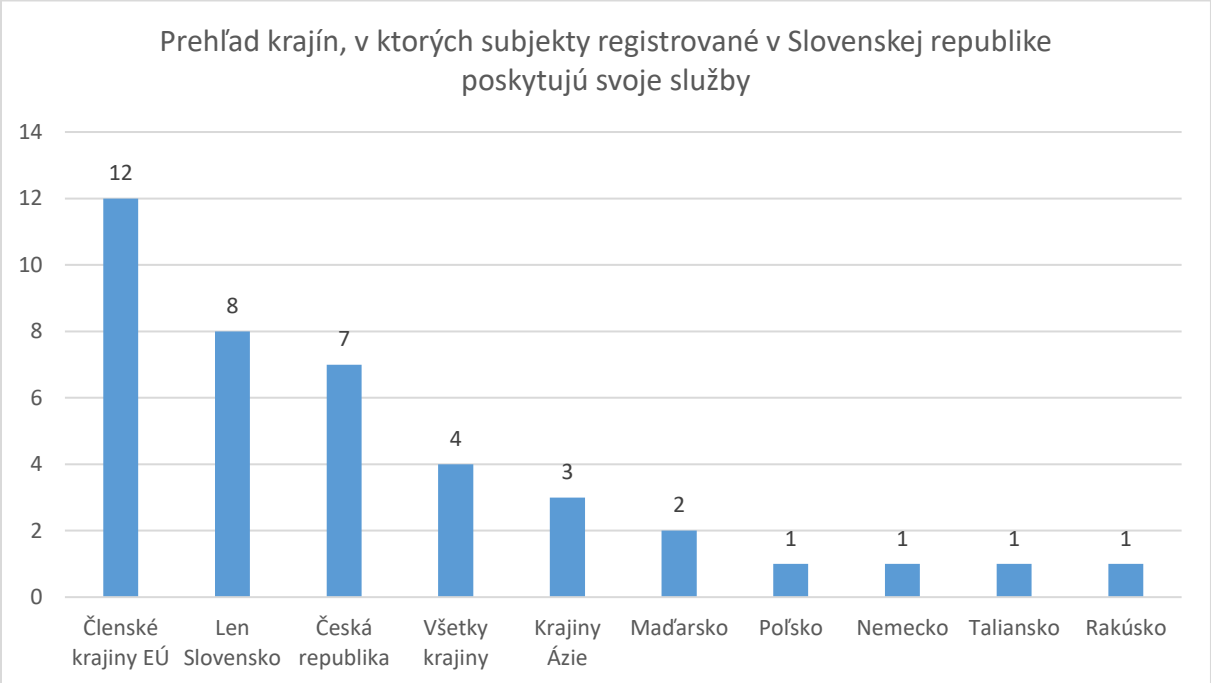


Graf č.8



Vzhľadom na nadnárodný charakter virtuálnych mien, väčšina subjektov registrovaných v Slovenskej republike poskytuje služby virtuálnej meny aj v iných krajinách, pričom väčšina sa orientuje na európske krajiny (najmä Česká republika, ale aj iné krajiny EÚ). Na tomto mieste je potrebné vyzdvihnúť, že všetky subjekty vyjadrili vysoké porozumenie a rešpekt vo vzťahu ku krajinám so zvýšeným bezpečnostným rizikom, s ktorými spoluprácu vylučujú.

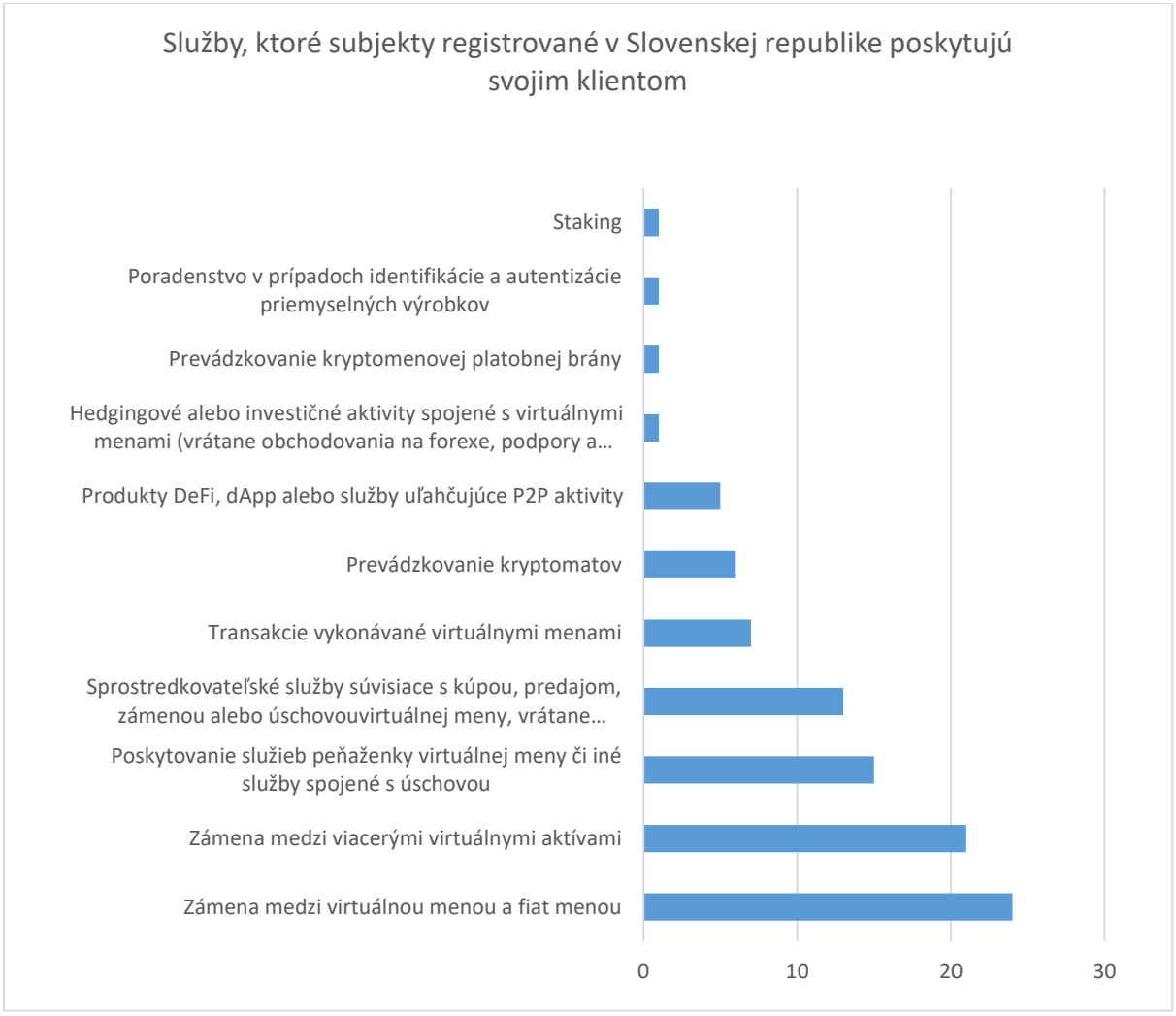
Graf č.9



6.2. Služby spojené s virtuálnou menou na území Slovenskej republiky

Medzi služby, ktoré subjekty registrované v Slovenskej republike najčastejšie poskytujú svojím klientom patrí zámena virtuálnej meny za fiat menu a zámena medzi viacerými virtuálnymi menami navzájom, poskytovanie služieb peňaženky virtuálnej meny či iné služby spojené s úschovou a sprostredkovateľské služby súvisiace s kúpou, predajom, zámenou alebo úschovou virtuálnej meny, vrátane stablecoinov, tokenov či privatcoinov. V menšom rozsahu subjekty uvádzali aj transakcie vykonávané virtuálnymi menami a produkty DeFi, dApp alebo služby uľahčujúce P2P aktivity. 6 subjektov ako činnosť uviedlo prevádzkovanie kryptomatov. Celkový prehľad poskytovaných služieb reflektuje graf č. 8.

Graf č.10

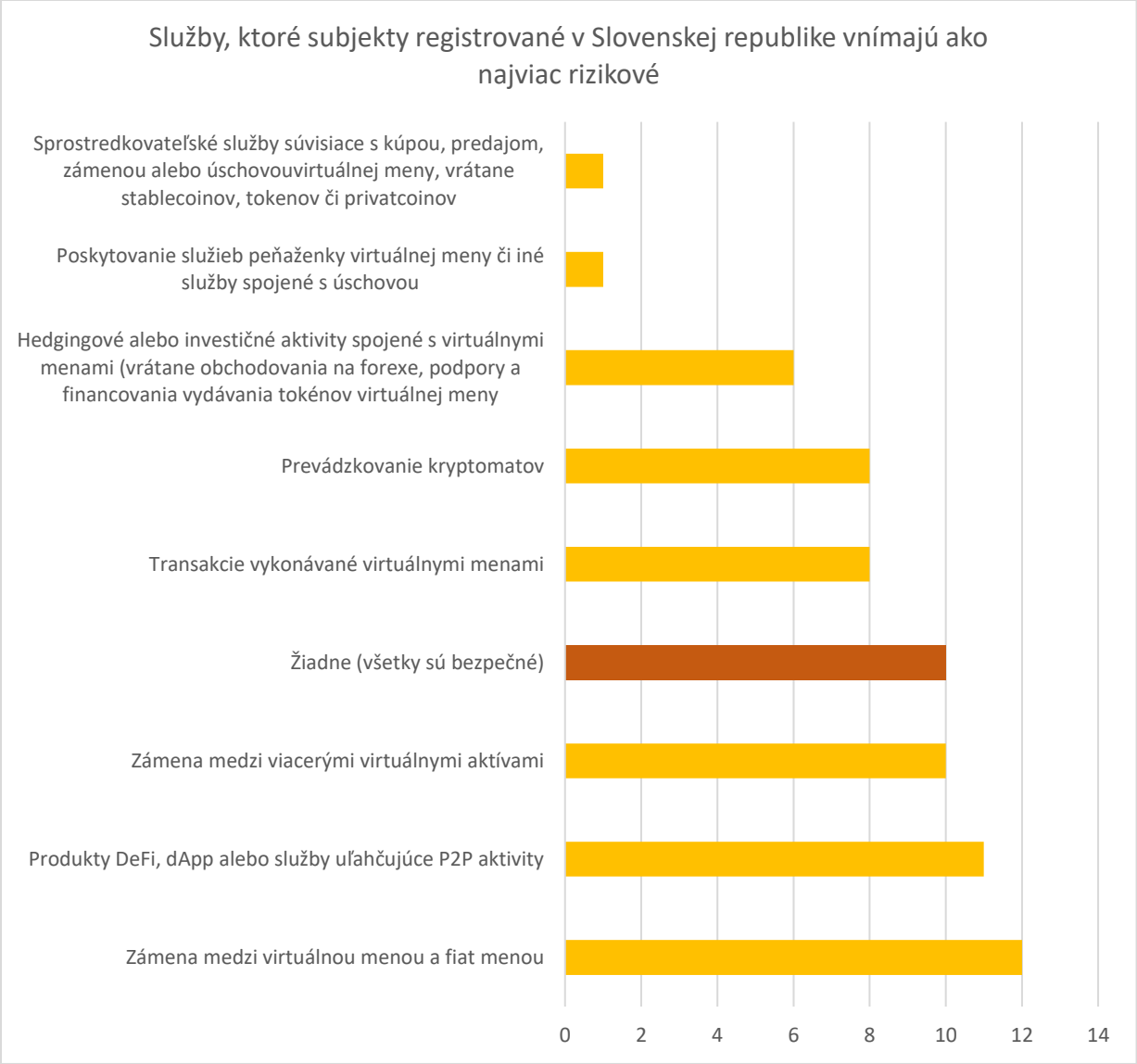


Zaujímavý vhľad do vnímania rizikovosti sektora poskytuje analýza odpovedí na otázku, ktoré zo služieb poskytovaných klientom považujú samotné subjekty podnikajúce ako zmenárne a/alebo peňaženky virtuálnej meny, za najviac rizikové v spojení s ich možným

zneužitím pre účely legalizovania výnosov z trestnej činnosti či financovania terorizmu, kde až 16% respondentov uviedlo, že riziko nevnímajú žiadne resp. si ho neuvedomujú.

Ďalší respondenti zvýšené riziko legalizovania výnosov z trestnej činnosti a/alebo financovania terorizmu vnímali hlavne v spojitosti s konverziou virtuálnej meny za fiat menu, v prípade zámeny medzi viacerými virtuálnymi menami navzájom a v spojitosti s produktmi DeFi, dApp alebo službami uľahčujúce P2P aktivity. Časť opýtaných vníma riziko aj v súvislosti s prevádzkovaním kryptomatov, v transakciách vykonávaných s virtuálnymi menami a v spojení s hedgingovými alebo investičnými aktivitami (vrátane obchodovania na forexe, podpory a financovania vydávania tokenov virtuálnej meny). Ako najmenej rizikové sa respondentom javia sprostredkovateľské služby súvisiace s kúpou, predajom, zámenou alebo úschovou virtuálnej meny, vrátane stablecoinov, tokenov či privatcoinov a poskytovanie služieb peňaženky virtuálnej meny alebo iné služby spojené s úschovou virtuálnej meny.

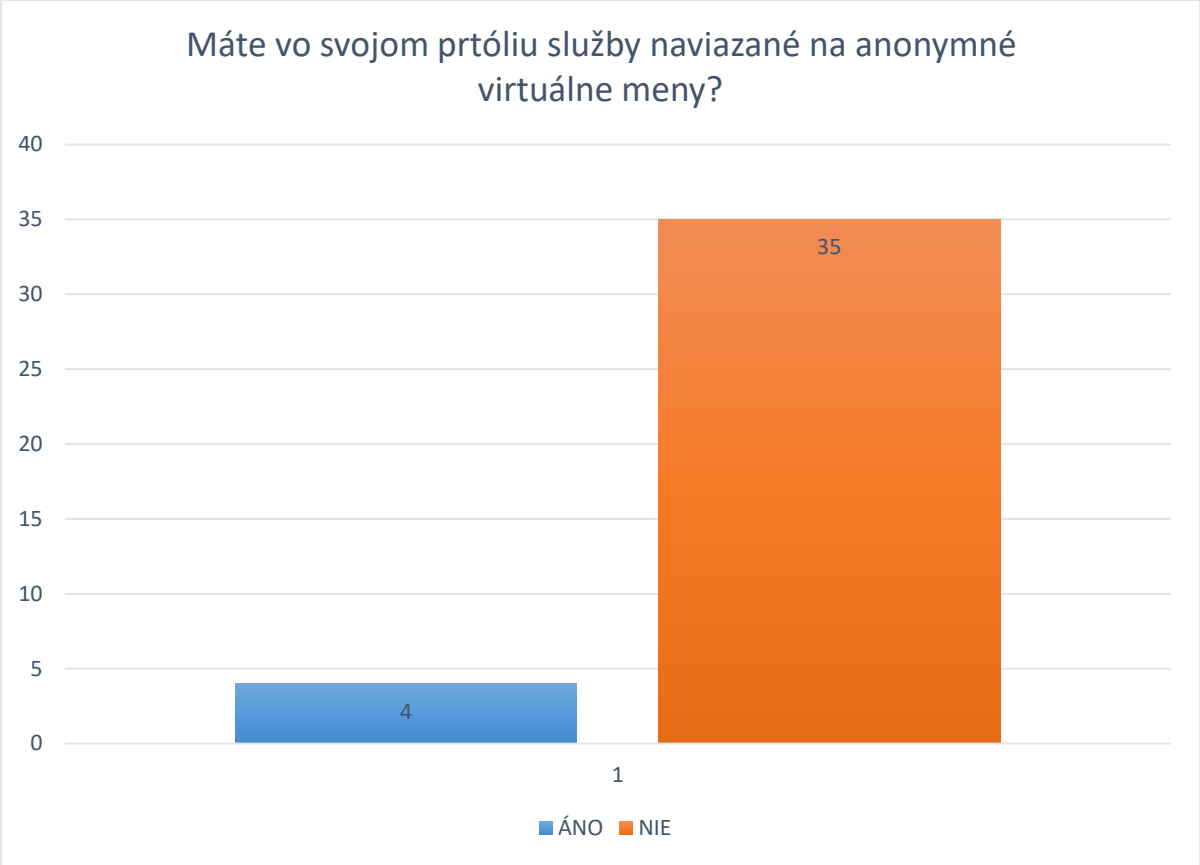
Graf č.11



6.3. Anonymné virtuálne meny a produkty zamerané na anonymizáciu a sťaženie identifikácie pôvodu virtuálnych mien.

V rámci analýzy služieb spojených s virtuálnou menou, ktoré sú subjektmi registrovanými v Slovenskej republike poskytované tretím osobám vo vzťahu k vyhodnoteniu potenciálneho rizika legalizovania výnosov z trestnej činnosti a/alebo financovania terorizmu sa ako dôležité javí monitorovanie využívania produktov naviazaných na anonymné virtuálne meny, ako aj produktov zameraných na anonymizáciu a sťaženie identifikácie pôvodu virtuálnych mien (napr. rôzne druhy mixérov, VPN a pod.).

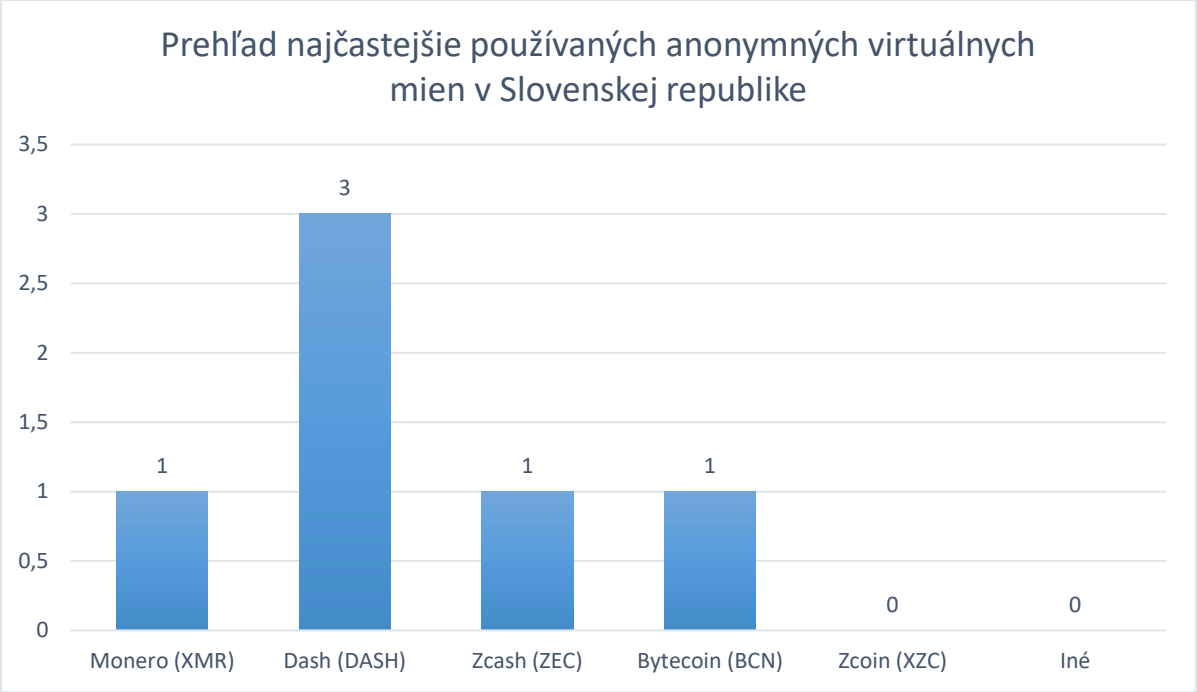
Graf č.12



Väčšina subjektov registrovaných v Slovenskej republike ako zmenárne a/alebo peňaženky virtuálnej meny uvádza, že v svojom portfóliu služby naviazané na anonymné virtuálne meny nevedie. Čiastočné používanie anonymných virtuálnych mien uviedli len štyri subjekty, pričom z ich odpovedí vyplýva, že najčastejšie používanou anonymnou virtuálnou menou v Slovenskej republike je Dash (DASH).

Využívanie produktov zameraných na anonymizáciu a sťaženie identifikácie pôvodu virtuálnych mien (napr. rôzne druhy mixérov, VPN a pod.) odmietajú zhodne všetky subjekty. Niektorí z respondentov nad rámec dotazníkovej otázky uviedli, že sami iniciatívne používajú softvér na detekciu kryptomenových peňaženiek pripojených k mixérom a takéto peňaženky následne odmietajú.

Graf č.13



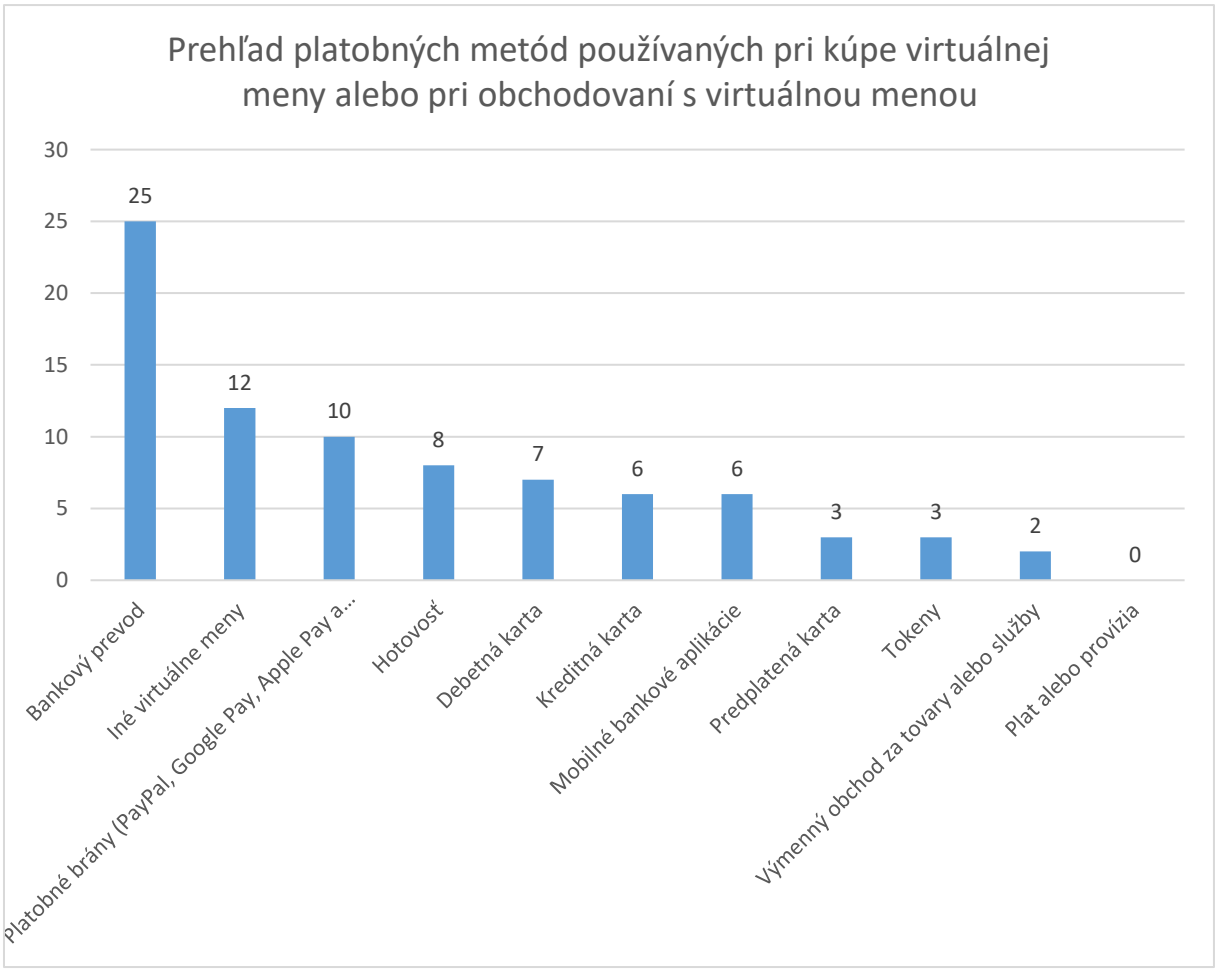
Graf č.14

6.4. Platobné metódy využívané na nákup virtuálnej meny alebo pri obchodovaní s virtuálnou menou.

Medzi najčastejšie uvádzané metódy používané klientmi zmenárni a/alebo peňaženiek virtuálnej meny registrovanými v Slovenskej republike pri kúpe virtuálnej meny alebo pri obchodovaní s virtuálnou menou patrí jednoznačne bankový prevod, ktorý primárne využíva pri poskytovaní služieb tretím osobám, väčšina subjektov registrovaná v Slovenskej republike.

Ďalšími platobnými metódami, ktoré boli respondentmi opakovane uvádzane sú hotovosť, iné virtuálne meny a platobné brány (PayPal, Google Pay, Apple Pay a pod.). Naopak na nákup virtuálnej meny a/alebo obchodovanie v Slovenskej republike vôbec nie je využívaný plat alebo provízia. Prehľad všetkých uvádzaných platobných metód bližšie reflektuje graf č. 15.

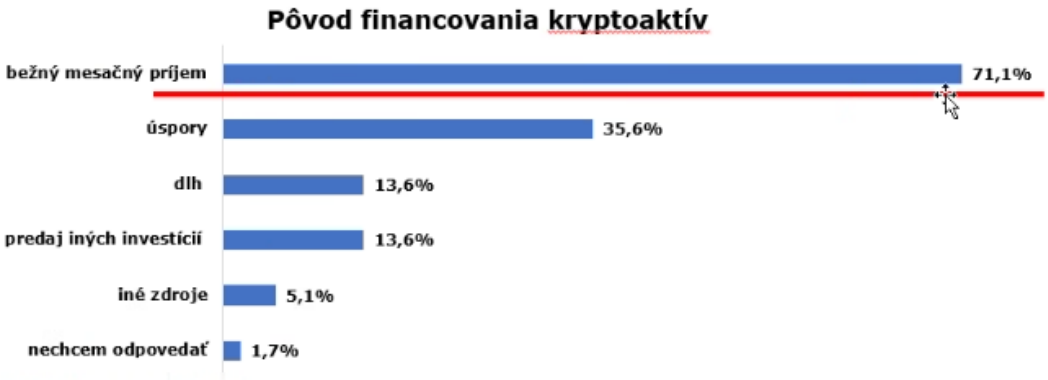
Graf č. 15



Je dôležité poznať aj formu financovania nákupu VA. NBS vykonala prieskum zameraný na využívanie virtuálnych aktív spotrebiteľmi (obdobie 26.11. – 3.12.2021) prieskum robila agentúra FOCUS: (1010 respondentov). Z tohto komplexného prieskumu NBS publikovala rozsiahlu správu dostupnú na webovej stránke NBS a nasledujúcom linku:

(https://nbs.sk/dokument/e7c683b5-f817-4abf-bd4d-34d19081f707/stiahnut/?force=false). Súčasťou tohto prieskumu bola aj otázka zameraná na pôvod finančných prostriedkov respondentov, ktorými financujú nákup VA.

Graf č. 16



Zdroj: Prieskum NBS

V uvedenom prieskume NBS, oslovení respondenti najčastejšie financovali nákup VA zo svojho bežného mesačného príjmu. S veľkým odstupom nasledujú financovanie pomocou úspor, ktoré využilo niečo cez 35 % respondentov. Vyše 13 % respondentov na účely nákupu VA predali iné investície vo svojom portfóliu a rovnaké percento financoval nákup VA pomocou dlhu. Iné zdroje využilo iba niečo cez 5 % oslovených respondentov. Financovať nákup VA pomocou dlhu je nesmierne rizikové, môže sa totiž stať, že dlžník bude potrebovať splatiť svoj dlh, ale vďaka významnej volatilite nebude schopný predať svoje VA za cenu za ktorú ich nakúpil. Väčšina oslovených respondentov si túto rizikovosť zrejme uvedomuje a preto dlh na financovanie nákupu VA nevyužíva.

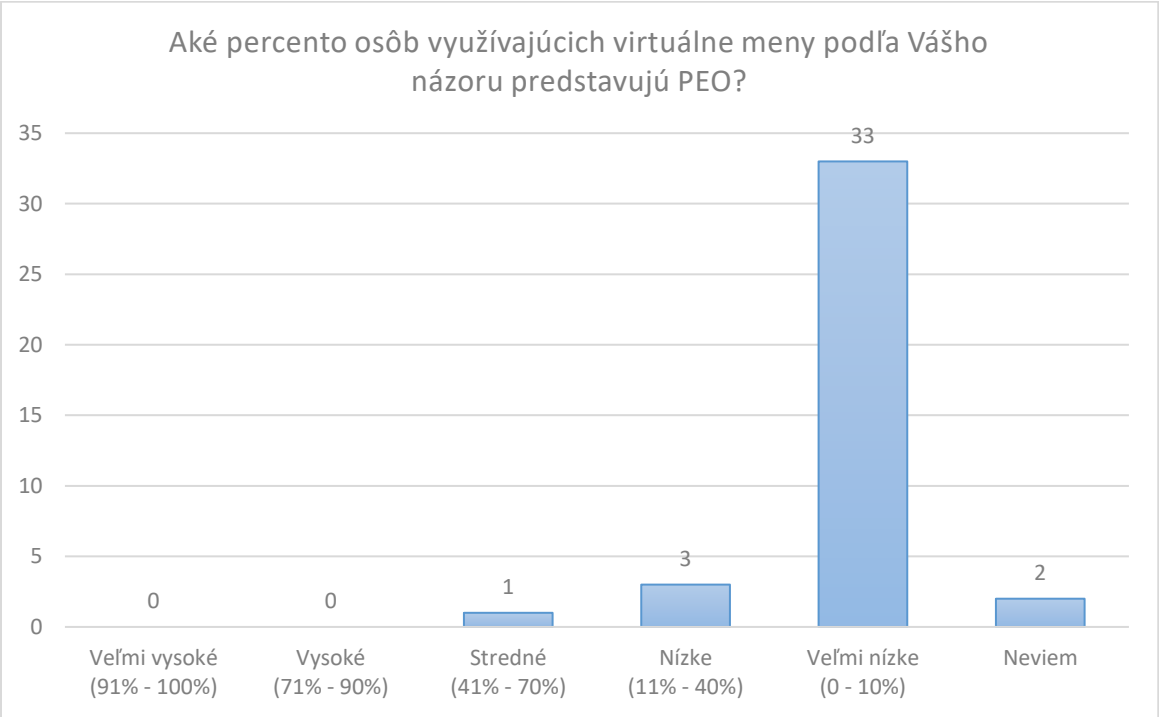
7. Súvislosť medzi virtuálnou menou a trestnou činnosťou

7.1. Politicky exponované osoby a trestná činnosť páchaná vo verejnej správe v kontexte virtuálnej meny.

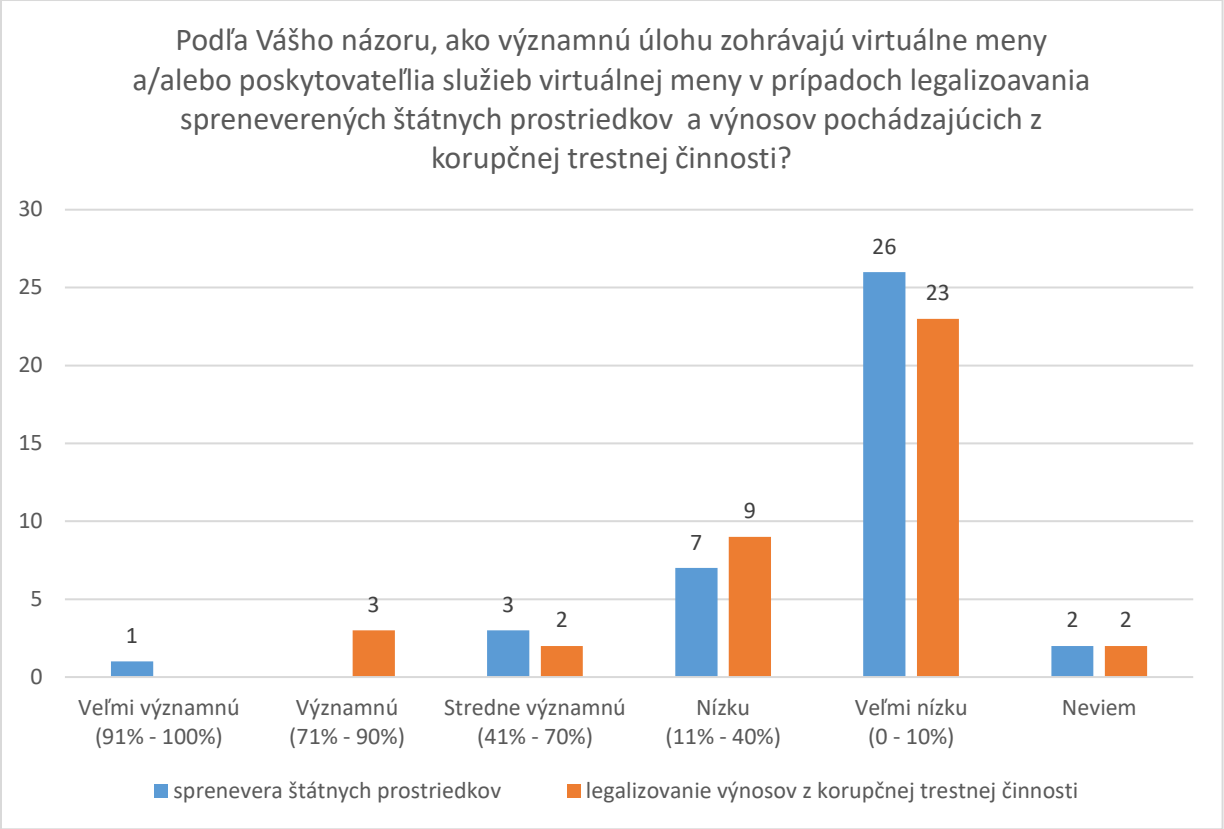
V rámci distribuovaných dotazníkoch bola časť otázok zameraná na zisťovanie počtu politicky exponovaných osôb, ktoré by svoje finančné prostriedky investovali do virtuálnej meny ako aj na zisťovanie úlohy, ktorú virtuálne meny ako také alebo služby s nimi spojené zohrávajú v prípadoch legalizovania sprenevierených finančných prostriedkov a korupčnej trestnej činnosti. V úvode je potrebné upozorniť, že zistené výsledky reflektované v grafoch 16 – 18 boli získané od subjektov, ktoré poskytujú služby virtuálnej meny v Slovenskej republike a odrážajú jednak ich osobné skúsenosti získané v priebehu výkonu ich podnikateľskej činnosti ako aj subjektívny názor na danú oblasť.

Jednotlivé odpovede, ktoré sa podarilo zozbierať, sa preto veľmi odlišovali, pričom škála vnímania danej problematiky korelovala od pragmatického a realistického postoja až po úplne odmietanie politicky exponovaných osôb ako klientov. Pozitívnym znakom však je, že väčšina subjektov uviedla, že pri vzniku obchodného vzťahu ako aj v priebehu jeho trvania zisťuje (resp. preveruje) politicky exponované a sankcionované osoby. Časť subjektov na niektoré otázky nevedela odpovedať a je zrejmé, že v danom smere by bolo vhodné posilniť edukáciu zo strany orgánov verejnej moci.

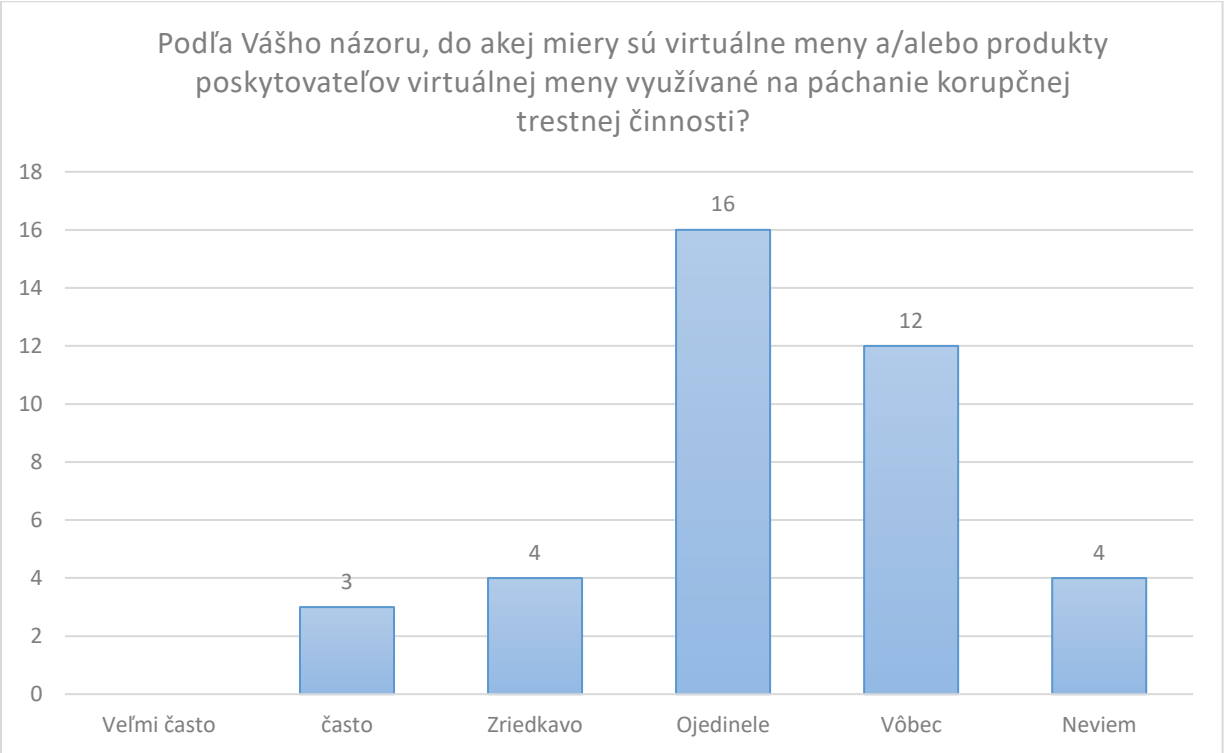
Graf č.17



Graf č.17



Graf č.189



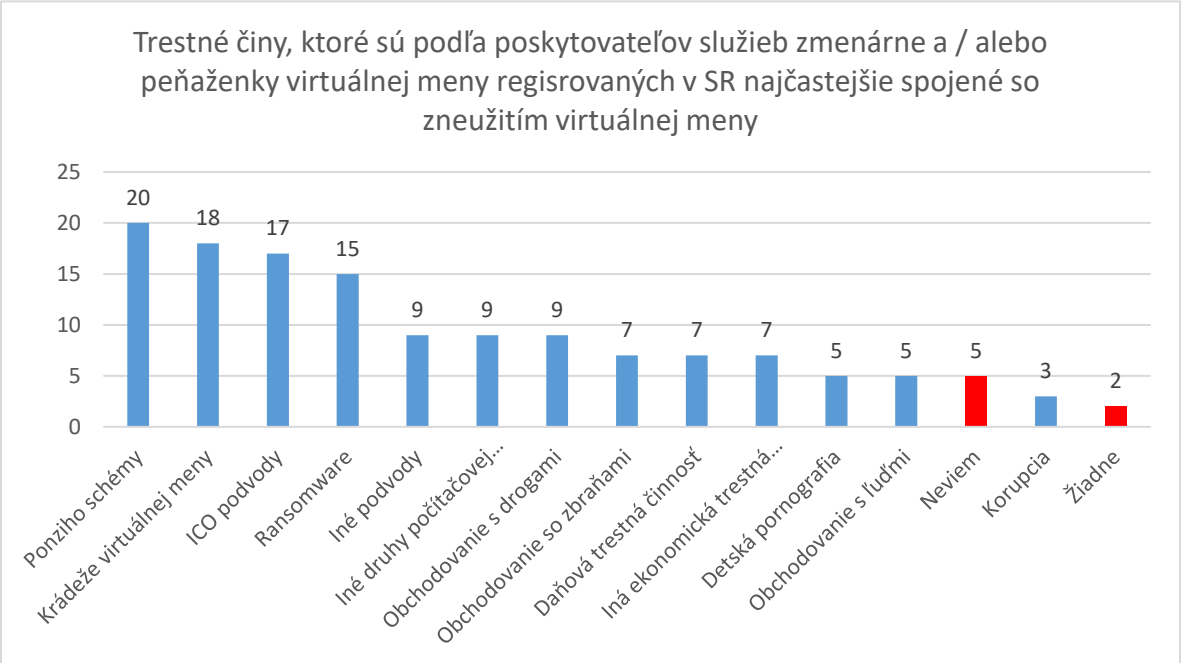
7.2. Trestné činy, najčastejšie spojené so zneužitím virtuálnej meny

To, že virtuálna mena môže byť ľahko zneužiteľná na páchanie trestnej činnosti alebo na zakrývanie pôvodu finančných prostriedkov získaných trestnou činnosťou je praxou preukázaný fakt, ktorý potvrdzujú aj skúsenosti Finančnej spravodajskej jednotky Slovenskej republiky a slovenských orgánov činných v trestnom konaní.

Odpovede na otázky vyhodnocovaného dotazníka však preukázali, že nie všetky subjekty podnikajúce v Slovenskej republike s virtuálnymi menami sú si dostatočne vedomé rizík spojených s využívaním virtuálnej meny na páchanie trestnej činnosti. Rozdiely v odpovediach však môžu byť spôsobené aj rôznou škálou činností a rôznorodým zložením klientely respondentov, ktorých odpovede boli vyhodnocované. Na jednej strane bola badateľná skupina subjektov, ktoré problematiku prepojenia virtuálnych mien na trestnú činnosť berú mimoriadne seriózne, sami iniciatívne registrujú a monitorujú situáciu nielen pokiaľ ide o vnútroštátne pomery, ale aj v medzinárodnom kontexte. Druhú stranu spektra však tvoria subjekty, ktoré s poukazom na charakter a rozsah ich podnikateľskej činnosti, okruh klientov alebo osobnostné nastavenie, riziko zneužitia virtuálnych mien na páchanie trestnej činnosti buď vôbec neriešia, alebo ho dokonca v ojedinelých prípadoch bagatelizujú.

Ktoré trestné činy vnímajú subjekty podnikajúce v Slovenskej republike ako zmenáreň a/alebo peňaženka virtuálnej meny ako najčastejšie spojené so zneužitím virtuálnej meny alebo služieb poskytovateľa virtuálnej meny reflektuje graf č. 19. Vo všeobecnosti najčastejšie uvádzali podvodné „ponziho“ schémy, krádeže virtuálnej meny, ICO podvody a randsomware.

Graf č.20



7.3. Krádeže virtuálnej meny

Krádež virtuálnej meny bol v rámci vyhodnocovania dotazníkového prieskumu jedným z najčastejšie uvádzaných trestných činov spojených s virtuálnou menou. Našťastie väčšina respondentov, ktorých dotazníky boli vyhodnocované krádež virtuálnej meny v ich spoločnosti nezažila, ale našli sa aj takí, čo museli čeliť pokusom páchateľov uvedeného trestného činu. Len jeden subjekt priznáva, že v jeho spoločnosti ku krádeži virtuálnej meny reálne došlo.

Graf č.21

Subjekty, ktoré vykonávajú činnosť zmenárne a/alebo peňaženky virtuálnej meny v Slovenskej republike bez príslušnej registrácie alebo licencie a subjekty, ktoré porušujú pravidla krajiny v AML oblasti.

Všetci respondenti, ktorých odpovede boli v rámci spracovania tejto analýzy vyhodnocované, zhodne uvideli, že nemajú vedomosť o tom, že by na území Slovenskej republiky existoval subjekt, ktorý činnosť zmenárne a/alebo peňaženky virtuálnej meny vykonáva bez príslušnej registrácie alebo licencie alebo subjekt, ktorý by systematicky porušoval pravidla krajiny v AML oblasti. V tomto bode je potrebné spomenúť, že nad rámec otázky subjekty (či už priamo v texte dotazníka, alebo pri osobnej komunikácií s pracovníkom FSJ) vyjadrovali vysokú mieru snahy a ochoty spolupracovať v AML oblasti a dodržiavať pravidlá, ktoré sú však pre mnohých nezrozumiteľné.

V nadväznosti na vyššie uvedené je však potrebné skonštatovať, že činnosťou Finančnej spravodajskej jednotky boli zaznamenané tri subjekty, ktoré v Slovenskej republike podnikajú ako poskytovatelia služieb zmenárne a peňaženky virtuálnej meny, ktoré pri svojej činnosti neaplikujú pravidla krajiny v AML oblasti úplne korektne a ich činnosť môže predstavovať zvýšené riziko legalizovania výnosov z trestnej činnosti. K týmto subjektom boli zo strany Finančnej spravodajskej jednotky v priebehu rokov 2021 a 2022 spracované viaceré rozsiahle operačné analytické výstupy, ktoré boli následne postúpené mieste a vecne príslušným policajným zložkám Slovenskej republiky na ďalšie previerky.

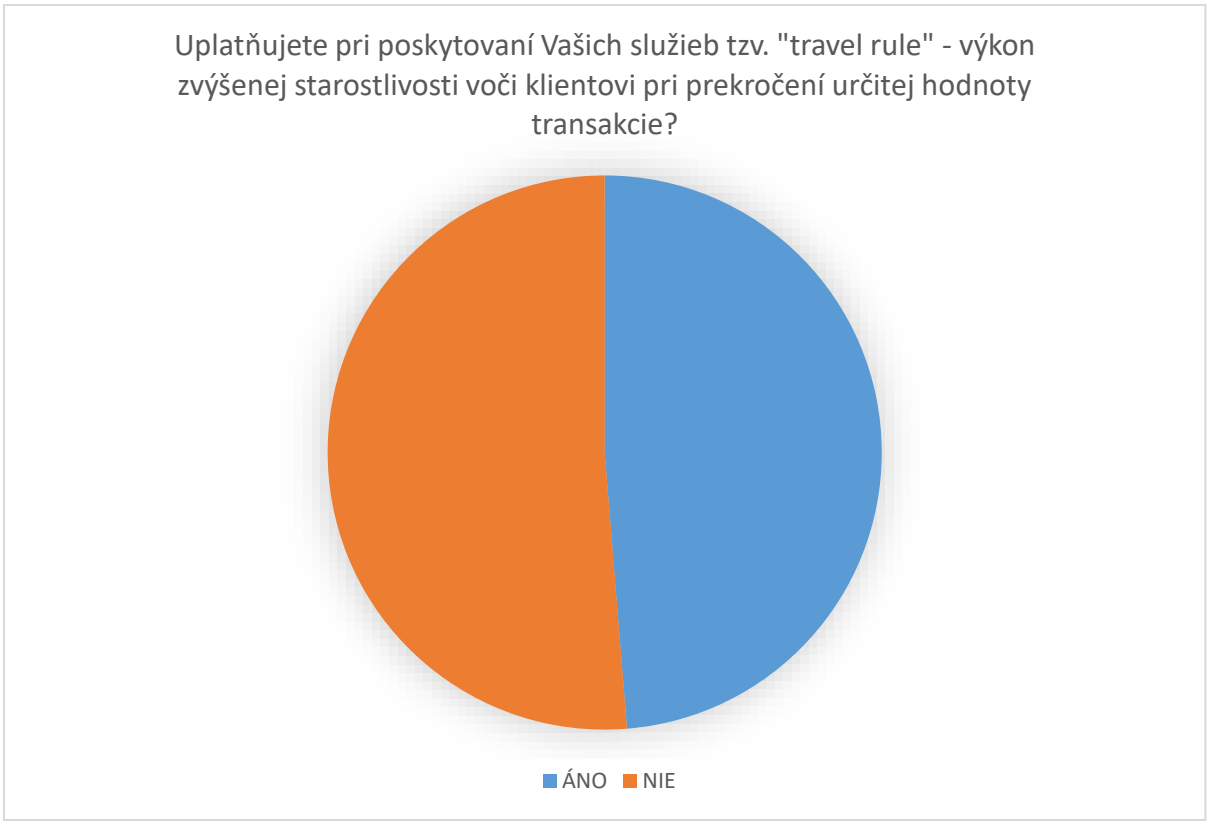
8. Aplikovanie preventívnych opatrení a rizikovo orientovaného prístupu subjektmi, ktoré vykonávajú činnosť zmenárne a/alebo peňaženky virtuálnej meny v Slovenskej republike.

Monitorovanie rizikových peňaženiek virtuálnych mien, nastavenie vhodných kritérií pre výkon zvýšenej starostlivosti a správne pochopenie a vyhodnotenie realizovaných transakcií z hľadiska ich neobvyklosti sú významnými faktormi úrovne povedomia subjektov podnikajúcimi v Slovenskej republike s virtuálnymi menami pokiaľ ide o oblasť trestnoprávnych rizík.

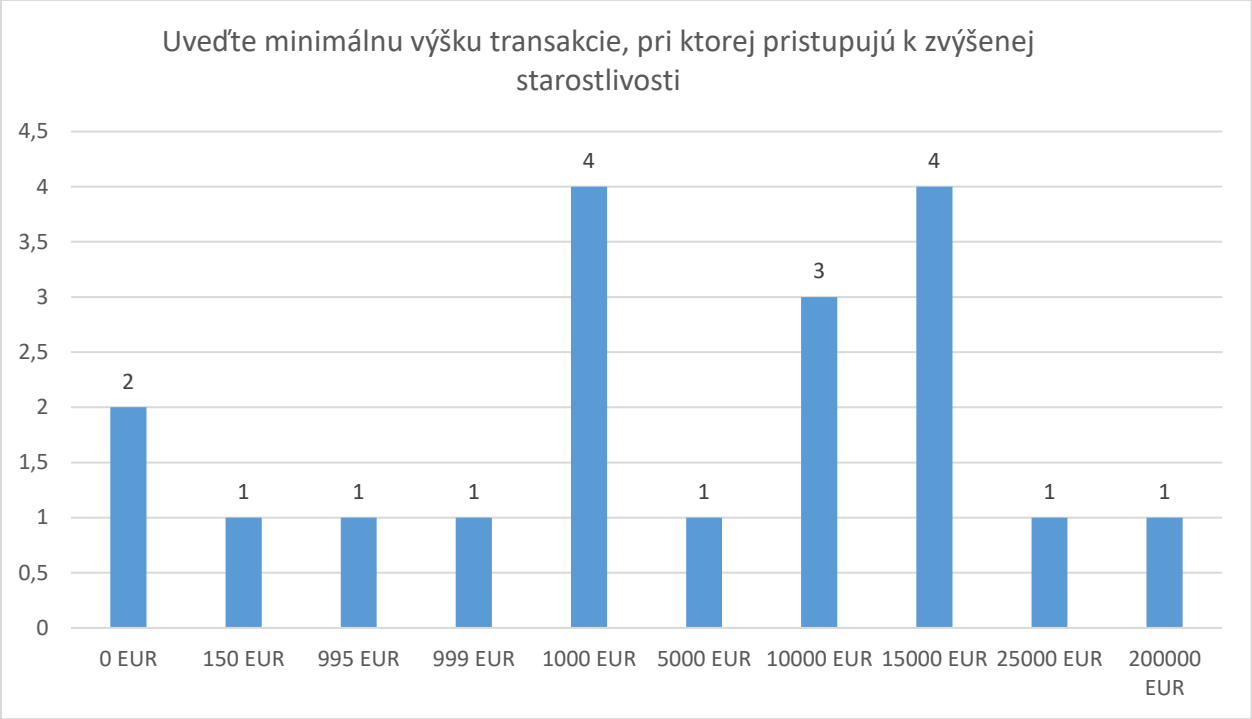
Výsledky získané vyhodnocovaním relevantných otázok zamierených na oblasť aplikácie preventívnych opatrení a rizikovo orientovaného prístupu subjektov, ktoré v Slovenskej republike podnikajú s virtuálnymi menami opäť poukázali na veľkú rôznorodosť (bližšie viď. graf č. 20 – graf č. 23). Aj v tomto prípade bolo možné na jednej strane určiť približne 50% skupinu subjektov, ktoré majú pravidlá nastavené veľmi dobre a je zrejme, že sú si vedomí aj ich dôležitosti. Druhú stranu spektra však tvoria subjekty, ktoré s poukazom na charakter a rozsah ich podnikateľskej činnosti, okruh klientov alebo osobnostné nastavenie, monitorovanie rizikových peňaženiek a/alebo kritéria zvýšenej starostlivosti neriešia. Vyhodnocovaním otázok minimálnej výšky transakcie, pri ktorej subjekty pristupujú k zvýšenej starostlivosti a počtu zaznamenaných neobvyklých obchodných transakcií, nie je zrejmé, či všetkým vyhodnocovaným respondentom je jednoznačne jasný rozdiel medzi výkonom základnej starostlivosti voči klientovi a výkon zvýšenej starostlivosti ako aj charakteristika neobvyklej obchodnej operácie. V týchto oblastiach by bolo vhodné posilniť edukáciu zo strany verejného sektora.

Graf č.22

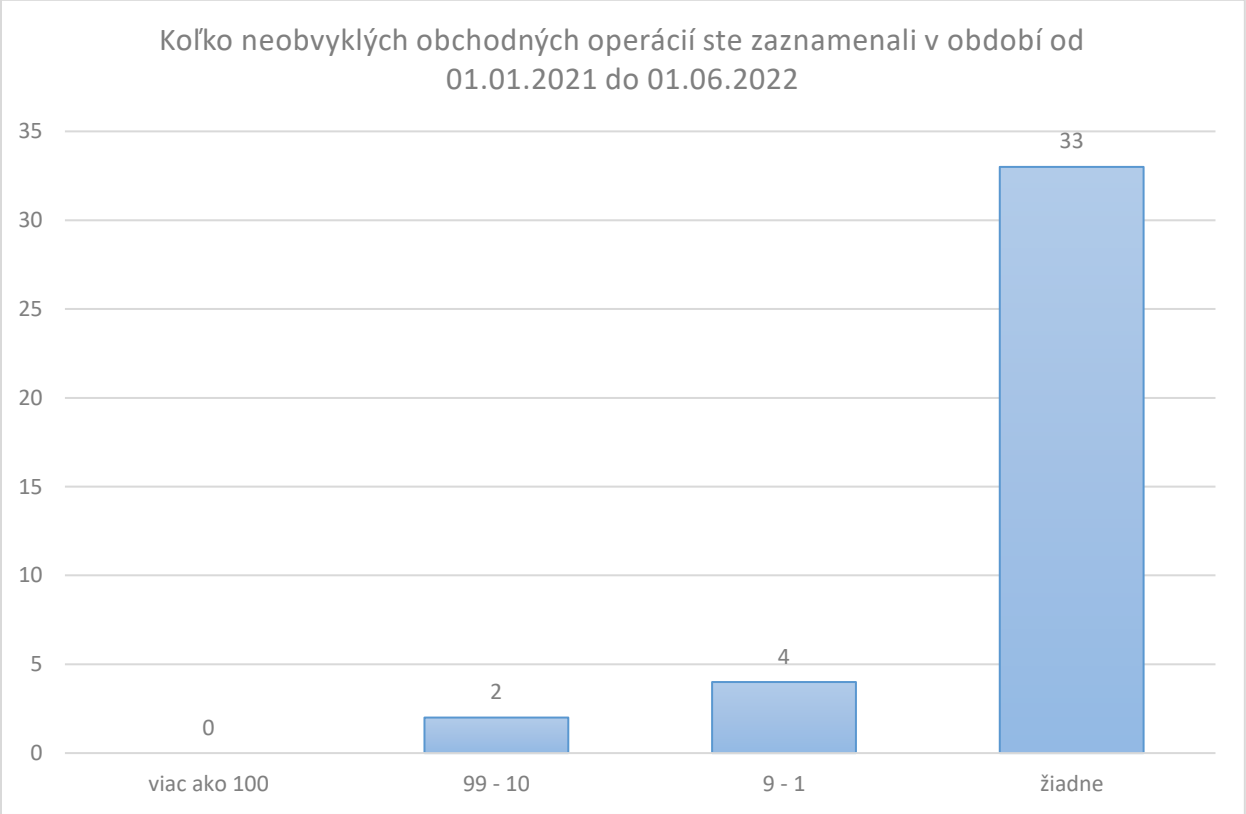
Graf č.23



Graf č.24



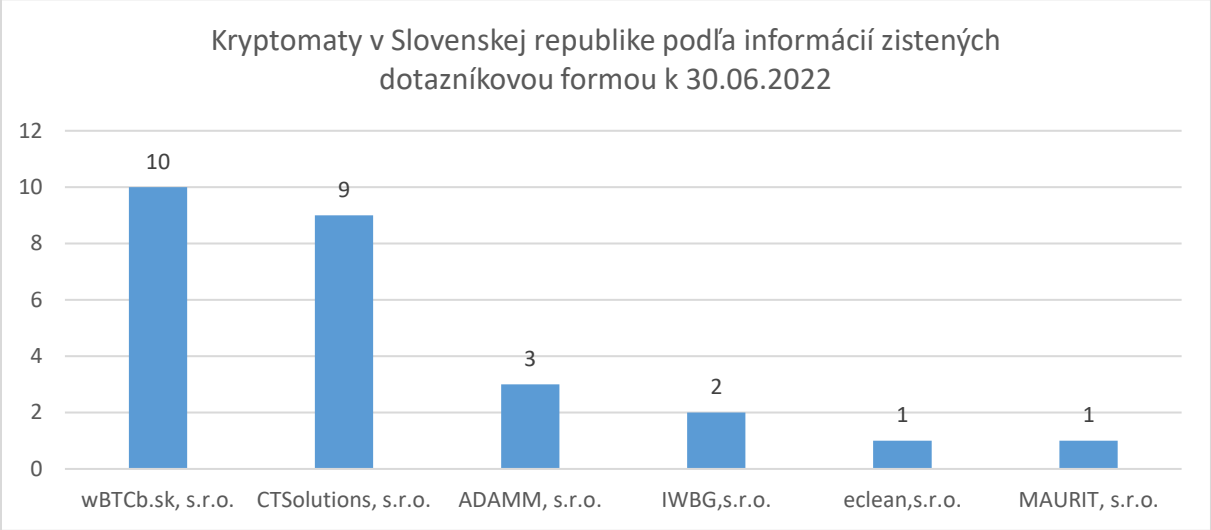
Graf č.19



9. Kryptomaty na Slovensku

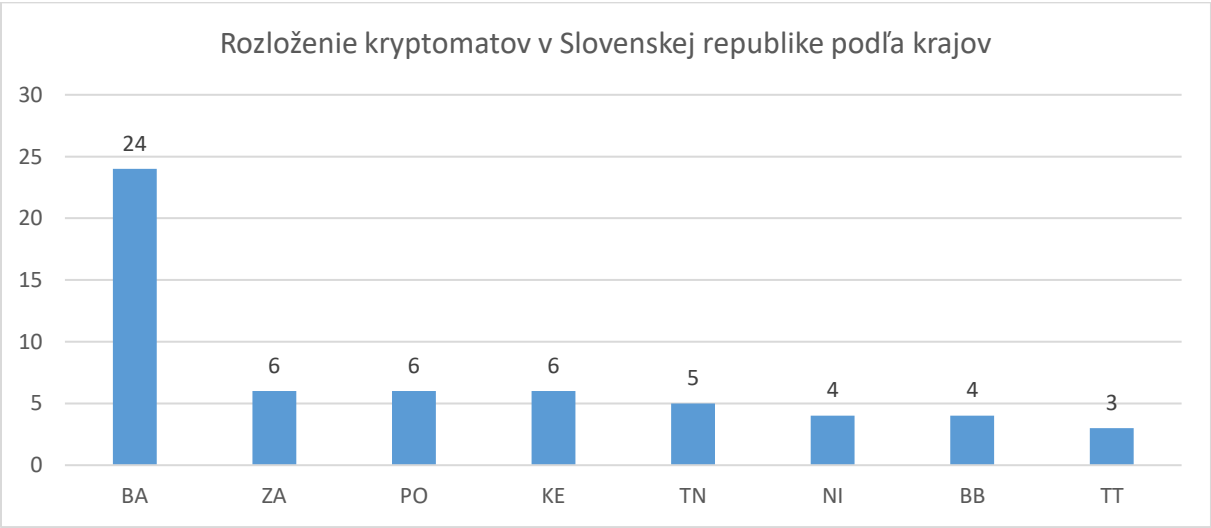
Preverovaním dotazníkovou formou bolo zistené, že zo subjektov, ktoré mali ku dňu 30.06.2022 v Slovenskej republike registrovaný predmet podnikania poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny, spolu 6 subjektov uviedlo, že v Slovenskej republike prevádzkuje spolu 26 kryptomatov.

Graf č.26



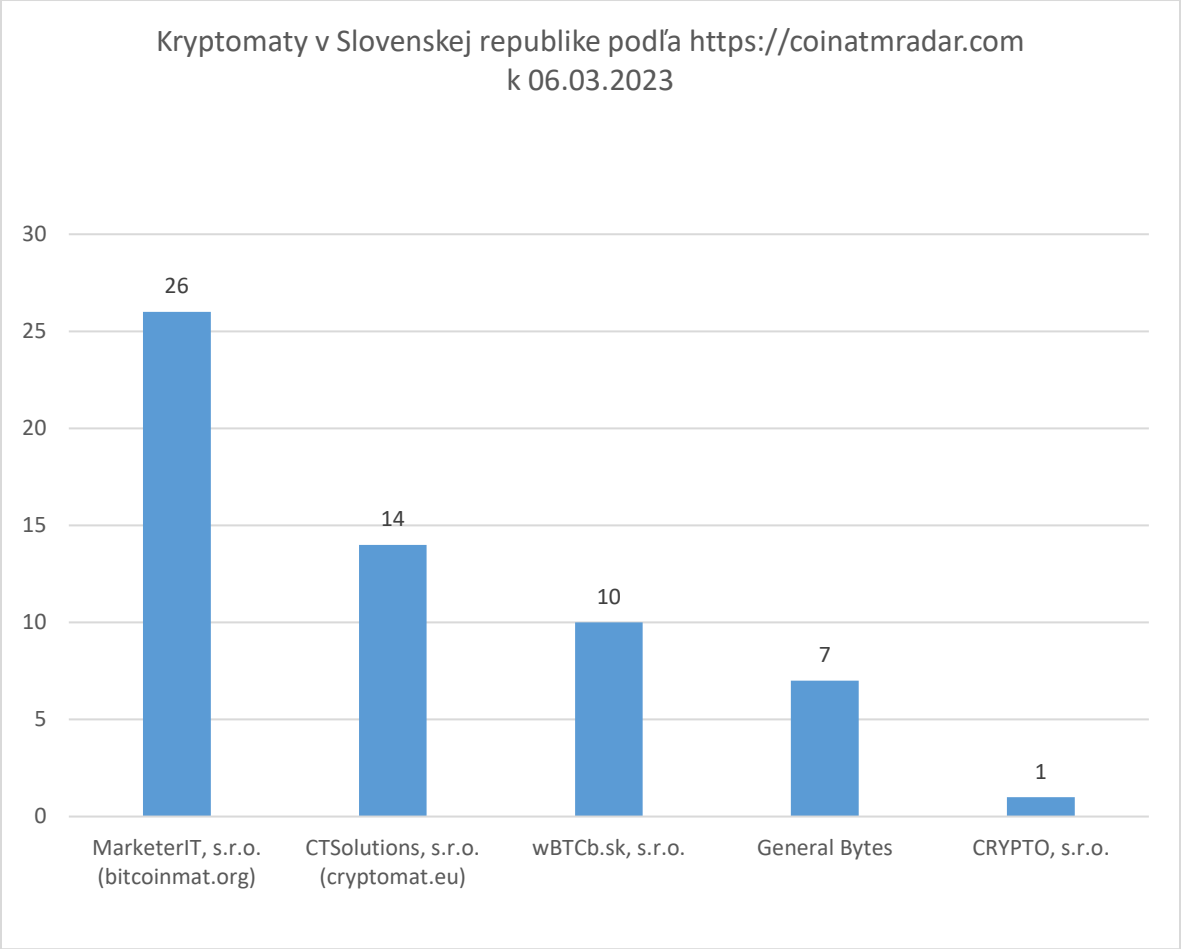
Následným preverovaním cez stránku https://coinatmradar.com/ bolo zistené, že ku dňu 06.03.2023 sa na území Slovenskej republiky nachádzalo spolu 58 kryptomatov rozvrstvených v rámci celého územia Slovenskej republiky s výraznou dominanciou bratislavského kraja (resp. Bratislavy).

Graf č.27



Následným preverovaním boli zistené rozdiely v subjektoch, ktoré v dotazníku uviedli, že spravujú kryptomat resp. kryptomaty na území Slovenskej republiky a informáciami zverejnenými na stránke https://coinatmradar.com/. Tu však treba podotknúť, že k zmenám mohlo prispieť aj časové obdobie niekoľkých mesiacov, ktoré vzniklo v rámci distribúcie a zberu dotazníkov a ktoré vo svete virtuálnych mien môže znamenať rapídny rozdiel.

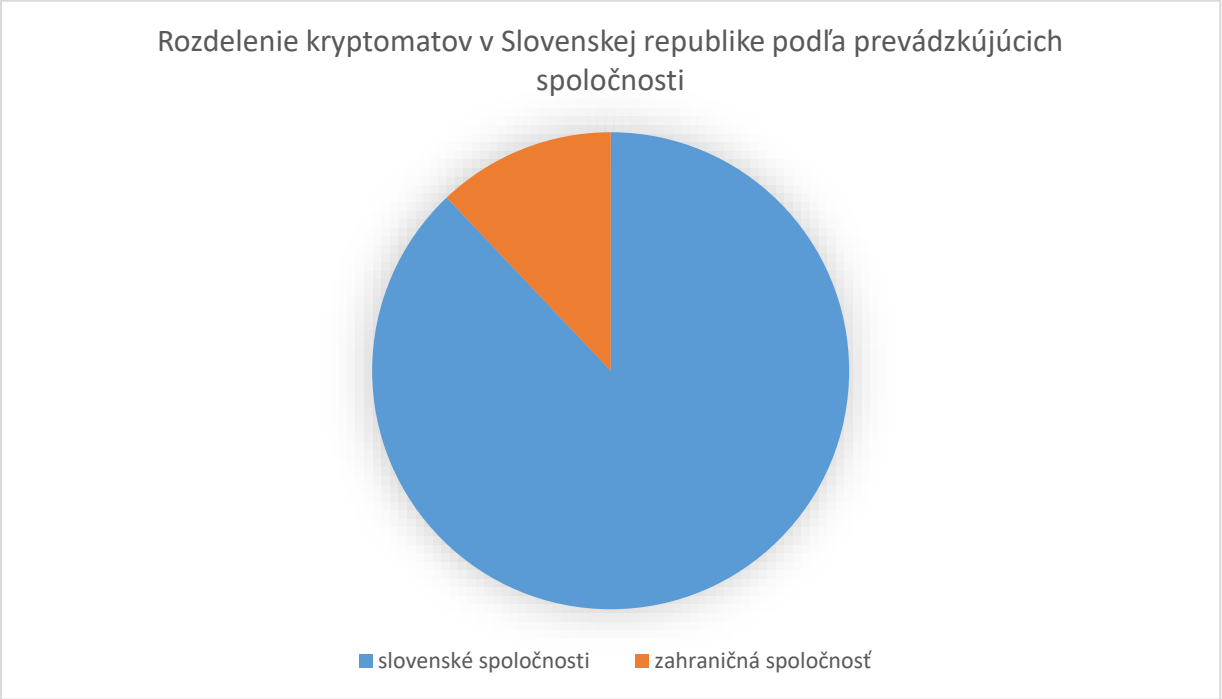
Graf č.28



Napriek zohľadneniu časového hľadiska je nevyhnutné vyzdvihnúť dva najvýznamnejšie rozdiely zistené porovnaním rozloženia kryptomatov na území Slovenskej republiky, ktoré môžu indikovať slabé miesto skúmanej oblasti.

Skôr ako sa začneme venovať zisteným nedostatkom, chceli by sme poukázať na pozitívnu skutočnosť, a to, že väčšina kryptomatov, ktoré sa podľa stránky https://coinatmradar.com/ nachádza na území Slovenskej republiky je spravovaná subjektmi registrovanými v Slovenskej republike, so sídlom v Slovenskej republike a s preukázateľným geografickým prepojením na našu oblasť. Na území Slovenskej republiky bol zaznamenaný len jeden zahraničný subjekt, bez preukázateľnej väzby k Slovenskej republike, ktorý má na našom území umiestnených 7 kryptomatov, čo predstavuje cca 12% podiel z celkového počtu kryptomatov.

Graf č.29



Zahraničné subjekty, ktoré prevádzkujú kryptomaty na území krajiny, ku ktorej nemajú žiadne preukázateľný vzťah, je vzhľadom na samotnú povahu kryptomatu fungujúceho na báze zámeny hotovosti, možné považovať za faktor indikujúci zvýšené riziko možného legalizovania výnosov z trestnej činnosti a/alebo financovania terorizmu. Na samotné fungovanie takto spravovaných kryptomatov v súčasnosti nemajú štátne orgány Slovenskej republiky žiaden legálny dosah, a ich činnosť nie je dohľadaná vo vzťahu k AML problematike ani zo strany Finančnej spravodajskej jednotky Slovenskej republiky, nakoľko tieto subjekty nespĺňajú podmienky pre povinnú osobu.

Preverovaním vo voľne dostupných zdrojoch na internete bolo zistené, že zahraničná spoločnosť, ktorá v Slovenskej republike prevádzkuje 7 kryptomatov, je registrovaná v Českej republike a k marcu 2023 mala po celom svete rozmiestnených viac ako 9.000 kryptomatov. V tomto kontexte je potrebné skonštatovať, že tento nedostatok nie je priamo viazaný k Slovenskej republike ale reflektuje úroveň regulácie kryptomatov v celosvetovom meradle.

Ako už bolo vyššie uvedené, v rámci Slovenskej republiky k marcu 2023, kryptomaty prevádzkovali vo väčšine subjekty s priamym vzťahom k Slovenskej republike. Avšak aj pri týchto subjektoch je badať postupný presun na širší trh zameraný prevažne do okolitých európskych krajín. Pri jednom subjekte prevádzkujúcom kryptomaty bola zaznamenaná neprehľadná štruktúra obchodných spoločností registrovaných na meno štatutára a v jednom bolo zistené, že spoločnosť prevádzkujúca kryptomat podľa verejných zdrojov nemá registrovanú živnosť prevádzkovanie zmenárne virtuálnej meny. Vzhľadom na to, že tieto

skutočnosti aktuálna slovenská legislatíva jednoznačne nerieši, je na mieste v týchto prípadoch do budúcna zvážiť otvorenie diskusie smerujúcej k dôkladnejšiemu nastaveniu právnej úpravy.

10. Nespolupracujúce subjekty

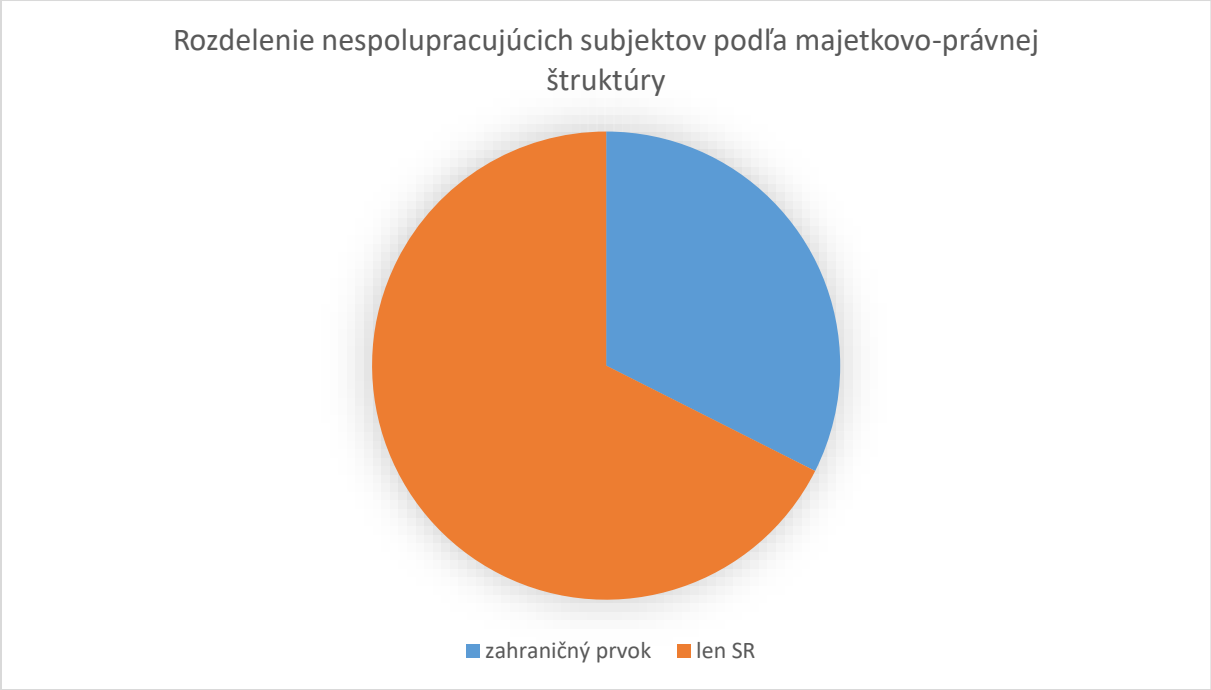
Analýzou a vyhodnocovaním dotazníkov zaslaných subjektom, ktoré mali k 30.06.2022 v Slovenskej republike registrované poskytovanie služieb zmenárne virtuálnej meny a/alebo poskytovanie služieb peňaženky virtuálnej meny bola vyšpecifikovaná skupina 111 subjektov, ktoré buď dotazník neprebrali, alebo ho prebrali, ale nevyplnili.

Vzhľadom na nedostatok dát, ktorými FSJ k týmto subjektom disponovala, ako aj vzhľadom na pomerne vysoké percentuálne zastúpenie tejto skupiny v pomere ku všetkým registrovaným poskytovateľom služieb virtuálnej meny, bola tejto skupine pri spracovaní sektorového hodnotenia rizík venovaná osobitná pozornosť a bolo vykonané ich individuálne preverenie jednak v databázach Obchodného registra Slovenskej republiky, databázach Finančnej spravodajskej jednotky ako aj vo verejne dostupných zdrojoch.

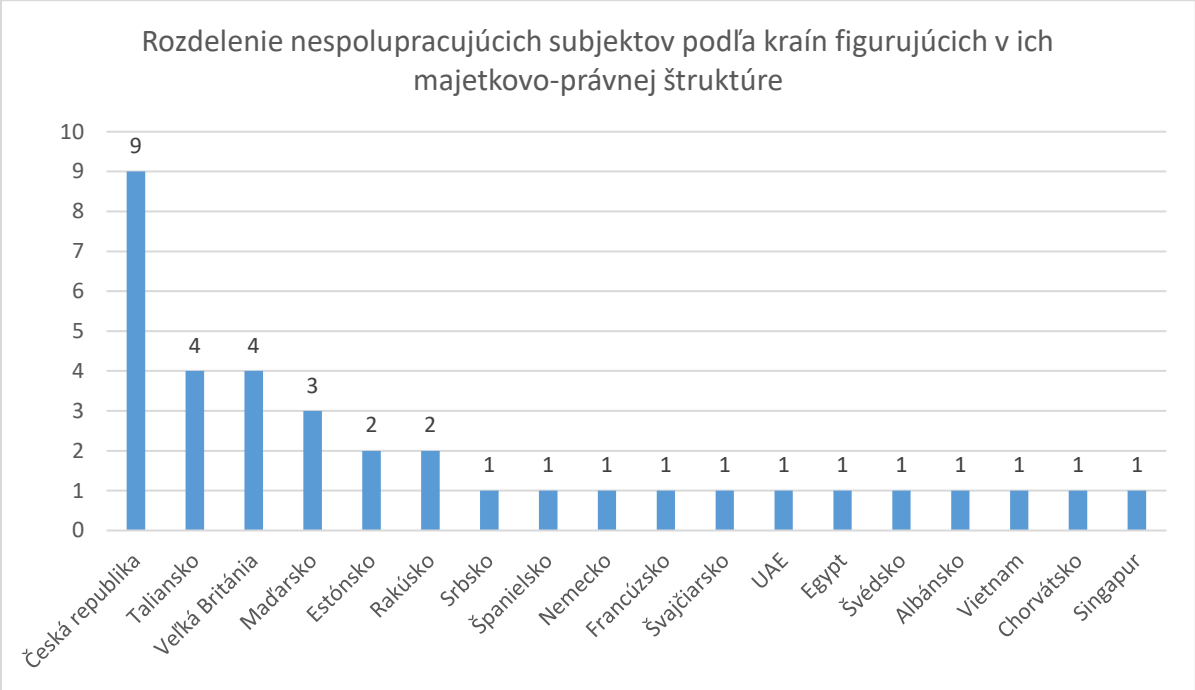
Dodatočne vykonaným preverovaním bolo zistené, že značnú časť tejto skupiny subjektov pravdepodobne tvoria obchodné spoločnosti, ktoré predmet činnosti zmenáreň virtuálnej meny a/alebo peňaženky virtuálnej meny reálne vo vzťahu k tretím osobám nevykonávajú.

Okrem uvedeného bolo zistené, že spolu 36 subjektov má úplne alebo čiastočne zahraničnú majetkovo - právu štruktúru so sídlom na virtuálnej adrese. Najčastejšie pritom šlo o prepojenie na subjekty v Českej republike, Taliansku, Veľkej Británii a v Maďarsku. Celkový prehľad demonštruje graf č. 29.

Graf č.30



Graf č.31



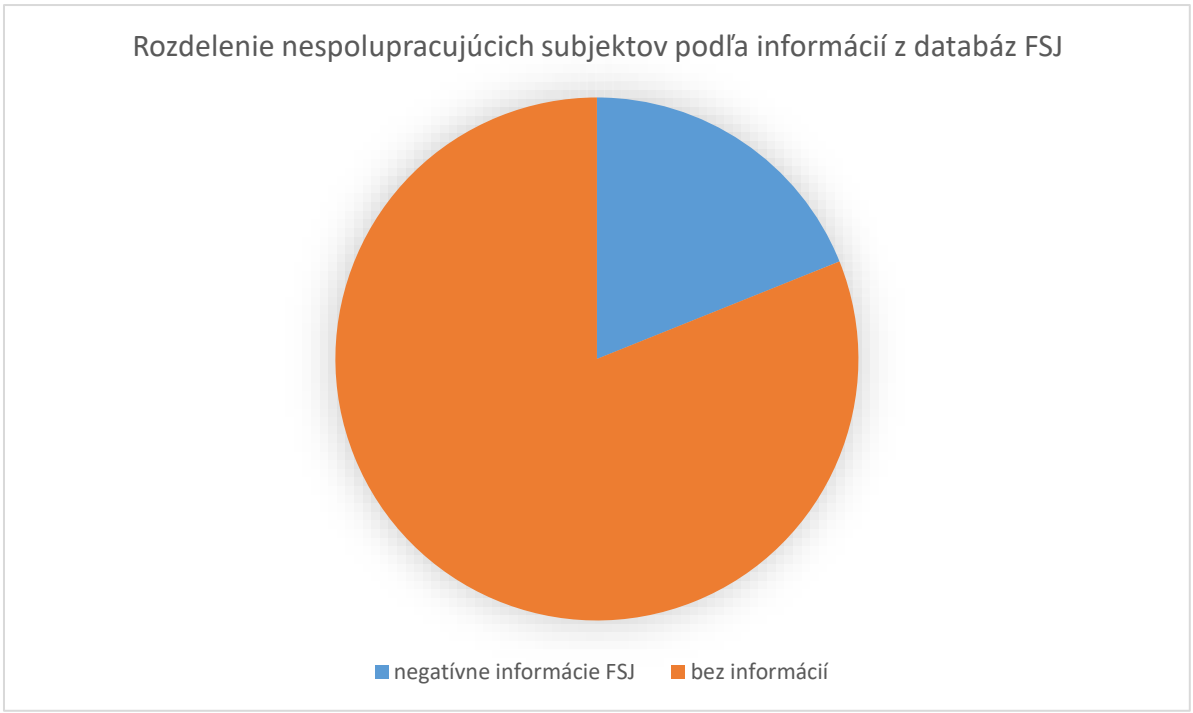
Previerkou subjektov v databázach Finančnej spravodajskej jednotky boli zaznamenané negatívne informácie pri 21 subjektoch. Tieto negatívne informácie boli rôzneho charakteru od podozrenia z trestnej činnosti, cez ekonomické delikty až po prepojenie na osoby, voči ktorým je v Slovenskej republike vedené trestné stíhanie pre závažnú trestnú činnosť. Tieto vzťahy majú väčšinou sekundárny charakter a nie sú jednoznačne preukázateľné pri bežnej

previerke, ktorá je toho času nastavená pri zakladaní obchodnej spoločnosti resp. pri registrácií predmetu podnikania poskytovanie služieb zmenáreň virtuálnej meny a/alebo poskytovanie služieb peňaženky virtuálnej meny. Zároveň pri 10 z týchto subjektov bol zistený zahraničný prvok v podobe zahraničnej spoločnosti a/alebo štatutára.

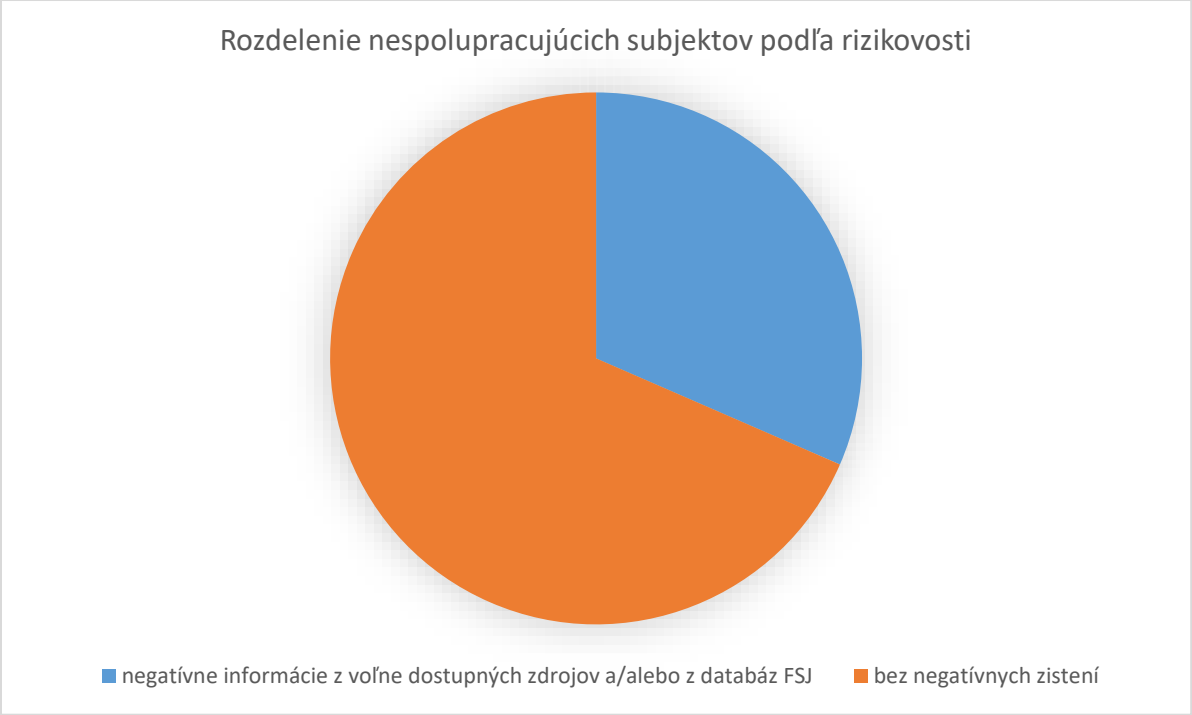
Preverovaním vo voľne dostupných zdrojoch bolo zadokumentované pri 21 subjektoch prepojenie na webové sídla (alebo informácie), ktoré majú súvislosť so zámenou virtuálnej meny alebo inými investičnými či platobnými spoločnosťami, alebo by mohli súvisieť s podozrivým (podvodnými) aktivitami na internete. Z toho pri troch subjektoch bolo zistené pozastavenie činnosti webových stránok.

V tomto bode je potrebné zdôrazniť, že napriek rovnakému percentuálnemu zastúpeniu subjektov ku ktorým disponuje negatívnymi informáciami FSJ a ku ktorým boli podozrivé informácie dohľadané na internete, nejde o totožné skupiny subjektov. Celkový počet subjektov, ktoré mali k 30.06.2022 registrovaný v Slovenskej republike predmet podnikania poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny a neposkytli FSJ súčinnosť pri sektorom hodnotení rizík vykonávanom dotazníkovou formou pričom dodatočnými previerkami k ním boli zistené negatívne skutočnosti predstavuje 32% podiel.

Graf č.32



Graf č.33



11. Záver dotazníkovo / analytickej časti sektoru VA/VASP

Pod vplyvom rokov poznačených pandémiou sa celý finančný sektor pomaly, ale isto začal presúvať do on-line prostredia, v ktorom sa hranice medzi štátmi stierajú a dohľad v oblasti AML / FT sa stáva náročnejším. Tento posun je badateľný jednak pri subjektoch etablovaných na slovenskom finančnom trhu, ako aj pri novo vznikajúcich subjektoch.

Rýchly vývoj a neustály posun vo vývoji nových technologicky stále vyspelejších nástrojov na jednej strane umožňuje bežnému spotrebiteľovi jednoduchšiu manipuláciu a správu jeho financií, na druhej však predstavuje široké možnosti pre páchateľov trestnej činnosti na zakrývanie pôvodu finančných prostriedkov v trestnom čine, financovanie terorizmu či páchanie iných druhov trestných činov.

Samostatnú kapitolu v rámci finančných technológií predstavujú virtuálne meny a subjekty poskytujúce služby spojené virtuálnymi menami. Tieto majú isté špecifiká a do istej miery prinášajú nové možnosti a výhody ako aj značnú transparentnosť transakcií. Aj v tomto prípade však platí odvrátená strana prinášajúca rýchly technologický progres zameraný na anonymizujúce spôsoby a technológie populárne u fanúšikov decentralizovanej správy financií rovnako ako aj u páchateľov trestných činov.

Uvedomujúc si tienisté stránky digitálnych financií a virtuálnych mien sa Slovenská republika pomaly, ale isto snaží adaptovať na nové technologicky vyspelejšie prostredie finančného sektora. Náročnosť jednotlivých procesov z hľadiska finančného, časového aj personálneho v kombinácií s progresom, ktorý v oblasti finančných technológií každým dňom rastie, nám

však neumožňuje napredovať tempom, ktoré by bolo maximálne efektívne a pomáhalo nám pokryť celú oblasť. Kroky, ktoré sa doteraz vykonali viedli predovšetkým k zorientovaniu sa v problematike a k vytypovaniu zraniteľných miest, ktorých postupné odstraňovanie bude definovať nadväzujúce kroky kompetentných orgánov verejnej moci Slovenskej republiky v nadchádzajúcom období:

Vykonanou analýzou v rámci vyhodnocovania došlých odpovedí na dotazníky distribuované subjektom, ktoré mali k 30.06.2022 ako predmet podnikania registrované poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny, bolo zistené, že z 340 odpovedí doručených Finančnej spravodajskej jednotke až 271 subjektov (cca 80 %) uvádza, že činnosť nevykonáva. Takmer polovica z týchto respondentov uviedla, že si predmet činnosti poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny registrovala v presvedčení, že ide o obligatórnu povinnosť v prípade ak chce svoje prostriedky či už osobné alebo z podnikania investovať do virtuálnej meny. Tieto subjekty majú reálne skúsenosti s nákupom a držbou virtuálnej meny pre vlastnú potrebu a považujú ju za veľmi bezpečný a dôveryhodný prostriedok na zhodnotenie investícií alebo formu sporenia. Obchodujú výlučne s vlastnými prostriedkami a služby pre tretie osoby neposkytujú. Tento fakt spolu s ďalšími skutočnosťami registrovaným v praxi poukazujú na systémové nedostatky registračného procesu obchodný spoločností v Slovenskej republike, a nedostatky v nastavení komunikačných kanálov medzi orgánmi štátnej správy navzájom ako aj medzi súkromným a verejným sektorom.

Špeciálnu kapitolu pri definovaní rizikových faktorov, ktoré nové finančné technológie prinášajú v rámci potenciálneho legalizovania výnosov z trestnej činnosti predstavujú bankomaty, ktoré umožňujú vkladanie finančných prostriedkov bez dostatočného overenia ich pôvodu. Rizikom sú jednak vkladové bankomaty zavedené bankami, ako aj automaty slúžiace na zámenu hotovosti za virtuálnu menu (tzv. kryptomaty). V prípade kryptomatov je potenciálne riziko ich využívania za účelom legalizovania výnosov z trestnej činnosti alebo financovania terorizmu priamo úmerne prepojené s možnosťami dohľadu a monitorovania týchto nástrojov zmenárenskej činnosti v rámci Slovenskej republiky.

12. Slovenská republika a jej prístup k problematike zadržiavania výnosov z trestnej činnosti

Generálna prokuratúra SR sa problematike virtuálnych mien/aktív problematike venuje od roku 2016. Na základe získaných poznatkov z Európskej únie, Rady Európy, OSN, FATF, či niektorých štátov bola v roku 2017 spracovaná "Pomôcka pre prokurátorov k problematike virtuálnych mien (najmä Bitcoinov)", ktorá bola aktualizovaná koncom septembra 2019. Ďalšia aktualizácia sa predpokladá v roku 2023.

Na základe írskych skúseností zdieľaných v rámci ARO podskupiny pre virtuálne meny bol v spolupráci medzi Prezídiom PZ a Generálnou prokuratúrou SR spracovaný leták - "Odoberanie virtuálnych výnosov z trestnej činnosti" - Informácia pre orgány činné v trestnom konaní - identifikácia Bitcoinu a iných virtuálnych mien. Tento je dostupný v papierovom formáte, ako aj v elektronickom formáte (pre prokurátorov na intranete prokuratúry).

Prokuratúra sa zúčastňuje činnosti Európskej justičnej siete na boj proti počítačovej kriminalite (EJCN), ktorá vznikla v roku 2016. V rámci plenárnych zasadnutí, aj mimo nich, spolupracuje EJCN aj so súkromným sektorom, vrátane spoločností ako Chainalysis, Binance, Coinbase a pod. Špecifické otázky spojené s virtuálnymi menami sú prezentované aj zástupcami Europolu (EC3. V rámci EJCN pôsobí aj podskupina pre virtuálne meny, ktorá spracovala manuál v danej oblasti a súčasne v roku 2022 zorganizovala 2 vzdelávacie podujatia pre zástupcov justičných orgánov v EÚ k problematike virtuálnych aktív. Prokurátori a sudcovia sú v danej oblasti vzdelávaní v rámci aktivít Justičnej akadémie SR, zúčastňujú sa aj medzinárodných vzdelávacích podujatí v danej oblasti (napríklad v ILEA v Budapešti, prípadne vzdelávanie organizované pre slovenských prokurátorov zo strany amerických orgánov).

Generálna prokuratúra SR dlhodobo podporovala zavedenie definície virtuálnej meny a procesného inštitútu zaistenia virtuálnej meny do právneho poriadku Slovenskej republiky. Súčasne sa podieľala na tvorbe legislatívy v danej oblasti.

12.1. Definícia virtuálnej meny podľa Trestného zákona

V zmysle ustanovenia § 131 odsek 7 Trestného zákona je virtuálna mena definovaná nasledovne:
"Virtuálnou menou sa na účely tohto zákona rozumie 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".

12.2. Právna úprava procesu zaistenia virtuálnej meny

Procesný postup zaistenia virtuálnej meny je upravený v ustanovení § 96d Trestného poriadku nasledovne:

1) Ak zistené skutočnosti nasvedčujú tomu, že virtuálna mena je nástrojom trestnej činnosti alebo výnosom z trestnej činnosti, môže predseda senátu a v prípravnom konaní prokurátor vydať príkaz na zaistenie virtuálnej meny.

2) Ak vec neznesie odklad, môže vydať príkaz podľa odseku 1 prokurátor aj pred začatím trestného stíhania. Taký príkaz musí najneskôr do 48 hodín potvrdiť sudca pre prípravné konanie, inak stráca platnosť.

3) V príkaze podľa odsekov 1 a 2 sa zakážu akékoľvek dispozície s virtuálnou menou a prikáže sa jej vydanie vrátane vydania hesla, prístupového kódu alebo podobných údajov umožňujúcich nakladanie s virtuálnou menou. Právne úkony urobené v rozpore so zákazom podľa predchádzajúcej vety sú neplatné.

4) Príkaz doručí predseda senátu a v prípravnom konaní prokurátor bezodkladne vlastníkovi virtuálnej meny alebo osobe, o ktorej možno dôvodne predpokladať, že má prístupové údaje k virtuálnej mene.

5) Ak pominuli dôvody na zaistenie virtuálnej meny, vydá predseda senátu a v prípravnom konaní prokurátor bezodkladne príkaz na zrušenie zaistenia virtuálnej meny.

6) Príkaz podľa odsekov 1 a 2 musí byť vydaný písomne a musí byť odôvodnený. V príkaze sa uvedie adresa úložiska virtuálnej meny orgánu, ktorý spravuje zaistený majetok podľa osobitného predpisu, označenie virtuálnej meny a počet jednotiek.

7) Vlastník virtuálnej meny, ktorá bola zaistená, alebo iná osoba, ktorej bola virtuálna mena zaistená, má právo žiadať o zrušenie alebo obmedzenie zaistenia. O takejto žiadosti musí predseda senátu a v prípravnom konaní prokurátor bezodkladne rozhodnúť. Proti tomuto rozhodnutiu je prípustná sťažnosť. Ak bola žiadosť zamietnutá, vlastník virtuálnej meny alebo iná osoba, ktorej bola virtuálna mena zaistená, ju môže, ak v nej neuvedie iné dôvody, opakovať až po uplynutí 30 dní odo dňa, keď rozhodnutie o jeho predchádzajúcej žiadosti nadobudlo právoplatnosť; inak sa o nej nekoná.

8) Ak je v trestnom konaní potrebné zaistiť virtuálnu menu na zabezpečenie nároku poškodeného na náhradu škody, postupuje sa primerane podľa odsekov 1 až 7.

Pred prijatím vyššie uvedenej právnej úpravy boli realizované zaistenia na základe ustanovenia § 90 Trestného poriadku (zaistenie počítačových údajov).

V rámci zaisťovacej činnosti boli identifikované problémy pri prevode aktív virtuálnej peňaženky z policajnej peňaženky do peňaženky príslušného úradu, ktorý ju nemal vytvorenú, s prevodom boli spojené ďalšie problémy, ktoré boli riešené na medzirezortnej úrovni.

Problematika virtuálnych mien/aktív sa objavuje v rôznych oblastiach trestnej činnosti, predovšetkým v prípadoch ransomvéru, rôznych foriem vydierania, online podvodov a osobitne v prípadoch investičných podvodov.

Zvýšené nároky na prokurátorov predstavuje skutočnosť, že virtuálne aktíva, ako aj dôkazy, sa nachádzajú primárne u zahraničných VASP. Viacerí z nich nemajú fyzické sídlo, čo výrazne sťažuje zabezpečovanie dôkazov, ale aj prípadné zaistenie virtuálnej meny.

Slovenská právna úprava neobsahuje cezhraničný priamy styk medzi justičnými orgánmi a súkromnými spoločnosťami a v prípadoch neexistencie fyzického sídla VASP, alebo vyhýbaniu sa deklarovania konkrétneho sídla na účely medzinárodnej justičnej spolupráce zo strany VASP, to spôsobuje ťažkosti v trestnom konaní. V konkrétnej veci sa realizuje priama spolupráca so spoločnosťou Binance. Ide o živú vec, ku ktorej Generálna Prokuratúra nemôže poskytnúť viac informácií.

13. Národná Banka Slovenska

Národná Banka Slovenska v súčasnosti nereguluje ani nevykonáva dohľad nad VASP sektorom.

Získané informácie sú kombináciou výsledku prieskumu vykonaného v dohliadaných subjektoch a vlastných expertných poznatkov, informácií a expertných skúseností v oblasti VA/VASP.

Z výsledkov prieskumu dohliadaných subjektov v rámci sektorov finančného trhu, z výkazov o aktívach subjektov a iných dostupných informácií NBS vyplýva, že v sektoroch kapitálový trh a poisťovníctvo nie sú zaznamenané informácie, ktoré by naznačovali, že dohliadané subjekty v uvedených sektoroch poskytujú služby VASP, vykonávali obchody s VA alebo vlastnili aktíva vo VA.

Z výsledkov prieskumu vyplýva, že v sektore bankovníctvo a platobné služby boli zaznamenané aktivity súvisiace s VA/VASP.

NBS konštatuje, že banky vnímajú sektor VASP ako klientov s vyšším až vysokým rizikom. V procese riadenia rizík vo vzťahu k VASP identifikovali konkrétne ML/TF riziká a nastavili k nim AML/CFT opatrenia, ktoré možno považovať ako primerané. Banky, ktoré poskytujú služby klientom VASP, dokážu riziká súvisiace s týmito klientmi účinne zmierňovať.

Banky, ktoré poskytujú služby klientom VASP, veľmi detailne vnímajú ML/TF riziká vyplývajúce z obchodného vzťahu s VASP. Pri poskytovaní služieb týmto klientom uplatňujú rizikovo-orientovaný prístup. V rámci poskytovania starostlivosti vo vzťahu k VASP vykonávajú širší okruh činností a opatrení v porovnaní s prístupom k iným klientom. Vykonávajú tiež podrobnejší transakčný monitoring transakcií klientov VASP.

Pri výkone starostlivosti vo vzťahu ku klientom VASP banky uplatňujú najmä nasledovné opatrenia:

- uzatvorenie obchodného vzťahu za fyzickej prítomnosti osôb konajúcich za klienta VASP

- označenie VASP v systéme AML v rizikovej kategórii „vysoké riziko“
- schválenie vzniku obchodného vzťahu s VASP klientom útvarom Compliance a AML,
- vykonanie dôkladnej identifikácie a overenia identifikácie klienta, prijatie opatrení na overenie informácií týkajúcich sa identifikácie konečného užívateľa výhod z viacerých zdrojov
- VASP musia mať poskytovanie služieb s VA uvedené v predmete podnikania,
- dôkladné preskúmanie a overenie vlastníckej a riadiacej štruktúry VASP,
- vykonanie opatrení na zistenie pôvodu majetku VASP a pôvodu finančných prostriedkov,
- zisťovanie pôvodu peňažných prostriedkov súvisiacich s konkrétnym obchodom
- pri uzatváraní obchodného vzťahu používajú KYC dotazník , ktorý obsahuje otázky špecificky zamerané na VASP,
- vyžadujú detailné informácie o budúcej povahe obchodného vzťahu a obchodného modelu klientov, aby sa uistili, že získali dostatok informácií o podstate a najmä o rizikách podnikania klientov VASP a aby sa tiež uistili, že vyššie ML/TF riziká súvisiace s VASP dokážu účinne riadiť a zmierňovať,
- v priebehu obchodného vzťahu s klientmi VASP banky vykonávajú podrobnejší monitoring transakcií v porovnaní s ostatnými klientmi
- vykonávajú zvýšený transakčný monitoring, najmä transakcie súvisiace s kryptoburzami, ktoré vnímajú ako vysoko rizikové.

NBS z prieskumu v bankovom sektore zistila najmä nasledovné ML/TF riziká identifikované pri uzatváraní a počas trvania obchodného vzťahu s klientmi VASP:

- VASP nemajú nastavené primerané systémy riadenia rizík v oblasti AML /CTF, najmä v oblasti identifikácie a overenia identifikácie klientov, ktorým poskytujú svoje služby,
- nedostatočné zisťovanie/preverovanie pôvodu finančných prostriedkov použitých pri obchodoch s VA,
- vysoká miera príznakov podporujúcich anonymitu (produkty, služby VASP)
- nedostatky v aktualizácii údajov o klientoch,
- nerealizovaná kontrola klientov voči sankčným zoznamom a zoznamu politicky exponovaných osôb,
- riziká súvisiace s hotovostnými operáciami (VASP, ktorí prevádzkujú VA-ATM robia vklady v hotovosti z týchto zariadení na svoj platobný účet v banke),
- sťažená identifikácia ekonomického opodstatnenia pri hromadných transakciách VASP,
- neprehľadná vlastnícka štruktúra konečných užívateľov výhod klientov VASP,

NBS z prieskumu v sektore platobných služieb a elektronických peňazí identifikovala najmä nasledovné riziká spojené s činnosťou klientov pôsobiacich v oblasti VA/VASP:

- vyššie až vysoké riziko ML/FT
- nedostatočná identifikácia klientov a platieb

- riziko nedostatočnej dokumentácie (v spojení s ICO, nedostatočne zabezpečená bezpečnosť tokenov)
- ťažšia vysledovateľnosť pôvodu majetku pri virtuálnych aktívach (možnosť viacnásobných prevodov, nižšia úroveň transparentnosti)
- možnosť anonymity (ak úvodná zámena prebehla anonymne)
- nemožnosť zabrániť prevedeniu virtuálnych aktív osobám na sankčnom zozname a do jurisdikcií s nedostatočnou legislatívou v oblasti AML/CFT
- reputačné riziko (z pohľadu neplnenia bezúhonnosti klientov)
- kybernetické hrozby (využitie medzier / slabých miest vo finančnom systéme)
- de-risking zo strany poskytovateľov platobných služieb vo vzťahu k VASP
- chýbajúca komplexná regulácia

Dohliadané subjekty (Banky a finančné inštitúcie), ktoré majú vo svojom portfóliu klientov VASP, majú vo vzťahu k týmto klientov vypracované osobitné vnútorné politiky pre akceptáciu VASP, ktoré sú nastavené na princípe rizikovo-orientovaného prístupu.
Vo vzťahu k VASP klientom uplatňujú dohliadané subjekty zvýšenú starostlivosť.
Pre uzatvorenie obchodného vzťahu s novým VASP klientom je spravidla potrebný súhlas štatutárneho orgánu dohliadaného subjektu. Subjekty tiež taktiež využívajú viaceré nezávislé a spoľahlivé zdroje informácií na overenie týchto klientov (najmä ich reputáciu, prípadné spojenie s rizikami ML/TF, s negatívnymi informáciami z médií a pod).

NBS v súvislosti s VA/VASP preskúmala aj podania spotrebiteľov k VA/VASP. Napriek tomu, že NBS nereguluje ani nedohliada sektor VA/VASP, spotrebitelia sa na NBS obrátili s negatívnymi skúsenosťami pri nákupe/obchodovaní s VA/VASP. Z charakteristiky podaní však nevyplýva, že sa jedná o AML riziká. Za obdobie rokov 2021-2022 NBS eviduje 24 takýchto podnetov od spotrebiteľov. Z uvedeného počtu má 12 podnetov v popise určité príznaky podvodu s VA, pričom najčastejším dôvodom negatívnej skúsenosti bolo, že spotrebiteľ odovzdal svoje prístupové kódy sprostredkovateľovi počas samotného nákupu/obchodovania s VA alebo sa spotrebiteľ obrátil na neznámeho VASP, ktorého následne nazval podvodným.
Ďalšie podania súviseli so žiadosťou spotrebiteľov o preverenie neznámych VASP, prípadne so žiadosťou o technickú pomoc.

Závery NBS:

NBS konštatuje, že výsledky prieskumu ako aj doterajšie expertné poznatky NBS preukázali, že banky primerane chápu ML/TF riziká súvisiace s VASP klientmi a uplatňujú vo vzťahu k VASP rizikovo-orientovaný prístup. Spolupráca bánk s touto klientelou vyžaduje zvýšený nárok na personálnu a odbornú kapacitu AML útvarov bánk. Rozsah prijatých opatrení zo strany bánk je možné v súčasnosti považovať za primeraný.

Možno tiež konštatovať, že inherentné riziko ktorému sú dohliadané subjekty vystavené v súvislosti s VASP, je primerane riadené a zmierňované vnútornými politikami subjektov.

Za reziduálne riziko vo vzťahu k VASP klientom NBS považuje nízku mieru povedomia VASP komunity o AML/CFT povinnostiach, najmä pri výkone CDD vo vzťahu k svojim klientom. V blízkej budúcnosti bude nevyhnutné, aby SR prijala systémový rámec opatrení, ktoré prispejú k zvýšeniu povedomia VASP o AML/CFT povinnostiach (najmä vzdelávanie, tréningy z oblasti AML/CFT). Zároveň pre efektívnu implementáciu odporúčania FATF č. 15 do AML/CFT systému SR bude nevyhnutné, aby VASP plnili preventívne opatrenia (FATF R 10-R 21) a zároveň aby bol prijatý efektívny systém výkonu AML/CFT kontroly VASP.

14. Analytická časť sektorovej analýzy

FSJ veľmi pozorne vníma vzrastajúci trend kryptoadopcie a to nielen na globálnej úrovni, ale i na lokálnej. Práve tento globálny aspekt virtuálnych aktív je treba zdôrazniť. Globálnosť je ich najnákladnejšia a najnatívnejšia vlastnosť. Na rozdiel od ostatných sektorov, sektor virtuálnych aktív je najmladší, najmenej regulovaný a vďaka svojmu prepojeniu s informačnými technológiami aj najdynamickejší, v neposlednom rade aj najflexibilnejší a najlepšie reagujúci na akékoľvek zmeny.

Práve týmto vlastnostiam sa v tomto sektore vo väčšine prípadov potiera tradičné rozdelenie na globálne a lokálne. Je dôležité na to pamätať a vnímať všetky aspekty spojené s kryptosvetom na globálnej úrovni. 99% technologických riešení je dostupných väčšine populácie na tejto planéte.

Spoločenská akceptácia Bitcoinu a nových technologických horizontov, ktoré so sebou prináša samozrejme vytvárajú nové typy kriminality a nové možnosti pôvodných typov kriminality využiť blockchain / virtuálne aktíva ako jednu z foriem, kanálov, na legalizáciu výnosov z trestnej činnosti, financovanie terorizmu alebo proliferáciu.

Bezprecedentná rýchlosť a flexibilita kryptosveta, aká v modernom svete ešte doteraz nebola, mu umožňuje reagovať na akékoľvek regulačné zásahy v podstate v rádoch hodín, maximálne dní. Príkladom môže byť reagovanie kryptosveta na regulačný zásah v podobe zákazu mixéra Tornado.Cash zo strany amerického OFAC-u v auguste 2022[11]. Reakcia kryptokomunity bola takmer okamžitá a technologické riešenie nahradzujúce zakázaný Tornado.Cash bolo dostupné pre používateľov v podstate do 24 hodín.

15. Zdanenie výnosov z kryptoaktív na Slovensku

Zdanenie výnosov z kryptoaktív na Slovensku je určené zákonom č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony – v súvislosti so zmenou zdanenia virtuálnych aktív.

Slovenská republika zaviedla povinné zdaňovanie virtuálnych aktív až v roku 2018, v doplnení zákona č. 595/2003 Z. z. a to nasledovne:

a) 19%, ak je ročný príjem do 37 981,94 €
b) 25%, ak je ročný príjem nad 37 981,94 €
c) 14 % zdravotné odvody

[11] https://home.treasury.gov/news/press-releases/jy0916

Samotný predaj virtuálnej meny je definovaný v zákone č. 595/2003 Z.z. §2 písmeno ai) zákona o dani z príjmu nasledovne:

a) predajom virtuálnej meny
b) výmena virtuálnej meny za majetok
c) výmena virtuálnej meny za inú virtuálnu menu
d) výmena virtuálnej meny za poskytnutie služby alebo odplatný prevod virtuálnej meny.

Od 1.1. 2024 je platné nové zdanenie v nasledujúcej výške:

a) 19% v prípade, že príjem do 41 445,46 €
b) 25% ak ročný príjem prekročí 41 445,46 €
c) odvod do zdravotnej poisťovne 15 %

Toto zdanenie bolo jedným z najvyšších v rámci Európskej únie a často čelilo kritike zo strany odbornej komunity. FSJ má informácie, že investori, ktorí dosiahli značné zisky počas dvoch výrazných rastových období na kryptotrhoch v rokoch 2018 a 2020-2021, často využívali daňové optimalizačné štruktúry, a to nielen v rámci EÚ, ale aj mimo nej, aby minimalizovali svoje daňové zaťaženie. Tento trend poukazuje na potrebu prehodnotenia daňovej politiky v oblasti virtuálnych aktív, aby sa podporila spravodlivá a efektívna daňová regulácia, ktorá zohľadňuje dynamickú povahu týchto trhov a zároveň stimuluje inovácie a rast v sektore. Rozšírenie právnych a regulačných rámcov by mohlo pomôcť predchádzať vyhýbaniu sa zdaňovaniu a zároveň zachovať konkurencieschopnosť domáceho trhu.

Niektoré spoločnosti dokonca priamo na svojich webových stránkach ponúkali riešenia na zníženie dane za pomoci vhodných optimalizačných schém.

Problematika zdanenia kryptomien je na Slovensku a aj globálne stále vo fáze rozvoja. Rôzne štáty, aj v rámci EU prijali rôzne daňové úpravy v súvislosti so zdanením kryptoaktív. Na jednej strane spektra môžeme nájsť napríklad Maltu, ktorá je globálne prezývaná „blockchain island“ (ostrov blockchainu), kde zdanenie variuje medzi 15% až 35%, v závislosti od rezidenčného statusu platiteľa[12], alebo exotické respektíve offshorové ako napríklad Panama, ktorá bola viacerými občanmi EU a aj Slovenska využitá s cieľom zoptimalizovať dane. Panama má veľmi miernu daňovú politiku, daň pre firmy je len vo výške 10% a pre zisky z daní alebo z kapitálových výnosov je 0%.[13] V príprave je zákon, ktorý by mal aplikovať zavedenie dane

Vzhľadom na globálne rozšírenie kryptomien, daňové úrady po celom svete čelia výzvam pri ich začleňovaní do existujúcich daňových systémov. Kryptomeny prinášajú nové riziká a povinnosti pre investorov, pričom ich decentralizovaná povaha komplikuje možnosti daňových úradov na efektívne zber daňových príjmov. Pri zvyšujúcej sa integrácii kryptomien do globálneho finančného systému, bude dôležité, aby regulačné orgány prispôsobili existujúce daňové zákony, aby reflektovali unikátne charakteristiky a výzvy, ktoré digitálne

[12] https://www.ccn.com/education/malta-crypto-tax-2023-everything-you-need-to-know/
[13] https://fastoffshorelicenses.com/offshore-crypto-license/panama/

aktíva prinášajú. Tento proces bude pravdepodobne vyžadovať medzinárodnú spoluprácu a inovácie v daňových prístupoch.

Tabuľka výnosov zo zdanenia, ktoré boli zaplatené do štátneho rozpočtu:

Tabuľka č.1

Rok	Výnosy zo zdanenia krypta (v tisícoch EUR)
2018	755
2019	451
2020	457
2021	4627
2022	645

Zdroj: Internet

Na základe výsledkov výnosov zo zisku krytomien zaplatených do štátnej pokladnice je možné sa domnievať, že platí hypotetická závislosť medzi výškou zdanenia a sumou vybratých daní z kryptomien, tak ako v prípade tzv. Lafferovej krivky.[14]

16. Zahraničné FinTech firmy a ich presah na Slovenský trh VASP-ov

Slovenská republika ako členský štát Európskej únie sa v poslednej dobre teší pozornosti svetovej odbornej kryptoverejnosti v negatívnom zmysle slova. Primárnym dôvodom je absencia akéhokoľvek dohľadu pri vydávaní licencie – na Slovensku sa jedná len o formu evidencie zo strany Živnostenského registra.

Istota udelenia povolenia na podnikanie v danom segmente (virtuálnych aktív), nízka cena, absencia zdĺhavého procesu ako pri iných štátoch, žiadne požiadavky na reporting (okrem tých v zmysle zákona 297/2008 Z.z., §5 zavedenie medzi Povinné osoba), možnosť podnikať z virtuálneho sídla a možnosť registrovať firmu / vlastniť firmu ako cudzí štátny príslušník patrí k najčastejšie skloňovaným prednostiam Slovenska ako vhodnej krajiny pre sídlo a činnosť VASP-u.

Absencia regulácie a samostatného licenčného procesu s jasne stanovenými komplexnými požiadavkami na žiadateľa, a následne z toho vyplývajúci veľmi jednoduchý prístup domácich a hlavne zahraničných subjektov k povoleniu na podnikanie na Slovensku v segmente poskytovania služieb zmenárne a kryptopeňaženiek vedie k tomu, že viaceré zahraničné Fintech právno - poradenské spoločnosti začali Slovensko odporúčať pre svoju medzinárodnú klientelu ako vhodné miesto pre založenie a prevádzkovanie VASP-u.

[14] https://e-news.cz/nazory/ceta-lafferova-krivka-aneb-proc-nelze-dane-zvysovat-vecne/

Viaceré krajiny a ich regulátory sa pri licenčnom procese zameriavajú okrem iných faktorov aj na odbornú a pracovnú minulosť žiadateľov o licenciu. V rámci procesu sa skúma aj personálne prepojenie žiadateľov. Tento proces sa na Slovensku nevykonáva. Kľúčovými požiadavkami sú: vek, ukončené stredoškolské vzdelanie a žiadateľ nesmie mať záznam v registri trestov.

Aj vďaka týmto faktom sa niektoré zahraničné právne fintech kancelárie zameriavajú na možnosť ponúknuť svojím klientom riešenia na kľúč, v rámci ktorých umožňujú aj personálne obsadenie firmy prostredníctvom tzv. nominee – dosadeného riaditeľa spoločnosti a v prípade záujmu aj možnosť dosadenia akcionárov spoločnosti (v prípade akciovej spoločnosti) alebo osoby spoločníka / spoločníkov a konateľa / konateľov v prípade s.r.o.

FSJ pri svojej činnosti identifikovalo, že viaceré VASP entity na Slovensku boli založené účelovo prostredníctvom zahraničných Fintech právnych kancelárií a ich lokálnych partnerov ako služba „na kľúč“. Za finálnu cenu v nižších desiatkach tisíc Eur dostane klient kompletné riešenie na kľuč spolu aj s možnosťou využiť lokálne personálne obsadenie spoločnosti a AML pracovníka.

Jednoduchosť procesu pre založenie VASP-u, chýbajúca povinná hĺbková kontrola osôb, ktoré si VASP zakladajú, tak ako napríklad v Nemecku, a minimálny resp. absentujúci proces udeľovania licencia vníma FSJ ako mimoriadne vysoké riziko pre vytvorenie schém umožňujúcich legalizáciu výnosov z trestnej činnosti alebo financovanie terorizmu.

Slovenská republika je preto čoraz častejšie promovaná zahraničnými právnymi a B2B spoločnosťami vyslovene preferovaná a radená ich klientom, ako ideálne miesto na podnikanie v segmente krypto.

Jednoduchosť registrácie subjektu a veľmi všeobecné vymedzenie pojmov vo svojej podstate umožňuje vytvoriť tzv. umbrella effect – zastrešenie jednou spoločnosťou, jednou (respektíve dvoma, poskytovateľ služby virtuálnej peňaženky a poskytovateľ služby virtuálnej zmenárne) registrovanými možnosťami, zastrešiť celú široké a veľmi rôznorodé možnosti ktoré svet krypta poskytuje, bez potreby žiadať, platiť a mať na jednotlivé činnosti ďalšie povolenia / licencie.

Obrázok č.12

Zdroj: Webová stránka Fintech právno – poradenskej spoločnosti

Horeuvedená fotografia poukazuje práve na túto jednoduchú možnosť pokryť široké a veľmi rôznorodé množstvo produktov a činností (napríklad NFT trhovisko, ICO a ITO ponuky / úpisy, DeFi projekty, konverzie FIAT do krypta a naopak) jednou registrovanou živnosťou na Slovensku, ktorú navyše nazýva licenciou a umožňuje subjektu následne podnikať na EU / globálnom trhu v podstate bez obmedzení.

Pre porovnanie, v niektorých krajinách platí, že každá jedna činnosť / set činností býva regulovaný samostatne a subjekty žiadajúce o licenciu v danom segmente musia o ňu žiadať samostatne, v individuálnom procese, čo samozrejme zvyšuje náklady pre žiadateľa a býva aj časovo náročný.

Nemenej dôležitou výhodou pre založenie VASPu na Slovensku je možnosť nominovať si konateľa / riaditeľa – občana krajiny z Európske hospodárske priestoru. Na pozíciu riaditeľa, na rozdiel od iných krajín, niesú kladené špecifické požiadavky alebo kritéria.

Z hľadiska problematiky AML / CFT je jednoduchosť založenia si novej spoločnosti, ktorá môže podnikať v segmente krypto na Slovensku a na základe jednotného trhu a nejasnej regulácie teda aj v EU hodnotená ako vysokoriziková. Absencia licenčného procesu, ako už niekoľkokrát bolo spomenuté v tejto sektorovej analýze vedie k nezdravému rastu množstva VASPov registrovaných na Slovensku.

17. Vymedzenie kriminality

Je veľmi dôležité uvedomiť si fakt, že kriminalita v spojitosti s modernými technológiami a aj kryptoaktívami je vo veľkej miere latentná.

Na Slovensku sa orgány činné v trestnom konaní neustále zameriavajú na zlepšovanie svojich technologických kapacít pre efektívnejšie sledovanie transakcií na blockchainových platformách. V súčasnosti sa prikladá veľký dôraz na rozvoj a integráciu sofistikovanejších softvérových riešení, ktoré by umožnili lepšiu analýzu a detekciu nelegálnych aktivít spojených s virtuálnymi aktívami. Hoci proces zavádzania pokročilých technológií si vyžaduje čas, je to kľúčový krok k zvyšovaniu účinnosti pri odhaľovaní a predchádzaní trestnej činnosti v digitálnom priestore.

Súčasťou sektorovej analýzy je aj kvantifikácia rizík spojených s latentnosťou kriminality v sektore krypto spôsobená:

a) Nedostatočná regulácia – vďaka enormnému množstvu registrovaných VASP-ov na území Slovenskej republiky a absencii prudenciálneho dohľadu, bolo a aj je veľmi jednoduché sa dostať k povoleniu na podnikanie v tomto segmente.

b) Neplnenie povinností reglementovaných v AML zákone VASP-ami - viaceré subjekty si dôsledne nerešpektujú status a povinnosti povinnej osoby. Vo viacerých prípadoch FSJ uložila sankcie za neplnenie povinností vyplývajúcich zo zákona 297/2008 Z.z.

c) Nedostatok technických a technologických nástrojov potrebných pre hĺbkovú analýzu a sledovanie digitálnych transakcií - tento stav pramení z absencie strategického vývoja infraštruktúry, ktorá si vyžaduje čas na implementáciu a optimalizáciu v rámci orgánu dohľadu, absencia technických a technologických nástrojov

18. Kryptokomunita

Dynamika kryptomien je úzko spojená s rýchlosťou a agilitou kryptokomunity, ktorá často reaguje na zmeny v sektore v priebehu niekoľkých hodín alebo dní. Táto rýchla odozva odráža adaptívnu a inovatívnu povahu komunity.

V rámci širšieho kryptosveta existuje tiež výrazná, hoci nie početná, skupina prívržencov tzv. krytoanarchizmu[15]. Tieto zoskupenia podporujú maximálnu anonymitu a snažia sa obmedziť štátnu kontrolu. Vďaka rastu kryptoaktív majú tieto skupiny k dispozícii mocné nástroje, ktoré pôsobia ako medzinárodne uznávané hodnoty nevydané žiadnou štátnou inštitúciou, ako

[15] https://paralelnapolis.sk/institut-kryptoanarchie/kryptoanarchisticke-manifesto/

je napríklad centrálna banka. Tieto nástroje nie sú pod kontrolou žiadneho štátneho orgánu a sú vytvárané a rozvíjané participáciou komunity.

Oproti tomu, omnoho početnejšia časť kryptokomunity sa identifikuje s pôvodným zámerom a významom kryptomien, najmä s Bitcoinom. Bitcoin predstavuje formu elektronických peňazí, ktorá umožňuje rovnomerné a priame online transakcie bez zásahu finančnej inštitúcie v peer-to-peer sieti[16]. K tomuto pôvodnému účelu a zamýšľanému použitiu sa opätovne vracia kryptokomunita na celom svete. Niekedy len s nádychom nostalgie, ale niekedy aj proaktívnym prístupom.

Tieto dve perspektívy ilustrujú rozmanitosť a dynamiku kryptokomunity, ktorá neustále formuje budúcnosť digitálnych financií a definuje nové paradigmy pre interakcie medzi technológiou, ekonomikou a spoločnosťou. Každý z týchto prístupov prispieva k celkovej mozaiky kryptoekosystému, čím sa zabezpečuje jeho rast, adaptabilita a inovatívnosť.

19. P2P v kryptokomunite

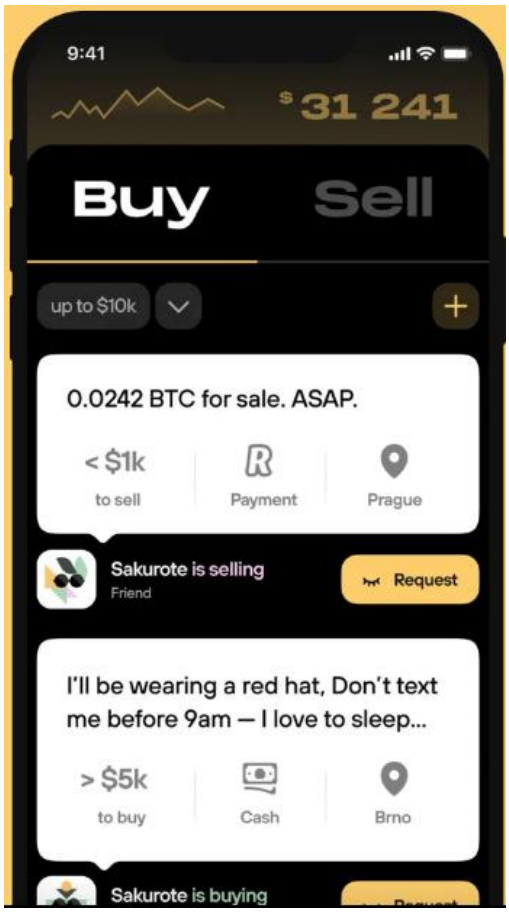
Jedným z takýchto proaktívnych prístupov v P2P je aj aplikácia Vexl.it.
Jej zmysel sa vracia k pôvodnému zámeru kryptomien a ich použitia kryptokomunitou respektíve komunitou – „bez práva na svobodnou transakci nemáme žádná jiná práva.“[17] respektíve, ako vraví na svojich stránkach: „Bitcoin has been in the hands of institutions for far too long. We want to make it accessible to everyone again.“[18] neoficiálny preklad pre účely tejto analýzy: „Bitcoin bol v rukách inštitúcií príliš dlho. Chceme to sprístupniť opäť všetkým.“

Samotná aplikácia Vexl.it o sebe prehlasuje, že je mobilnou aplikáciou, ktorá svojím používateľom poskytuje jednoduchý, dostupný a bezpečný spôsob ako obchodovať Bitcoin tak, ako bolo zamýšlané – peer 2 – peer a bez KYC.

Jej princíp je založený na algoritme, ktorý prostredníctvom telefónnych čísel (kontakty prvého a druhého stupňa), užívateľom vybranej lokality, navolenia hodnoty obchodu, platobnej metódy, ktorú preferuje kupujúci / predávajúci (bankový transfer FIAT meny alebo napríklad hotovosť), nájde vhodnú protistranu, resp. ukáže zvolenému okruhu anonymizovanú ponuku a po nájdení vyhovujúcej ponuky umožní kontakt osoby cez online možnost rozhovoru na doladenie detailov. Samotná aplikácia pri chatovaní využíva end – to - end šifrovanie, takže ani prevádzkovateľ aplikácie k nej nemá prístup. Aplikácia umožňuje aj vymazať chat a vtedy sú všetky konverzácie nenávratne stratené.

[16] https://blockchainslovakia.sk/wp-content/uploads/2018/06/bitcoin_whitepaper_sk.pdf
[17] https://vexl.it/
[18] https://vexl.it/

Obrázok č.13



Zdroj: webová stránka https://vexl.it/

Ilustratívny obrázok z webu aplikácie Vexl.it ukazuje všetky relevantné náležitosti, ktoré sa zobrazia kupujúcemu a zároveň ich vypĺňa predávajúci: hodnota obchodu, spôsob vysporiadania transakcie, lokalita a na záver žiadosť o kontakt.

Z hľadiska AML / CFT sa jedná o rizikové formy konverzia kryptoaktív do FIAT meny, kedy neprebieha žiadne KYC procesy, neexistuje záznam o konverzii jednotlivých kryptoaktív, žiadna identifikácia osôb podieľajúcich sa na transakcii ani pôvodu finančných prostriedkov.
Fakt, že podobné formy konverzie sú realizované cezhranične respektíve zahraničnými osobami len zvyšuje rizikovosť z hľadiska AML / CFT.

Rast hodnoty kryptoaktív a všeobecné zvyšovanie kryptoadopcie v posledných rokoch viedol k rozšíreniu akceptácie kryptoaktív nielen ako platidiel, ale aj ako investičných príležitostí a pre určitú skupinu ľudí aj ako uchovávateľov hodnoty. Z tohto dôvodu sa vytvoril dopyt na možnosť okamžitej výmeny hotovosti za kryptoaktíva.

20. Komunikačné nástroje v ére krypta

Rozvoj kryptoaktív a ich adopcia je neoddeliteľne spojený s rozvojom internetu ako komunikačného kanálu. 11. februára 2009 Satoshi Nakamoto predstavil white paper (biely dokument) Bitcoinu na diskusnom fóre P2P foundation.[19] Statické formy diskusných fór sa zmenili na dynamické komunikačné aplikácie modernej doby ako sú napríklad Whatsapp, Signal alebo Telegram.
Zvlášť posledný menovaný sa v kryptokomunite teší veľkej popularite vďaka svojmu protekcionistickému prístupu k dátam užívateľov a nevôli jeho tvorcov zdieľať ich s OČTK kdekoľvek vo svete.

Samotný Telegram na jednej strane deklaruje vôľu spolupracovať s jednotlivými OČTK priamo vo svojich užívateľských podmienkach, kde špecifikuje, že môže odhaliť IP adresu užívateľa alebo prípadne jeho telefónne číslo, na druhej strane hneď v ďalšej vete pripája respektíve zdôrazňuje informáciu, že doteraz tak nikdy neučinil.

Fotografia užívateľských podmienok aplikácie Telegram, bod 8.3 – Spolupráca s OČTK

Obrázok č.14

8.3. Law Enforcement Authorities

If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened. When it does, we will include it in a semiannual transparency report published at: https://t.me/transparency.

Zdroj: https://telegram.org/privacy, 22.08.2023

Práve kvôli tejto politike Telegramu, ktorá veľmi podporuje anonymitu a ochranu užívateľských dát sa Telegram drží vo veľkej obľube kryptokomunity na celom svete.
Slovenská kryptokomunita nieje samozrejme výnimkou a tento trend aplikuje v plnom rozsahu. Rôzne kanály zaoberajúce sa problematikou spojenou s kryptomenami majú neraz presah minimálne cez hranice a sú často spájané do Česko – Slovenských komunít a kanálov.

Jedným z trendov je aj využitie tejto aplikácie a kanálov na nej pôsobiacich na skontaktovanie sa medzi rôznymi osobami, ktoré ponúkajú anonymnou formou možnosť výmeny hotovosti za kryptoaktíva a naopak. Tieto osoby sa do veľkej miery opierajú o silné šifrovanie aplikácie a jej nevôľu vydávať užívateľské dáta komukoľvek, vrátane OČTK.

Z hľadiska problematiky AML / CFT sú tieto formy transferov a konverzií finančných prostriedkov za kryptoaktíva a naopak mimoriadne rizikové. Nakoľko neexistuje o nich

[19] https://news.bitcoin.com/13-years-ago-today-satoshi-nakamoto-published-the-first-forum-post-introducing-bitcoin/

žiadny záznam, absentujú procesy KYC a tieto konverzie môžu byť bez akýchkoľvek obmedzení aj cezhraničné, je možne využiť tieto schémy na legalizáciou výnosov z trestnej činnosti alebo financovanie terorizmu. Nemenej závažnou problematikou môže byť využitie týchto schém na obchádzanie obchodných sankcií zavedených na Ruskú federáciu a jej občanov po začatí invázie na Ukrajinu v roku 2022.

Aplikácia Telegram býva často spájaná s faktom, že ju vďaka jej protekcionistickej politike využívajú rôzne radikálne skupiny na celom svete. V roku 2023 brazílsky súd rozhodol o zákaze aplikácie na území Brazílie z dôvodu nedostatočnej súčinnosti s brazílskymi OČTK.[20] Reštriktívnu politiku ale uplatňujú aj iné štáty sveta.[21]

21. AOS / Boti

V neposlednom rade je výhodou aplikácie Telegram z hľadiska kryptokomunity aj fakt, že umožňuje prepojenie na tzv. obchodných botov.
Obchodny bot (na Telegrame) – sú malé automatizované programy, ktoré môžu byť implementované do Telegramu, umožňujú prepojenie, najčastejšie na decentralizované burzy a vykonávajú obchodné príkazy na základe vopred definovaných kritérií.
Tento trend ma prudko stúpajúcu tendenciu. Vďaka tomu, že doteraz niesú obmedzované žiadnou reguláciou ich množstvo a hlavne možnosti sú obrovské.

Z hľadiska funkcionality botov sa najčastejšie objavujú funkcie zamerané na:

a) Stop Loss / Take Profit – vykonávanie príkazov spojených s ukončenie obchodovania pri dosiahnutí požadovanej hranice v prípade profitu, alebo vopred nastavenej hranice straty v prípade prepadu hodnoty
b) Anti Rug-Pull detekcia – prevencia rug-pullu zo strany developera, v prípade, že bot také niečo detekuje, okamžite sa snaží vykonať predajný príkaz
c) Copy Trading – užívateľ si môže zvoliť sledovanie určitej peňaženky a pohyby na nej (predaj a nákup určitých tokenov) sú následne kopírované na jeho účet

Z technického hľadiska niesú v podstate žiadne obmedzenia, čokoľvek môže byť naprogramované ako algoritmus bota a ten to je schopný vykonať veľakrát v extrémne krátkom čase (rádovo v milisekundách).

S rôznymi botmi je možné sa stretnúť na nízkolikvidných malých nových tokenoch, kedy niektorý krypto používateľia nasadzujú tzv. Front Running Botov.

Front Running Bots – sú typom software, ktoré má za cieľ využiť latenciu v blochkchaine. Zameriava sa pri tom na to, že sa snaží detekovať veľkú objednávku (jej veľkosť môže byť

[20] https://www.nytimes.com/2023/04/26/briefing/brazil-telegram-ban.html
[21] https://restoreprivacy.com/telegram-sharing-user-data/

zadaná tvorcom tohto botu, alebo nastavená jeho používateľom, ktorý tento soft využíva). Aj keď slovenská legislatíva neupravuje používanie týchto botov, v medzinárodnom kontexte, resp. najme vo vyspelých krajinách býva táto metóda považovaná za tzv. insider trading – v slovenskom ekvivalente zneužitie informácií v obchodnom styku, čo je trestný čin.

FSJ poukazuje na potrebu legislatívne upraviť a rozšíriť aj problematiku obchodovania s kryptoaktívami, nielen reguláciu zameranú na služby poskytovateľov.

22 A.I.

Kontinuálny vývoj v oblasti technológie a informačných technológií umožňuje systematické prepojenie rôznych vedecko-technických odvetví. V sektore virtuálnych aktív, ktorý je svojou podstatou veľmi mladý a dynamický, sa objavuje začleňovanie technológií založených na umelej inteligencii (ďalej len AI). Prvotná implementácia AI v tomto sektore signalizuje začiatok novej éry v poskytovaní služieb virtuálnych aktív.

Samotný rozvoj A.I. v širšom kontexte nastáva práve v týchto rokoch. Prvotným impulzom pre verejnosť bolo sprístupnenie Chat GPT americkej neziskovej organizácií Open A.I. v novembri 2022. Už počas prvých mesiacov nastal vyslovený boom tejto technológie a momentálne počet prístupov mesačne prekonáva 1,5 miliardy.[22]
V prvých mesiacoch bol obmedzený počet interakcií pre registrovaných užívateľov a už vo februári 2023 bola predstavená predplatená verzia ChatGPT Plus, za mesačný poplatok 20 USD mesačne.[23]
V tomto balíčku je prioritný prístup ku funkciám ChatGPT, zrýchlený čas odoziev na položené otázky a prístup k novinkám a úpravám pred bežnými užívateľmi.
Na tento nový trend vo svete okamžite reagovali aj najväčšie technologické spoločnosti zo zoskupenia FAANG[24] a implementovali tento typ technológie do svojich riešení. V prípade spoločnosti Microsoft je to napríklad Office 365 a jeho A.I. nadstavba nazvaná Copilot.[25]

Na základe samotného rozvoja A.I. sa ale rozvíjajú aj jej rôzne iné nadstavby. Jedným z najdôležitejších a momentálne najvyužívanejších je takzvaný Large Language Model, známy pod skratkou LLM.

22.1. LLM

Large Language Model – je typom modulu, ktorý je založený na strojovom učení[26] a dokáže používať štatistické modely na spracovanie veľkého množstva dát, naučiť sa vzorce medzi slovami a jednotlivými frázami používanými v podporovaných jazykoch[27].

[22] https://www.similarweb.com/website/chat.openai.com/#overview
[23] https://openai.com/blog/chatgpt-plus
[24] Facebook (teraz Meta), Amazon, Apple, Netflix, Google (teraz Alphabet)
[25] https://blogs.microsoft.com/blog/2023/03/16/introducing-microsoft-365-copilot-your-copilot-for-work/
[26] https://www.techopedia.com/definition/34948/large-language-model-llm
[27] https://www.boost.ai/blog/llms-large-language-models

Pre podporu ich rozvoja a samotného procesu učenia je dôležité „nakŕmiť“ tento jazykový modul čo najširokospektrálnejším množstvom dát, ktoré pokrýva veľké množstvo slov, viet, fráz a rozmanitosť slov. Čím viac dát má modul k dispozícií, tým lepšie vie vygenerovať nový obsah.[28]
V momente, keď jazykový modul obsahuje dostatočné množstvo dát, môže jeho tvorca alebo používateľ vyšpecifikovať podmienky a parametre výstupného obsahu, ktorý ma modul vygenerovať.[29]
Tieto moduly môžu byť využívané aj inými službami a aplikáciami.[30]

Mimoriadne dynamický rozvoj technológie A.I. a na ňu nadviazaných ďalších technológií sa dostal do pozornosti bezpečnostných zložiek jednotlivých štátov, ich regulátorov a samozrejme aj kriminálneho prostredia.
Jednou z prvých reakcií bolo dočasné zakázanie modulu ChatBot GPT od americkej spoločnosti Open A.I. zo strany talianskych úradov.[31]
Jedným z faktorov, ktoré talianske úrady pokladali za vysokorizikové bolo ich podozrenie z porušovania nariadení týkajúcich sa ochrany súkromia.[32] Regulátor v tomto prípade odkázal na bezpečnostnú dieru, ktorá umožnila užívateľom vidieť témy konverzácií iných užívateľov.[33]
V súčasnej dobe sa regulácia na A.I. primárne tvorí v USA, Číne a samozrejme v EU, pričom každý z týchto regiónov uplatňuje dosť rozdielny pohľad na problematiku a najkľúčovejšie problémy spojené s umelou inteligenciou.[34]

22.2. A.I. a Europol

Problematikou A.I. sa samozrejme zaoberajú aj OČTK, EUROPOL zverejnil na svojích stránkach krátky materiál, kde sa snaží odhaliť vplyv A.I. na kriminálne prostredie. Dostupné na nasledujúcom odkaze:
https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

ChatGPT vyniká tým, že poskytuje používateľovi informácie pripravené na použitie v reakcii na širokú škálu podnetov. Ak potenciálny zločinec nevie nič o konkrétnej oblasti zločinu, môže ChatGPT výrazne urýchliť výskumný proces tým, že ponúkne kľúč informácie, ktoré potom možno ďalej skúmať v ďalších krokoch. Ako taký, ChatGPT možno použiť na získanie informácií o obrovskom množstve oblastí potenciálnej kriminality bez predchádzajúceho znalosti, od toho, ako sa vlámať do domu, až po terorizmus, počítačovú kriminalitu

[28] https://www.boost.ai/blog/llms-large-language-models
[29] https://www.boost.ai/blog/llms-large-language-models
[30] https://www.boost.ai/blog/llms-large-language-models
[31] https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html
[32] https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html
[33] https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html
[34] https://www.euronews.com/2023/05/23/what-can-the-eu-learn-from-chinas-generative-ai-regulation-before-it-adopts-its-ai-act

a sexuálne zneužívanie detí. Identifikované prípady použitia, ktoré vyplynuli z workshopov Europolu s odborníkmi nie sú v žiadnom prípade úplné. Cieľom je skôr dať predstavu o tom, aké rôznorodé a potenciálne nebezpečné môžu byť LLM ako ChatGPT v nesprávnych rukách. Zatiaľ čo všetky informácie, ktoré ChatGPT poskytuje, sú voľne dostupné na internete, možnosť použiť modul na poskytnutie konkrétnych krokov kladením kontextových otázok znamená, že pre kriminálne živly je podstatne jednoduchšie lepšie pochopiť a následne páchajú rôzne druhy trestnej činnosti.[35]

22.3. Deepfake

Jeden z najnovších trendov s ktorým sú spojené najväčšie bezpečnostné hrozby nielen z hľadiska problematiky AML / CFT ale aj z bezpečnostného je bez pochýb Deepfake.
Deepfake - značenie vzniklo spojením deep learning a fake a svoj pôvod ma v pornografickom priemysle.[36] Umelá inteligencia a video a najnovšie aj živý prenos cez programy umožňuje skombinovať fotografie a obraz, čoho výsledkom je výsledný obraz osoby A s tvárou a tie najpokročilejšie aj s hlasom osoby X. Tento postup môže slúžiť napríklad na vylákanie citlivých informácií od rôznych fyzických ale i právnických osôb. Cieľom môže byť dostať sa k údajom a informácia spojenými s finančnými prostriedkami, prihlasovacím údajom do banky alebo krypto seedom.
Príkladom môže byť nedávny deepfake hovor od osoby, tváriacej sa, že je konateľ firmy a druhej, ktorá sa prezentovala ako právnik. Cieľom bolo podvodnou cestou vylákať informácie o financiách firmy.
Viac o prípade na nasledujúcom webovom odkaze: https://domov.sme.sk/c/23205010/umela-inteligencia-deep-fake-video-banky-slovensko.html?ref=njctse

FSJ ale vníma aj pozitívne trendy vo využití technológie A.I. v problematike boja proti legalizácie výnosov z trestnej činnosti a financovania terorizmu.
Jedným z pozitívnych trendov je začatie využívania umelej inteligencie v segmentoch náročných na spracovanie veľkého množstva dát za krátku dobu a vo vysokej rýchlosti.

22.4. Kontrola smartkontraktov prostredníctvom A.I.

V segmente kryptomien sú takto náročnými dátami napríklad zdrojové kódy smart kontraktov.
Smart kontakt - je program uložený na blockchaine, ktorý po splnení vopred stanovených podmienok automaticky presadzuje konkrétne kroky. V decentralizovanom systéme môžu dve strany interagovať tak, že nahradia sprostredkovateľa, ktorý je zvyčajne potrebný na uľahčenie transakcií, pomocou smart kontraktu. Blockchainy, vrátane siete Bitcoin a Ethereum, využívajú smart kontrakty na uľahčenie transakcií a automatizáciu procesov.[37]

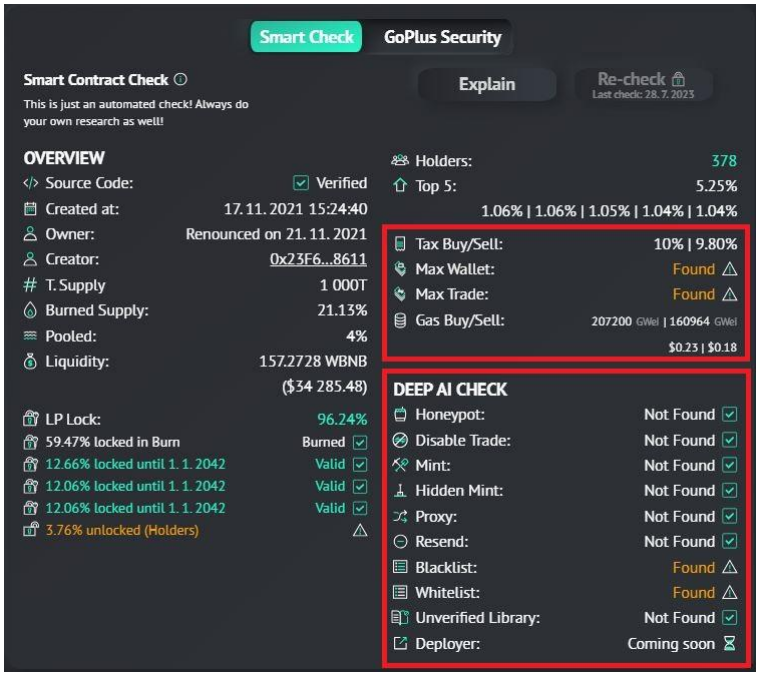
[35] https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf
[36] https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise
[37] https://www.binance.com/sk/blog/nft/v%C5%A1etko-%C4%8Do-potrebujete-vedie%C5%A5-o-smart-kontraktoch-nft-568745413587703085

Čo robí smart kontrakty „inteligentnými“? Tieto kusy kódu automatizujú procesy a nerobia ľudské chyby, čo v konečnom dôsledku znižuje čas a náklady spojené s tradičnými kontraktmi. Okrem prekonávania ľudských chýb majú smart kontrakty aj ďalšie výhody, vďaka ktorým sú dôležité pre blockchainový priemysel.[38]

Smart kontrakty presne determinujú čo sa bude diať v prípade, že nastane nejaká podmienka. Nakoľko sa jedná o zložité zdrojové texty, sú náročné na množstvo dát, ktoré obsahujú. Zároveň ale akákoľvek funkcia, musí byť zaimplementovaná aj s podmienkami plnenia priamo do zdrojového kódu.

Obrázok ukazuje, výsledok scanu smartkontraktu prostredníctvom A.I. GuardiaNNN.ai, v červených rámčekoch sú označené možné hrozby aj s vysvetleniami.

Obrázok č. 15



Zdroj: https://guardiannn.ai/bsc/token/0xcb008773ebef8c527fc33a4382659b13c9e73f70

A.I. v jednotkách sekúnd skontroluje celý zdrojový kód emisie alebo smart kontraktu a zameriava sa na hrozby zaimplementované do zdrojového kódu. Nie vždy implementovaná časť zdrojového kódu ale musí nutne znamenať, že projekt je podvodom. A.I. preto len upozorňuje na jej prítomnosť, samotné rozhodnutie o nákupe / predaji ostáva ale na samotnom užívateľovi, v duchu jedného z kľúčových hesiel kryptokomunity DYOR - “Do Your Own Research“ – vykonaj si vlastný prieskum.

[38] https://www.binance.com/sk/blog/nft/v%C5%A1etko-%C4%8Do-potrebujete-vedie%C5%A5-o-smart-kontraktoch-nft-568745413587703085

Jedná sa preto o preventívny typ scanu, ktoreho cieľom je odhaliť potencionálne riziká ako sú podvody v rôznych formách (viď pasáž o možnostiach scam-ov pri ICO v tejto sektorovej analýze).
Nevýhodou A.I. je fakt, že na to aby sa nejakú novú techniky podvodného chovania naučila, musia podvodné alebo nelegálne vlastnosti toho ktorého smart kontraktu naplniť. Následne sa A.I. dokáže na základe dát a vzorcu chovania (napr. transfery tokenov, vypnutie možnosti obchodovnia, likviditná pasca, proxy a rôzne iné) naučiť a následne predikovať hrozbu.

Veľmi zaujímavým trendom, najmä z oblasti compliance, respektíve kontroly je aj pokusné nasadzovanie modulov umelej inteligencie na decentralizovaných burzách. V pokusných fázach, ktoré momentálne prebiehajú, sa členovia komunity snažia skonsolidovať a následne „nakŕmiť“ A.I. čo najviac informáciami a vzorcami spojenými s rizikovým alebo vyslovene nelegálnym využívaním kryptomien, spojené najčastejšie s nákupom nelegálneho materiálu, ako napríklad detská pornografia, alebo nákupom na dark marketoch, podporovaním extrémistických skupín a rôzne iné.
V neposlednom rade sú to rôzne formy A.I. ktoré sú testované a implementované aj v orgánoch presadzujúcich právo na celom svete. FSJ má informácie o krajinách, ktorým A.I. prinieslo zefektívnenie a umožnilo sofistikovanejšie a rýchlejšie plniť úlohy.

Problematika vývoja a nasadzovania A.I. patrí z hľadiska boja proti legalizácií výnosov z trestnej činnosti v sektore kryptoaktív k jedným z kľúčových aspektov a FSJ zdôrazňuje potrebu monitorovať tento segment a v budúcnosti presadzovať nasadenie tohto typu technológie aj u orgánov činných v trestnom konaní na Slovensku.

23. CEX vs DEX vs DEX Agregátor

FSJ sa pri zostavovaní analýzy sektoru VA / VASP zamerala nielen na problematiku centralizovaných búrz (CEX) ale v rámci komplexného zberu dát aj na decentralizované burzy, ktoré sú často využívane na tzv. medzi sieťové obchodovanie (cross – chain), decentralizované autonómne organizácie (DAO) a pokročilú reguláciu v niektorých častiach sveta zameranú na možnosť využitia technológie blockchain v štátnej správe – napríklad pri zakladaní a riadení firiem.
Je potrebné mať na pamäti komplexnosť problematiky a kvantifikovať riziká spojené nielen s konverziou ale aj so samotným obchodom.

V problematike VASP a kvantifikácie hrozieb sa musíme zamerať aj na jednotlivé hlavné typy búrz, ktoré umožňujúce konverziu alebo obchodovanie s kryptoaktívami.

23.1. CEX

CEX - Centralizované burzy – je platformou ktorá umožňuje vymieňať krypto za krypto a navyše oproti DEX-om aj nákup / predaj / výmenu FIAT meny za krypto. Na rozdiel od DEX,

CEX burzy musia mať vždy podobu právnej entity a k tomu prislúchajúcu reguláciu.
Z hľadiska regulácie AML usmerňuje zákon č. 297/2008 Z.z. pre právnické alebo fyzické osoby, ktoré poskytujú služby peňaženky virtuálnej meny a zmenárne virtuálnej meny ich zaradenie medzi povinné osoby. Podmienkami naplnenia definície povinnej osoby podľa §5 ods. 1 písm. o) a p) zákona sú tak nasledovné predpoklady:

a) Príslušné živnostenské oprávnenie v zmysle živnostenského zákona
b) Poskytovanie služieb zmenárne virtuálnej meny a/alebo peňaženky virtuálnej meny klientom, ako predmet svojej podnikateľskej činnosti

Za výkon podnikateľskej činnosti sa nepovažuje správu vlastného majetku, ak pri nej nedochádza k výkonu podnikateľskej činnosti.

Na základe § 26 ods. 2 písm. c) a § 29 zákona, kontrolu plnenia a dodržiavania povinností povinných osôb zo zákona vykonáva FSJ, ktorá je centrálnou národnou jednotkou v oblasti predchádzania a odhaľovania legalizácie a financovania terorizmu.

Jednou z primárnych podstát kryptoaktív okrem ich decentralizácie, rýchlosti je aj ich globálnosť. Globálnosťou môžeme rozumieť fakt, že v podstate ktokoľvek, kto vlastní krypto peňaženku a má prístup na internet môže vykonať transakciu, ktorá sa vykoná (v závislosti na stanovených poplatokch v prípade BTC) v podstate okamžite.
Taktiež ale môžeme pod pojmom globálnosť rozumiet, že akýkoľvek krypto-užívateľ nieje viazaný len na vopred stanovenú geografickú lokalitu[39].

Vďaka tejto globálnosti je pre kryptoužívateľov na celom svete prirodzené, že vyhľadávajú ponuky a služby, ktoré im vyhovujú. Množstvo búrz, či už DEX alebo CEX je veľké, ponuka ich služieb rozmanitá a kontinuálne vznikajú nové burzy a nimi ponúkané nové služby.

Vďaka globálnosti kryptoaktív je veľmi rozdielny aj prístup v rámci regulácie. Vďaka kontinuálnemu tlaku veľkých regulátorov najmä v západnej Európe, SEA a USA sa zaviedli povinné procesy KYC pri otváraní a verifikovaní nových účtov.
Na druhú stranu je dôležité zdôrazniť, že nie všetky jurisdikcie nasledujú tieto trendy. Ich pohľad na problematiku AML je rozdielny a umožňujú pod dohľadom svojho regulátora zakladať VASP-ov, ktorí ponúkajú tzv. Non-KYC možnosť pre klientov, kedy od svojich používateľov nevyžadujú identifikačné dokumenty na overenie ich účtu.

[39] Samozrejme, za výnimku môžeme považovať štáty, ktoré v dobe písania tejto sektorovej analýzy majú zavedené reštriktívne opatrenia na nákup, predaj a držanie kryptoaktív, ako napríklad Čína, India. Čína má reštriktívne opatrenia nielen voči kryptoaktívam ale reguluje aj prístup aj prístup na internet.

23.2. Non- KYC burzy

Samotné Non-KYC burzy sa tiež vyvíjajú a býva ich zvykom, že ponúkajú niekoľko typov účtov pre svojich klientov, veľmi často rozdelené aj podľa ochoty klienta akceptovať proces KYC.
Pre neverifikovaných klientov bývajú často zavádzané určité limity, alebo reštrikcie. Najčastejšie majú podobu limitu na výber prostriedkov nad / do určitej výšky na určité, presne stanovené časové obdobie. V praxi má takáto reštrikcia pre neverifikovaný účet podobu napríklad: výber prostriedkov do výšky 5 BTC / ekvivalent v inej kryptomene, raz za 24 hodín.

Iné CEX burzy na druhú stranu majú zavedené reštrikcie pre neverifikovaných klientov v podobe limitovaného prístupu k ponúkaným službám. Najčastejšie, okrem obmedzení na výšku vyťahovaných prostriedkov, je to aj obmedzený prístup k pákovým obchodom alebo derivátom.

Non-KYC burzy sa veľakrát bránia náboru klientov z určitých oblastí, pretože sa nechcú dostať do problémov s určitými úradmi. Najčastejším príkladom sú reštrikcie na nábor klientov z USA. Avšak, nakoľko neprebieha proces KYC, jedinou formou, ako sa takáto burza bráni klientom z tejto oblasti je zavedenie reštrikcií na základe IP adries. Ako slabou je táto forma ochrany je veľmi jednoduché ukázať na možnosti zakúpiť si VPN a využiť IP adresu inej krajiny na prístup k týmto službám pre akéhokoľvek občana / osobu takmer z ktorejkoľvek krajiny.

Osobným druhom sú niektoré špecializované burzy / obchodníci, kde prichádza k obchodovaniu prostredníctvom aplikácie, nie internetovej stránky. Príkladom je aplikácia, ktorá umožňuje konvertovať BTC za FIAT, a to bez obmedzenia zo strany burzy, len obmedzenie zo strany dopytu investorov. Aplikácia nezbiera podľa informácií žiadne relevantné dáta o užívateľoch a nevyžaduje žiadnu formu verifikácie klienta a jeho účtu, ani pôvodu finančných prostriedkov.

Okrem FIAT mien umožňuje aj obchodovanie / konverziu aj medzi kryptomenami samotnými. Za vysokorizikové musíme považovať najmä obchody spájané s tzv. Dark Coins – anonymnými menami, ktoré sú primárne zamerané na neodhalenie vlastníkov peňaženky a aj samotného transferu. Kvôli týmto natívnym vlastnostiam anonymných kryptomien je takmer nemožné ich sledovať. Aplikácia uvádza na svojej stránke, že kryptomena Monero a jej trh patrí medzi jej najväčšie.

Všetky tieto typy predstavuje významné riziko v procese potenciálneho procesu legalizácie výnosov z trestnej činnosti alebo financovania terorizmu, vzhľadom na možnosť obchodovať kryptoaktíva prostriedky bez akéhokoľvek procesu preverenia pôvodu prostriedkov alebo bez povinnej starostlivosti zo strany burzy voči osobe.

23.3. DEX

DEX – Decentralizované burzy: tento typ búrz sa teší vzrastajúcej obľube medzi užívateľmi na celom svete a vo svojej podstate je tým pôvodným zamýšľaným spôsobom obchodovania krypto. Zo vzrastajúcou adopciou krypto vzrastá aj popularita týchto búrz. Jednoznačne sa to opiera aj o fakt, že vďaka 2 veľkým tzv. „bull run-om“ respektíve „bull marketom“ – býčím obdobím na trhu v rokoch 2018 a 2021, v zmysle významného vzrastu hodnoty krypta. Tieto býčie obdobia na trhu mali výrazný vplyv na množstvo prostriedkov, ktoré momentálne na trhu je.

V porovnaní s CEX, DEX sprocesúvavá transakcie prostredníctvom smart kontraktov, peer – 2 peer alebo prostredníctvom tzv. LP – liquidity providera – poskytovateľa likvidity. Samotné transakcie sú z ekonomického hľadiska pre užívateľov výrazne výhodnejšie vďaka oveľa nižším poplatkom (v čase písania tejto správy sa pohybujú okolo 0,13% z veľkosti transakcie).

Na rozdiel od CEX , DEX neumožňuje obchodovať s tzv. FIAT menou (meny vydávané centrálnymi bankami alebo inými štátnymi inštitúciami) a podporuje obchodovanie len krypto za krypto.
Pre DEX môže ale nemusí platiť, že vedia ponúknuť coiny len na jeden sieti. Viaceré DEX-y už podporujú tzv. „bridge“ – premostenie medzi sieťami a tým pádom aj medzisieťové obchodovanie.

DEX burzy, na rozdiel od CEX búrz nemajú žiadnu kontrolu nad finančnými prostriedkami klientov, klient sa prihlasuje do DEX-u len prostredníctvom svojej privátnej peňaženky a vlastní privátny kľúč od nej. V zmysle AML / CFT je veľmi náročné respektíve takmer nereálne stotožniť peňaženku s tou ktorou konkrétnou osobou.

Burzy DEX nedržia žiadne informácie o klientovi (osobné údaje), nevyžadujú od klienta žiadne dokumenty na vykonanie KYC, žiadnu AML starostlivosť. Prihlasovanie do DEX-u prebieha cez non-custodial peňaženku a všetky transakcie prebiehajú na blockchaine, čo ich robí transparentné a sledovateľné, ale i anonymné v zmysle tradičných identifikátorov ako je meno, dátum narodenia, bydlisko, národnosť, pôvod finančných prostriedkov...

23.4. DEX agregátor

V poslednej dobe sa tešia čoraz väčšej popularite DEX agregátori – ktoré fungujú na princípe agregácie (zoskupovania, respektíve kumulácie) ponúk jednotlivých virtuálnych aktív obchodovaných na jednotlivých DEX-och. DEX agregátori ponúkajú, respektíve sa snažia ponúkať svojím užívateľom prístup k najlepšej cene a najväčšej likvidite toho ktorého

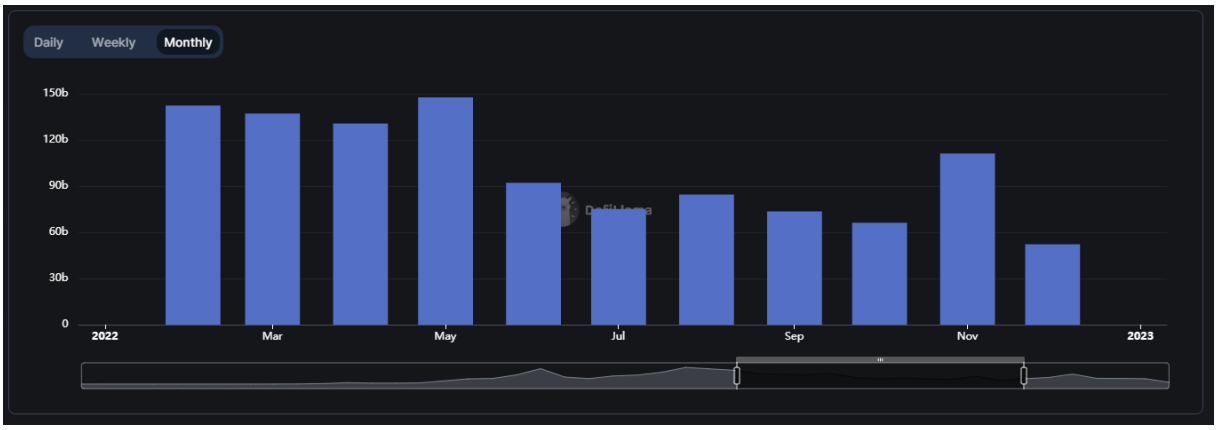
virtuálneho aktíva. Podporujú aj možnosť rozdelených obchodov medzi viacerými burzami s cieľom poskytnúť obchodníkovi najlepšie možné dostupné ceny.

S rastom kryptoadopcie v rokoch 2017 až 2020 (viď nasledujúci) kontinuálne rástol aj tlak regulátorov na zavádzanie nástrojov na dohľad v problematike AML / CFT z strany búrz. Od roku 2020, kedy všetky najväčšie burzy začali zavádzať / zaviedli nástroje na dohľad, kryptokomunita reagovala rozvojom a masívnym spopularizovaním decentralizovaných búrz.

Nasledujúci graf popisuje jednotlivé mesačné transakcie realizované na decentralizovaných burzách za rok 2022, kedy celkový objem obchodov dosiahol sumu presahujúcu 1100 mld. USD.[40]

Objem obchodov: 1100 mld USD za rok 2022

Obrázok č.16



Zdroj: https://defillama.com/dexs

Decentralizované burzy sú výrazným trendom posledného obdobia a reakciou kryptokomunity na tlak regulátorov presadiť v centralizovaných burzách povinné procesy KYC a dohľad jednotlivých búrz nad problematikou AML / CFT.

Absencia akéhokoľvek procesu verifikácie klienta, žiadny procesu KYC, ani dohľad v problematike AML / CFT z ich robí veľmi ťažko monitorovateľné a vysokorizikové platformy pre orgány presadzujúce právo. Ich schopnosť stotožniť peňaženku s tou ktorou konkrétnou osobou je len minimálna a preto v budúcnosti bude potrebné zakúpiť technologické riešenie, ktoré umožní sledovanie blochchainu. Nemenej dôležitá bude medzinárodná spolupráca, aby sa pravidelne vytvárali a aktualizovali peňaženky a adresy podozrivé z činnosti, ktorá porušuje zákon.

[40] https://www.elliptic.co/blog/money-laundering-through-dexs-and-mixers

23.5. DEX & A.I.

Najnovším trendom posledných mesiacov roku 2022 je sprístupnenie pokročilej technológie artificial-intelligence (AI) (umelá inteligencia) chatbot-a pre verejnosť. Po prvotnom nadšení sa začali objavovať snahy jednotlivých štátov o otvorení otázky regulácie AI, Taliansko dokonca 04/2023 pristúpilo k dočasnému zákazu Chat GPT[41]. Problematike A.I a jej zneužiteľnosti pre kriminálne prípady sa venuje aj štúdia EUROPOL-u dostupná na nasledujúcom odkaze: www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

Technológia umelej inteligencie prináša aj nové možnosti súvisiace s prevenciou ML / CFT najmä na trhoch VA a VASP. Objavujú sa prvé informácie o použití A.I. za účelom vytvorenia a následného testovania A.I. ako Compliance / AML / CFT modulu pre niektoré DEX burzy. Pilotné fázy boli spustené u menších búrz pred niekoľkými dňami a bude dôležité tento trend sledovať. Samotné DEX burzy vďaka absencii povinnej starostlivosti, vykonávaniu KYC a iných procesov sú hodnotené ako vysoko rizikové z hľadiska AML / CFT.

24.Prienik TradFi a DeFi

Vývoj na trhu kryptoaktív už od svojho počiatku hľadá technické a technologické možnosti ako prepojiť svet decentralizovaných financií (DeFi) a tradičného sveta financií (TradFi).

Až doteraz boli koncepcie DeFi a TradFi brané ako dva opozitné smery, každý z nich reprezentujúci jeden vývojový stupeň finančného sveta. S rozvojom blockchainu, zvyšovaním kryptoadopcie medzi užívateľmi po celom svete, rastom tržnej kapitalizácie kryptoaktív v rokoch 2018 a 2020 rástla aj relevancia DeFi. Jeden zo smerov rozvoja kryptokomunity deklaroval snahu o prepojenie tradičného finančného sveta a sveta DeFi.

Prvotný rozvoj, avšak ešte nie doslovné prepojenie bol, že viaceré svetové brokerské domy začali do svojho portfólia služieb pridávať možnosť obchodovať s kryptoaktívami. Ako príklad môžeme uviesť Saxo Bank, Interactive Brokers, eToro a rôzne iné medzinárodné obchodné platformy.

Zvlášť veľký rast počtu obchodných účtov a hodnoty tržnej kapitalizácie kryptoaktív je spojených s obdobím počas pandémie koronavírusu vo svete. Tento trend je ešte umocnený s nástupom novej generácie Z do pracovného procesu a jej vzťahom k inováciám.

[41] https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html

V neposlednom rade je tento rozvoj spojený s tzv. gamifikáciou investovania. Pojem gamifikácia investovania sa dáva do spojitosti s rozvojom aplikácií používaných na zadávanie obchodných príkazov toho ktorého brokera. Gamifikácia samotná je najviac spájaná s rozvojom americkej aplikácie resp. obchodnej platformy Robin Hood[42], ktorý sa ako jeden z prvých viac zameral na zatraktívnenie procesu investovania metódou hry pre užívateľov.

Všetky horeuvedené faktory pozitívne vplývali na kryptoadopciu či už vo forme dostupnosti nákupu kryptomien v užívateľsky priateľskom rozhraní, trendovosť v rámci generácie alebo nakupovanie ako hry, respektíve zážitku pre užívateľa.

S rozvojom kryptoadopcie a následne aj DeFi prichádzajú prvotné pokusy o prepojenie DeFi a TradFi v rôznych podobách. TradFi môžeme z pohľadu kryptoaktív brať ako staršieho súrodenca, ktorý do veľkej miery ovplyvnil aj DeFi.

Kľúčové prvky TradFi:

- Opiera sa o centralizovaný systém autorít (regulačné a dozorné orgány)
- Je dosiahnuteľná pre všetky osoby, ktoré spĺňajú určité požiadavky alebo kritéria (vek, otvorenie účtu, preukázanie pôvodu majetku, súhlasenie s podmienkami obchodovania..)
- Užívateľsky bezpečnejšie z hľadiska centrálnych autorít a jasne stanovených procesov dozerajúcich na činnosť subjektov a práva používateľov

Kľúčové prvky DeFi:

- Eliminuje prítomnosť sprostredkovateľkách subjektov (napríklad banka) ako súčasti reťazca potrebných na vykonanie príkazu.
- Zaručuje prístup každému, kto má prístup na internet a vlastní peňaženku (hardvérovú ako napr. Trezor, alebo softvérovú ako napr. MetaMusk).
- Globálnosť a okamžitosť vykonania transakcií – vďaka absencii sprostredkovateľa a globálnosti kryptomien je každá reakcia vykonaná v rámci jednotiek sekúnd / minút (len výnimočne dlhšie, záleží ale od sieti, na ktorej má byť transakcia vykonaná)
- Peer – 2 – Peer transakcie – transakcie medzi dvoma rovnocennými subjektami, bez prítomnosti a potreby sprostredkovateľa alebo dozoru / dohľadu centralizovanej inštitúcie
- Otvorenosť a transparentnosť – verejnosť a transparentnosť blockchainu a jeho transakcií

Na prvý pohľad rozdielne svety TradFi a DeFi sa postupne viac a viac zbližujú a vzájomne dopĺňajú a do určitej miery aj kopírujú, viď rôzne druhy derivátov postavených na kryptoaktívach.

[42] https://openiazoch.zoznam.sk/cl/223740/Inovacie-a-regulacia-Ked-je-obchodovanie-s-akciami-jednoduche-ako-hra/

Najnovším trendom je prienik použitia kryptoaktív na nákup tradičných finančných inštrumentov. Tento proces tokenizácie aktív ako sú napríklad akcie, finančné deriváty (najčastejšie spomínané futures a opice), a nehnuteľnosti je ďalším krokom inštitúciu v kryptoadopcii.

S týmto procesom sú ale momentálne spojené veľké nejasnosti najme v oblasti regulácie a regulačno – licenčných požiadaviek zo strany dozorných orgánov. Je pravdepodobne len otázkou času, kedy sa tento trend začne šíriť viac a podobný vzorec budú replikovať aj ďalšie decentralizované burzy.

Za určitý príklad fúzie medzi TradFi a DeFi z hľadiska prepojenia možností finančného derivátu a vlastnosti kryptomeny z hľadiska tokenizácie možno považovať pákové tokeny, ktoré je možné nakúpiť na burze Binance.

Z technického hľadiska na ne môžeme pozerať ako na „koš“ otvorených pozícií perpetual futures (derivátov), ktoré sú tokenizované s pákovým efektom. Samotné futures reflektujú ceny podkladového aktíva, v tomto prípade kryptomien.
Je dôležité poznamenať, že s týmto typom tokenov je spojené výrazne vyššie riziko straty (ale aj zisku) ako v prípade ich podkladového aktíva, čo je samozrejme dané ich natívnou vlastnosťou pákového efektu zakomponovaného do týchto tokenov.

Kvantifikácia hrozieb AML / CFT vyplývajúca z tohto prepojenia TradFin a DeFi je veľmi náročná. Na jednej strane je náročnosť spojená s technológiami potrebnými na trasovanie transferov kryptoaktív na jednotlivých sieťach. Na druhej strane stojí výrazne regulovaný trh obchodovania s aktívami ako sú akcie a napríklad finančné deriváty s jasne stanovenými pravidlami a dozornými orgánmi.
V prípade, že jednotlivé OČTK (možno povedať, že globálne) nebudú disponovať potrebnými technologickými riešeniami potrebnými na trasovanie kryptoaktív, mohlo by byť pre medzinárodné zločinecké organizácie / teroristické skupiny vytvárať štruktúry na legalizáciu prostriedkov prostredníctvom finančných trhov. Je preto potrebné tento trend monitorovať od samotného počiatku a veľmi pozorne sledovať vývoj regulácie v iných štátoch v tomto segmente.

25. DAO

Pojem DAO – decentralizovaná autonómna organizácia je typom organizácie, ktorá je prevádzkovaná, resp. operuje bez centrálnej autority, dohľadu, či dozoru, a veľakrát bez jasne stanovenej manažérskej štruktúry. Založené sú výhradne na blockchainovej technológií a k svojej činnosti využívajú smart kontrakty.
Je potrebné zdôrazniť, že samotný pojem DAO sa v súčasnej dobe dynamický vyvíja a nieje jednoznačne ustálený v samotnom kryptosvete. Z právneho hľadiska sa nejedná o právnické osoby a fungujú výhradne v online svete, presnejšie povedané na blockchaine.

DAO sa pri svojej činnosti opierajú o natívne vlastnosti blockchainov ako sú napríklad:

1) Decentralizácia – neexistuje konkrétna osoba ale inštitúcia, ktorá rozhoduje, ale rozhodnutia sú najčastejšie prijímané kolektívne, často na princípe hlasovania jej členov / účastníkov
2) Transparentnosť - všetky rozhodnutia a transakcie sú viditeľné pre všetkých ostatných členov vďaka transparentnosti technológie blockchain
3) Komunita – prioritou web3 technologických riešení je participácia komunity na vývoji, výskume a následnej implementácií noviniek do systému
4) Podpory spojené s členstvom – rôzne podpory pre členov a participujúcu časť komunity s cieľom podporiť rozvoj, zväčšiť členskú základňu a zaviesť do praxe čo najviac inovácií

V niektorých diskusiách v odborných kruhoch sa objavujú teórie o tom, že samotné DAO nepotrebuje právne zaštítenie v zákonoch, pretože samotný zdrojový kód jasne vymedzuje jeho funkčnosť a možnosti a je pre to proklamovaná myšlienka „kód je zákonom“.[43]

Je veľmi náročné klasifikovať miestnu príslušnosť nejakej DAO, vďaka jej decentralizácií, absencii právnej podoby a veľakrát anonymnej sieti zakladateľov. Tým pádom je myšlienka o nejak regulácií v súčasnej dobe len veľmi ťažko nerealizovateľná.

25.1 DAO vo svete

Príkladom výnimiek, kedy prišlo k ustanoveniu právnej podoby DAO na základe súdneho rozhodnutia môžu byť brané príklady súdnych rozhodnutí z USA, napríklad:

1) American CryptoFED – DAO uznaná súdom ako právna entita, konkrétne súdom štátu Wyoming, kde DAO bola uznaná ako „osobitá forma s.r.o“.[44]

[43] https://cointelegraph.com/magazine/legal-dangers-getting-involved-daos/
[44] https://coingeek.com/the-first-legally-recognized-dao-in-the-usa/

Cieľom American CryptoFED je v blízkej dobe začať fungovať plne bez riadenia CEO, kedy riadenie celej organizácie bude prebiehať prostredníctvom Governance tokenov, držaných a používaných naprieč komunitou[45]

2) dOrg – DAO na blockchain sieti Ethereum, ako prvá spoločnosť na svete použila svoj zdrojový kód ako svoj systém riadenia, celé jej riadenie, majetková a vlastnícka štruktúra je riadená prostredníctvom blockchainu.[46]
Právny systém amerického štátu Vermont v kapitole 25, podkapitole 012 dostupnom na nasledujúcom odkaze: https://legislature.vermont.gov/statutes/section/11/025/04173
špecifikuje založenie tzv. Blockchain-based Limited Liability Companies – spoločností s ručeným obmedzeným založenými na technológií blockchain.
Práve tento právny status využíva na svoju činnosť dOrg.

25.2 Prepojenie DAO a tradičných právnych foriem podnikania

Práve kombinácia DAO a tradičných právnych foriem je jedným z nových odvetví, ktoré vzniká prienikom blockchainu do iných segmentov.

BBLLC - Blockchain-based Limited Liability Companies – spoločnosť s ručeným obmedzeným založená na technológií blockchain.[47]
Celý systém riadenia sa už celkovo spolieha len na technológiu blochchainu, respektíve na ňom bežiacich smart kontraktov.

Tento prirodzený vývoj fúzie bežného právneho systému, reprezentovaný tradičnými schémami a formami podnikania a nových technológií, ktoré vedia replikovať jasne stanovené mantinely regulovaného podnikateľského prostredia a zároveň inovovať jeho prvky implementáciou nových technológií a procesov sa už začínajú objavovať v niektorých štátoch sveta. Opätovne ale platí, že tie štáty, ktoré tieto inovácie zavádzajú majú veľakrát veľmi dostupné podnikateľské prostredie a umožňujú založenie takýchto foriem aj pre cudzincov.

Je opätovne dôležité zdôrazniť jeden z hlavných aspektov krypta – globálnosť. V modernom svete, ktorý vo veľa segmentoch razí teóriu globalizmu je proces začatia podnikania / založenia si firmy veľmi zjednodušený. Progresívne podnikateľské myšlienky a regulačné zmeny sa šíria veľkou rýchlosťou. Preto je potrebné aj z hľadiska regulačných orgánov vnímať zmeny implementované v USA ako inšpiráciu na zlepšenie podnikateľského prostredia na Slovensku.

[45] https://coingeek.com/the-first-legally-recognized-dao-in-the-usa/
[46] https://www.coindesk.com/markets/2019/06/11/dorg-founders-have-created-the-first-limited-liability-dao/
[47] https://legislature.vermont.gov/statutes/section/11/025/04173

25.3 DAO & Governance token

Práve DAO bez právnej entity sú ale jedinečným príkladom aktívneho využívania takzvaných governance token – preložiteľných do slovenčiny ako tokeny riadenia.
Governance token je veľmi exaktne definovaný na webových stránkach kryptoburzy Kraken nasledovne: je typ kryptomeny, ktorá sa snaží demokratizovať správu decentralizovaných aplikácií (dApps) a iných protokolov založených na blockchaine.[48]

Technicky vzato, vlastník governance tokenov má právo, možnosť, alebo doslova povinnosť aktívne participovať na komunitnom chode a rozhodovaní toho ktorého DAO, ktorého tokeny daná osoba alebo inštitúcia vlastní.

Samozrejme existujú rôzne formy limitácie využiteľnosti governance tokenov, niektoré môžu mať len obmedzené hlasovacie práva spojené s vopred vyšpecifikovanou oblasťou, v ktorej môže napríklad ich držiteľ hlasovať alebo realizovať iné svoje práva.

Príkladom „tradičných“ DAO, ktoré jasne nasledujú svoju decentralizovanú funkciu a fungujú výhradne na technológii blockchain a práve naopak, úplne ignorujú tradičnú reguláciu sú celé stovky.

Projekt DAO s významnou funkciou governance tokenov pri procese smerovania a riadenia DAO je napríklad projekt MakerDAO, ktorý vydal vlastný stablecoin DAI[49], a zároveň má vlastný token, Maker (MKR)[50], definovaný respektíve fungujúci ako governance token, ktorého držitelia majú hlasovacie práva v súvislosti s vývojom a smerovaním projektu MakerDAO. DAO sa chová ako komunitne riadený projekt, ale zároveň governance tokenov môžeme považovať za ekvivalent akcií s hlasovacím právom vo svete tradičných financií.

Samotný proces hlasovania prebieha prostredníctvom vyhlásených hlasovaní dostupných na adrese: https://vote.makerdao.com/ , a množstvo hlasov je ekvivalentné množstvu tokenov, ktoré je držané jednotlivými majiteľmi. Vopred sa stanoví, aké sú parametre hlasovania (či 50% + 1 hlas, alebo 51% všetkých hlasov) a následne sa odhlasovaná zmena implementuje v vo vopred stanovenom časovom rámci.

V prípade governance tokenov je jasne vidieť prelínanie, respektíve inšpirácia tradičným svetom financií a tým, ako fungujú akcie a s nimi spojené hlasovacie práva. Samozrejme, DeFi v tomto prípade aplikuje technologicky výhodné a časovo flexibilné hlasovania, bez potreby zvolávať valné zhromaždenie, a notárskym zápisom je samotný blockchain a v ňom zapísané údaje.

[48] https://www.kraken.com/learn/what-is-a-governance-token
[49] https://coinmarketcap.com/currencies/multi-collateral-dai/
[50] https://coinmarketcap.com/currencies/maker/

FSJ pozorne monitoruje postupný rozvoj DAO ktoré sú prepojené na slovenských občanov, respektíve na DAO, ktoré sú populárne v kryptokomunite na Slovensku.

Je dôležité kvantifikovať aj hrozby spojené s AML / CFT v prípade DAO. DAO samotné už zo svojho názvu funguje ako decentralizovaná organizácia, bez potreby alebo nutnosti zbierať o svojich užívateľoch akékoľvek dáta alebo informácie. Práve táto absencia dát a akejkoľvek verifikácie osôb podieľajúcich sa na ich chode, riadení, hlasovaní a prevodoch robí DAO veľmi vhodné ako prostriedok[51] spojený s konverziou prostriedkov (pokiaľ to dané DAO ako svoju funkciu umožňuje) z krypta na krypto a tým skomplikovanie respektíve znemožnenie trasovania transakcie.

Mimo prípadov, kedy DAO má aj svoju právnu entitu, OČTK vo svete nedisponujú, respektíve ak disponujú tak len v limitovanej miere a vo výnimočných prípadoch, možnosťami prinútiť akékoľvek DAO na spoluprácu a zdieľanie potrebných informácií na procesné úkony.

Na druhej strane, je dôležité uvedomiť si, že DAO stále fungujú v interakcii s vonkajším svetom, ich činnosť a smerovanie je určované konkrétnymi fyzickými osobami, ktoré môžu na tom finančne profitovať. Chod samotného DAO je usmerňované nielen hlasovaním komunity ale aj samotnou prácou developerov, ktorí taktiež berú benefity, niekedy aj vo forme kryptomien. A v neposlednom rade sú to platby spojené s chodom serverov, promo a marketingovými akciami a rôznymi inými formami propagácie projektu. Všetky tieto aspekty by mohli byť brané ako pomyselné kamienky do mozaiky potencionálneho boja s AML / CFT v prípade DAO.

26 ICO

S rozvojom kryptoaktív a zvyšujúcou sa kryptoadopciou sa začali objavovať aj nové procesy a pojmy, často odvodené pôvodom z finančného sektora. Za jeden z takýchto pojmov a zároveň novovzniknutých procesov, je aj tzv. ICO - Initial Coin Offering - prvotný úpis mince (v zmysle kryptomince, resp. kryptoaktíva).

Vznik pojmu a celého procesu vychádza z pôvodného – IPO (Initial Public Offering): ktorý sa vzťahuje na proces prvej verejnej ponuky akcií súkromnej spoločnosti pri novej emisii akcií. IPO umožňuje spoločnosti získať kapitál od verejných (privátnych alebo inštitucionálnych) investorov.[52]

Tento proces inšpiroval aj kryptokomunitu a s rozvojom nových sietí a na nich bežiacich alt-coinov bolo potrebné zoštandardizovať a proces aj terminológiu. Proces, ktorý prebieha na rôznych sietiach (chains) bol pomenovaný ICO - Samotný proces ICO – prvotný úpis mince definuje Národná Banka Slovenska na svojich webových stránkach nasledovne: Alternatívna

[51] https://compliancelatam.legal/en/decentralized-autonomous-organizations-and-money-laundering/
[52] https://www.investopedia.com/terms/i/ipo.asp

forma financovania označovaná ako „Initial Coin Offerings“ (ICOs) je inovatívny a výrazne sa rozmáhajúci spôsob zhromažďovania finančných prostriedkov od verejnosti za účelom financovania projektov konkrétnych osôb. Ide o vytvorenie elektronických „mincí”, resp. „tokenov“ a ich následnú ponuku a predaj verejnosti výmenou za zákonné meny (napríklad euro), alebo častejšie za virtuálne aktíva (napríklad bitcoin alebo ether). K takejto ponuke dochádza najčastejšie prostredníctvom internetu a sociálnych médií.[53]

Zákon 297/2008 Z.z. bližšie špecifikuje proces ICO v §9 písmeno l) a to nasledovne:
„virtuálnou menou 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 fyzickými osobami alebo právnickými osobami ako nástroj výmeny, ktorý možno elektronicky prevádzať, uchovávať alebo s ním elektronicky obchodovať,“

ICO býva vo veľkej miere spájané s výrazným marketingom najmä na moderných platformách ako sú napríklad sociálne siete. Tak ako platí globalita, resp. nadnárodnosť kryptoaktív v bežnom obchodovaní, vďaka internetu sa ani marketing veľakrát nelimituje len na jednu konkrétnu geografickú oblasť. Slovenskí občania sa preto môžu aktívne podieľať na procese ICO zahraničného subjektu v podstate veľmi jednoducho.

Je dôležité zdôrazniť, že pri procesoch ICO sa jedná veľakrát o problém tzv. podvodných ICO, v angličtine nazývaných jednotným názvom „scam“.
Samotný proces ICO sa často stáva zneužívaným procesom ako podvodná metóda, ako od investorov vylákať finančné prostriedky.
Vďaka mimoriadne dynamickému rozvoju rôznych sietí na ktorých jednotlivé kryptomeny resp. tokeny bežia a vzrastajúcej kryptoadopci a v neposlednom rade aj v výrazným zjednodušením procesu vytvorenia tokenu na jednotlivých sieťach, môžeme hovoriť o výraznom náraste trendu zneužívania ICO v podvodných schémach.

Problematike spustenia vlastného tokenu či už na hlavnej sieti alebo na tzv. „testnete“ sa venuje veľké množstvo článkov a youtube videí. Vďaka rastu popularity kryptomien už užívatelia nepotrebujú hlboké znalosti programovania alebo informatiky na to, aby vedeli nájsť veľmi exaktný návod na spustenie vlastného tokenu bežiaceho na niektorej z najznámejších a najbežnejších sietí.
Príkladom môže byť tento jednoduchý návod, obsahujúci aj odkazy na videa, dostupné na nasledujúcom odkaze: https://moralis.io/how-to-create-a-bsc-token-in-5-steps/

Vďaka dostupnosti veľkého množstva informácií, návodov a procesu, kedy sa celá krypto-scéna pohla smerom od IT nadšencov k bežným používateľom, môžeme sledovať rast množstva podvodných schém na jednotlivých sieťach.

[53] https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/

Špeciálne sa procesu ICO venuje Národná Banka Slovenska priamo na svojich webových stránkach, v sekcii dohľadu nad finančným trhom, dostupné na nasledujúcom odkaze: https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/

26.1 NBS a ICO

NBS definuje na svojich webových stránkach proces ICO nasledovne:
Čo je Initial Coin Offerings (ICOs)
Alternatívna forma financovania označovaná ako „Initial Coin Offerings“ (ICOs) je inovatívny a výrazne sa rozmáhajúci spôsob zhromažďovania finančných prostriedkov od verejnosti za účelom financovania projektov konkrétnych osôb. Ide o vytvorenie elektronických „mincí”, resp. „tokenov“ a ich následnú ponuku a predaj verejnosti výmenou za zákonné meny (napríklad euro), alebo častejšie za virtuálne aktíva (napríklad bitcoin alebo ether). K takejto ponuke dochádza najčastejšie prostredníctvom internetu a sociálnych médií.[54]

Informácia pre spotrebiteľov
Národná banka Slovenska upozorňuje širokú verejnosť, že legislatíva Slovenskej republiky výslovne neupravuje a nevymedzuje kryptoaktíva a obchodovanie s nimi. Oblasť kryptoaktív nie je regulovaná a dohliadaná Národnou bankou Slovenska.

Produkty, služby a činnosti, ktoré zahŕňajú kryptoaktíva, vrátane tzv. Initial Coin Offerings (ICOs), sú poskytované osobám v Slovenskej republike najmä prostredníctvom internetu, a to aj zo strany obchodných platforiem z iných štátov. Právny poriadok týchto štátov môže kryptoaktíva a služby, ktoré s nimi súvisia, upravovať, a teda osobám, ktoré sa zúčastňujú na obchodoch s kryptoaktívami, môžu z neho vyplývať určité práva alebo povinnosti.

Národná banka Slovenska zdôrazňuje, že kryptoaktíva nemajú fyzickú protihodnotu vo forme zákonného platidla. Výmeny alebo nákupy kryptoaktív za iné kryptoaktíva alebo oficiálne uznané meny (napríklad euro) sa uskutočňujú na vlastné riziko osôb, ktoré sa zúčastňujú na takýchto obchodoch. Na výplaty prípadných náhrad za straty spôsobené týmito výmenami alebo nákupmi nie je žiaden zákonný nárok.

S produktmi alebo službami, ktoré poskytujú obchodné platformy, ľudovo označované aj ako „kryptoburzy“ alebo „kryptozmenárne“, sú spojené viaceré významné riziká. Týmito rizikami môžu byť najmä:

- vysoká kolísavosť cien, ktorá môže viesť k vytváraniu bubliny a výraznej finančnej strate pre účastníkov obchodov, vrátane straty všetkých vložených finančných prostriedkov,

[54] https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/

- vo väčšine prípadov účastníci obchodov nemajú garanciu získania alebo vymožiteľnosti dohodnutej odmeny alebo poskytnutia dohodnutých služieb alebo produktov,
- pre účastníkov obchodov môže byť náročné, alebo až nemožné, predať alebo zameniť kúpené kryptoaktíva za iné kryptoaktíva alebo za oficiálne uznané meny,
- účastníci obchodov sa môžu stať obeťou zavádzajúcich obchodných praktík, podvodu alebo iných nezákonných aktivít,
- obmedzená alebo úplná nefunkčnosť technológií, ktoré umožňujú obchodovanie s kryptoaktívami, čo môže spôsobiť účastníkom takýchto obchodov finančné straty.[55]

NBS ďalej na svojich stránkach jasne upozorňuje na fakt, že ICO samotné nie je v slovenskej legislatíve zatiaľ jednoznačne upravené.

Legislatíva
Problematika kryptoaktív, resp. ICO a otázka jej regulácie je predmetom diskusií tak v rámci jednotlivých členských štátov a orgánov Európskej únie, ako aj celosvetovo. Dôvodom je rast významu kryptoaktív, resp. ICOs a zvyšujúci sa objem finančných prostriedkov v tejto oblasti, ako aj potreba reagovať na riziká, ktoré sú s týmto alternatívnym spôsobom financovania spojené.

V súčasnosti nie sú kryptoaktíva, resp. ICO výslovne upravené v slovenskej a európskej legislatíve, avšak niektoré ich prvky v nej upravené byť môžu.

Európsky orgán pre cenné papiere a trhy (ESMA) vydal v januári 2019 materiál (technickú pomoc) obsahujúci analýzu súčasného trhu s kryptoaktívami a opis fungovania kryptoaktív a ICOs. Dokument rieši aj otázku, či sa súčasná legislatíva EÚ, resp. jej členských štátov, vzťahuje na kryptoaktíva, resp. ICOs.

Niektoré kryptoaktíva môžu byť podľa tejto analýzy finančnými nástrojmi, avšak väčšina z nich nespadá pod reguláciu EÚ. Ak sú kryptoaktíva v konkrétnom prípade považované za finančné nástroje, podľa orgánu ESMA by sa na ne (vrátane ich vydavateľa a/alebo spoločnosti poskytujúcej súvisiace investičné služby/aktivity) mala vzťahovať príslušná regulácia EÚ, najmä:

- MiCA ktorá doteraz najkomplexnejšie nazerá na problematiku ICO
- smernica MiFID II,
- prospektové nariadenie,
- Market Abuse smernica,
- nariadenie o Short Sellingu,
- nariadenie o centrálnych depozitároch cenných papierov,
- smernica o konečnom zúčtovaní v platobných systémoch a zúčtovacích systémoch cenných papierov.

[55] https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/

Analýza konštatuje, že posúdenie, či kryptoaktívum predstavuje finančný nástroj, sa odvíja od implementácie smernice MiFID II do právneho poriadku členského štátu EÚ a je v kompetencii príslušných orgánov dohľadu, pričom pri posúdení je potrebné vychádzať zo špecifík každého konkrétneho prípadu.

Európsky orgán pre bankovníctvo (EBA) vydal stanovisko v otázke vhodnosti súčasnej regulácie EÚ vo vzťahu ku kryptoaktívam. Dokument konštatuje, že niektoré kryptoaktíva by bolo možné považovať za elektronické peniaze, ak splnia všetky príslušné definičné znaky, avšak aj EBA vo svojom stanovisku uvádza, že väčšina aktivít súvisiacich s kryptoaktívami nie je regulovaná súčasnou legislatívou EÚ. V prípade kryptoaktív, ktoré by boli považované za elektronické peniaze, by podľa orgánu EBA bolo potrebné zvažovať aj aplikáciu revidovanej smernice o platobných službách na vnútornom trhu.

Právne predpisy v pôsobnosti Národnej banky Slovenska neupravujú kryptoaktíva, ich ťažbu (mining), obchodovanie s nimi a neobsahujú ani ich definíciu. Tieto právne predpisy zároveň neustanovujú povinnosť získania oprávnenia na vydávanie kryptoaktív, resp. na obchodovanie s nimi a v tejto súvislosti neupravujú ani požiadavky, ktoré je potrebné splniť pre účely výkonu takýchto činností.

Oprávnenia na vykonávanie regulovaných činností, udeľované podľa príslušných právnych predpisov Národnou bankou Slovenska (napríklad devízová licencia, povolenie na poskytovanie platobných služieb, povolenie na vydávanie elektronických peňazí), nesúvisia s vydávaním kryptoaktív, resp. obchodovaním s nimi, a to ani v prípade, ak dochádza ku kúpe alebo predaju kryptoaktív za menu euro alebo cudziu menu.

Podľa právneho poriadku Slovenskej republiky kryptoaktíva nemožno považovať za finančné nástroje podľa zákona č. 566/2001 Z. z. o cenných papieroch a investičných službách. Nemožno ich považovať ani za cenné papiere, keďže nespĺňajú definíciu cenného papiera, a to najmä požiadavku zápisu v zákonom ustanovenej podobe a forme.[56]

27. SCAM schémy

FSJ vníma rast počtu podvodných schém, ktoré využívajú rôzne podvodné prvky s cieľom vylákať od užívateľov finančné prostriedky.
S rozvojom smartkontraktov prebieha aj rozvoj potencionálnych možností implementovať do zdrojového kódu kontraktu aj rôzne varianty tzv. zadných vrátok, ktoré následne môžu viesť k zneužitiu na neetické alebo dokonca nelegálne účely.

[56] https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/

Nie všetky podvodné schémy musia však byť nutne spojené s implementáciou zadných vrátok priamo do zdrojového kódu pri ICO. Veľakrát sa jedná aj o zavedenie ľudí do omylu alebo podvod. V neposlednom rade býva častou podvodnou schémou aj úmyselná manipulácia málo likvidného trhu / tokenu a vytvorenie umelého nafúknutia ceny.

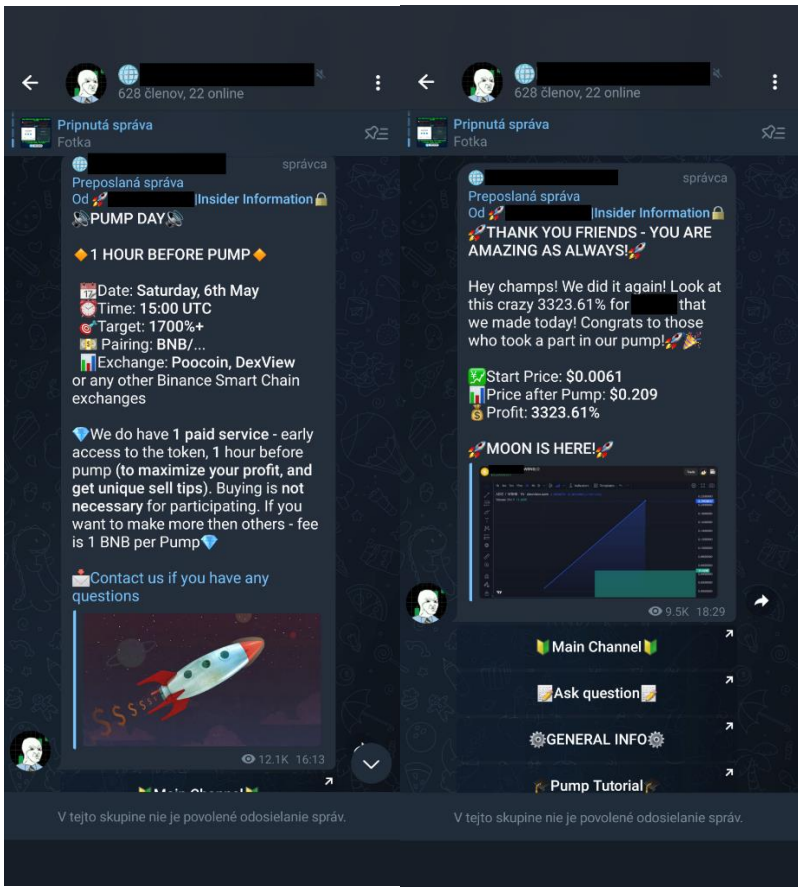
1) Pump n´ Dump – komunita akcia, ktorá umelo vyženie cenu nejakého tokenu, zväčša obchodovaného na decentralizovanej burze (DEX), spolieha sa na tzv. FOMO (fear of missing out – strach z premeškania príležitosti), kedy vysoký rast ceny nejakého tokenu priláka aj ďalších investorov – špekulantov a vyvolá zvýšený dopyt po tokene a následne exponenciálny vzrast jeho ceny.

   FSJ v rámci svojej činnosti zachytila existenciu účelových skupín vedených na sociálnej sieti Telegram, ktoré slúžia na zjednotenie ľudí a následne účelovú manipuláciu trhu pomocou vytvorenia umelého dopytu po kryptoaktíve.

   Takýto typ manipulácie trhu býva veľmi často prísne vyšetrovaný zo strany regulátora, ak sa deje na regulovanom trhu, ako sú akcie alebo finančné deriváty, pri kryptoaktívach, ktoré sú stále ešte v procese rozvoja a vznikajúcej regulácie sú tieto podvody zatiaľ bez vyšetrovania, resp. ich pôvodcovia bez trestov.

   Obrázok:
   Na ľavej strane výzva na vytvorenie „pumpy“ – dopytu po určenom tokene
   Na pravej strane poďakovanie a informovanie členov Telegram skupiny, aký bol výsledok umelo vyvolaného dopytu po tokene.

Obrázok č.17



Zdroj: Vlastná činnosť FSJ

2) Honeypot – môže mať veľa podôb, ale najčastejšie sa jedná o zavádzanie spojené s vysokým výnosom alebo exkluzívnymi príležitosťami, ktoré sú využité ako lákadlo pre investorov. Následne podvodník / smart kontrakt nim naprogramovaný môže spôsobiť nechcenú aktivitu ako je napr. prevod na inú peňaženku, zabránenie možnosti predaja tokenu, alebo stratu hneď po nákupe.

3) Zastavenie obchodovania – tvorca tokenu môže zaimplementovať funkciu, ktorá mu umožní zastaviť obchodovanie s tokenom a tým pádom ho spraviť bezcenným

4) Mint – zdrojový kód môže obsahovať možnosť kontinuálne emitovať nové tokeny a tým pádom vytvoriť silný inflačný trend na cenu tokenu

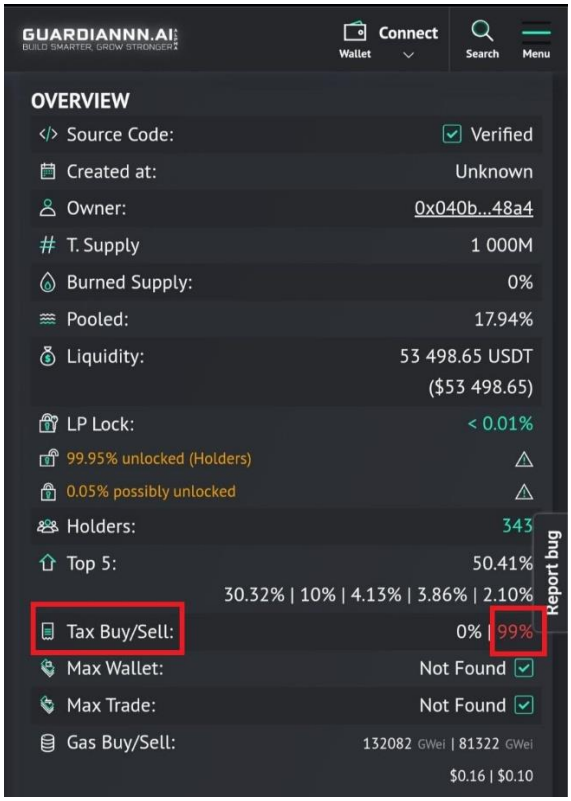
5) Hidden Mint – tak horeuvedený Mint, ale rozšírený ale o komplexnejšie funkcie, ako je napríklad obmedzenie obchodovania prostredníctvom limitovania likvidity. Hidden mint býva náročnejší na detekciu, pretože býva skrytý sofistikovanejšie v zdrojovom kóde.

6) Neverifikovaná knižnica – knižnica ktorá nemôže byť verifikovaná môže obsahovať typ kódu, ktorý môže byť škodlivý pre kupcov tokenu, respektíve jeho držiteľov

7) Preposielanie na vopred stanovenú adresu – po nákupe tokenov zo strany používateľa sú tieto tokeny zaslané na vopred stanovenú adresu v kontrakte, nie na tú, ktorú kupujúci určil pri nákupe týchto tokenov

8) Predajná daň – pri vydaní / emisií nových tokenov býva zakomponované tvorcom v zdrojovom kóde možnosť tzv. predajnej dane, kedy sa veľká (na obrázku dole až 99% daň aplikuje pri predaji tokenu. Nákupca preto po predaji zmieneného / nakúpeného tokenu dostane naspäť menej ako 1% z investovanej sumy (po započítaní poplatkov na sieti).

Obrázok č.18



Zdroj: GuardiaNNN.ai

9) Rug Pull – typ podvodného chovania, kde sa developer snaží nalákať investorov do nákupu aktíva, najčastejšie nového tokenu na základe prezentovania mimoriadnej výhodnosti projektu a následne ujde aj s ich investovanými prostriedkami a investorom ostanú len veľakrát bezcenné tokeny. Rug Pull sú typom tzv. „exit scams“ – výstupných podvodov najčastejšie na decentralizovaných burzách.
Najčastejšie typy Rug Pull-ov môžeme rozdeliť do 3 kategórií[57]:

[57] https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it

a) „Ukradnutie likvidity“
b) „Obmedzenie príkazov na predaj“
c) „Dumpingový predaj“

10) Ponziho schéma – schéma známa a bežná zo segmentu tradičných financií, kedy sa tvorca tokenu zameriava na nalákanie čo najväčšieho množstva investorov, ktorým sú vyplácané nadštandardné výnosy. Systém funguje do bodu, pokiaľ je prítok kapitálu z nových investorov vyšší ako náklad na výplatu už existujúcim investorom, alebo do bodu, kedy sa tvorca tokenu rozhodne celú schému vypnúť.
Najväčšou Ponziho schémou v segmente kryptomien je kauza OneCoin, ktorý sa prezentoval ako „zabijak Bitcoinu“ a ktorá bežala od roku 2014 do roku 2019 na princípe MLM – Multi Level Marketingu a celková suma sa blížila 5,8 miliardy USD.[58]
OneCoin bol distribuovaný aj na území Slovenskej republiky prostredníctvom MLM sietí.
Zo skúsenosti môžeme povedať, že táto forma distribúcie býva často zneužívaná na rozširovanie SCAM-ov v kryptosvete.

11) Marketingová peňaženka - nejedná sa o formu skrytého / podvodného vyťahovania finančných prostriedkov z projektu, ale formu zneužitia finančných prostriedkov na financovanie opulentného životného štýlu tvorcov projektu. S cieľom zaujať čo najviac bežných retailových investorov sa tvorcovia projektov radi prezentujú mimoriadne úspešným a bohatým životným štýlom. Veľakrát finančné prostriedky naň čerpajú zo samotného projektu a na to vyhradeného rozpočtu pomocou tzv. marketingovej peňaženky. Niektoré projekty na to vyhradzujú až 30 % príjmov.

[58] https://coinmarketcap.com/alexandria/article/5-of-the-biggest-crypto-ponzi-schemes

Obrázok č.19

Zdroj: Vlastná činnosť FSJ

Medzi globálne najznámejšie respektíve, najvyužívanejšie formy podvodov, ktoré ohrozujú aj slovenských klientov patria nasledujúce:

1) Podvodné aplikácie – podvodníci využívajú známe značky a ich aplikácie / weby, aby od držiteľov krypta vylákali ich privátne kľúče, emaily a heslá, alebo iné osobné údaje za cieľom dostať sa k ich krypto aktívam

2) Vydieranie – prostredníctvom emailu alebo sociálnych sietí je obeť informovaná, že existujú jej nahrávky ako navštívila pornografické stránky, alebo dôkazy, o návšteve webových stránok a stiahnutí obrázkov / videí, ktoré obsahujú detskú pornografiu. Útočník vyžaduje zaslanie finančných prostriedkov v podobe kryptoaktív na stanovenú adresu, inak budú tieto záznamy zverejnené.

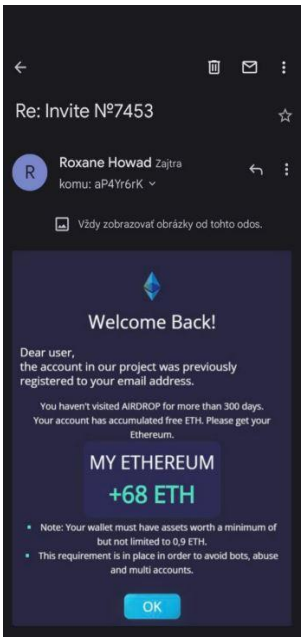
3) Darovací podvod – podvodníci oznámia prostredníctvom emailu / sociálnych sieti, že zašlú vyššiu sumu, len za menší poplatok, alebo, pod podmienkou, že peňaženka na ktorú budú zaslané prostriedky drží určitú kryptomenu a jej majiteľ bude zdieľať napr. privátny kľúč s nimi.

4) Phishingové podvody - podvodníci zašlú link na podvodné stránky a snažia sa o vylákanie potrebných údajov od užívateľom, cieľom je dostať sa k ich osobným údajom, prístupovým heslám alebo privátnym kľúčom

5) Falošné upozornenia od spoločností – podvodníci zašlú falošnú výzvu užívateľom ktorá môže obsahovať žiadosť o poskytnutie údajov, z dôvodov, že ich účet bol napadnutý hackerom, alebo sa môže jednať o „pre-sale“ výzvu od známej svetovej firmy, ktorá sa chystá vydať vlastný token a ponúka užívateľovi výnimočnú ponuku na nákup v predpredaji. Množstvo derivátov týchto falošných upozornení je nespočetné a pravidelne vznikajú nové.

   Obrázok ukazuje podvodný email, ktorý oznamuje naakumulovanú vysokú sumu a informáciu, že peňaženka, na ktorú to bude odoslané musí mať aktíva v určitej minimálnej hodnote.

   Obrázok č.20



Zdroj: Vlastná činnosť FSJ

Samozrejme, existujú aj desiatky iných podvodných schém, ktorých cieľom je buď vylákať finančné prostriedky od užívateľov, alebo sa nelegálnou cestou zmocniť ich osobných alebo prístupových údajov a následne prostriedky ukradnúť.

Každá z týchto schém sa opiera o určitú, veľakrát veľmi krátkodobú trendovosť na kryptotrhoch a zároveň o kombináciu nízkej miery regulácie a vysokej miery akceptácie rizika zo strany používateľov kryptoaktív. V neposlednom rade môžeme citovať aj známeho ekonóma J.M. Keynesa a jeho „animal spirit“ – zmes emócií, ktoré môžu mať vplyv na finančné rozhodnutia človeka.

Jedným z najúčinnejších bojov proti SCAMom pri ICO je systematické vzdelávanie, finančná gramotnosť a prevencia zo strany orgánov dohľadu, poprípade represívnych zložiek, kde budú nové trendy pravidelne monitorované a ich hrozba aktívne odkomunikovaná voči verejnosti.

28. Stablecoiny

S rozvojom kryptoaktív v poslednom období kryptokomunita hľadala efektívne riešenia, ktoré spájajú efektívnosť, rýchlosť a prevoditeľnosť kryptomien a zároveň negujú ich najväčší problém – extrémnu volatilitu. Prvotnou reakciou bolo uvedenie tzv. stablecoinov, ktoré sa rozvinuli do samostatného segmentu v rámci kryptoaktív.

Stablecoiny boli identifikované ako potenciálny nástroj na pranie špinavých peňazí a financovanie terorizmu. Zatiaľ čo súčasné používanie stablecoinov pri praní špinavých peňazí sa zdá byť malé, existujú obavy, že hromadné prijímanie stablecoinov by mohlo zvýšiť riziko ich zneužitia na nezákonné účely. Globálnym trendom je, že stablecoiny a ich poskytovatelia podliehajú zvýšeným kontrolám a dozoru zo strany vládnych regulátorov a iných dohľadových orgánov . Americká vláda tiež zverejnila správu o stablecoinoch a ich potenciálnych rizikách vrátane prania špinavých peňazí a využívania nadmerného pákového efektu.

FSJ vníma riziko využitie stablecoinov v legalizačných schémach spojených s nákupom / predajom stablecoinu pre zahraničné subjekty prostredníctvom lokálnych VASP-ov pri nedodržaní zvýšenej miere starostlivosti o klienta ako veľmi aktuálne.

Stablecoiny sú typy kryptoaktív, ktorých hodnota je naviazaná na nejaké podkladové aktívum a podľa toho, aké je to aktívum ich môžeme rozdeliť do:

a) Kolaterálnych – s 3 najčastejšími formami
b) Algoritmických

28.1. Kolaterálne

Stablecoiny s podkladovým aktívom FIAT menu - v tomto prípade je hodnota Stablecoinu naviazaná na množstvo FIAT meny, ktoré je uložené v bežných bankách, najčastejšie v podobe samotnej meny napríklad USD, EUR, JPY a niekedy aj vo forme krátkodobých finančných inštrumentov vydávaných centrálnymi bankami. Pád banky Sillicion Valley Bank (03/2023), ktorá bola jednou z hlavných bánk pre USDC, Stablecoin na etherneovej sieti ale ukázalo, že aj tento, doteraz globálne veľmi preferovaný systém je citlivý na externé vplyvy.

Graf č.34

Zdroj: finance.yahoo.com, 13.04.2023

Horeuvedený graf ukazuje reakciu trhu resp. stablecoinu USDC, fixovaného na USD po zverejnení informácií o problémoch banky SVB, ktorá bola držala cca 8% rezerv z celkovej kapitalizácie stablecoinu USDC[59].
Na grafe je vidieť moment, kedy vznikla obdoba tzv. „run na bank“ – „behu na banku“ kedy bol trh zahltený požiadavkami na vybratie finančných prostriedkov a to následne viedlo k výraznému poklesu hodnoty stablecoina. FDIC (Federal Deposit Insurance Corporationsa) sa ale ihneď (03/ 2023) vyjadril, že bude vyplácať depozity v plnej výške, čo trh prijal s veľkým nadšením a viedlo to k zastabilizovaniu bankového a finančného sektora v USA.

Komoditné Stablecoiny – respektíve, Stablecoiny s podkladovým aktívom v podobe komodít. Stablecoiny s podkladovým aktívom v podobe komodít využívajú jednotlivé komodity ako kolaterál, (zábezpeku) a garanciu svojej stability. Prvotné pokusy boli spojené s ropou ako primárnym podkladovým aktívom, ale trend jednoznačne prešiel ku vzácnym kovom, ako najčastejšie použitým podkladovým aktívom. Takéto stablecoiny sú v podstate reprezentantmi komodít založenými na blockchaine a sú kryté rezervami v držbe vopred stanovenej centrálnej entity. Ako jeden z najlepších príkladov môžeme uviesť PAXOS GOLD (PAXG) alebo Tether Gold (xAUT). V prípade Tether Gold (xAUT) je jeden token reprezentantom 1 trójskej unce zlata podľa špecifikácie London Gold Bar.

Stablecoiny s podkladovým aktívom v podobe kryptoaktív - Stablecoiny s podkladovým aktívom v podobe kryptoaktív je veľmi populárny typ stablecoinov, ktorých cena je krytá buď

[59] https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html

jednotlivým typom kryptomeny – napríklad Bitcoin alebo košíkom kryptomien, najčastejšie tých s najväčšou tržnou kapitalizáciou.

28.1. Algoritmické

Algoritmické stablecoiny sú typom kryptoaktív, ktoré sú navrhnutá tak, aby udržiavala stabilnú hodnotu vo vzťahu k inému aktívu, zvyčajne FIAT mene, ako je americký dolár alebo v poslednej dobe aj EUR-o. Na rozdiel od stablecoinov s podkladovým aktívom v podobe kryptoaktív, alebo tými ktoré sú kolateralizované rezervami vo FIAT mene, algoritmické stablecoiny sa spoliehajú na vysoko sofistikované algoritmy, ktoré vo svojej činnosti v podstate v vysokej rýchlosti simulujú činnosť centrálnych bánk a riadia na základe vzťahu dopytu a ponuky množstvo tokenov v obehu. Pri zvýšenom dopyte, aby zabránili prílišnému vzrastu ceny stablecoinu, reagujú vydávaním nových tokenov, pri tlaku na pokles ceny v podobe prevahy ponuky nad dopytom nastáva „pálenie“ tokenov, ktoré znižuje ich ponuku na trhu a to následne vedie k rastu a následnej stabilizácií ceny. Celý tento proces sa deje vo veľmi krátkom čase a cieľom stablecoinových algoritmov je docieliť minimálnu volatilitu stablecoinov.
Algoritmické stablecoiny nemajú nezávislé aktíva v rezervách na krytie hodnoty ich stablecoinov a plne sa opierajú o sofistikované algoritmy.

Najnovšou udalosťou ktorá vo finančnom svete doteraz nemala precedens a je možné, že nejakým spôsobom usmerní trh platieb vo svete je rozhodnutie americkej spoločnosti PayPal o spustení vlastného stablecoinu[60] najprv pre používateľov v USA ale s cieľom rozšíriť postupne aj pre ďalších mimo územia USA.

Stablecoin PayPal-u, pomenovaný PYUSD beží na sieti Ethereum a patrí do skupiny stablecoinov ktoré sú kryté aktívami. Samotný PayPal špecifikuje, že PYUSD bude krytý vysokolikvidnými aktívami.[61]

Stablecoin PYUSD bol prijatý kryptokomunitou s veľkým nadšením, avšak po analýze zdrojového kódu sa objavili prvé kritiky možnosti, ktoré si spoločnosť PayPal nechala doprogramovať. Niektorými z nich je napríklad tá, že spoločnosť PayPal si ponechala možnosť zmraziť aktíva vedené v stablecoinoch alebo vymazanie zmrazenej peňaženky. Tieto funkcie nazýva PayPal jednotným názvom: „Asset Protection“.[62]

Slovenská legislatíva sa momentálne nepozerá samostatne na problematiku stablecoinov ani ani ich nijak samostatne nereguluje.

Zo zistení FSJ vyplýva, že v súčasnej dobe je na území Slovenskej republiky jedna právnická osoba, ktorej vlastníci a konatelia sú zo zahraničia a ktorá vyvíja stablecoin, ktorý bude

[60] https://www.paypal.com/us/digital-wallet/manage-money/crypto/pyusd
[61] https://www.paypal.com/us/digital-wallet/manage-money/crypto/pyusd
[62] https://blockworks.co/news/paypal-pyusd-stablecoin-centralization

naviazaný na FIAT menu EURO. Jej stablecoin beží na sieti Ethereum a jedna sa o typ, ktorý je krytý aktívami v podobe FIAT meny a krátkodobých finančných inštrumentov.

Obrázok č.21: Zoznam najväčších stablecoinov z hľadiska tržnej kapitalizácie

Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
Tether USDt USDT	$0.9988	0.02%	0.06%	0.08%	$83,479,935,914	$23,678,281,639 23,707,900,558 USDT	83,578,639,640 USDT	
USD Coin USDC	$1.00	0.02%	0.01%	0.01%	$26,158,092,106	$3,004,384,255 3,004,303,151 USDC	26,154,856,704 USDC	
Dai DAI	$0.9999	0.04%	0.02%	0.07%	$4,903,812,817	$183,684,145 183,698,757 DAI	4,904,256,127 DAI	
Binance USD BUSD	$1.00	0.02%	0.06%	0.05%	$3,394,656,350	$1,485,037,233 1,484,447,141 BUSD	3,393,563,657 BUSD	
TrueUSD TUSD	$0.9997	0.02%	0.08%	0.09%	$2,996,158,391	$2,195,840,183 2,196,211,570 TUSD	2,997,074,781 TUSD	
USDD USDD	$0.9987	0.03%	0.04%	0.05%	$742,296,264	$21,932,611 21,967,303 USDD	743,297,903 USDD	
Pax Dollar USDP	$1.00	0.10%	0.83%	0.77%	$508,601,381	$2,124,557 2,117,414 USDP	507,056,423 USDP	
Gemini Dollar GUSD	$0.9838	0.17%	0.05%	0.92%	$354,454,867	$1,058,288 1,075,817 GUSD	360,298,538 GUSD	
TerraClassicUSD USTC	$0.01527	0.03%	1.01%	6.78%	$149,463,467	$20,998,081 1,373,213,657 USTC	9,790,496,464 USTC	
Frax FRAX	$0.9982	0.01%	0.20%	0.29%	$811,189,661	$7,185,495 7,195,675 FRAX	812,641,409 FRAX	

Zdroj: Coinmarketcap.com

Brevan Howard Digital vo svojej štúdií zverejnilo zaujímavé porovnanie hodnoty transakcií medzi VISA, svetovou jednotkou v elektronických platbách a používaním stablecoinov na blockchaine.

Z výsledkov porovnania vyšlo, že za rok 2022 bolo 11 biliónov USD v transakciách na sieťach stablecoinov v porovnaní s 11,6 biliónom USD globálne cez VISA.[63] Nemenej relevantným faktom, svedčiacim o vzrastajúcej kryptoadopci v segmente stablecoinov na globálnom trhu je množstvo realizovaných transakcií.

Štúdia na základe zanalyzovaných blockchainových transakcií poukazuje na fakt, že viac ako 5 000 000 peňaženiek týždenne je aktívnych, z čoho ¾ transakcií mala sumu nižšiu ako 1 000 USD.[64]

Tieto dáta jednoznačne poukazujú na postupnú kryptoadopciu zo strany bežných retailových užívateľov v segmente stablecoinov.

[63] https://www.ledgerinsights.com/brevan-howard-digital-stablecoins/
[64] https://www.ledgerinsights.com/brevan-howard-digital-stablecoins/

O záujme o stablecoiny svedčí aj fakt, že od posledného býčieho obdobia v roku 2021, množstvo transakcií stablecoinov kleslo len o 11%, oproti decentralizovaným a centralizovaným burzám, kde objem transakcií klesol o viac ako 60%.[65]

Rizikovosť stablecoinov z hľadiska problematiky AML / CFT musíme vnímať širokospektrálne. Kľúčový faktor rizikovosti v prípade stablecoinov neleží v ich anonymite / pseudoanonymite ako v prípade bežných kryptomien, ale v mixe ich natívnych vlastností ako sú napríklad: ich nízka volatilita, možnosť generovať profit na úrokoch, lacnom celosvetovom transfere, jednoduchej zameniteľnosti / konvertibilite za FIAT menu, zvýšenej akceptácií zo strany obchodníkov ale i vysokej akceptácií zo strany decentralizovaných búrz (najmä pri obchodovaní na pároch stablecoin / kryptomena) a iných.

29. Mixér

Za jeden z najvýraznejších ukážok rozdielnosti prístupu k kryptomenám medzi kryptokomunitou a štátnymi orgánmi môžeme považovať postoj ku tzv. mixérom.
Mixéri sú zároveň jedinečnou ukážkou spolupráce medzi kryptokomunitou a tajnými službami rôznych krajín na strane druhej.

Mixér - je služba, ktorá používateľovi umožňuje zaslať kryptoaktíva prostredníctvom jednej alebo viacerých transakcií anonymne. Funguje na báze kombinácie rôznych zdrojov, ktoré sa vzájomne premiešajú a tým sťažujú možnú identifikáciu na blockchaine. Cieľom mixéru je zabrániť iným osobám ale softwarovým riešeniam (rôzne formy trackovacích softwarových riešení) sledovať a potenciálne stotožniť adresu peňaženky s tou ktorou konkrétnou osobou alebo používateľom.

Pre účely sektorovej analýzy VA / VASP si rozoberieme technické možnosti a z nich vyplývajúce riziká spojené s umožnením legalizácie výnosov z trestnej činnosti, prania špinavých peňazí a možností financovania terorizmu. V neposlednom rade poukážeme na prepojenia na tzv. APT – štátom podporované kybernetické skupiny a ich využitie kryptoaktív.

Sindbad.io

Softwarová služba a momentálne (v čase písania tejto sektorovej analýzy – rok 2023) najpoužívanejší krypto mixér na trhu. Krypto výskumná firma Elliptic publikovala štúdiu na

[65] https://www.ledgerinsights.com/brevan-howard-digital-stablecoins/

základe ktorej považuje Sinbad.io za vysoko pravdepodobne nanovo spustenou verziou zakázaného Blender.io.[66]
V máji 2022 americký Office of Foreign Assets Control (OFAC), spadajúci pod Ministerstvo financií USA informoval o úplne prvom sankcionovaní služby mixéra kryptomien a to konkrétne Blender.io.
V tlačovej správe publikovanej na ich webových stránkach OFAC informoval[67], že Blender.io je využívaný Kórejskou ľudovodemokratickou republikou na podporu jej škodlivých kybernetických aktivít a prania špinavých peňazí z ukradnutých kryptomien. Dňa 23. marca 2022 uskutočnila Lazarus Group, štátom (KĽDR) podporovaná kybernetická skupina, doteraz najväčšiu lúpež kryptomien v hodnote takmer 620 miliónov dolárov z blockchainového projektu spojeného s online hrou Axie Infinity; Blender sa použil pri zmixovaní viac ako 20,5 milióna dolárov z nezákonných výnosov. Pod tlakom silných sankcií USA a OSN sa KĽDR uchýlila k nezákonným aktivitám, vrátane kybernetických lúpeží z búrz kryptomien a finančných inštitúcií, aby generovala príjmy pre svoje nezákonné programy zbraní hromadného ničenia (ZHN) a balistických rakiet.[68]
Tlačová správa ďalej uvádza citát námestníka ministerstva financií: „Dnes vôbec po prvýkrát ministerstvo financií schválilo sankcie na mixér kryptomien," povedal námestník ministra financií pre terorizmus a finančnú spravodajskú činnosť Brian E. Nelson. „Mixéry kryptomien ktoré pomáhajú nezákonným transakciám, predstavujú hrozbu pre záujmy národnej bezpečnosti USA. Podnikáme kroky proti nezákonnej finančnej aktivite zo strany KĽDR a nedovolíme, aby štátom podporovaná zlodejina a jej prostriedky na pranie špinavých peňazí zostali bez odpovede.[69]

Tento dovtedy bezprecedentný krok amerického ministerstva financií priamo implikuje fakt, akou veľkou hrozbou pre národnú bezpečnosť môžu byť finančné prostriedky, pri ktorých nieje možné verifikovať ich pôvod, stotožniť platbu respektíve jej pôvodcu s konkrétnou fyzickou alebo právnickou osobou.
Samotný Blender.io a v súčasnej dobe Sinbad.io býva v odborných kruhoch priamo spájaný s kyberskupinou Lazarus, ktorej členovia sú spájaní so severokórejskou rozviedkou.[70]

Po kroku amerického ministerstva financií a daní mixéra Blender.io na sankčný zoznam sa v krátkej dobe objavilo niekoľko ďalších mixovacích služieb ako okamžitá odpoveď kryptokomunity na zavedené sankcie.
OFAC opätovne zaviedol sankcie v auguste 2022 na službu Tornado Cash, ktoré podľa informácií OFAC-u od svojho vzniku v roku 2019 až do augusta 2022 bolo využité na vypratie sumy presahujúcej viac ako 7 miliárd dolárov.[71] Samotnej kryptoskupine Lazarus je prisudzované prepratie prostriedkov presahujúcich stovky miliónov USD.[72]

[66] https://decrypt.co/121222/new-sinbad-bitcoin-mixer-is-sanctioned-blender
[67] https://home.treasury.gov/news/press-releases/jy0768
[68] https://home.treasury.gov/news/press-releases/jy0768
[69] https://home.treasury.gov/news/press-releases/jy0768
[70] https://www.fbi.gov/wanted/cyber/park-jin-hyok
[71] https://home.treasury.gov/news/press-releases/jy0916
[72] https://home.treasury.gov/news/press-releases/jy0916

Vyjadrenie Ministerstva financií Spojených štátov amerických v tlačovej správe spojenej s uvedením mixéra Tornado Cash na sankčný zoznam a všeobecne k problematike mixérov ďalej hovorí: „Mixéry kryptomien, ktoré pomáhajú zločincom, sú hrozbou pre národnú bezpečnosť USA. Ministerstvo financií bude naďalej vyšetrovať používanie mixérov na nezákonné účely a využívať svoje orgány na riešenie rizík nezákonného financovania v ekosystéme virtuálnej meny.“[73]

Typický zmonitorovaný príklad využitia kryptomixéra Tornado Cash pri zakrytí pôvodu nelegálne získaných kryptoprostriedkov vďaka podvodu na investoroch na nemenovanej schéme.

Obrázok č.22

Txn Hash	Method	Block	Age	From		To	Value	[Txn Fee]
0xc2b2c840a1757ea06e...	Transfer	16011914	500 days 5 hrs ago	0x91fbb5adf8d328eb690...	OUT	0xd990759720c4515c87...	0.49191370848108 BNB	0.000105
0x0e2636fe34f9c8ee736...	Deposit	15131149	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB	0.004638805
0x430d8e3d3733cca088...	Deposit	15131147	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB	0.004664155
0x7fa760761859b72741...	Deposit	15131143	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB	0.004664215
0x731ae590ac9ac913ab...	Deposit	15131140	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	10 BNB	0.004689625
0xb1c42748362802b731...	Deposit	12279089	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x3f0c42d81b336c9b2d...	Deposit	12279087	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664155
0xbc14d80e5d6497b11d...	Deposit	12279085	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004613395
0x2f0af1cae8970fb64e2...	Deposit	12279084	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x3369ad9021c14b78e6...	Deposit	12279081	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x92f0afecb8e91a02287...	Deposit	12279080	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664215
0x28141f851bfc8799c81...	Deposit	12278990	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x64df449f6ea2a9b3cfc...	Deposit	12278987	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664215
0xd2274817cf8f36f4256...	Deposit	12278984	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664095
0xeeea212b87b3a2b253...	Deposit	12278981	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004689625
0x65336dc4ea85ad4d4f...	Deposit	12278977	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004613335
0xcbc6662fb6d1a642ad...	Deposit	12278827	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x7a33931997d1a7e652...	Deposit	12278824	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0xbd04fafcb1a1206e520...	Deposit	12278821	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664215
0xb8c3294650fe8fb9667...	Deposit	12278818	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x22b36ab043417fcb04f...	Deposit	12278802	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664215
0x3ea0ff6b986acb85077...	Deposit	12278630	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664215
0xa57b9c55a0a66a144e...	Deposit	12278628	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004689565
0x57675926939831f2e7b...	Deposit	12278625	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004638805
0x9ac44327ceca1efca3d...	Deposit	12278623	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT	Tornado.Cash: Proxy	100 BNB	0.004664215

Zdroj: Vlastná činnosť FSJ

V súčasnej dobe (leto 2023) je vnímaný ako technicky najprepracovanejší a preto z hľadiska problematiky AML / CFT najťažší na monitorovanie kryptomixér od pravdepodobne pôvodných tvorcov Blender.io, Sindbad.io.

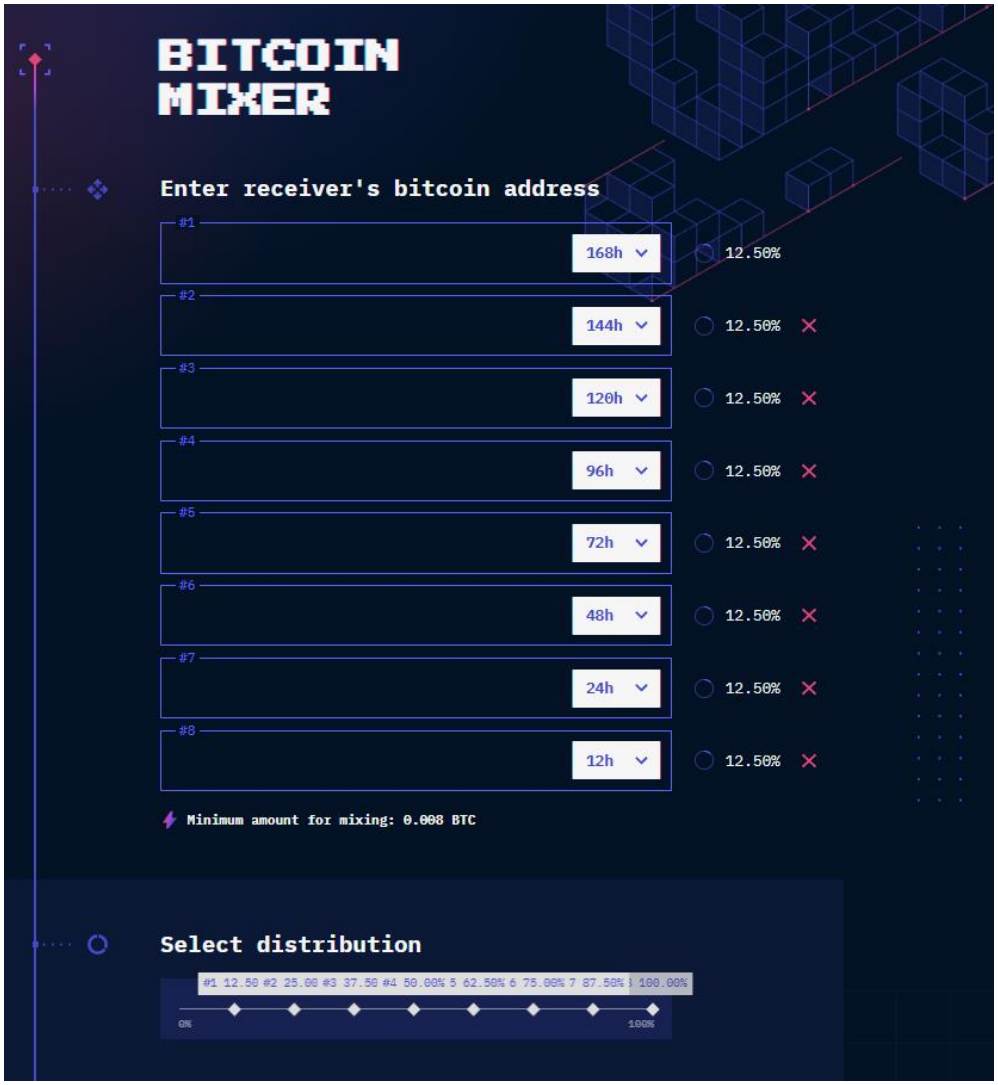
[73] https://home.treasury.gov/news/press-releases/jy0916

Odborné zdroje poukazujú kontinuálne na prepojenia skupiny Lazarus na kryptomixér Sindbad.io.[74]

Nové funkcie, implementované do kryptomixéra Sindbad.io umožňujú rozdeliť transakciu na až 8 adries a na každú adresu stanoviť samostatný čas transakcie v rozsahu 0 až 168 hodín.

Foto funkcionality kyptomixéra Sindbad.io:

Obrázok č.23



Zdroj: https://sinbad.io/en

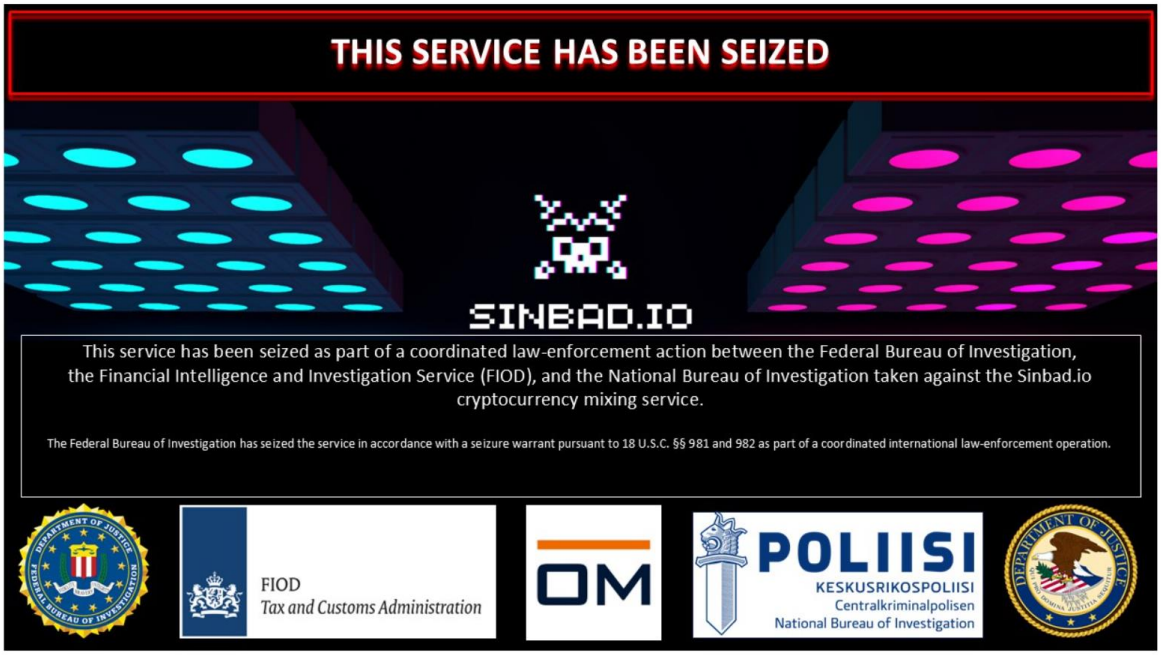
[74] https://crypto.news/stolen-crypto-from-atomic-wallet-traced-to-north-korean-linked-mixer/

OFAC zverejnil 29.11.2023 na svojich webových stránkach https://ofac.treasury.gov/ zoznam nových sankcionovaných subjektov a medzi inými je sankcionovaný aj mixér Sindbad.io so svojím webom www.sinbad.io ale i s adresou dostupnou na Darknete, respektíve prostredníctvom siete TOR a to na nasledovnom odkaze: http://sinbadiovklgdbafpqvwfwjh2tfrisahtxmrskiovt62nirragcnkcad.onion, emailovými adresami a sériou kryptoadries spojených s týmto mixérom. [75]

OFAC v odôvodení uvedenom na svojom webe a v tlačovej správe uvádza dôvody na zavedenie tejto služby na sankčný zoznam nasledovne: „Sinbad je zodpovedný za materiálnu pomoc pri praní miliónov dolárov ukradnutých vo virtuálnej mene a je preferovanou mixovaciou službou pre skupinu Lazarus. Sinbad funguje na bitcoinovom blockchaine a uľahčuje nezákonné transakcie zahmlievaním ich pôvodu, miesta určenia a protistrán. Niektorí odborníci z odvetvia považujú Sinbada za nástupcu mixéra Blender.io, ktorý OFAC sankcionoval za poskytovanie mixážnych služieb skupine Lazarus.[76]

V rovnakom čase kedy boli zavedené sankcie na Sindbad.io sa na jeho webových stránkach objavila nasledujúca správa:

Obrázok č.24



Zdroj: www.sindbad.io

Z hľadiska problematiky AML / CFT sú kryptomixéry vnímané ako vysokorizikové služby. Ich jednoznačným cieľom je zahmliť / sťažiť identifikovať / znemožniť identifikovať pôvod respektíve pôvodnú adresu prostriedkov, cieľ prostriedkov a jednotlivé protistrany transakcie ktorá je realizovaná prostredníctvom mixéru.

[75] https://ofac.treasury.gov/recent-actions/20231129
[76] https://home.treasury.gov/news/press-releases/jy1933

Postoj a jednotlivé kroky voči mixérom zo strany Ministerstva financí USA, kde poukazuje na ich rizikovosť na úrovni národnej bezpečnosti jasne indikuje smer nazerania na kryptomixéry, ktorý by mal byť inšpiratívny pre bezpečnostné zložky na celom svete.

Je dôležité zdôrazniť fakt, že i keď sa na problematiku využívania anonymizačných nástrojov nazerá objektivitou podpory latentnej kriminality, v globálnom geopolitickom podnebí radikalizácie spoločnosti, vzrastu podpory diktátorov a posilňovania pravice, respektíve krajnej pravice tieto anonymizačné nástroje ponúkajú bezprecedentnú a jedinečnú možnosť podpory osôb, komunít, štruktúr, organizácií alebo i štátov.

Príkladom môže byť Ukrajina, ktorá po začatí plnej inváze zo strany Ruskej federácie vo februári 2022, pripravila v spolupráci s odborníkmi a štátnymi organizáciami kryptoadresy pre najpoužívanejšie kryptomeny: BTC, EHT a stablecoin USDT, dostupné na webovej adrese: https://standwithukraine.com.ua/donation/crypto

Za povšimnutie stojí fakt, že Ukrajina príma dary na 3 blokchainových sietiach: BTC na sieti Bitcoin, ETH na sieti Ethereum a stablecoin USDT na sieti Tron.[77]
Prvok diverzifikácie, tak príznačný pre finančné trhy sa uplatňuje úplne jednoznačne aj pri problematike kryptomien.
OSInt informácie dostupné na internetových stránkach informujú, že ekvivalent celkovej sumy vo FIAT mene, vyzbieranej počas rokov 2022 a 2023 bol 225 miliónov USD.[78]

Vitalik Buterin, tvorca ETH, a jedna z najvplyvnejších osôb v rámci kryptokomunity, sám priznal využívanie služby Tornado.Cash pri darovaní prostriedkov pre Ukrajinu.[79]
Jeff Coleman pri Twittrovej diskusi s Vitalikom Buterinom poukázal na „„Aj keď vláda, v ktorej žijete, vás plne podporuje, možno nebudete chcieť, aby (ruská) vláda mala všetky podrobnosti o vašich krokoch“.[80]

Práve problematika súkromia a snaha štátnych orgánov o kontrolu je jedným z najvýraznejších bodov stretu medzi kryptokomunitou a štátnymi orgánmi.

[77] https://standwithukraine.com.ua/donation/crypto
[78] https://www.coindesk.com/consensus-magazine/2023/07/27/ukraine-has-raised-225m-in-crypto-to-fight-russian-invasion-but-donations-have-stagnated-over-the-last-year-crystal/
[79] https://forkast.news/vitalik-buterin-says-used-tornado-cash-donate-ukraine/
[80] https://forkast.news/vitalik-buterin-says-used-tornado-cash-donate-ukraine/

30. Návrh opatrení

FSJ v spolupráci s ďalšími inštitúciami a orgánmi veľmi rozsiahlo a do veľkej hĺbky preskúmala slovenský trh s poskytovateľmi služieb kryptopeňaženiek / zmenárne virtuálnych mien. Na základe zistení uvedených v tejto analýze FSJ organizovala sériu prednášok a školení určených pre partnerské inštitúcie a organizácie. Tieto podujatia poskytli platformu pre prezentáciu zistení, relevantných informácií a kvantifikovaných rizík spojených s domácim trhom. Okrem toho, tieto školenia poslúžili ako príležitosť na diskusiu o najlepších postupoch a strategických krokoch potrebných na zvládanie identifikovaných rizík a na zlepšenie prepojení medzi rôznymi účastníkmi trhu, orgánmi verejnej moci a orgánmi dohľadu. Celkovým cieľom týchto iniciatív bolo zvýšiť povedomie a zlepšiť pripravenosť na potenciálne hrozby v sektore kryptoaktív.

Na základe svojich zistení FSJ navrhuje sériu opatrení zameraných na zmiernenie identifikovaných rizík a zraniteľností na slovenskom trhu s virtuálnymi aktívami. Tieto opatrenia majú za cieľ posilniť ochranu trhu a zlepšiť regulačné prostredie s cieľom efektívnejšie čeliť potenciálnym hrozbám a výzvam.
Návrh opatrení:

1) Stanoviť regulačný orgán – ustanovenie respektíve určenie inštitúcie, ktorá bude celý sektor regulovať, dozorovať a usmerňovať a bude u nej prebiehať aj samotný licenčný proces.

2) Impletovať licenčný proces – nastavenie komplexného licenčného procesu, počas ktorého by bol každý žiadateľ / subjekt preskúmaný z hľadiska pôvodu kapitálu, zámeru využitia licencie, technického a technologického vybavenia, plánovanej geografickej pôsobnosti a personálneho obsadenia kľúčových firemných pozícií

3) Zaviesť do praxe technologické riešenia na sledovanie a analýzu - zavedenie sofistikovanejších softvérových riešení, ktoré by umožnili lepšiu analýzu a detekciu nelegálnych aktivít spojených s virtuálnymi aktívami

4) Zvýšiť medzinárodnú spoluprácu – vzhľadom na natívnu globálnosť kryptomien a kryptoaktív je veľmi dôležité rozšíriť a prehĺbiť medzinárodnú spoluprácu v týchto segmentoch

5) Pokračovať v edukačnej činnosti pre VASPov a orgány verejnej moci – aj naďalej venovať úsilie prehĺbeniu povedomia o sektore kryptoaktív a rizikám ním prislucháajúcich medzi orgánymi verejnej moci, ako aj širokou verejnosťou.

31. Záver

Celý sektor virtuálnych aktív a s ním spojené inovácie a služby k ním prislúchajúce, respektíve vďaka nim existujúce je pre svet a spoločnosť úplne novým a stále sa formujúcim. Ako bolo už niekoľkokrát v tejto sektorovej analýze zdôraznené, musíme zabudnúť na posudzovanie z hľadiska lokálnosti/globálnosti, ale pozerať celkovo na trh ako na primárne globálny, s okamžitými platbami, technologickými riešeniami dostupnými pre všetkých ktorí v danom momente na blockchaine pôsobia.

Jeho komplexnosť a prepojenosť na svet informačných technológií a internetu ho predurčuje na dynamický rozvoj a tendenciu na rýchle implementácie inovácií. Vďaka tejto rýchlosti a flexibilite je sektor kryptomien aj s jeho podsegmentami pre všetky orgány štátneho dozoru, pre OČTK a v neposlednom rade pre bezpečnostné služby jednotlivých štátov, veľmi náročný na udržanie tempa s jeho dynamickými zmenami.

Práve nesprávne respektíve nejednoznačné nastavenie legislatívy na Slovensku hodnotíme ako najvýznamnejšie riziko. Absencia riadneho licenčného procesu viedla k prebujnenému zakladaniu VASPov na Slovensku, niektoré pravdepodobne boli založené ako účelové subjekty v medzinárodných optimalizačných schémach.

Vysokým rizikom je aj fakt, že okrem jednoduchého zakladania VASPov chýba akýkoľvek proces kontroly osôb spojených s VASPom, či už ako konatelia, koneční užívatelia výhod alebo majitelia spoločnosti.

Tieto aspekty sú najvýraznejším lokálnym rizikom priamo sa týkajúcim Slovenskej republiky ako domicilom VASPov a aj ako ich regulátorom.

Globálne riziká vyplývajú jednoznačne zo samotnej globálnej povahy kryptomien a ich služieb a možností. Geografické hranice takmer vôbec nehrajú rolu a práve kvôli nim sa hrozby, ktorým čelí užívateľ/investor/člen kryptokomunity takmer nijako nelíšia pre užívateľa zo Slovenska, alebo z Grécka, alebo Austrálie.

Problémom týchto hrozieb je na jednej strane ich latentný charakter a na druhej strane aj ich veľmi náročná štruktúra a veľakrát cezhraničný presah. To, čo na jednej strane je natívnou vlastnosťou krypta - globálnosť a nerešpektovanie geografických hraníc, je na druhej strane veľkým problémom pre OČTK na celom svete.

V neposlednom rade je to fakt, že problém prevencie proti podvodom, SCAMom a scamovým štruktúram vo svete i na Slovensku ešte nie je správne poňatý zo strany regulátorov ani zo strany jednotlivých OČTK.

Európska únia očakáva reguláciu MiCA a jej spustenie už v najbližšej dobe a Slovenská republika bude jednoznačne jednou z viacerých krajín, ktorej prijatie tohto nariadenie pomôže s konsolidáciou na trhu.

32. Prílohy

Zoznam použitých skratiek:

A.I.	-	Artificial Intelligence – umelá inteligencia
AML/CFT	-	Anti-Money Laundering / Countering the Financing of Terrorism
APT	-	Advanced Persistent Threats – skupiny naviazané na zahr. rozviedky
CEX	-	Centralized Exchange – centralizovaná burza
KYC	-	„Know your customer“ - proces identifikácie zákazníka zo strany povinnej osoby, pojem zahrňujúci Základnú starostlivosť podľa §10, §12 zákona 297/2008 Z.z.
DAO	-	Decentralizovaná autonómna organizácia
DeFi	-	Decentralizované financie
DEX	-	Decentralized Exchange - decentralizovaná burza
EBA	-	Európsky orgán pre bankovníctvo
FATF	-	Financial Action Task Force – medzinárodná organizácia
TradFi	-	Tradičné financie
VA	-	Virtual Assets - Virtuálne aktívum
VASP	-	Virtual Assets Service Providers - poskytovateľ služieb virt. aktív
MiCA	-	Markets in Crypto Assets – regulácia EU
OČTK	-	Orgány činné v trestnom konaní
OSInt	-	Open Source Intelligence – verejne dostupné zdroje
FSJ	-	Finančná spravodajská jednotka
FIU	-	Financial Intelligence Unit – anglická skratka
NBS	-	Národná Banka Slovenska
AML	-	Anti Money Laundering – boj proti praniu špinavých peňazí
OFAC	-	Office of Foreign Assets Control – inštitúcia USA
TOR	-	The Onion Router
ICO	-	Initial Coin Offering – prvotný úpis tokenov
FIAT mena	-	zákonné platidlo
P2P	-	peer-to-peer respektíve: rovný s rovným