

# VA /VASP Sectoral Analysis

## Table of Contents

Table of Contents .....	2
Introduction .....	4
1. Slovak Republic – basic information .....	6
2. Crypto adoption.....	9
3. Development of the virtual currency sector in the Slovak Republic until 31 December 2022 ....	13
4. Current licensing process in Slovakia .....	16
5. Situation in Slovakia .....	20
6. Results of a survey of the sector of virtual currency service providers in the Slovak Republic carried out for the period until 30 June 2022 in the form of a questionnaire .....	22
6.1. Geographic criteria .....	25
6.2. Virtual currency services in the Slovak Republic .....	28
6.3. Anonymous virtual currencies and products aimed at anonymising and making it more difficult to identify the origin of virtual currencies .....	30
6.4. Payment methods used to purchase or trade virtual currency .....	32
7. The link between virtual currency and crime .....	34
7.1. Politically exposed persons and crime in general government in the context of virtual currency.....	34
7.2. Crimes most commonly associated with the abuse of virtual currency.....	36
7.3. Virtual currency theft .....	37
8. Application of preventive measures and a risk-based approach by entities operating a virtual currency exchange or virtual currency wallet in the Slovak Republic .....	39
9. Cryptocurrency ATMs in Slovakia .....	42
10. Non-cooperating entities .....	45
11. Conclusion of the questionnaire-analytical part of the VA/VASP sector .....	48
12. The Slovak Republic and its approach to the issue of seizure of proceeds of crime.....	50
12.1. Definition of virtual currency under the Criminal Code .....	50
12.2. Legal regulation of the virtual currency seizure process .....	51
13. National Bank of Slovakia.....	53
14. Analytical part of the sectoral analysis.....	56
15. Taxation of proceeds from crypto-assets in Slovakia.....	57
16. Foreign FinTech companies and their overlap on the Slovak market of VASPs .....	59
17. Definition of criminality.....	62
18. Crypto community.....	63
19. P2P in the crypto community .....	64
20. Communication tools in the crypto era .....	66
21. ATS / Bots.....	68
22. A.I.....	69

22.1.	LLM.....	69
22.2.	A.I. and Europol .....	70
22.3.	Deepfake.....	71
22.4.	Control of smart contracts through A.I.....	71
23.	CEX vs DEX vs DEX Aggregator .....	74
23.1.	CEX.....	74
23.1.	Non-KYC exchanges.....	75
23.2.	DEX.....	76
23.3.	DEX Aggregator.....	77
23.4.	DEX & A.I. ....	78
24.	TradFi and DeFi convergence .....	79
25.	DAO .....	82
25.1.	DAOs in the world.....	82
25.2.	Linking the DAO and traditional legal forms of business .....	83
25.3.	DAO & Governance token .....	83
26.	ICO .....	86
26.1.	NBS and ICO.....	87
27.	SCAM schemes .....	90
28.	Stablecoins.....	96
28.1.	Collateralised.....	96
28.2.	Algorithmic .....	98
29.	Mixer .....	101
30.	Proposal for measures .....	107
	Conclusion.....	108
	Annexes.....	110

## Introduction

The Financial Intelligence Unit of the Presidium of the Police Force fulfils the tasks of a central national unit in the area of preventing and detecting money laundering and terrorist financing. As part of this work, it also produces the National Risk Assessment, of which the VA/VASP Sectoral Analysis is an integral part.

This sectoral analysis builds on the sectoral analysis produced by the Financial Intelligence Unit entitled “Sectoral assessment of the risks of money laundering, terrorist financing and proliferation in relation to virtual assets and virtual asset service providers”. It aims to identify and monitor potential weaknesses associated with this sector, primarily focusing on uncovering risks associated with AML/CFT issues.

For the first time ever, the methodology provided by the European Commission to the individual states has been used to develop a VA/VASP sectoral analysis. The methodology is designed in such a way that it assumes the existence of a central institution for a separate licensing process, which also fulfils the role of a supervisory authority. Last but not least, the methodology is based primarily on the collection of data or reports from relevant entities. However, the Slovak Republic has not yet established any such central entity, as the Slovak legislative framework does not require a separate licensing process for the provision of services related to virtual assets through VASPs. Applicants for the provision of services related to virtual assets through VASPs are only obliged to register the necessary trades or activities (more on this issue in a separate chapter of the sectoral analysis) with the Trade Licensing Office. However, it is essential to note that the Financial Intelligence Unit is an AML/CFT supervisory authority and, therefore, each VASP must comply with the obligations under the applicable laundering law, which include, among others, the reporting obligation (reporting of unusual transactions).

One of the biggest challenges in compiling the sectoral analysis was to correctly identify the sources of information among the various state authorities. A hybrid use of the provided methodology was adopted - a comprehensive questionnaire was developed in accordance with the methodology and subsequently distributed to all VASPs registered in Slovakia. In the next round, the National AML/CFT Expert Group (NES LP), which brings together a wide range of state institutions such as ministries, authorities, law enforcement authorities and intelligence services, was involved in the process of developing this sectoral analysis through the Interministerial Expert Coordination Body (MEKO). It is the NES LP and its members that have become another source of data and information which, together with questionnaire data, have become the basis for the sectoral analysis.

In line with the methodology, the monitoring of OSInt was also expanded by the Financial Intelligence Unit, with an emphasis on the VA segment. It is the native property of the blockchain - its public nature (anonymous coins, so-called “dark coins”, are a separate case, but the sectoral analysis deals with them in a separate chapter) and the OSInt sources tied to it

that are the third and at the same time important and relevant source of data for the sectoral analysis.

To augment the data, the Financial Intelligence Unit has also made use of monitoring various components of the crypto world, such as discussion forums and discussion groups (often closed), testing of automated trading systems (ATS), P2P communities, and various other possibilities that exist and may harbour potential threats related to AML/CFT issues.

It is important to highlight a native characteristic of crypto - globality. As will be highlighted several more times in the text of this sectoral analysis, the globality and extraordinary flexibility of the crypto community are clear elements pointing to the extraordinary dynamism of this new industry.

In its first part, the sectoral analysis monitors in great detail only a small slice of this global industry - the entities that operate as VASPs in Slovakia. The second part of the sectoral analysis focuses on global trends, new opportunities and technologies and specifics of the crypto market, which due to their global nature are directly reflected on the Slovak market.

Each chapter addresses a separate issue not only from a technical, regulatory, legal or technological perspective, but always attempts to quantify the risks associated with the AML/CFT issue, along with adequate recommendations to mitigate the identified risks.

## 1. Slovak Republic – basic information

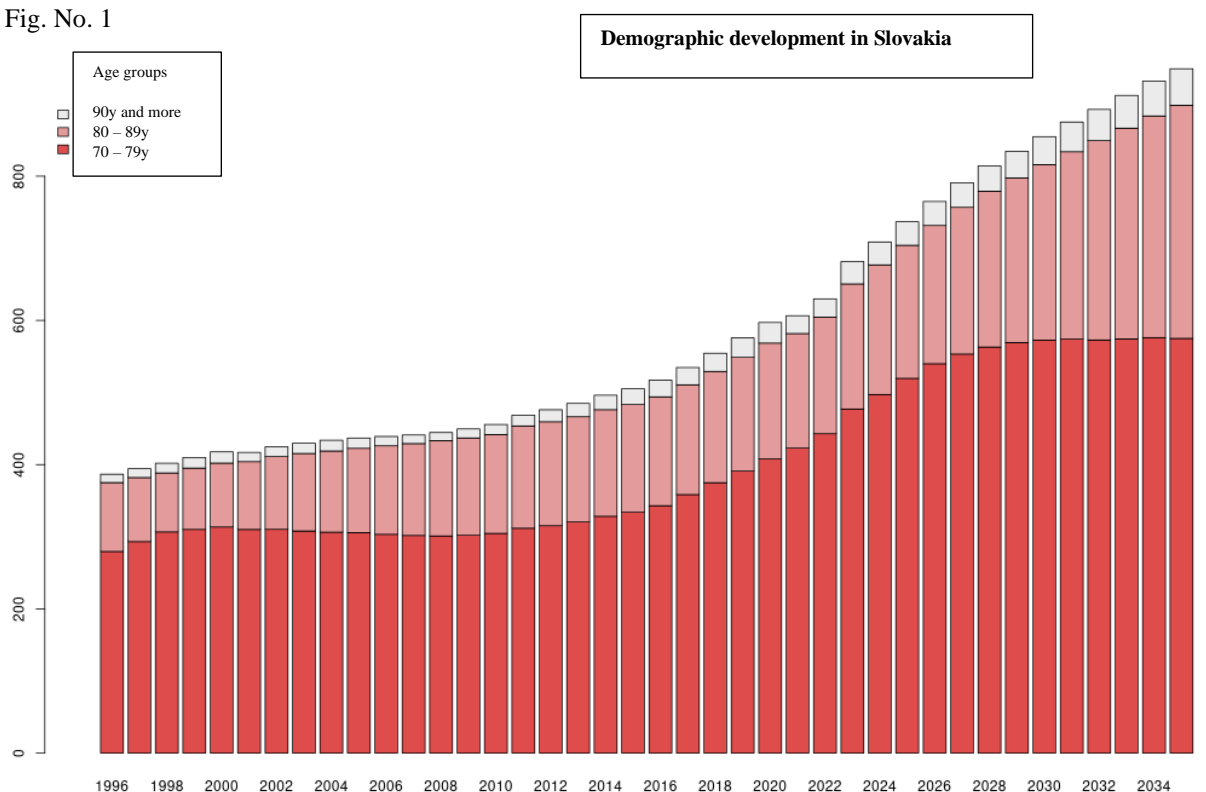
The Slovak Republic was established as the legal successor after the dissolution of the Czech and Slovak Federative Republic on 1 January 1993. With an area of 49,036 km<sup>2</sup> and a geographical location in Central Europe, it is crucial for the state to engage in international structures and alliances. This inclusion is essential at several levels: locally, such as the Visegrad Group (V4), regionally - the European Union (EU) and the North Atlantic Treaty Organization (NATO), and globally, represented by the United Nations (UN).

- Since 19 January 1993 the Slovak Republic has been a member of the United Nations,
- since 29 March 2004 it has been a member of the North Atlantic Treaty Organization (NATO),
- since 1 May 2004 it has been a Member State of the EU,
- since 21 December 2007 it has been part of the Schengen area,
- since 1 January 2009 it has been a member of the European currency union, known as the Eurozone, where it became the sixteenth member country.

The population of the Slovak Republic is 5,426,857 (as of 31 March 2023).

The demographic structure of the population is as follows:

Fig. No. 1

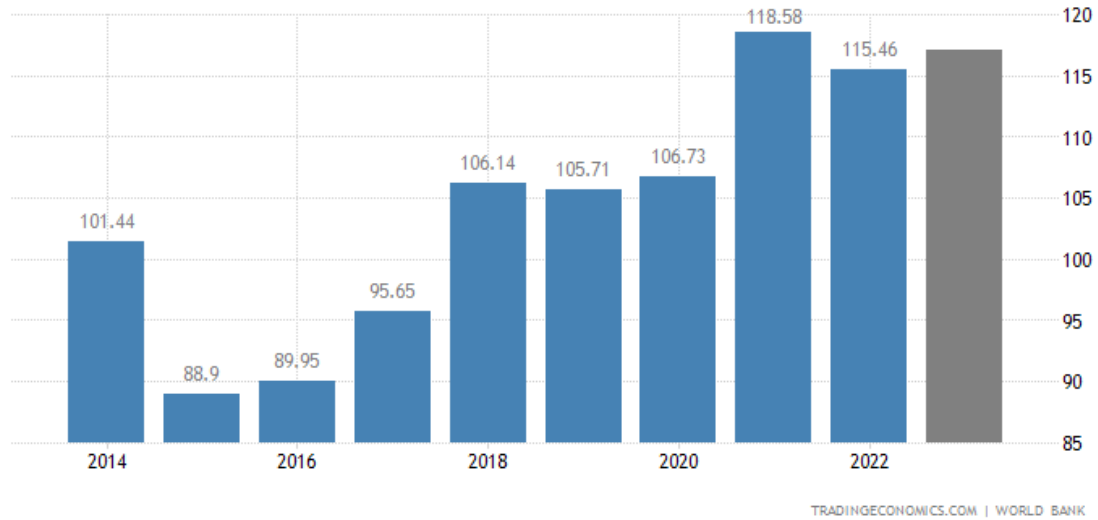


Source: <https://www.iz.sk/30-grafov-o-zdravotnictve/demograficky-vyvoj-na-slovensku>

The Slovak Republic ranks 61st in the international comparison of gross domestic product (GDP).

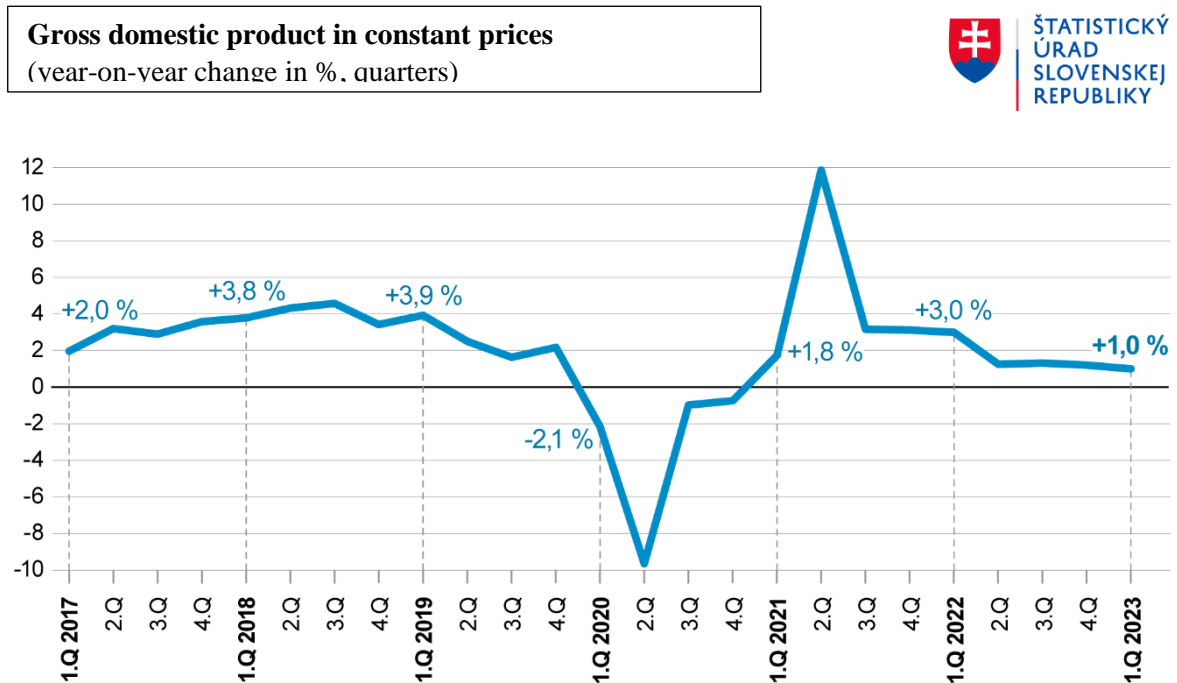
GDP of the Slovak Republic in absolute terms (in billions of USD):

Fig. No. 2



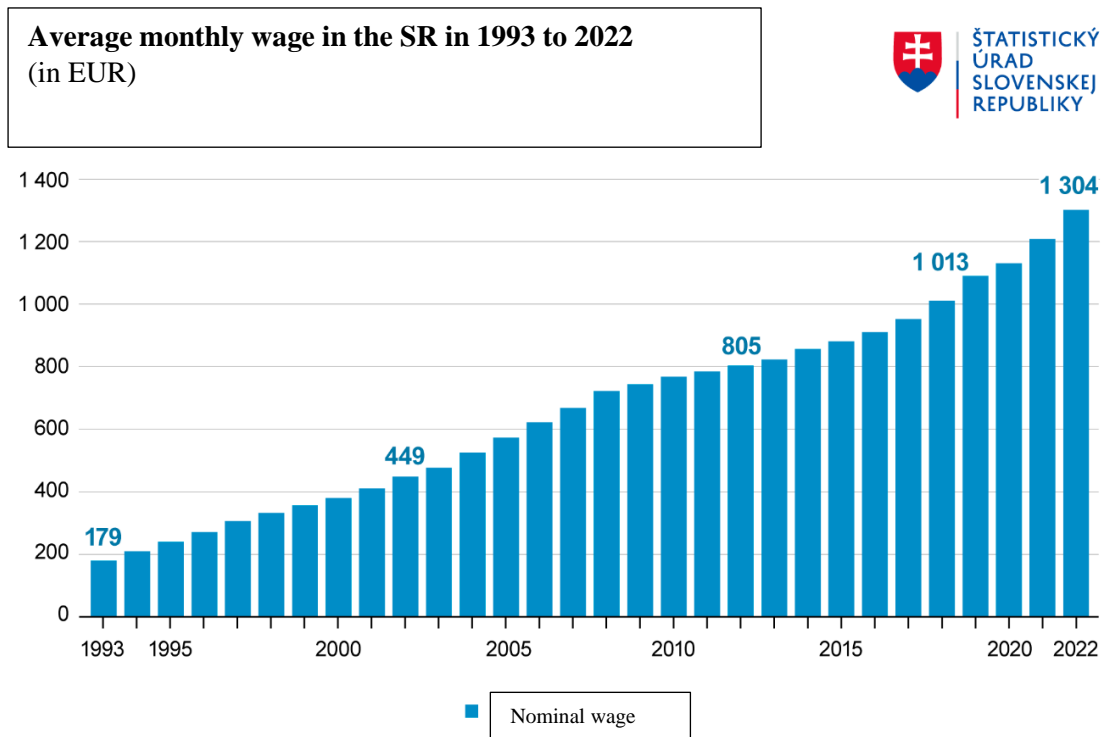
Source: <https://tradingeconomics.com/slovakia/gdp>

Fig. No. 3



Source: Statistical Office of the Slovak Republic

Fig. No. 4



Source: Statistical Office of the Slovak Republic

In addition to the economic indicators pointing to the stability and growth of the economy, it is also very important in the context of the VA / VASP sector to perceive the improving availability of the Internet and the growth in the number of Internet users in Slovakia.

Number of Internet users:

Fig. No. 5



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



## 2. Crypto adoption

Over the past decade, the virtual asset (VA) sector has evolved from a marginal market that from 2009 (the founding of Bitcoin) to 2011 (its expansion among users, mainly from the IT community), was characterised by only limited interest, into a major economic sector with a value in the billions or trillions of dollars. Today, this sector is penetrating into many other areas, including banking, finance and information technology, thus becoming an integral part of the global economy.

The following chart shows the total market capitalization of VA - crypto-assets since 2013:

Fig. No. 6



Source: <https://coinmarketcap.com/charts/>, date: 04 April 2023

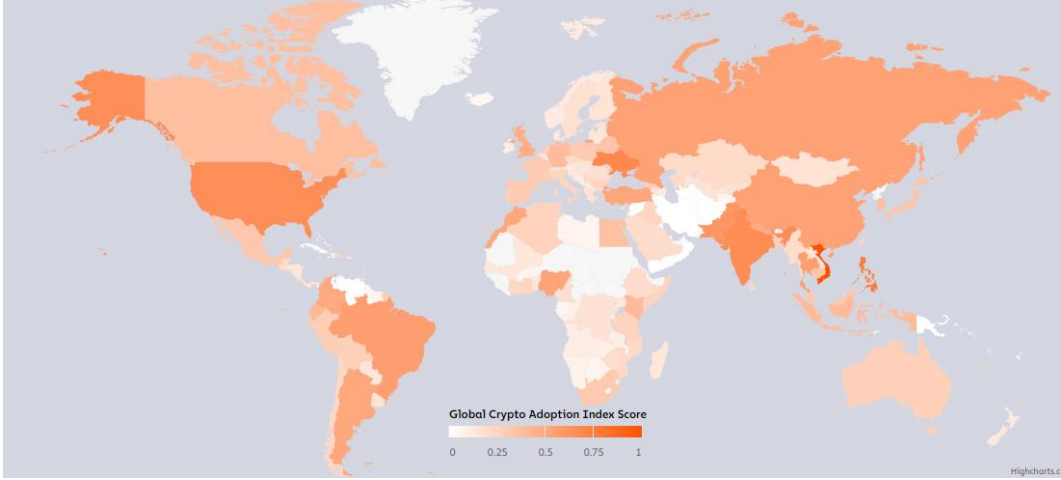
The two most significant periods of market growth, known as bull runs, when market capitalisation increased as a result of inflows of new investors and capital, occurred in 2018 and 2021.

Chainalysis has published Chainalysis' 2022 Global Crypto Adoption Index on its website, which tracks cryptocurrency adoption by country. Out of the 146 countries evaluated, the Slovak Republic ranked 80th with an overall cryptocurrency adoption index score of 0.168. The highest cryptocurrency adoption rate was recorded by Vietnam, which ranked 1st with an index score of 1.000.

The map below clearly shows that countries in our neighbourhood, such as Ukraine (3rd place), Poland (33rd place) and the Czech Republic (62nd place), have higher rates of crypto adoption among citizens and institutions, and conversely Hungary (91st place) and Austria (107th place) have lower adoption rates.

The following figure describes global crypto adoption in 2022:

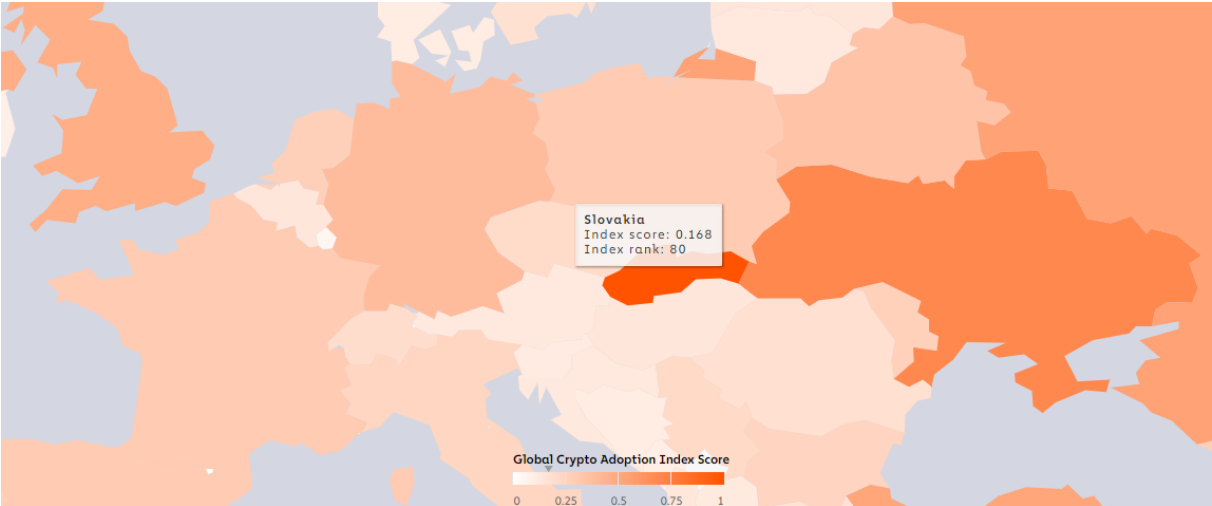
Fig. No. 7



Source: <https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/>

Comparison of the neighbouring countries with Slovakia:

Fig. No. 8



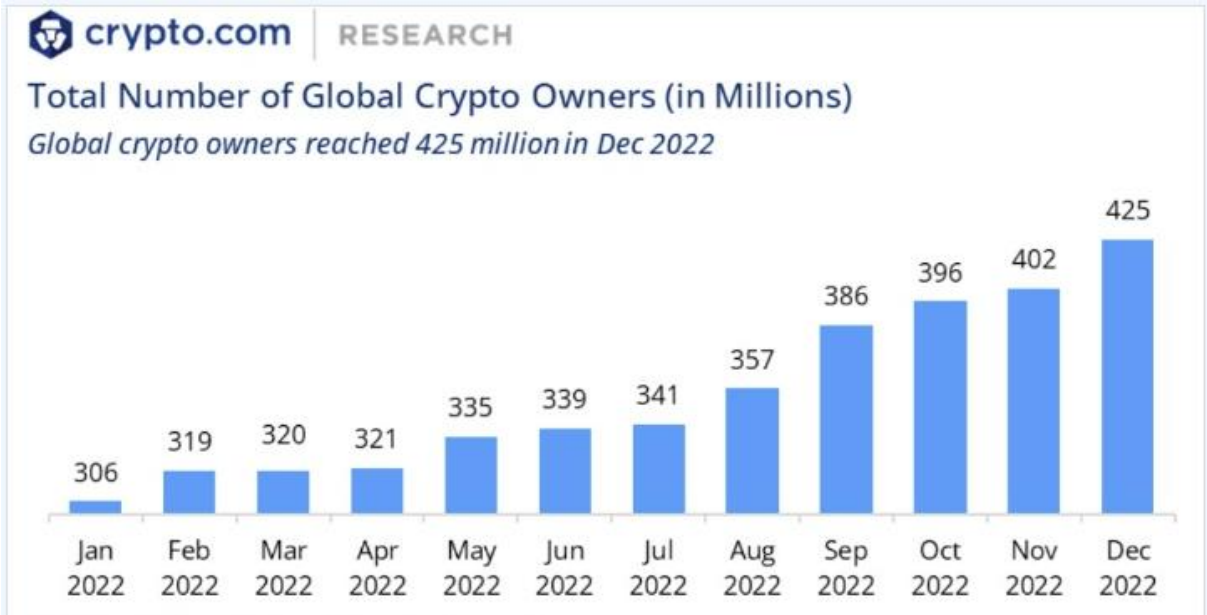
Source: <https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/>

The map clearly shows that countries in our neighbourhood such as Ukraine (ranked 3), Poland (ranked 33) and the Czech Republic (ranked 62) have higher rates of crypto adoption among citizens and institutions, and conversely Hungary (ranked 91) and Austria (ranked 107) have lower rates of adoption.

Globally, cryptocurrency adoption has been on a continuous upward trend, with the total number of users increasing to a total of 425 million from 01/2022 to 12/2022, according to a Crypto.com survey.

The following figure describes the trend of the increase in the number of crypto-asset holders for 2022:

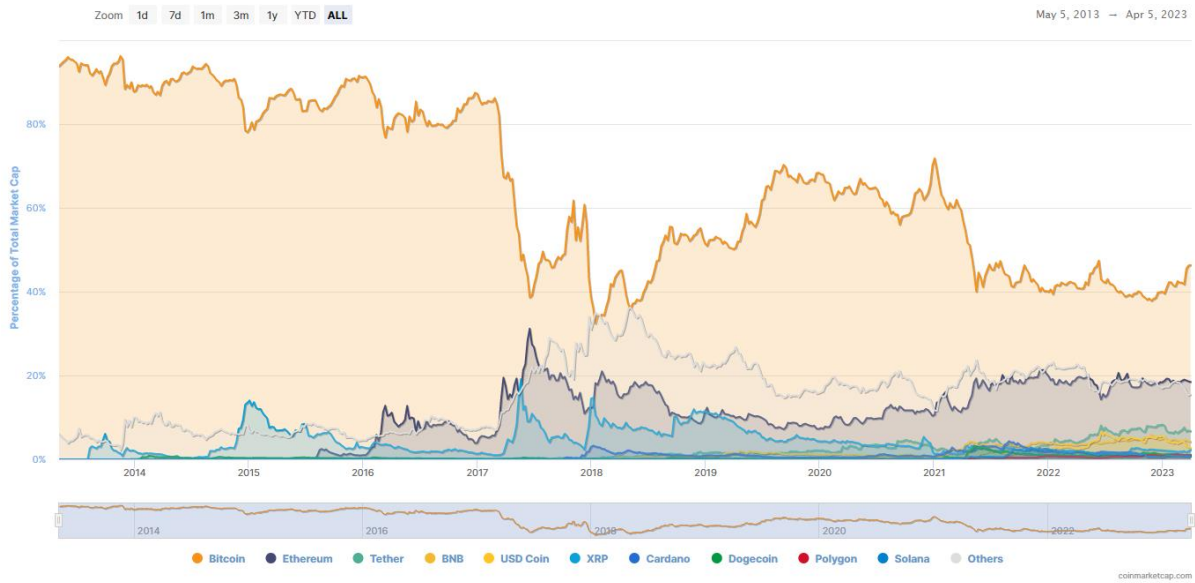
Fig. No. 9



Source: Crypto.com

In the context of the growth of cryptocurrency adoption, it is also important to look at the structure of the so-called “Bitcoin Dominance Chart”, which indicates the percentage of Bitcoin’s share of the total market capitalization of the entire crypto. The following chart graphically illustrates this:

Fig. No. 10



Source: <https://coinmarketcap.com/charts/#dominance-percentage>, date: 05 April 2023

As of 5 April 2023, the Coinmarketcap.com website, as a key point accumulating data on the market capitalizations of individual cryptocurrencies and tokens, reported data on 23,199<sup>1</sup> cryptocurrencies and tokens. This enormous number of cryptocurrencies and tokens is almost impossible to comprehensively track and evaluate in real time.

The amount of potential threats associated with AML/CFT risk is growing exponentially relative to conventional cryptocurrencies and tokens for cryptocurrencies called privacy coins, also called anonymous currencies.

A separate chapter of this sectoral analysis will be devoted to anonymous cryptocurrencies. However, it is important to point out the restrictive practices of some countries towards these anonymous currencies. An example is South Korea, which has banned the trading of the anonymous currencies Monero and Zcash because of the major threat associated with AML/CFT<sup>2</sup>. Dubai also proceeded to ban anonymous cryptocurrencies in 2023 following the adoption of new regulations. Dubai defines anonymous cryptocurrencies as “a type of Virtual Asset which prevents the tracing of transactions or record of ownership through distributed public ledgers and for which the [Virtual Asset Service Provider (VASP)] has no mitigating technologies or mechanisms to allow traceability or identification of ownership.”<sup>3</sup>

---

<sup>1</sup> <https://coinmarketcap.com/charts/>

<sup>2</sup> <https://www.cpomagazine.com/data-privacy/south-koreas-new-crypto-aml-law-bans-trading-of-privacy-coins-monero-zcash/>.

<sup>3</sup> <https://www.coindesk.com/policy/2023/02/08/dubai-prohibits-privacy-coins-under-new-crypto-rules/>.

### 3. Development of the virtual currency sector in the Slovak Republic until 31 December 2022

Virtual currencies (e.g. Bitcoin, Litecoin, Ethereum and others) are not recognised as official domestic or foreign currencies in the Slovak Republic, do not constitute electronic money within the meaning of the Payment Services Act<sup>4</sup> and do not have a physical counterpart in the form of legal tender. Despite this, it is possible to observe a permanent dynamic development in this area in the Slovak Republic, both in the technological direction and in the area of the ever-increasing number of entities operating on the market of virtual currencies and services, the supply of which directly correlates with the correspondingly increasing demand for virtual currencies among the general population. There are currently no specific requirements (in terms of any regulatory process) for such trading and until recently a general trade licence was sufficient to do business in the form of an unregulated trade, and such entities were not subject to AML supervision/control.

Definition:

Methodological Guideline of the Ministry of Finance of the Slovak Republic No. MF/10386/2018-721 on the procedure of taxation of virtual currencies (hereinafter referred to as the “Methodological Guideline”) also provides a definition of virtual currency, which is understood as a digital medium of value that is neither issued nor guaranteed by a central bank or a public authority, nor is it necessarily tied to legal tender, does not have the legal status of currency or money, but is accepted by certain natural or legal persons as a means of payment and which can be transferred, stored or traded electronically.

The amendment to Act No. 297/2008 Coll. on protection against money laundering and terrorist financing and on the amendment to certain acts as amended (hereinafter referred to as the “AML Act”), effective from 1 November 2020, has extended the exhaustively defined circle of obliged persons to legal and natural persons providing virtual currency wallet services and virtual currency exchange services (hereinafter referred to as “Virtual Asset Service Providers”) - VASPs. The amendment was in this part the implementation of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing into the legal order of the Slovak Republic.

It is precisely the constant and rapid technological development on the one hand, combined with the length of legislative processes at European and national level on the other hand, that represents one of the greatest limits in setting the optimal legal framework for regulation and control in this area.

---

<sup>4</sup> Act No. 492/2009 Coll. on payment services and on the amendment to certain acts as amended

The foundations of the legal framework for virtual currencies have gradually started to be incorporated into the Slovak legal order since 2018.

On 1 October 2018, the Insurance Tax Act<sup>5</sup> and the Accounting Act<sup>6</sup> came into effect to the extent of defining terms related to virtual currencies and their taxation.

These amendments were preceded by the Methodological Guideline of the Ministry of Finance of the Slovak Republic No. MF/10386/2018-721 on the procedure of taxation of virtual currencies (hereinafter referred to as the “Methodological Guideline”), which ensures a uniform interpretation in the taxation of income derived from the sale of virtual currencies under the Income Tax Act<sup>7</sup>. According to this Methodological Guideline, income derived from the sale of virtual currencies is also considered taxable income under the Income Tax Act.

A detailed elaboration of taxation and identified trends in this area will be presented in detail in later sections of this sectoral analysis. On 1 November 2020, an amendment to the AML Act came into effect, which included among the obliged persons in the AML area entities providing services related to virtual currencies, namely virtual currency wallet service providers and virtual currency exchange service providers professionally engaged in exchange services between virtual currency and fiat currencies<sup>8</sup>.

At the same time, with effect from 1 November 2020, the Trade Licensing Act was amended by the amendment to the AML Act<sup>9</sup>, whereby virtual currency exchange service providers and virtual currency wallet service providers were classified as regulated trades.

It is the amendment to the AML Act of 1 November 2020 that has become crucial in guiding and monitoring the further development of the virtual currency sector in the Slovak Republic. All entities that until that time were engaged in the provision of virtual currency exchange and/or virtual currency wallet services were obliged to register a trade with the relevant Trade Licensing Office under point 82a (provision of virtual currency exchange services) and/or point 82b (provision of virtual currency wallet services) of Annex No 2 to the Trade Licensing Act.

From 1 November 2020 to 28 February 2021, there was a transitional period during which entities providing virtual currency exchange services and/or virtual currency wallet services were obliged to register these trades, as the trade licence issued for a trade which, by its content, fulfilled the characteristics of the provision of virtual currency exchange services or the provision of virtual currency wallet services, issued until 31 October 2020, on 28 February 2021 expired.

---

<sup>5</sup> Act No. 213/2018 Coll. on insurance tax, amending, inter alia, Act No. 595/2003 Coll. on income tax as amended

<sup>6</sup> Act No. 431/2002 Coll. on accounting as amended

<sup>7</sup> Act No. 595/2003 Coll. on income tax as amended

<sup>8</sup> i.e. coins and banknotes that are designated as legal tender and a country’s electronic money accepted as a medium of exchange in the issuing country.

<sup>9</sup> Act No. 455/1991 Coll. on trade licensing as amended

A transitional period has also been introduced for the changes adopted by the AML Act. In the period from 1 November 2020 to 31 January 2021 the providers of virtual currency exchange services and virtual currency wallet services were obliged to draw up a programme of their own activities pursuant to Article 20 of the AML Act. In the period until 31 May 2021, virtual currency exchange service providers and virtual currency wallet service providers were obliged to additionally carry out due diligence according to the provisions of the AML Act for all existing customers.

After the end of the transitional period in October 2021, the Financial Intelligence Unit organised an introductory (online) meeting for obliged persons. The training was conducted online via WEBEX and was aimed at highlighting the obligations of providers of virtual currency exchange or virtual currency wallet services and the application of the provisions of the Act in the process of prevention and detection of money laundering and terrorist financing in the activities of an obliged person, which are imposed on them as obliged persons under the AML Act.

Already when the invitations to the training were delivered, a great diversity of entities that registered the activities in question was observed, with a relatively high percentage of those that do not actually carry out the activity. A secondary problem observed during the organisation of the training was the poorly set up communication channel between the Financial Intelligence Unit as AML supervisor and the providers of virtual currency exchange or virtual currency wallet services as obliged persons under the AML Act. The delivery of invitations to the training via the electronic delivery system "slovensko.sk" to electronic mailboxes proved to be ineffective, as a larger number of entities did not receive an invitation about the planned training. The situation was promptly addressed by the Financial Intelligence Unit staff and communicated on an ad hoc basis. Subsequently, 24 persons (out of 92 entities that were sent invitations via Fabasoft) attended the training, while only 19 persons identified themselves.

## 4. Current licensing process in Slovakia

I) The general conditions for the operation of a regulated trade are:

- attainment of the age of 18 years,
- legal capacity,
- integrity (proved by an extract from the Criminal Record).

II) The condition for operating a trade is fulfilment of the condition of professional competence, as follows:

- proof of completion of general secondary education or vocational secondary education.

Registered entities which carry out the activities referred to in Article 5(1)(o) and (p) of the AML Act, i.e. virtual currency wallet service providers and virtual currency exchange service providers, become obliged to third parties and must comply with all the obligations laid down in the AML Act. However, there is no specialised legislation in Slovakia in the segment in question. For comparison in other financial segments these are, for example, Act No. 483/2011 Coll. on banks, specifically Article 7 (banking permits), Act No. 492/2009 Coll. on payment services, specifically Articles 63, 64, 79a, Act No. 566/2001 Coll. on securities and investment services, specifically Articles 54, 55, 70 (permits, conditions for granting permits), Act No. 202/1995 Coll., Foreign Exchange Act, specifically Article 6 (foreign exchange licence), Act No. 171/2005 Coll. on gambling, specifically Article 16 (conditions of the licence).

The AML Act sets out the obligations of an entity conducting business in the VA/VASP segment and also determines its duties. In terms of money laundering prevention, a logical sequence is chosen, starting with the determination of performance of customer due diligence.

Basic customer due diligence must always be carried out to the full extent of Article 10(1) of the AML Act. The AML Act itself, taking into account the teleological interpretation of the provisions of Article 10 of the AML Act, does not allow the exercise of basic customer due diligence to be postponed until the funds are withdrawn from the customer's account. The obligation to exercise basic customer due diligence at the inception of the business relationship applies irrespective of the size of the transaction.

Pursuant to Article 10(1) of the AML Act, basic customer due diligence applied by the obliged person shall include

- a) identification of the customer and verification of the customer's identification,
- b) identification of the beneficial owner and taking reasonable steps to verify the information relating to the identification of the beneficial owner, including steps to establish the ownership structure and management structure of the customer which is a legal person or pool of assets; the obliged person shall not rely solely on data obtained



from the Register of Legal Entities, Entrepreneurs and Public Authorities for the identification of the beneficial owner if, on the basis of a risk assessment pursuant to Article 20a, there is a higher risk of money laundering or terrorist financing and it is obliged to verify the information relating to the identification of the beneficial owner from an additional credible source,

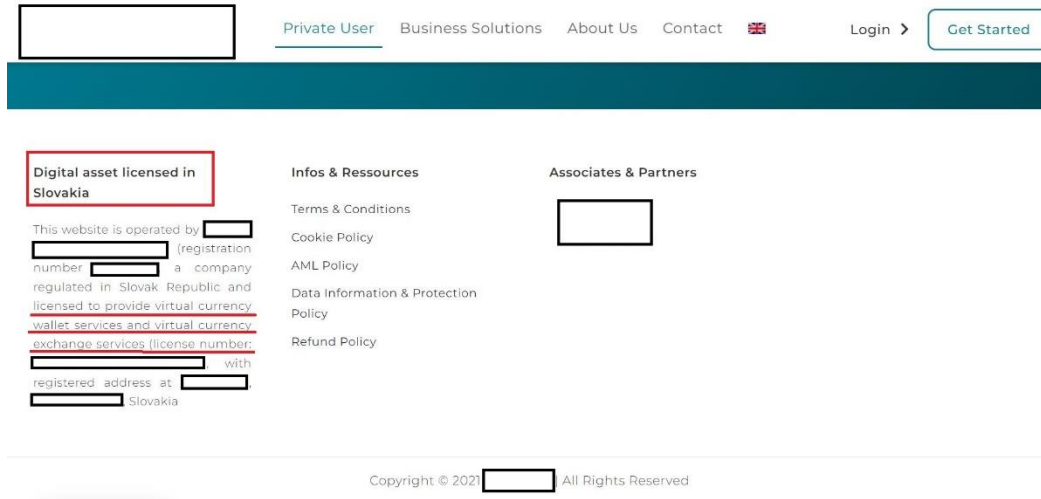
- c) obtaining and evaluating information about the purpose and intended nature of the transaction or business relationship and information about the nature of the customer's business,
- d) determining whether the customer or the beneficial owner of the customer is a politically exposed person or a sanctioned person,
- e) depending on the risk of money laundering or terrorist financing, the determination of the origin of funds or property used in the transaction or business relationship,
- f) the ascertainment whether the customer acts in their own name,
- g) conducting ongoing monitoring of the business relationship including the review of particular transactions carried out throughout the duration of the business relationship in order to find out whether the transactions being carried out are consistent with obliged person's knowledge of the customer, the customer's business profile, an overview of the potential risks associated with the customer and the source of funds and assets used in the business relationship or transaction, and the assurance of updating of the documents, data or information on the customer available to the obliged person.

The Financial Intelligence Unit carries out ongoing inspections of VASPs, but due to their complexity and staffing capacity, the number of entities inspected is only in the order of units out of the total number of VASPs. On the basis of three inspections carried out, the FIU imposed a fine upon two entities including the sanction of publication of the decision, which have not yet entered into force. Another entity is subject to administrative proceedings for violation of the provisions of the AML Act, and one entity is subject to an ongoing inspection.

Entities operating in the virtual asset sector on the basis of a trade licence and based in Slovakia often use the European passporting principle. They then state on their websites that they are "regulated and licensed" in Slovakia. This claim, although partially true, may be misleading in the regulatory sense, as it is a misleading claim given the zero requirements from regulators, or the absence of a regulator.

Example of a VASP registered in Slovakia (Fig. No. 11) claiming to be licensed to provide virtual currency wallet services and virtual currency exchange services, in accordance with the law. It provides different identification data as the licence number and this may lead to confusion for potential customers and to the presumption that the activities of the entity are fully supervised and regulated by the Slovak regulatory and supervisory authorities.

Fig. No. 11



Source: website of the VASP, 12/2022, the FIU's monitoring

In practice, the Trade Licensing Office was only given the registration obligation for VASPs without any licensing procedure.

Risks associated with the absence of processes aimed at verifying the origin of assets and background of persons establishing and managing VASPs in Slovakia:

It can be considered as an extraordinary risk that there is no vetting of the persons and background of the initial assets of a company operating as a

- I) virtual currency wallet service provider - virtual currency wallet service provider shall mean a person providing services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currency,  
  
and/or
- II) virtual currency exchange service provider - virtual currency exchange service provider shall mean a person, who, within their business activities, offers or carries out transactions with virtual currency entailing purchase of virtual currency for euros or a foreign currency or sale of virtual currency for euros or foreign currency.

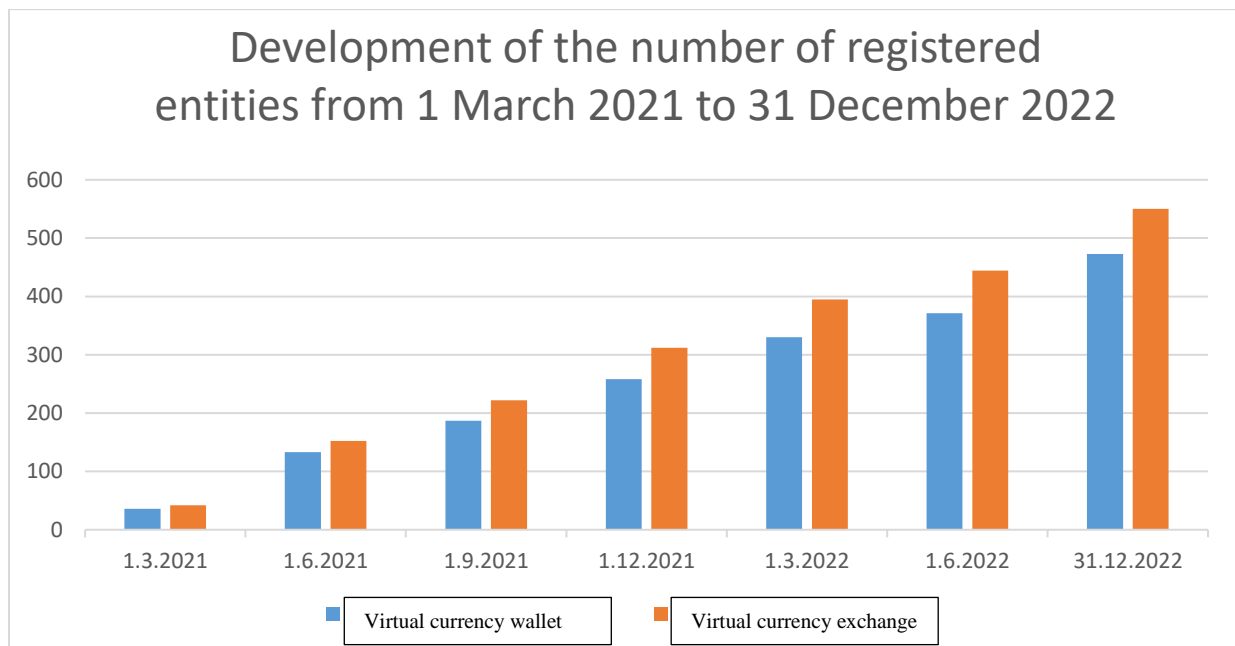
In many jurisdictions, including EU Member States but also outside the EU, the process of licensing a crypto-asset business by a regulator often involves a thorough examination of the origin of the funds that have been used to establish and operate the company applying for the licence. The regulators, together with other relevant authorities, focus on verifying the identity of the persons behind the project, the beneficial owners and also the staffing of the company, especially in top positions - in management and especially in compliance. Some regulators even explicitly require the compliance director or chief compliance officer to be a local citizen, i.e. from the country in question.

One of the significant risks is the possibility for VASPs to be based in so-called virtual addresses. These addresses can facilitate circumvention of regulatory requirements and the actual physical location of the company often remains unclear, making it difficult for regulators to carry out effective supervision and inspections.

## 5. Situation in Slovakia

A continuous verification by the Department of Trade Business of the General Government Section of the Ministry of Interior of the Slovak Republic revealed a disproportionately high number of entities registered for the provision of virtual currency exchange and/or virtual currency wallet services, given the size of the Slovak Republic (see Chart No. 1).

Chart No. 1



The high increase in the number of entities that have registered the provision of virtual currency exchange and/or virtual currency wallet services as their business object, as well as the information obtained by the Financial Intelligence Unit during the organisation of the training of obliged persons in autumn 2021, has led to the issuance of a guideline by the Financial Intelligence Unit on the fulfilment of obligations under the AML Act for legal entities and natural persons - entrepreneurs providing virtual currency wallet and virtual currency exchange services, which are classified as obliged persons under Article 5(1)(o) and (p) of the AML Act, which implies the following:

Currently, under the legislation in force, a virtual currency service provider may only carry out the activity in question provided that it has the relevant trade licence. Details on the notification, types and scope of trades are set out in the Trade Licensing Act and in Annex 2 (regulated trades) to the Trade Licensing Act. Entry of data specified by the Trade Licensing Act is carried out by District Offices, Departments of Trade Business.

On the basis of the relevant trade licence, within the business activities, the person provides services to customers (third parties). Provision of virtual currency services means, in particular, the operation of websites or mobile applications enabling virtual currency transactions (purchase of virtual currency for fiat currency and vice versa), or the operation,

provision of applications or other mechanisms to hold, store and transfer virtual currency on behalf of their customers.

A provider of virtual currency services must hold a relevant trade licence under the Trade Licensing Act and must actually carry out the activity, i.e. provide their services to customers (third parties). If a person fulfils the above-mentioned prerequisites, they can be classified as an obliged person pursuant to Article 5(1)(o) and (p) of the AML Act. The above legal opinion is based on the logical interpretation of the Act that a person who does not actually provide their services in the aforementioned field, has no customers, does not carry out transactions and does not enter into business relationships as referred to in Article 9(d), (f) and (g) of the AML Act.

Conditions for fulfilling the definition of obliged person under Article 5(1)(o) and (p) of the AML Act are therefore the relevant trade licences under the Trade Licensing Act and at the same time the provision of virtual currency exchange or virtual currency wallet services to customers as the object of business activity.

On the basis of the above, a Slovak legal entity or natural person - entrepreneur, which holds the trade licence in question for the provision of virtual currency wallet or virtual currency exchange services, but does not actually provide this service to any customers, is not an obliged person under Article 5(1)(o) and (p) of the AML Act. A person is an obliged person only if they provide virtual currency services within the business activities. The management of one's own assets cannot be considered to be the exercise of a business activity if it does not involve the exercise of a specific business activity. Thus, buying and selling virtual currency for fiat currency on exchanges, holding virtual currency in a virtual currency wallet, etc., cannot be considered to be the exercise of a virtual currency business activity if the person is acting in their own name (on their own account) and with their own assets, i.e. using the services of other entities but providing no services to third parties.

Slovak legal entities or natural persons - entrepreneurs providing services in the field of virtual currencies are, in providing such services, classified as obliged persons under Article 5(1)(o) and (p) of the AML Act only if they have this activity listed in their objects of business, i.e. they hold a trade licence for it. Otherwise, it will be an illegal act which violates the obligation under the Trade Licensing Act to carry out a certain business activity on the basis of a trade licence, and will also give rise to a person's tort or criminal liability for such an act (unauthorised business activity).

## 6. Results of a survey of the sector of virtual currency service providers in the Slovak Republic carried out for the period until 30 June 2022 in the form of a questionnaire

During July 2022, a total of 451 questionnaires were distributed by the Financial Intelligence Unit, which were sent to all entities with the registered object of activity being provision of virtual currency exchange services or provision of virtual currency wallet services registered by 30 June 2022. In view of previous experience with delivery via slovensko.sk, as it was necessary to track more closely the actual deliverability of questionnaires to the entities, this time the form of postal delivery was chosen by the Financial Intelligence Unit. The results thus obtained were more relevant and provided an interesting insight into the sector of virtual currency service providers in the Slovak Republic.

The questionnaires sent also included the Financial Intelligence Unit's methodological guideline on the fulfilment of obligations under the AML Act for legal entities and natural persons - entrepreneurs providing virtual currency wallet and virtual currency exchange services, which are classified as obliged persons under Article 5(1)(o) and (p) of the AML Act, and the Risk Indicators for virtual currency exchange service providers and virtual currency wallet service providers, compiled by the Financial Intelligence Unit. The sending of the above documents, which are published on the website of the Financial Intelligence Unit but of which many entities were unaware, had a positive mutual educational effect. On the basis of the questionnaire received, many entities contacted the Financial Intelligence Unit by telephone or e-mail and expressed their willingness to cooperate in the sectoral risk assessment. However, these interviews resulted in questions and misunderstandings raised by the current legislation in the virtual currency sector.

A detailed analysis and evaluation of the mails delivered and not taken over revealed that of the total number of questionnaires sent (451 in total), approximately 82% were successfully delivered to the addressees. For various reasons, 80 entities (about 18%) did not take over the mails. The Financial Intelligence Unit received replies from a total of 340 entities, representing approximately 74%. It should be noted at this point that some of the entities who took over the questionnaire did not send a reply, while others delivered the completed questionnaire to the Financial Intelligence Unit despite the fact that they did not manage to take over the mail.

This aspect indicates that the entities operating in the virtual asset infrastructure in Slovakia are interconnected and have well established communication channels between them. These links and communication structures could be used effectively in the future to improve cooperation with supervisory and regulatory authorities. The expansion and optimisation of these communication channels could contribute significantly to transparency, better monitoring and more effective regulation of the whole sector, thereby increasing its security and credibility. This synergy would also provide regulators with better tools for preventing and addressing potential risks in the virtual asset sector.

Chart No. 2

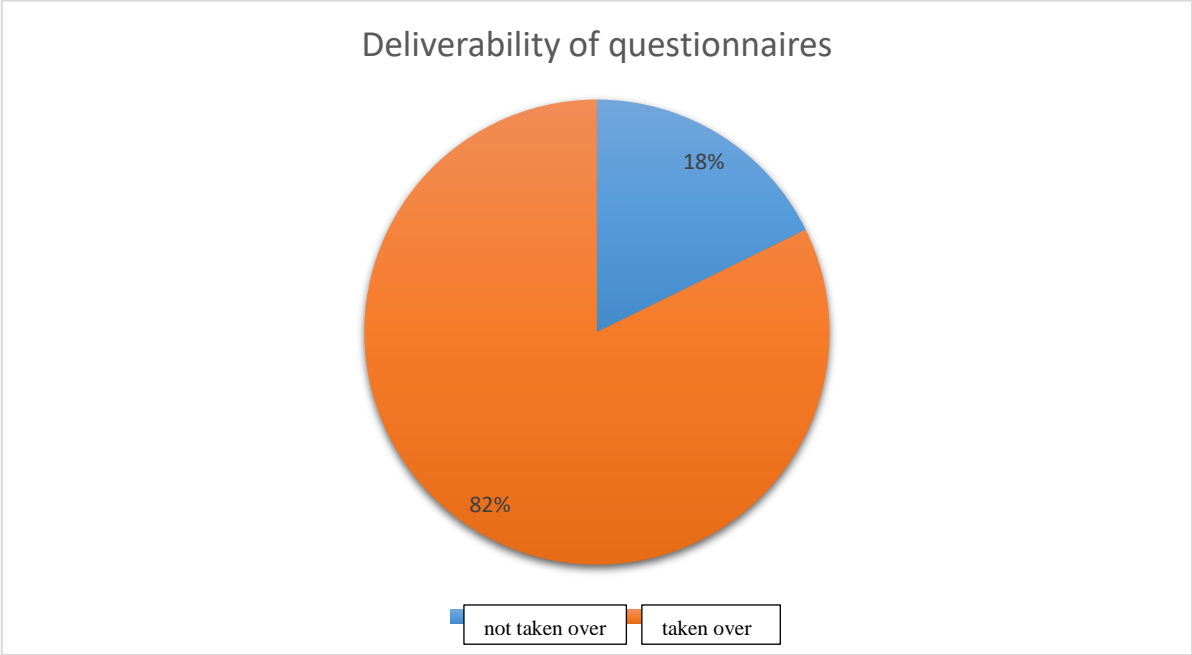
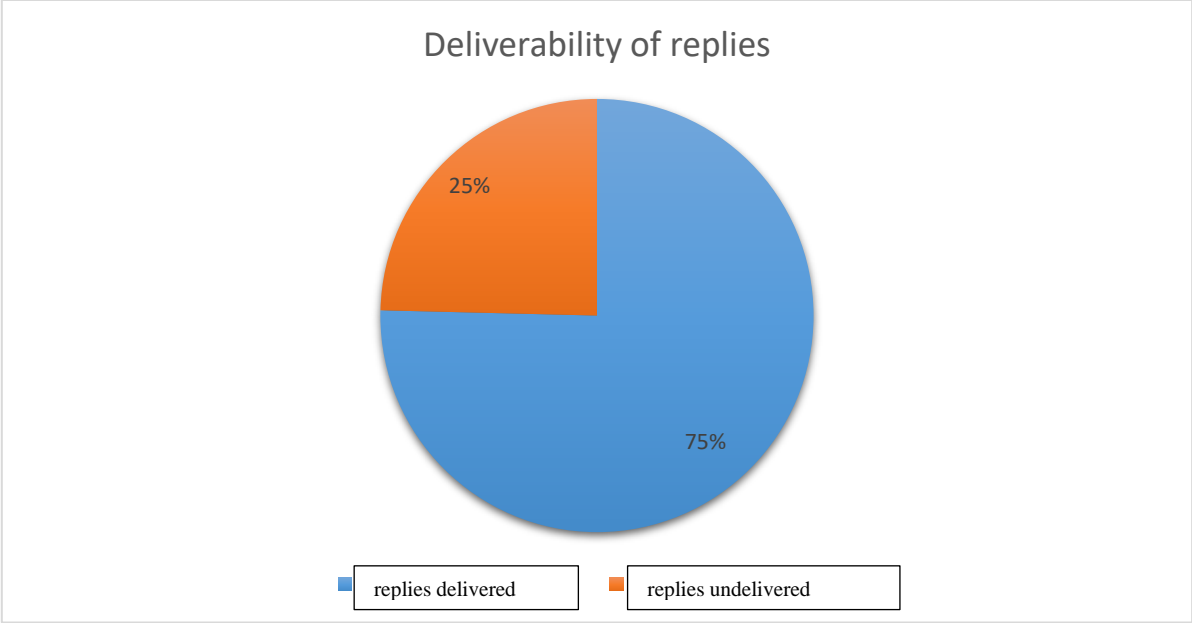


Chart No. 3



Further analysis and evaluation of the responses received revealed that out of the 340 responses received by the Financial Intelligence Unit, as many as 271 entities (approximately 80%) indicated that they did not carry out the activity. Almost half of these respondents indicated that they had registered the activity of providing virtual currency exchange or virtual currency wallet services in the belief that this is a mandatory obligation if they wish to invest their funds, whether personal or from business, in virtual currency. These entities have real-world experience in purchasing and holding virtual currency for their own use and consider it

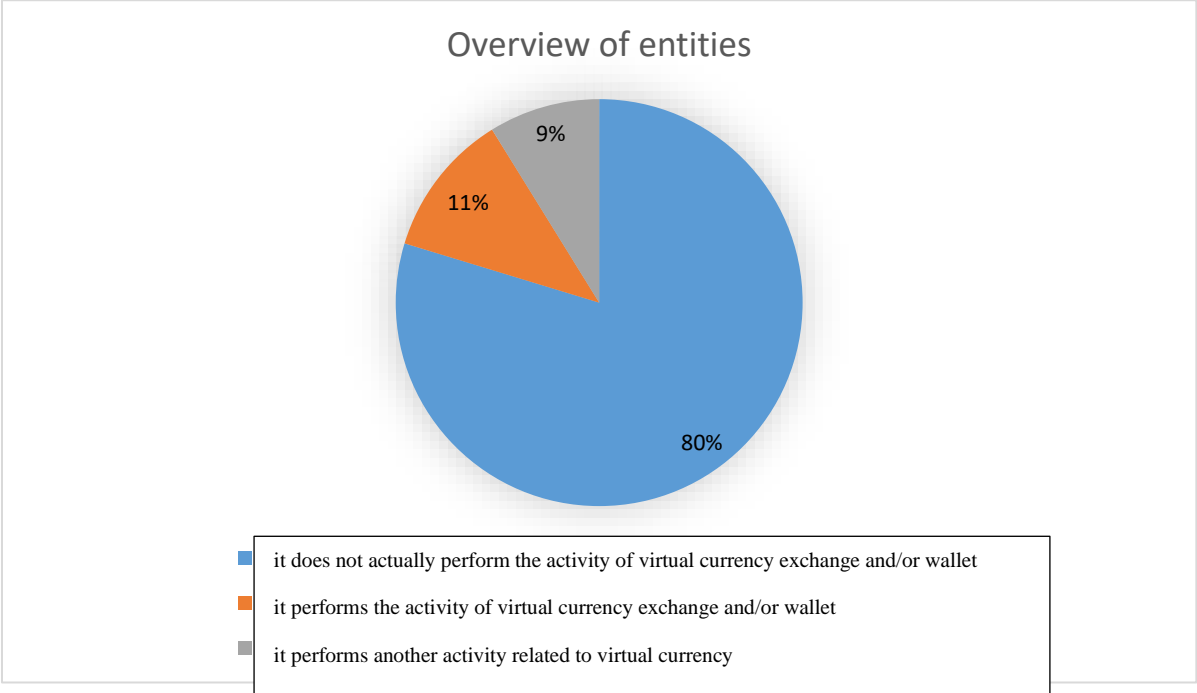
a very safe and trustworthy means of return on investment or form of savings. They deal exclusively with their own funds and do not provide services to third parties.

The remaining entities, which had registered the provision of virtual currency exchange services or virtual currency wallet services as the objects of their activity and stated that they did not carry out the activity, did not come into contact with virtual currency at all and the reasons for which they applied for a trade licence in that area can be summarised as lay interest, supported by positive media information about attractive profits, combined with a simple registration process, the absence of more complicated requirements for issuing a licence for the provision of virtual currency exchange services or virtual currency wallet services (the same as for others), which is not subject to a fee (no matter how many trades an entity registers, the fee is still the same). Most of these entities were not even minimally aware that by registering a trade for the provision of virtual currency exchange or virtual currency wallet services, they were also meeting the prerequisite for an obliged person under the AML Act, which imposes specific obligations on them.

The evaluation of the responses also identified a separate group of entities that do not provide virtual currency exchange or virtual currency wallet services, but are actively engaged in business activities on the virtual currency market as such or are actively preparing for virtual currency activities. This group includes entities that declare activities such as cryptocurrency mining, development of new software solutions, staking or the provision of marketing and educational services.

Among the entities that state that they perform other services, there is also a cryptocurrency fund that was established in Slovakia and states on its website that it is registered under the National Bank of Slovakia (<https://www.cveu.eu/>).

Chart No. 4



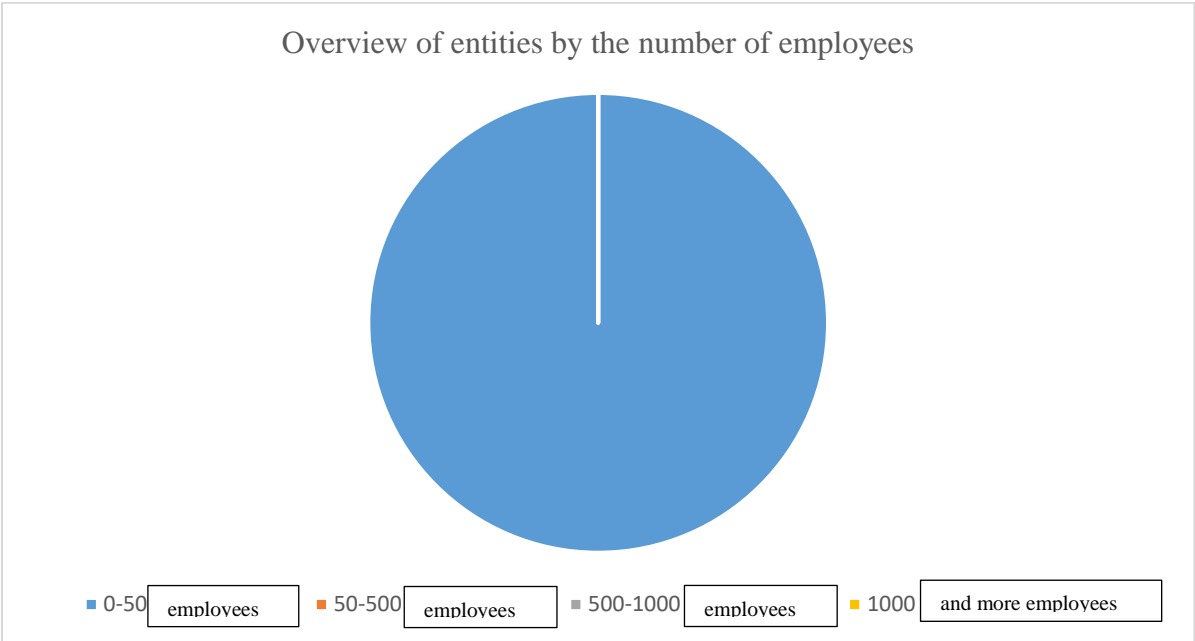


Further evaluation of the questionnaires was primarily focused on information from entities that had a valid trade licence for the provision of virtual currency exchange or virtual currency wallet services as of 30 June 2022 and also actually carried out this activity for third parties (customers).

### 6.1. Geographic criteria

In this way, it was found that 100% of the entities carrying out virtual currency exchange or virtual currency wallet activities in the Slovak Republic are smaller in scale and indicate the number of employees up to 50. A significant part of the entities even reported that they have no employees.

Chart No. 5



By analysing the criteria of geographic location of the entities, it was found that the vast majority were registered as VASPs only in the Slovak Republic. Only one entity stated that it was registered in both the Slovak Republic and the Czech Republic.

By comparing the addresses of the registered offices of the companies, it was found that the individual entities are stratified throughout the territory of the Slovak Republic, with a stronger dominance of the Bratislava region. For more information see Chart No. 7.

An interesting geographic criterion, which was evaluated beyond the scope of the questions from the questionnaire, was the property background of individual companies registered and operating as virtual currency service providers in the Slovak Republic. In the evaluation of this area, sources from the Commercial Register of the Slovak Republic were used for the entities appearing as a statutory body, owner or shareholder of the company. From the above, it was found that the evaluated entities operating virtual currency business in the Slovak

Republic also have a property background in the Slovak Republic, however, some of the entities exhibit features of a more complex property and legal structure with links to foreign legal or natural persons with no proven relationship to the Slovak Republic. These facts are reflected in more detail in Chart No. 8.

Chart No. 6

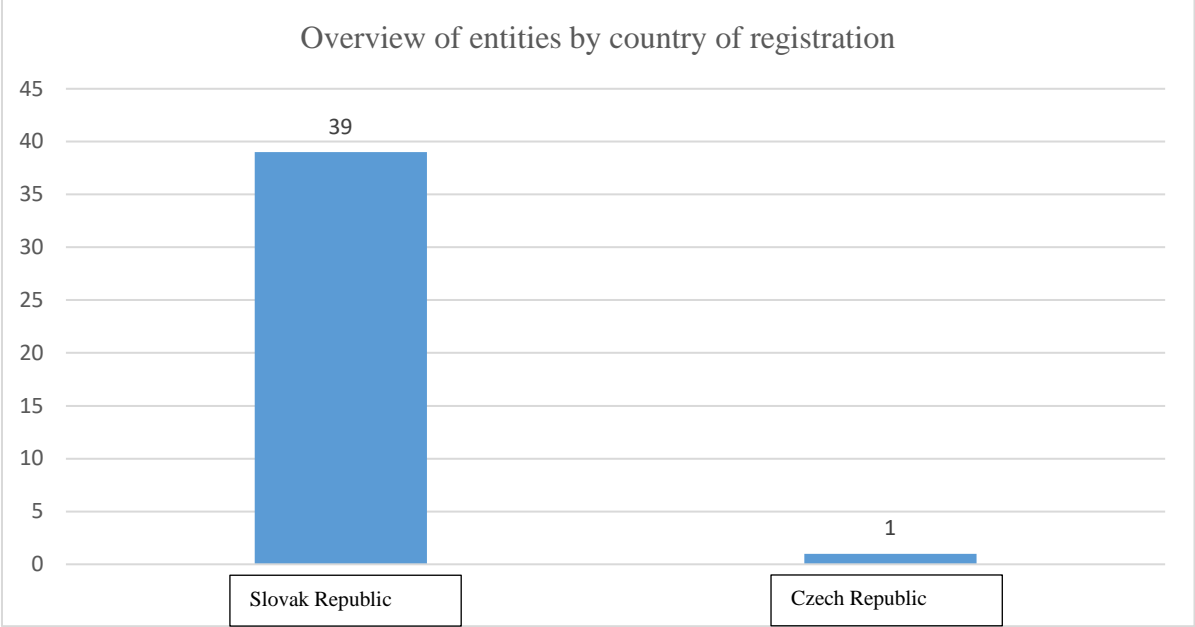


Chart No. 7

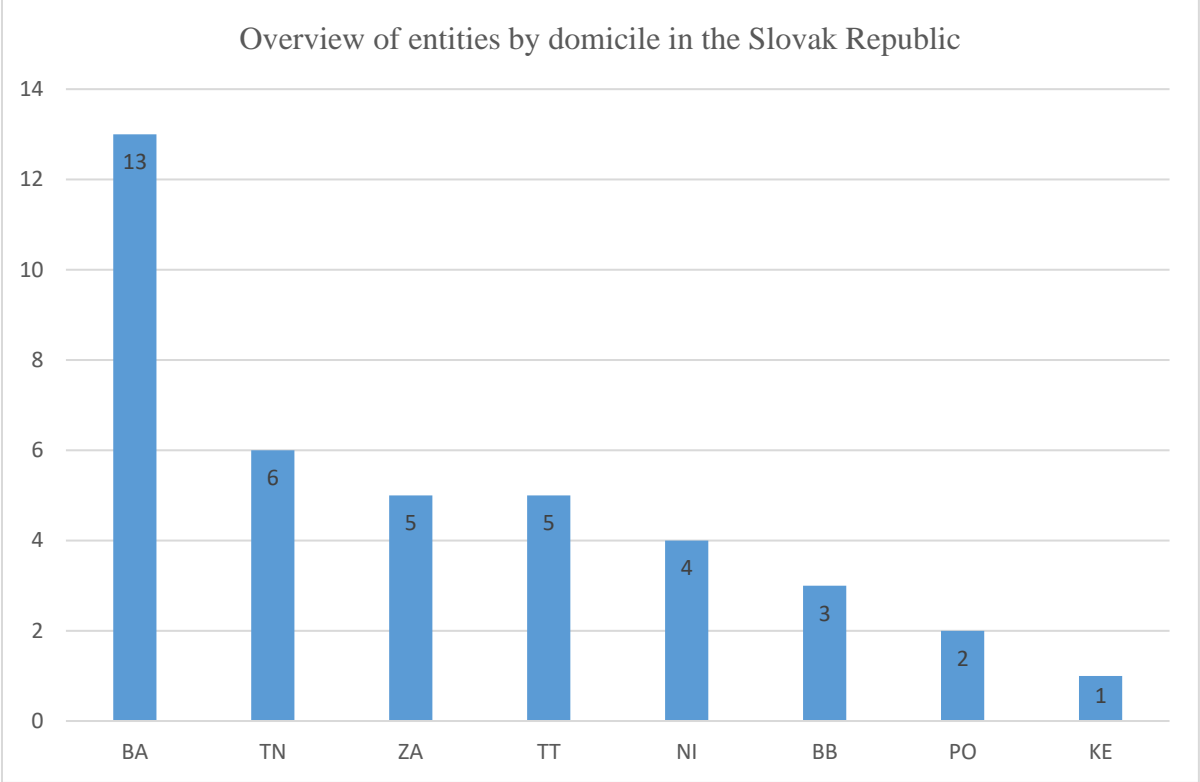
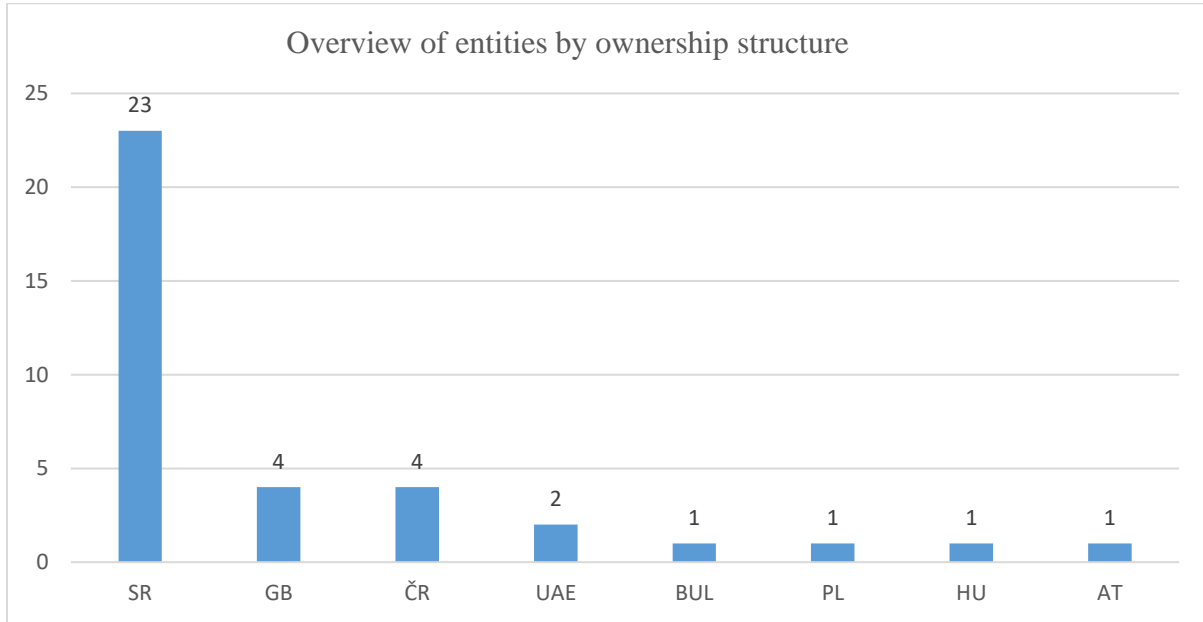
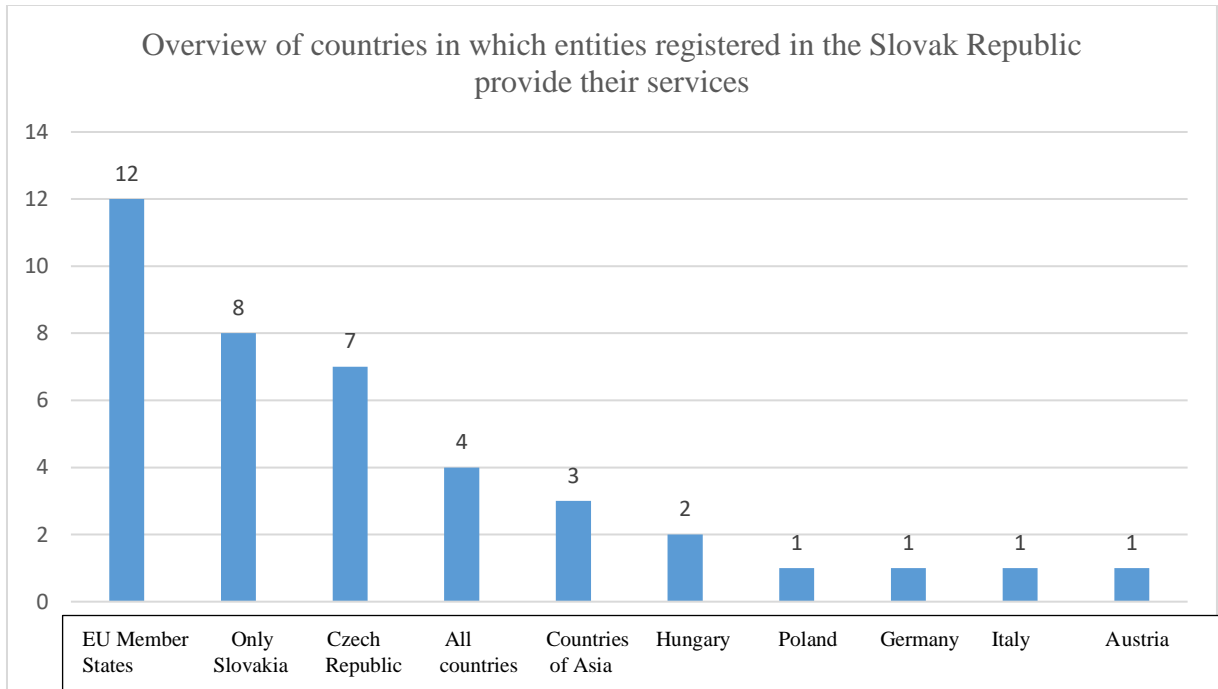


Chart No. 8



Due to the transnational nature of virtual currencies, most entities registered in the Slovak Republic also provide virtual currency services in other countries, most of them focusing on European countries (mainly the Czech Republic, but also other EU countries). At this point it should be highlighted that all entities have expressed a high level of understanding and respect in relation to countries with increased security risks with which they exclude cooperation.

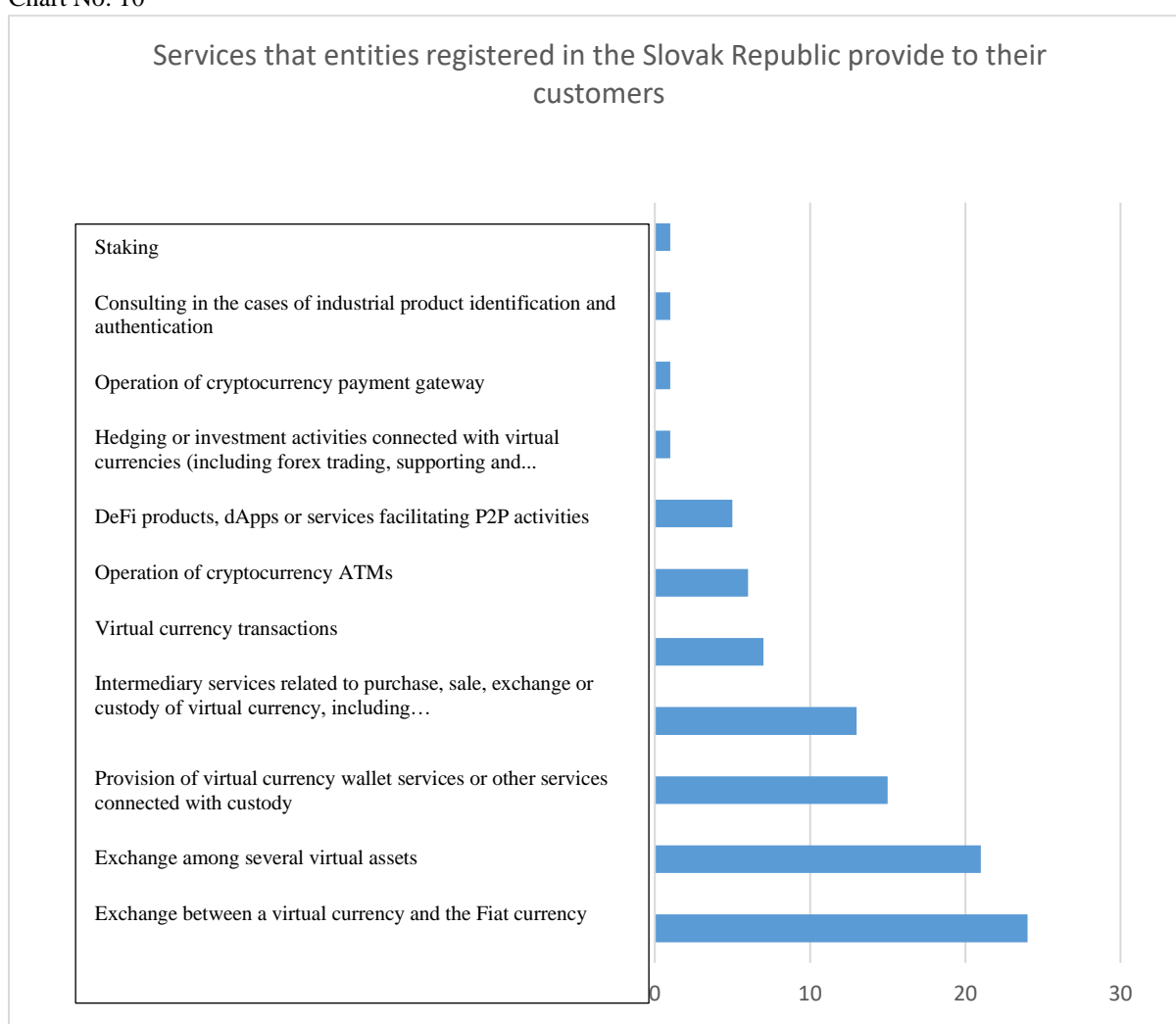
Chart No. 9



## 6.2. Virtual currency services in the Slovak Republic

The services most commonly provided by entities registered in the Slovak Republic to their customers include the exchange of virtual currency for fiat currency and the exchange of multiple virtual currencies with each other, the provision of virtual currency wallet services or other custodial services, and intermediary services related to the purchase, sale, exchange or custody of virtual currency, including stablecoins, tokens or privacy coins. To a lesser extent, entities also reported transactions carried out with virtual currencies and DeFi products, dApps or services facilitating P2P activities. Six entities reported the operation of cryptocurrency ATMs as an activity. The overall overview of the services provided is reflected in Chart 8.

Chart No. 10

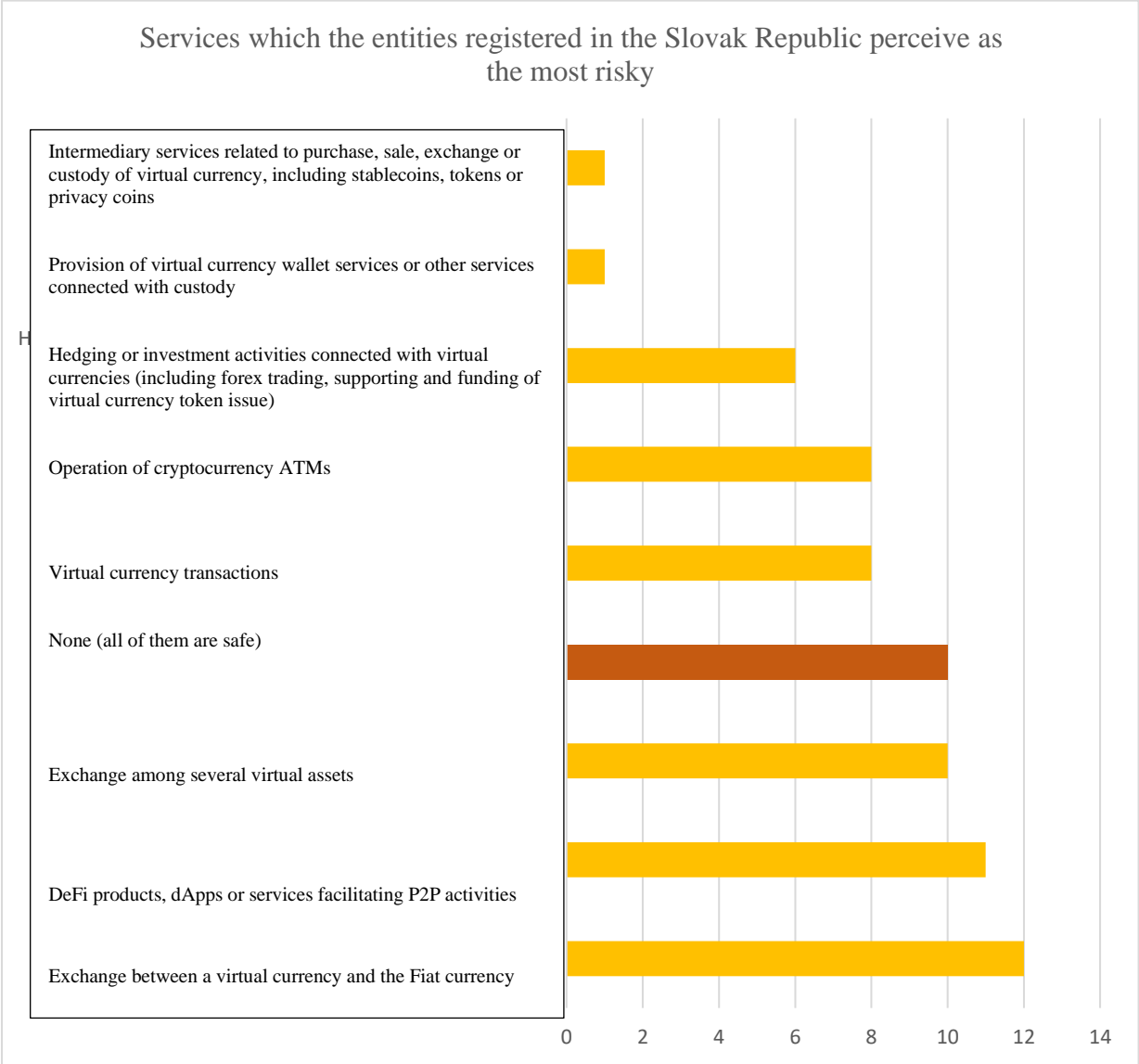


An interesting insight into the sector risk perception is provided by the analysis of the answers to the question which of the services provided to customers are considered by the entities operating as virtual currency exchangers or virtual currency wallets to be the most risky, in connection with their possible abuse for the purpose of money laundering or terrorist

financing, where up to 16% of respondents stated that they do not perceive any risk or are not aware of it.

Other respondents perceived an increased risk of money laundering or terrorist financing mainly in connection with the conversion of virtual currency into fiat currency, in case of exchange between multiple virtual currencies and in connection with DeFi products, dApps or services facilitating P2P activities. Some interviewees also perceive risk in connection with the operation of cryptocurrency ATMs, in transactions conducted with virtual currencies and in connection with hedging or investment activities (including forex trading, supporting and financing the issuance of virtual currency tokens). Respondents perceive intermediary services related to the purchase, sale, exchange or custody of virtual currency, including stablecoins, tokens or privacy coins, and the provision of virtual currency wallet services or other services related to the custody of virtual currency to be the least risky.

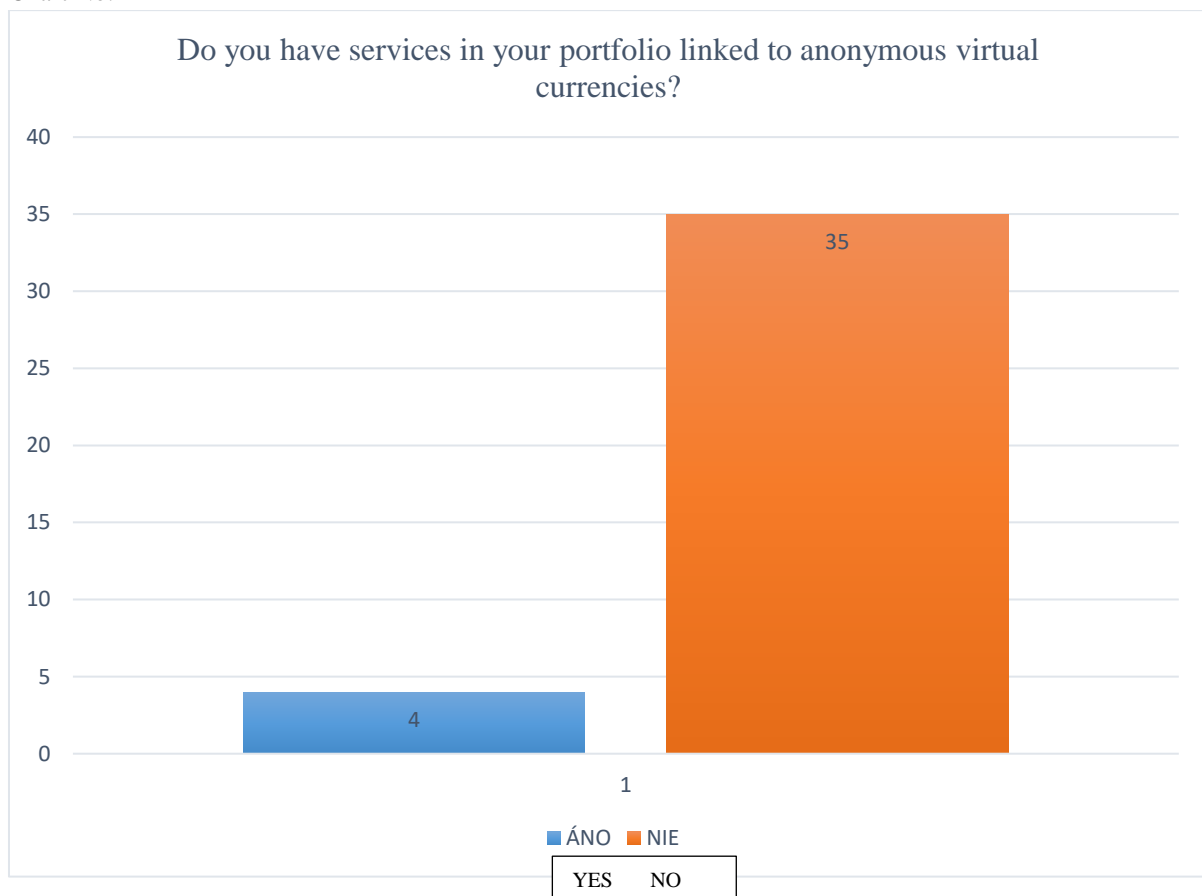
Chart No. 11



### 6.3. Anonymous virtual currencies and products aimed at anonymising and making it more difficult to identify the origin of virtual currencies

In the context of the analysis of virtual currency-related services provided by entities registered in the Slovak Republic to third parties in relation to the assessment of the potential risk of money laundering or terrorist financing, it appears important to monitor the use of products linked to anonymous virtual currencies as well as products aimed at anonymising and making it more difficult to identify the origin of virtual currencies (e.g. various types of mixers, VPNs, etc.).

Chart No. 12



The majority of entities registered in the Slovak Republic as virtual currency exchange service or virtual currency wallet service providers state that they do not maintain services linked to anonymous virtual currencies in their portfolio. Only four entities reported partial use of anonymous virtual currencies, and their responses indicate that the most commonly used anonymous virtual currency in the Slovak Republic is Dash (DASH).

The use of products aimed at anonymising and making it more difficult to identify the origin of virtual currencies (e.g. various types of mixers, VPNs, etc.) is uniformly rejected by all entities. Beyond the questionnaire question, some of the respondents indicated that they themselves take the initiative to use software to detect cryptocurrency wallets attached to mixers and subsequently reject such wallets.

Chart No. 13

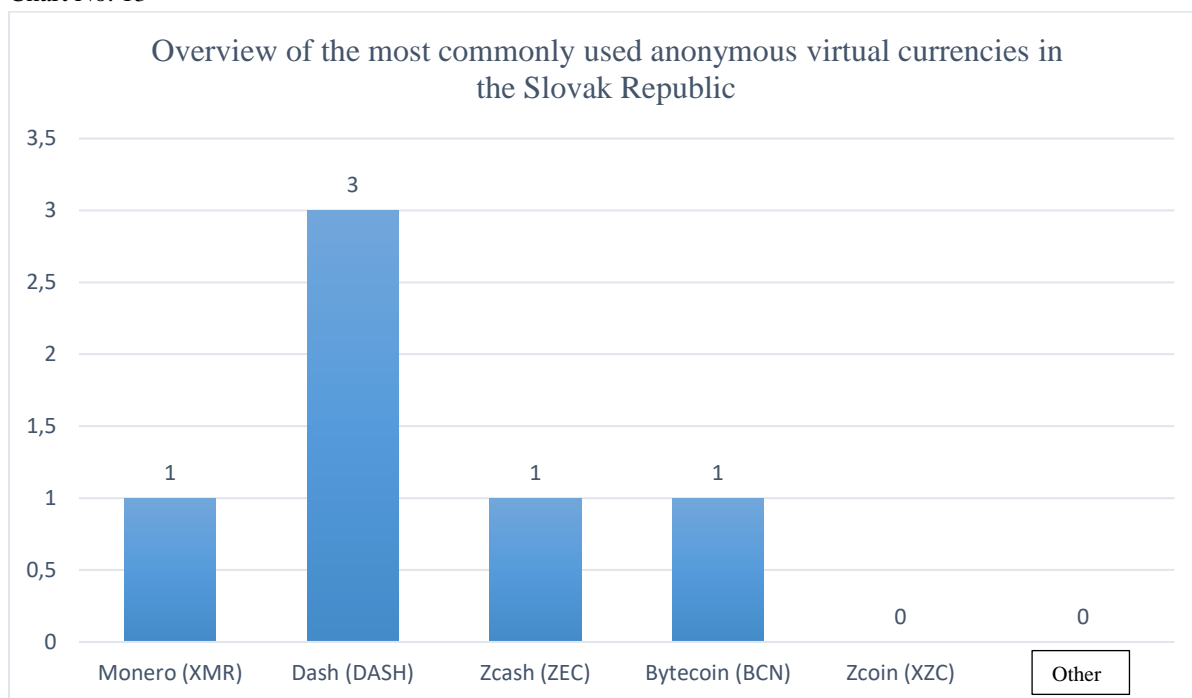
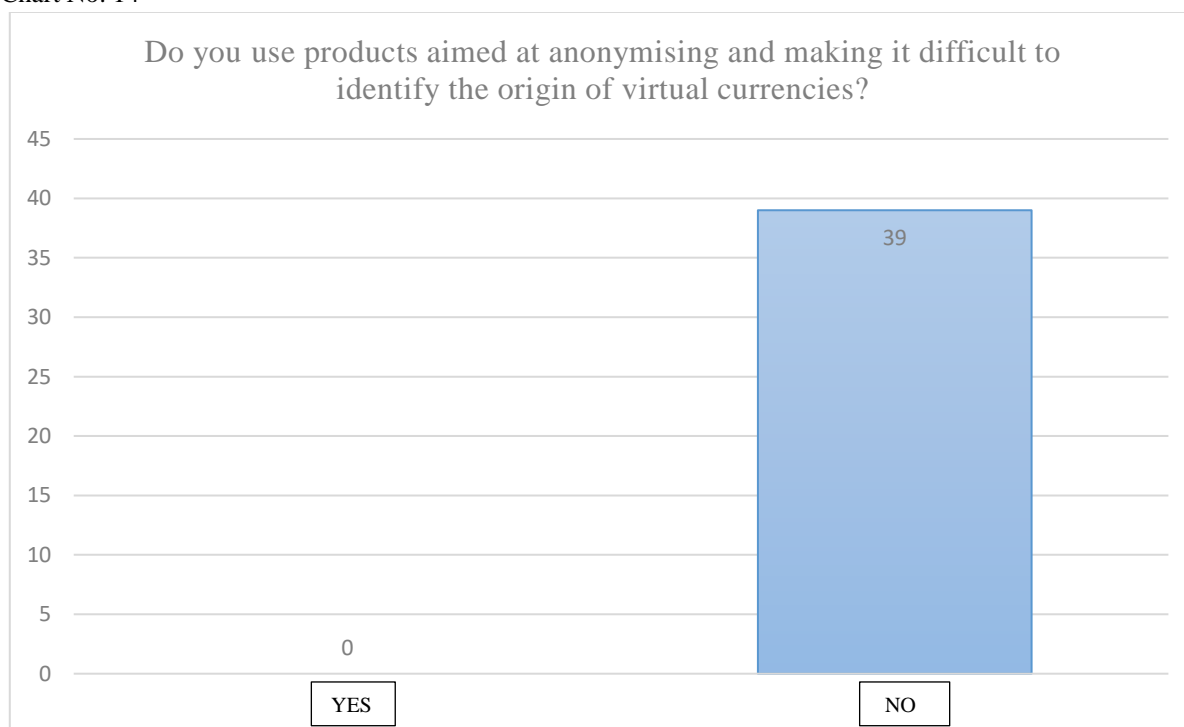


Chart No. 14

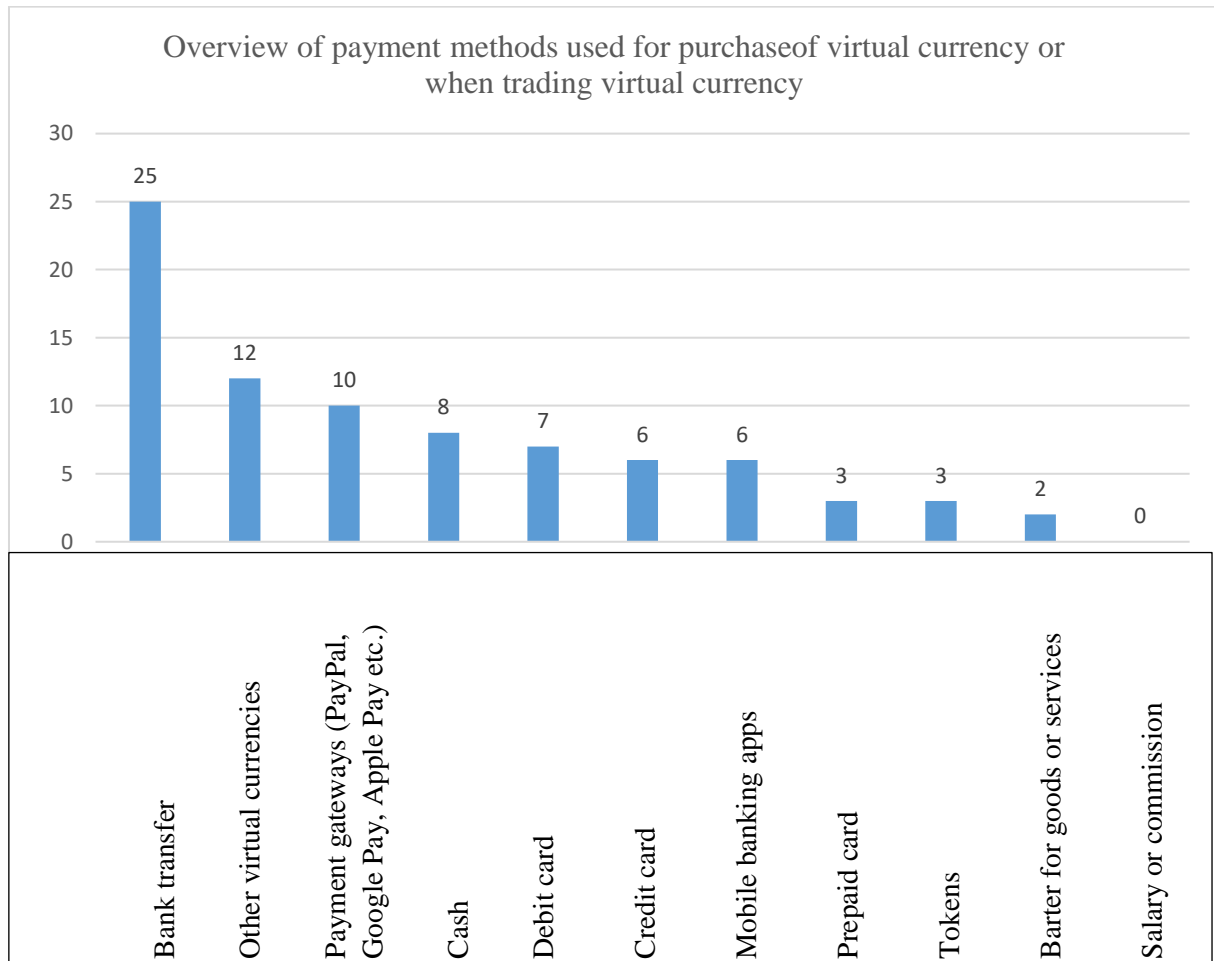


#### 6.4. Payment methods used to purchase or trade virtual currency

The most frequently cited methods used by customers of virtual currency exchanges or virtual currency wallets registered in the Slovak Republic to purchase virtual currency or when trading in virtual currency is clearly the bank transfer, which is primarily used by the majority of entities registered in the Slovak Republic when providing services to third parties.

Other payment methods repeatedly mentioned by respondents are cash, other virtual currencies and payment gateways (PayPal, Google Pay, Apple Pay, etc.). In contrast, no salary or commission is used at all to purchase virtual currency or to trade in the Slovak Republic. An overview of all the payment methods mentioned is reflected in more detail in Chart No. 15.

Chart No. 15

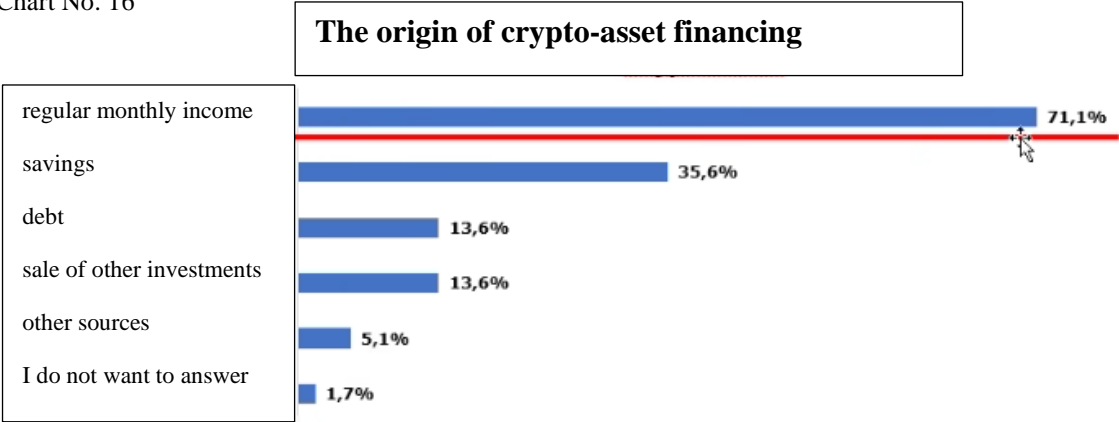


It is also important to know the form of VA purchase financing. The National Bank of Slovakia (hereinafter referred to as the “NBS”) conducted a survey focused on the use of virtual assets by consumers (period 26 November – 03 December 2021), the survey was conducted by the FOCUS agency: (1010 respondents). From this comprehensive survey, the NBS published an extensive report available on the NBS website and the following link: (<https://nbs.sk/dokument/e7c683b5-f817-4abf-bd4d-34d19081f707/stiahnut/?force=false>). A



question focused on the origin of respondents' funds used to finance VA purchases was part of this survey.

Chart No. 16



Source: NBS survey

In that NBS survey, respondents most frequently financed the purchase of VA from their regular monthly income. Financing through savings followed by a wide margin, with just over 35% of respondents using it. Over 13% of respondents had sold other investments in their portfolio to purchase VA, and the same percentage had financed a VA purchase using debt. Other sources were used by just over 5% of respondents. Financing the purchase of VA with debt is extremely risky, as the borrower may need to repay their debt but will not be able to sell their VA at the price at which they purchased them due to the significant volatility. Most respondents interviewed seem to be aware of this risk and therefore do not use debt to finance their VA purchases.

## 7. The link between virtual currency and crime

### 7.1. Politically exposed persons and crime in general government in the context of virtual currency

Within the distributed questionnaires, part of the questions was aimed at identifying the number of politically exposed persons who would invest their funds in virtual currencies, as well as the role that virtual currencies as such or the services associated with them play in cases of embezzled money laundering and corruption crimes. At the outset, it should be noted that the findings reflected in Charts No. 17 - 19 were obtained from entities providing virtual currency services in the Slovak Republic and reflect both their personal experience gained in the course of their business activities and their subjective opinion on the area.

The individual responses that were collected therefore varied widely, with the range of perceptions correlating from a pragmatic and realistic attitude to a complete rejection of politically exposed persons as customers. However, a positive sign is that the majority of the entities stated that they identified (or vetted) politically exposed and sanctioned persons at the inception of the business relationship as well as during the course of the relationship. Part of the entities did not know how to answer some of the questions and it is clear that it would be advisable to strengthen education by public authorities in this respect.

Chart No. 17

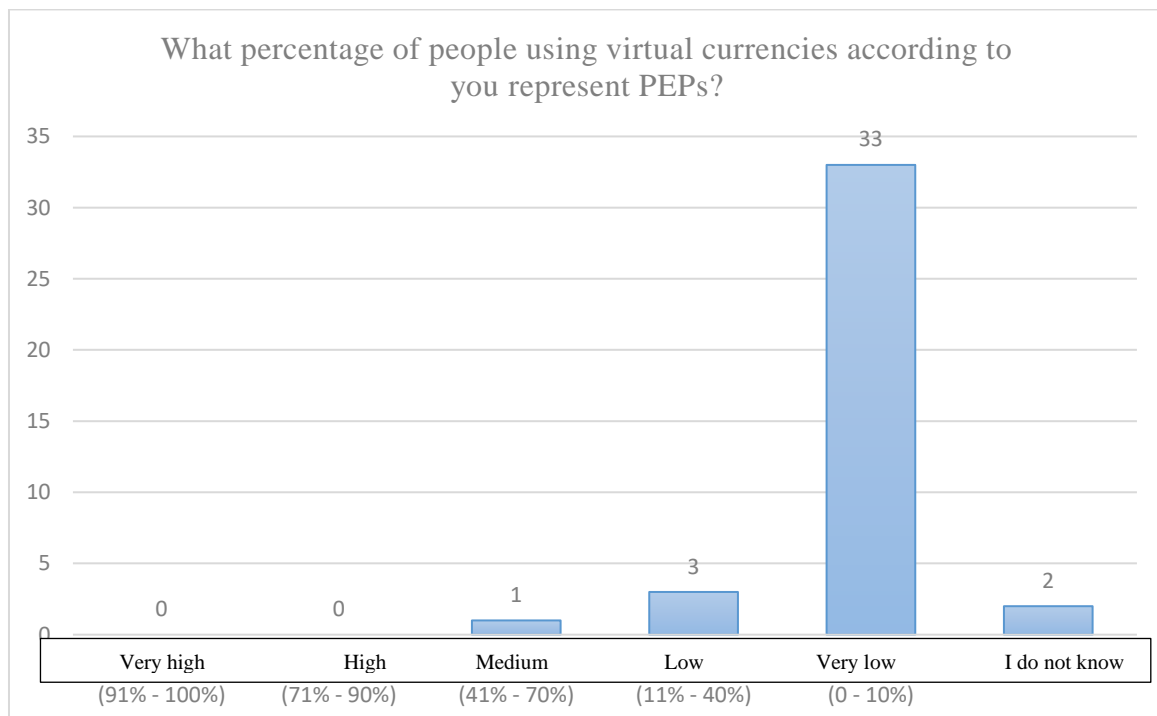


Chart No. 18

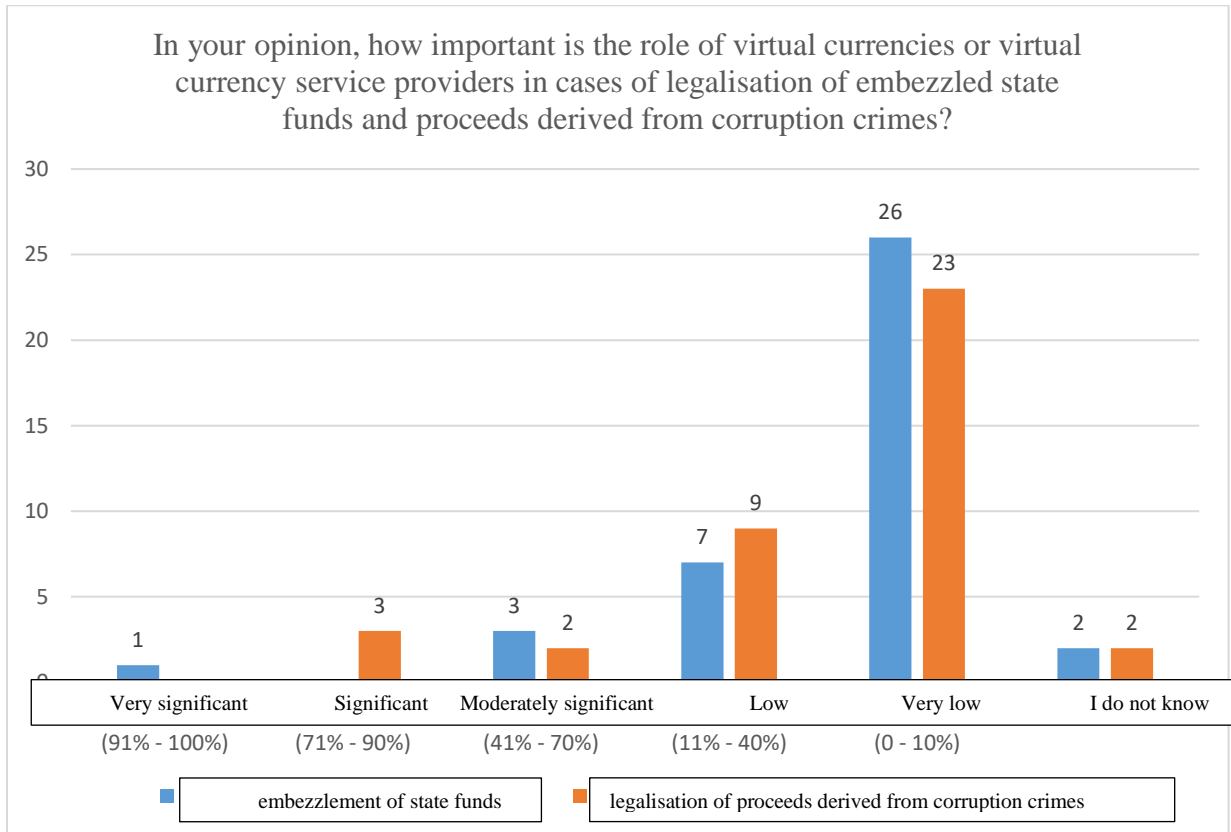
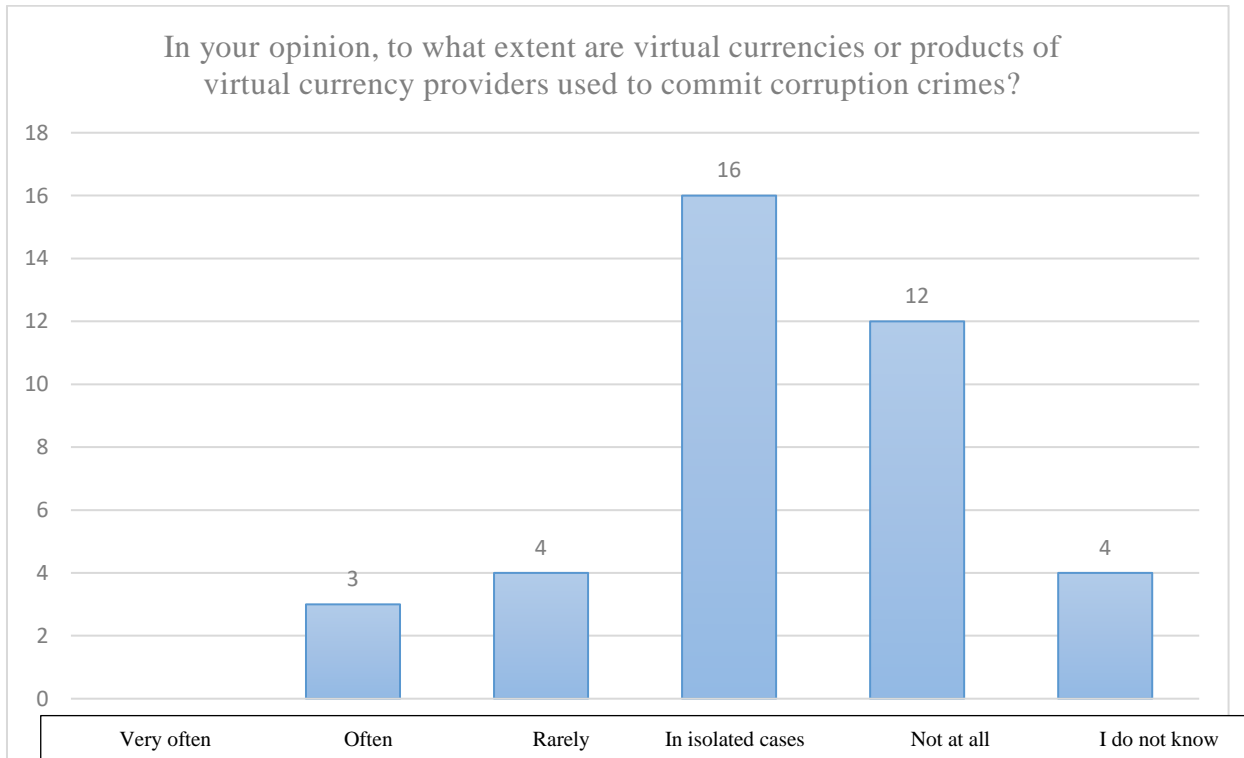


Chart No. 19



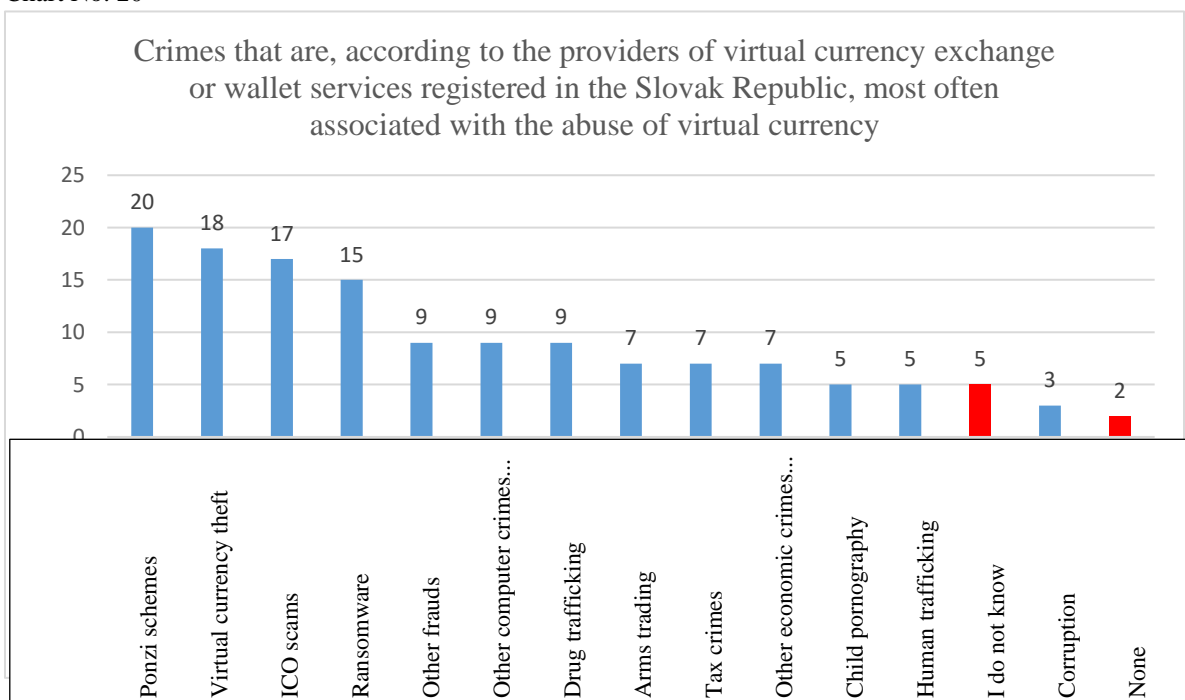
## 7.2. Crimes most commonly associated with the abuse of virtual currency

The fact that virtual currency can be easily abused to commit crimes or to conceal the origin of funds obtained through criminal activity is a fact proven by practice and confirmed by the experience of the Financial Intelligence Unit of the Slovak Republic and Slovak law enforcement authorities.

However, the answers to the questions of the questionnaire under evaluation showed that not all entities doing business with virtual currencies in the Slovak Republic are sufficiently aware of the risks associated with the use of virtual currencies for criminal activities. However, the differences in the responses may also be due to the different range of activities and the diverse composition of the clientele of the respondents whose answers were evaluated. On the one hand, there was a noticeable group of entities that take the issue of the link between virtual currencies and criminal activity extremely seriously, taking the initiative themselves to register and monitor the situation not only in terms of national circumstances, but also in the international context. At the other end of the spectrum, however, are entities which, with reference to the nature and scope of their business activities, the range of their customers or their personal set-up, either do not address the risk of abuse of virtual currencies for committing criminal activities at all or even downplay it in isolated cases.

Chart No. 19 reflects which crimes are perceived by entities doing business in the Slovak Republic as a virtual currency exchange or virtual currency wallet as the most frequently associated with the abuse of virtual currency or virtual currency provider services. In general, fraudulent “Ponzi” schemes, virtual currency theft, ICO scams, and ransomware were most frequently cited.

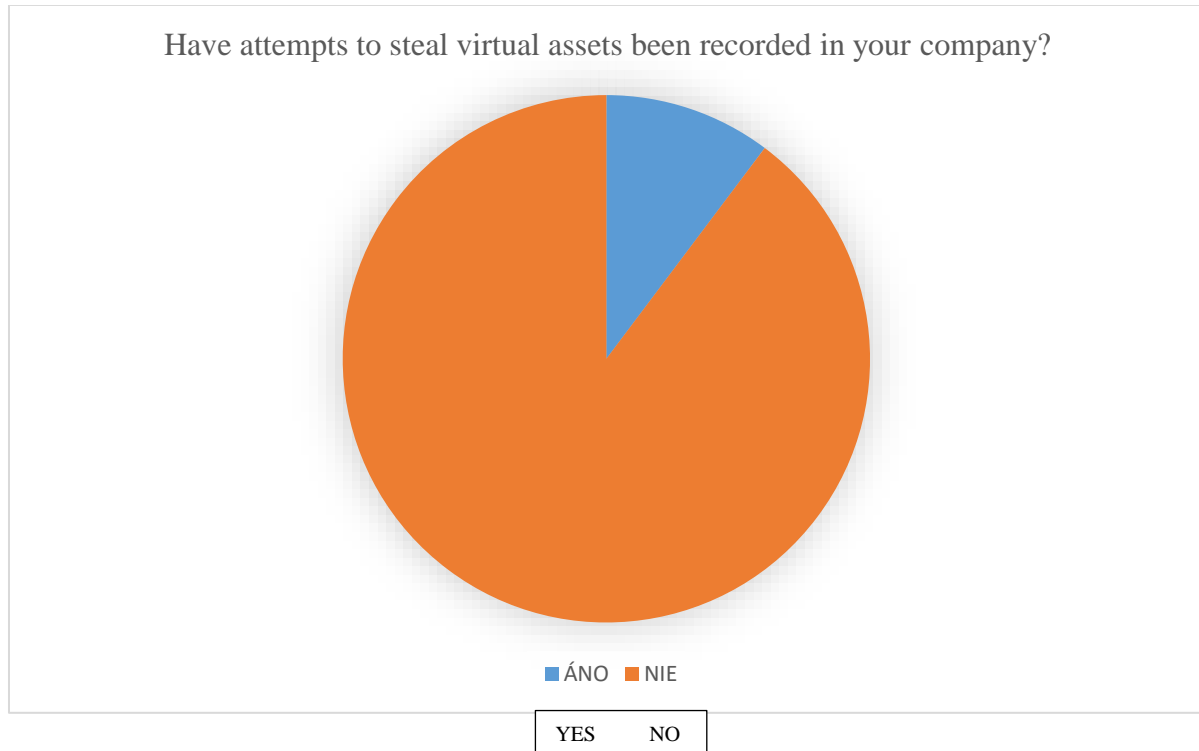
Chart No. 20



### 7.3. Virtual currency theft

Theft of virtual currency was one of the most frequently cited virtual currency-related offences in the evaluation of the questionnaire survey. Fortunately, most of the respondents whose questionnaires were evaluated had not experienced the theft of virtual currency in their company, but there were some who had to face attempts by the perpetrators of that crime. Only one entity admits that virtual currency theft has actually occurred in their company.

Chart No. 21



Entities that operate a virtual currency exchange or virtual currency wallet in the Slovak Republic without the appropriate registration or licence and entities that violate the country's AML rules

All respondents whose answers were evaluated in the processing of this analysis consistently indicated that they were not aware of any entity that operates a virtual currency exchange or virtual currency wallet in the Slovak Republic without the relevant registration or licence or an entity that systematically violates the country's AML rules. At this point it should be mentioned that beyond the question, the entities (either directly in the text of the questionnaire or in personal communication with the staff of the Financial Intelligence Unit) expressed a high level of effort and willingness to cooperate in the AML area and to comply with the rules, which are, however, incomprehensible for many.

However, in relation to the above, it should be noted that the activities of the Financial Intelligence Unit have identified three entities operating in the Slovak Republic as providers of virtual currency exchange and virtual currency wallet services which do not apply the country's AML rules in a fully correct manner and whose activities may pose an increased

risk of money laundering. The Financial Intelligence Unit processed a number of extensive operational analytical outputs on these entities during 2021 and 2022, which were subsequently forwarded to the locally and materially competent police units of the Slovak Republic for further reviews.

## 8. Application of preventive measures and a risk-based approach by entities operating a virtual currency exchange or virtual currency wallet in the Slovak Republic

The monitoring of risky virtual currency wallets, the setting of appropriate criteria for the exercise of enhanced due diligence and the correct understanding and evaluation of the transactions carried out in terms of their unusualness are important factors in the level of awareness of entities doing business with virtual currencies in the Slovak Republic with regard to the area of criminal law risks.

The results obtained by evaluating the relevant questions focused on the application of preventive measures and the risk-based approach of entities operating in the Slovak Republic with virtual currencies again showed a great diversity (see Chart No. 20 - Chart No. 23 for more details). Also in this case it was possible to identify on the one hand a group of about 50% of entities that have the rules set very well and it is obvious that they are also aware of their importance. At the other end of the spectrum, however, are the entities who, pointing to the nature and scope of their business activities, range of customers or personal set-up, do not address the monitoring of risk wallets or the enhanced due diligence criteria. By evaluating the questions on the minimum transaction amount at which entities proceed to enhanced due diligence and the number of recorded unusual transactions, it is not obvious that all respondents evaluated are clear about the distinction between exercising basic customer due diligence and exercising enhanced due diligence, as well as the characteristics of an unusual transaction. It would be suitable to strengthen public sector education in these areas.

Chart No. 22

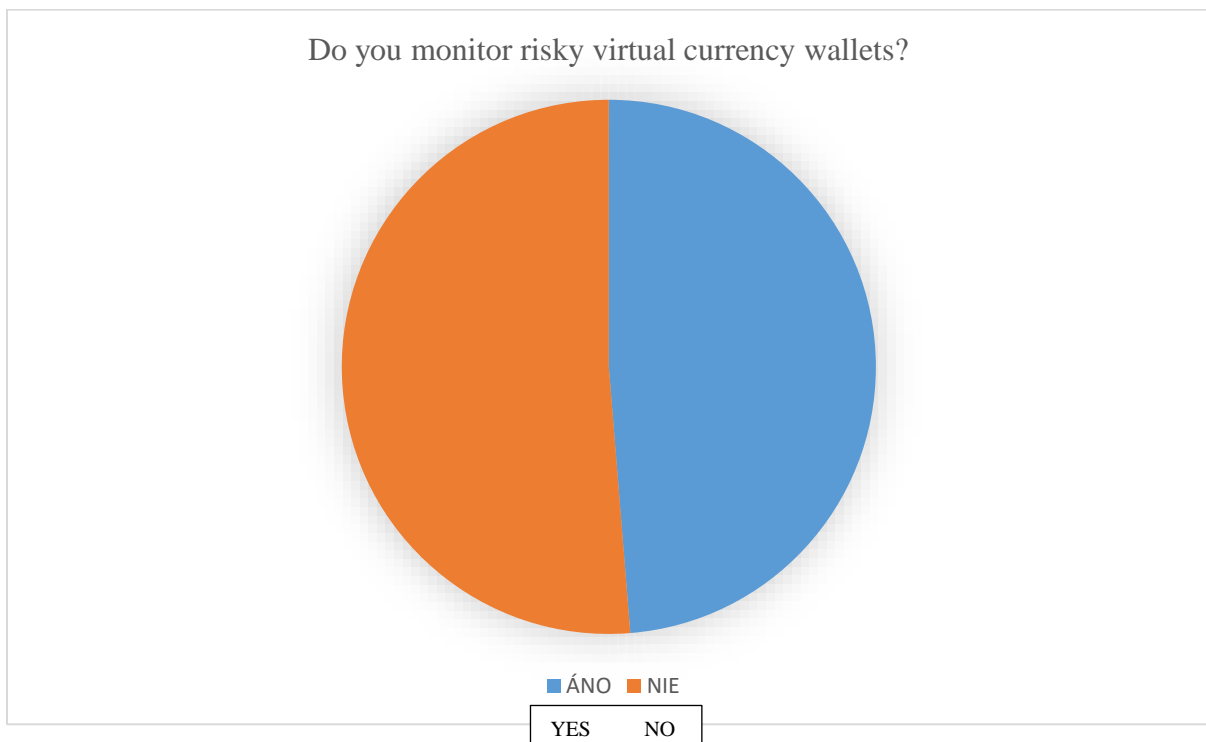


Chart No. 23



Chart No. 24

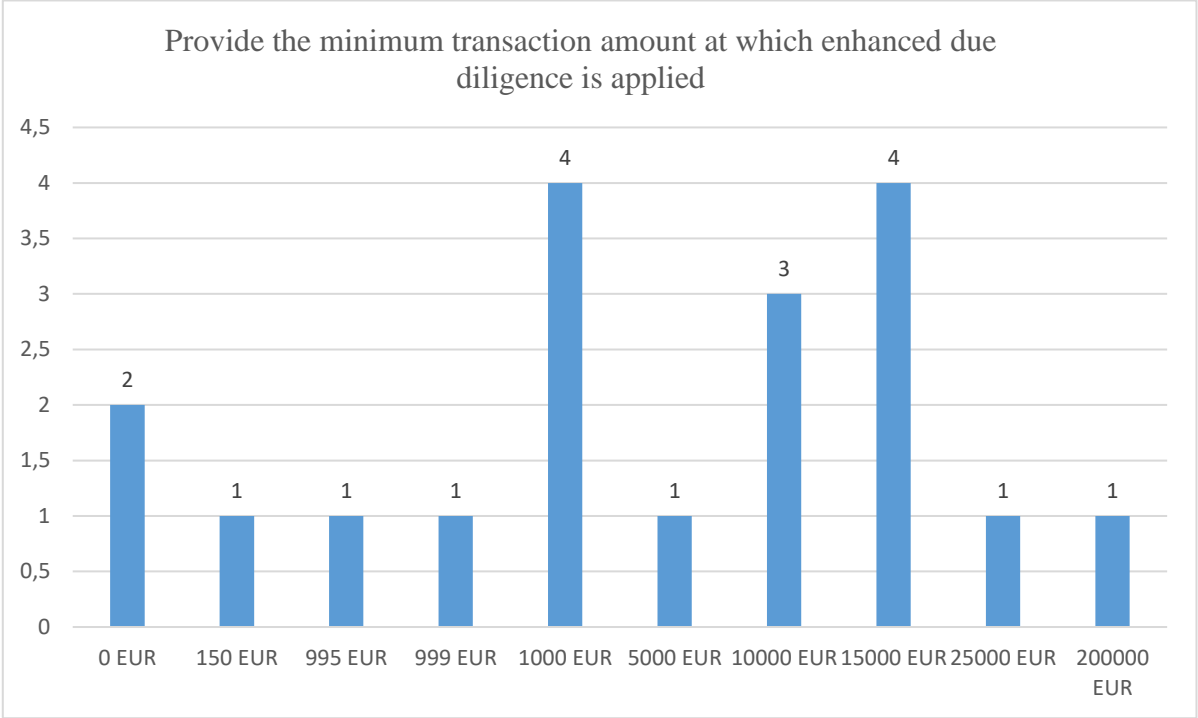
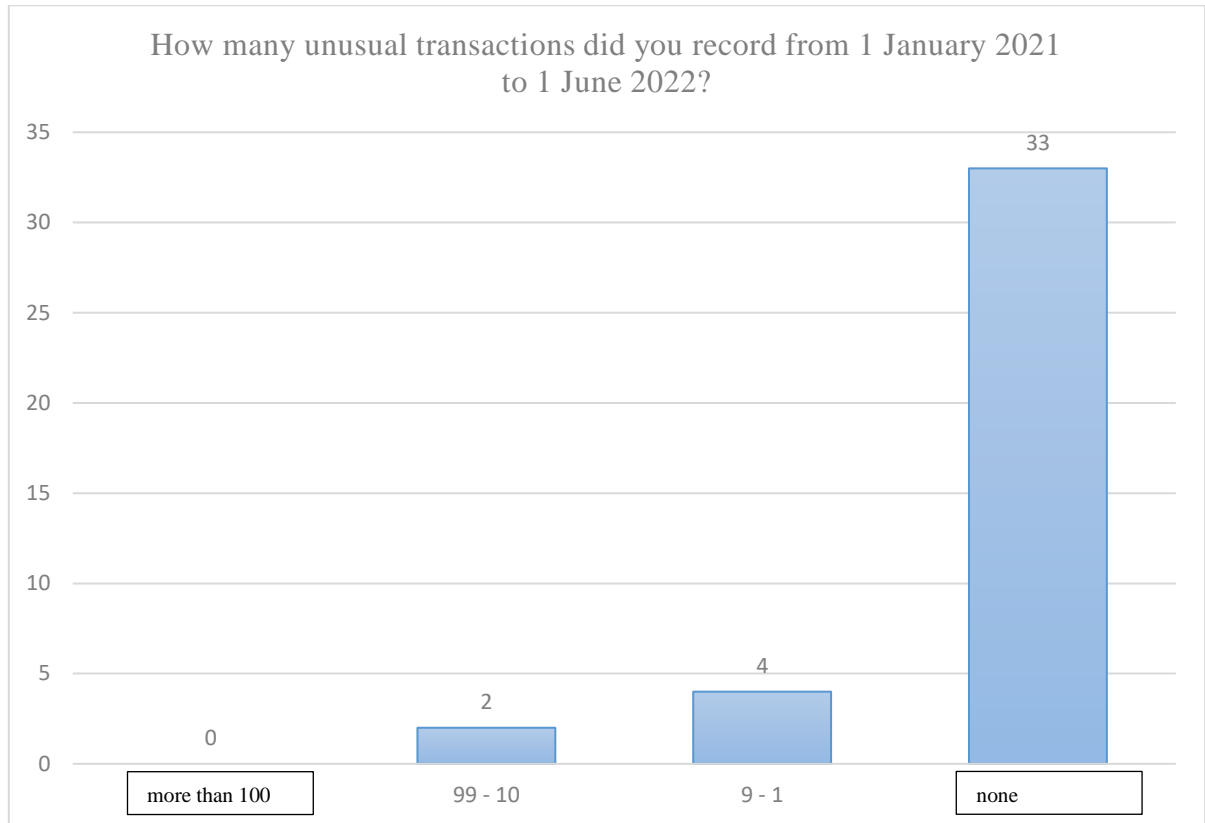




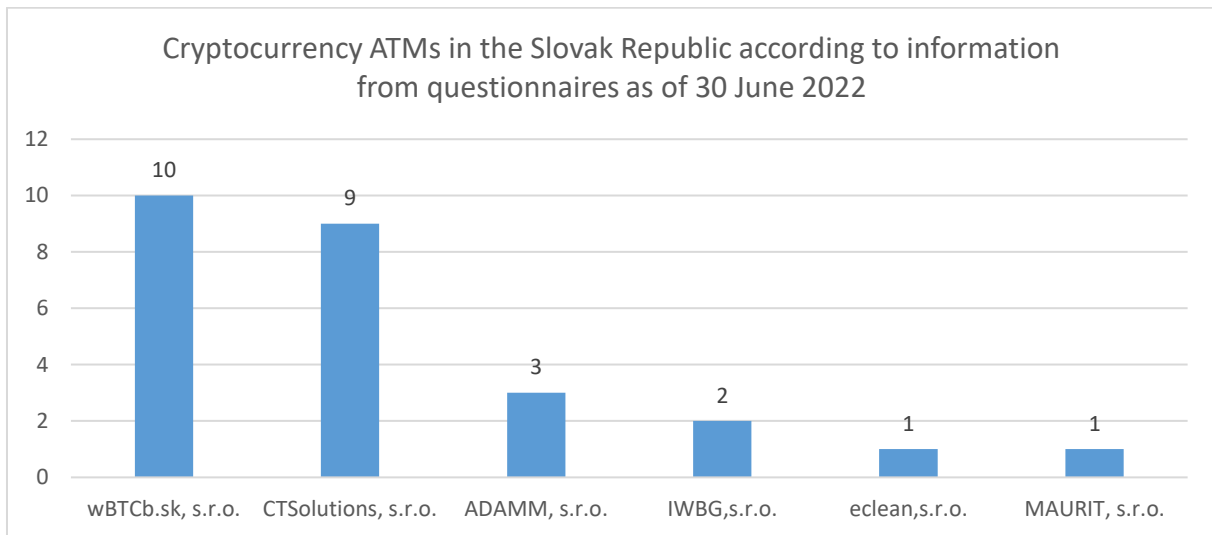
Chart No. 25



## 9. Cryptocurrency ATMs in Slovakia

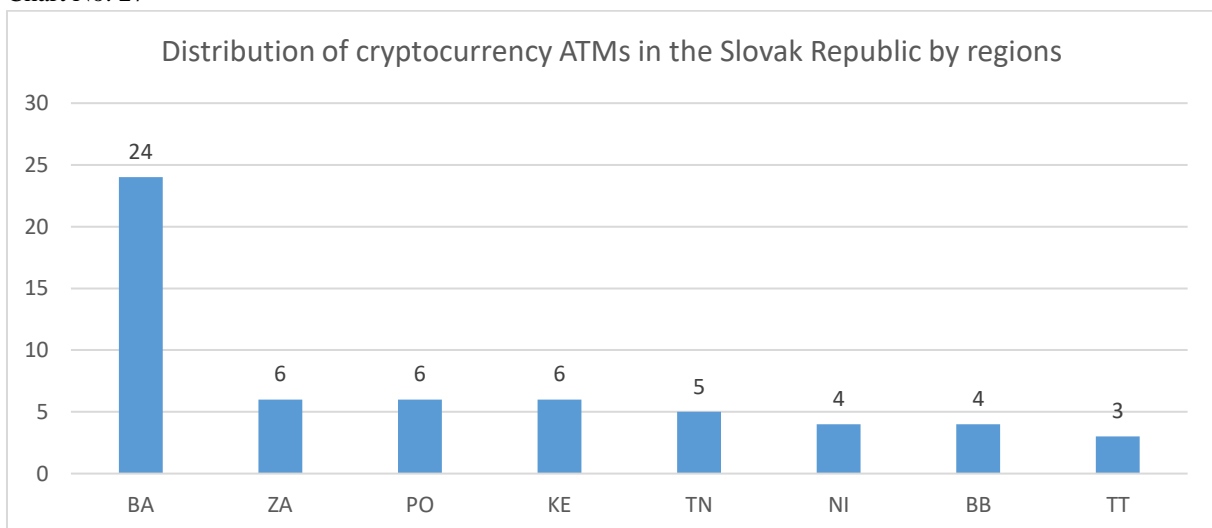
The questionnaire-based screening found that of the entities that had a registered business in the Slovak Republic as of 30 June 2022 to provide virtual currency exchange or virtual currency wallet services, six entities stated that they operated a total of 26 cryptocurrency ATMs in the Slovak Republic.

Chart No. 26



Subsequent screening via <https://coinatmradar.com/> revealed that as of 6 March 2023 there were a total of 58 cryptocurrency ATMs located in the territory of the Slovak Republic, distributed throughout the territory of the Slovak Republic, with a significant dominance of the Bratislava region (or Bratislava).

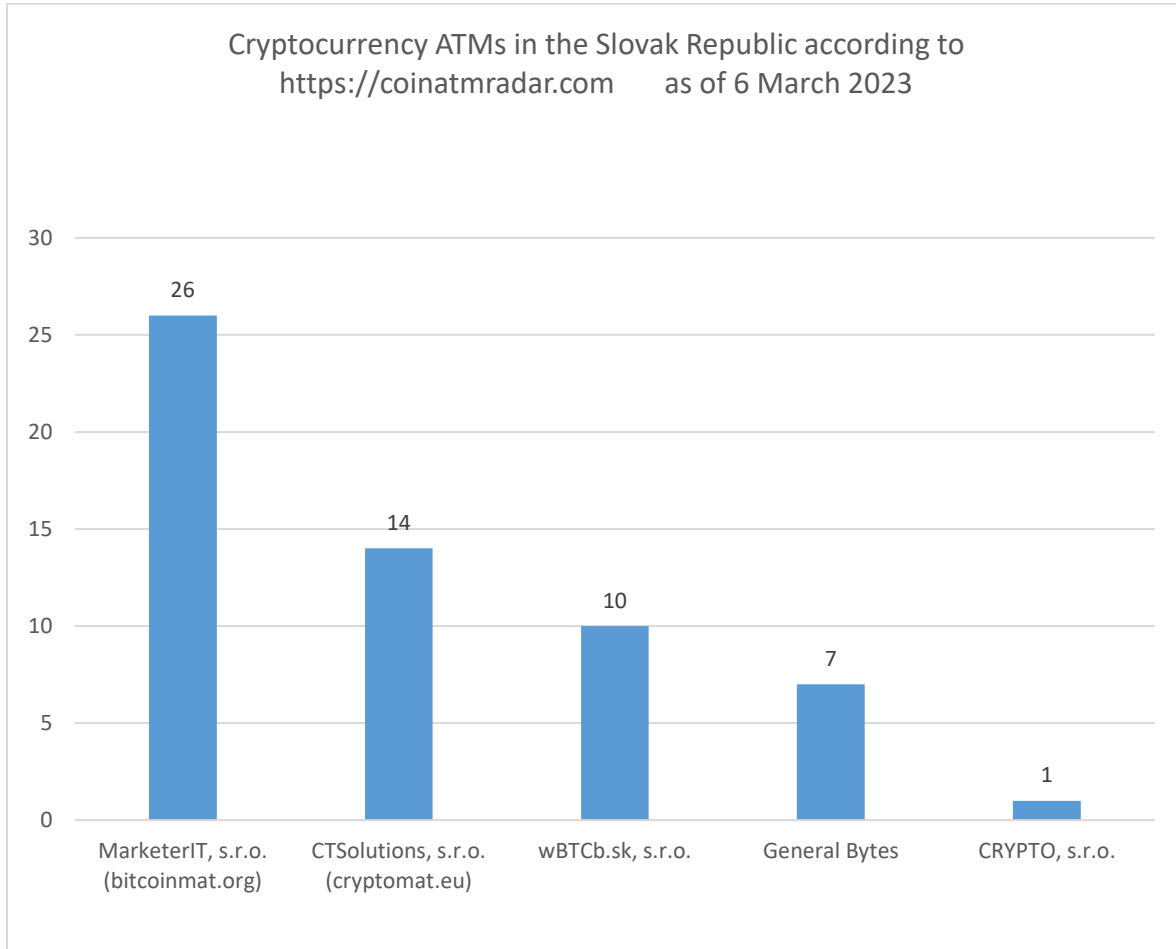
Chart No. 27



Subsequent verification revealed differences in the entities that stated in the questionnaire that they managed cryptocurrency ATM(s) in the territory of the Slovak Republic and the information published on the website <https://coinatmradar.com/>. However, it should be noted here that the time period

of several months during the distribution and collection of questionnaires may have contributed to the changes as in the world of virtual currencies it can make a considerable difference.

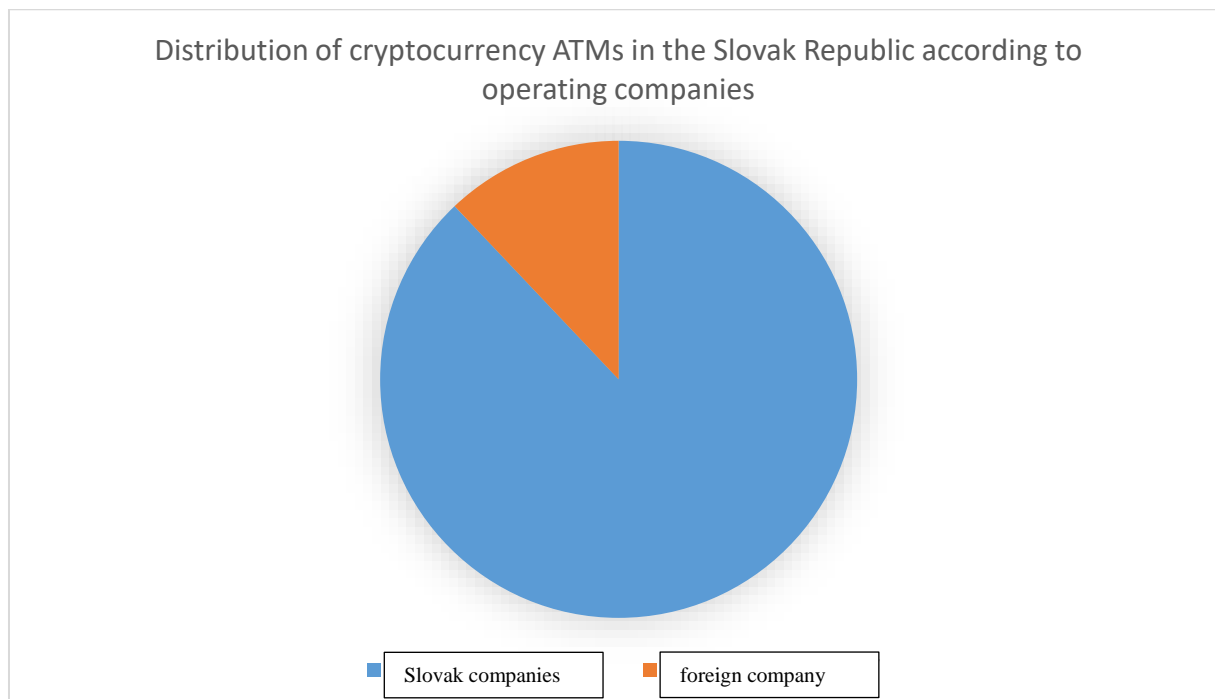
Chart No. 28



Despite the consideration of the time perspective, it is necessary to highlight the two most significant differences found by comparing the distribution of cryptocurrency ATMs in the Slovak Republic, which may indicate a weak point of the area under study.

Before addressing the identified weaknesses, we would like to point out a positive fact, namely that the majority of cryptocurrency ATMs located in the territory of the Slovak Republic, according to the website <https://coinatmradar.com/>, are managed by entities registered in the Slovak Republic, with their registered office in the Slovak Republic and with a demonstrable geographical link to our area. Only one foreign entity, with no demonstrable link to the Slovak Republic, has been recorded as having seven cryptocurrency ATMs located in our territory, which represents approximately 12% of the total number of cryptocurrency ATMs.

Chart No. 29



Foreign entities operating cryptocurrency ATMs in the territory of a country to which they have no demonstrable relationship can be, by the very nature of a cryptocurrency ATM operating based on cash exchange, considered as a factor indicating an increased risk of potential money laundering or terrorist financing. The actual operation of cryptocurrency ATMs managed in this way is currently beyond the legal reach of the Slovak state authorities and their activities are not monitored in relation to AML issues even by the Financial Intelligence Unit, as these entities do not qualify as an obliged person.

A search of freely available sources on the internet revealed that a foreign company operating 7 cryptocurrency ATMs in the Slovak Republic is registered in the Czech Republic and as of March 2023 had more than 9,000 cryptocurrency ATMs deployed worldwide. In this context, it should be noted that this shortcoming is not directly related to the Slovak Republic, but reflects the level of regulation of cryptocurrency ATMs globally.

As mentioned above, within the Slovak Republic, as of March 2023, cryptocurrency ATMs were mostly operated by entities with a direct relationship to the Slovak Republic. However, even for these entities, there is a gradual shift to a broader market focused mainly on neighbouring European countries. For one cryptocurrency ATM operator, the structure of the companies registered in the name of the statutory body was found to be unclear and in one case it was found, according to public sources, that the company operating the cryptocurrency ATM did not hold a registered trade licence for operating a virtual currency exchange. Given that these facts are not clearly addressed by the current Slovak legislation, it is appropriate to consider opening a discussion in these cases in the future with a view to a more thorough adjustment of the legal regulation.

## 10. Non-cooperating entities

By analysing and evaluating the questionnaires sent to entities that had registered the provision of virtual currency exchange services or virtual currency wallet services in the Slovak Republic as of 30 June 2022, a group of 111 entities was identified that either did not take over the questionnaire or took it over but did not fill it in.

Given the lack of data available to the Financial Intelligence Unit on these entities, as well as the relatively high percentage of this group in relation to all registered providers of virtual currency services, special attention was paid to this group in the processing of the sectoral risk assessment and their individual verification was carried out both in the databases of the Commercial Register of the Slovak Republic, the databases of the Financial Intelligence Unit, as well as in publicly available sources.

The additional screening revealed that a significant part of this group of entities is likely to consist of business companies which do not actually carry out the activity of virtual currency exchange or virtual currency wallets in relation to third parties. In addition to the above, a total of 36 entities were found to have a wholly or partly foreign ownership structure with a virtual domicile. The most frequent links were to entities in the Czech Republic, Italy, the United Kingdom and Hungary. An overview is shown in Chart No. 30.

Chart No. 30

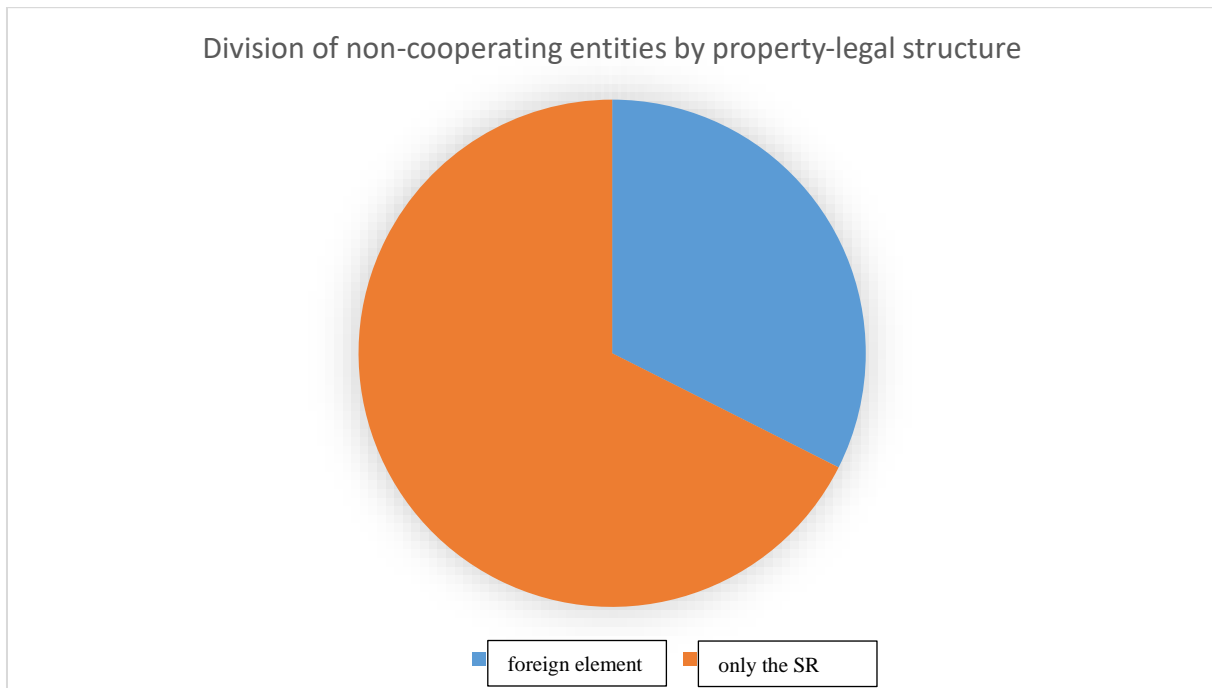
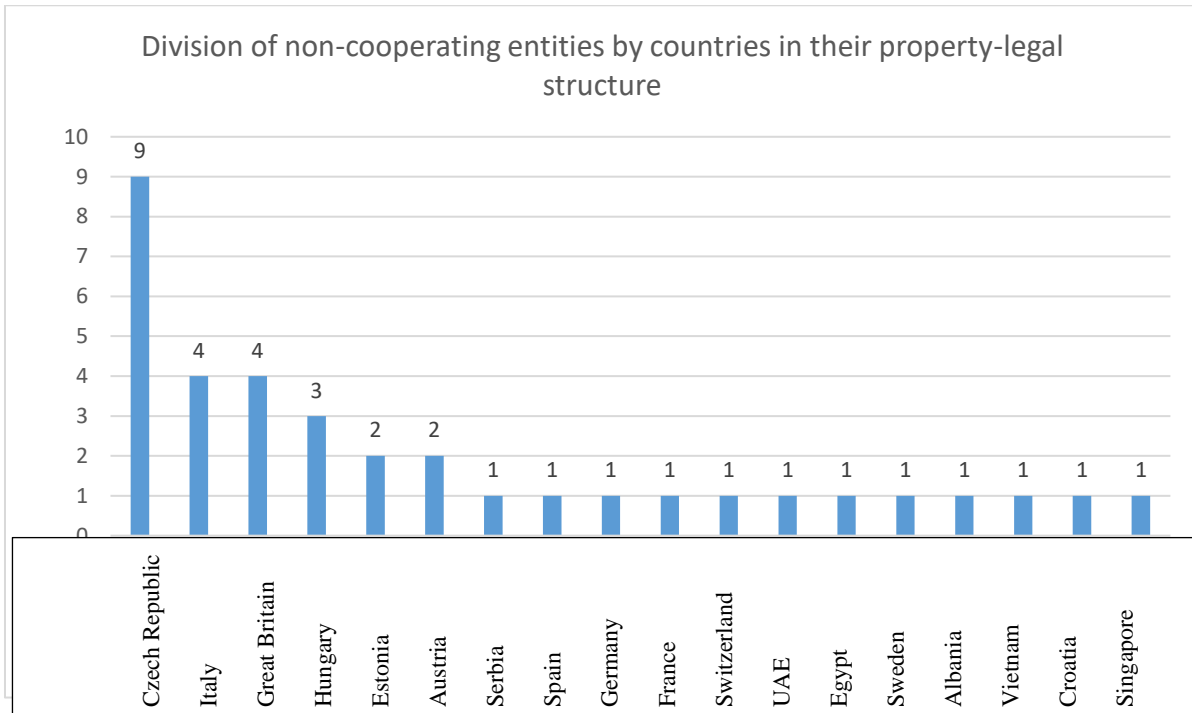


Chart No. 31



A check of the entities in the databases of the Financial Intelligence Unit recorded negative information for 21 entities. The negative information varied from suspected criminal activity, through economic offences to links to persons who are being prosecuted for serious criminal activity in the Slovak Republic. These relationships are mostly of a secondary nature and are not clearly demonstrable in the normal vetting process that is currently set up when establishing a company or registering the business object of providing virtual currency exchange services or providing virtual currency wallet services. At the same time, for 10 of these entities, a foreign element in the form of a foreign company or statutory body was detected.

A search of freely available sources documented, for 21 entities, links to websites (or information) that are related to virtual currency exchange or other investment or payment companies, or could be related to suspicious (fraudulent) activities on the Internet. Of these, three entities were found to have suspended websites.

At this point, it should be stressed that, despite the same percentage of entities for which the Financial Intelligence Unit has negative information and for which suspicious information has been traced on the internet, they are not identical groups of entities. The total number of entities that were registered in the Slovak Republic as of 30 June 2022 for the provision of virtual currency exchange or virtual currency wallet services and did not provide the Financial Intelligence Unit with cooperation in the sectoral risk assessment carried out in the form of a questionnaire, while additional checks on them revealed negative facts, represents the share of 32%.

Chart No. 32

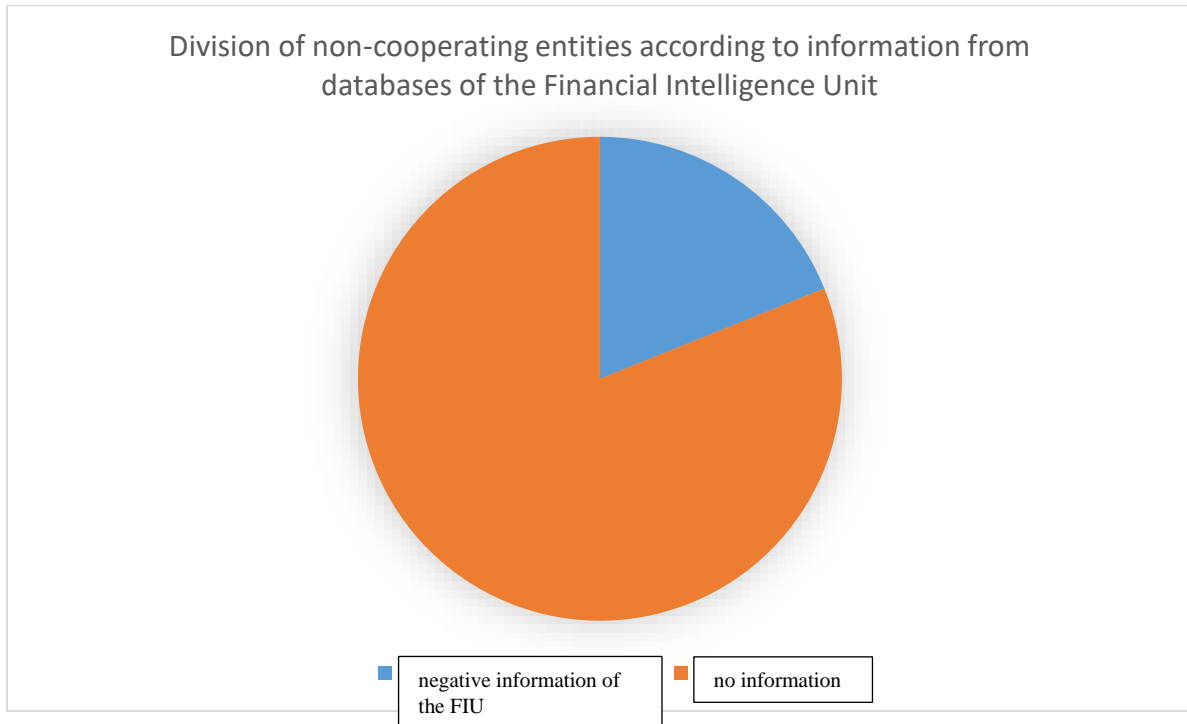
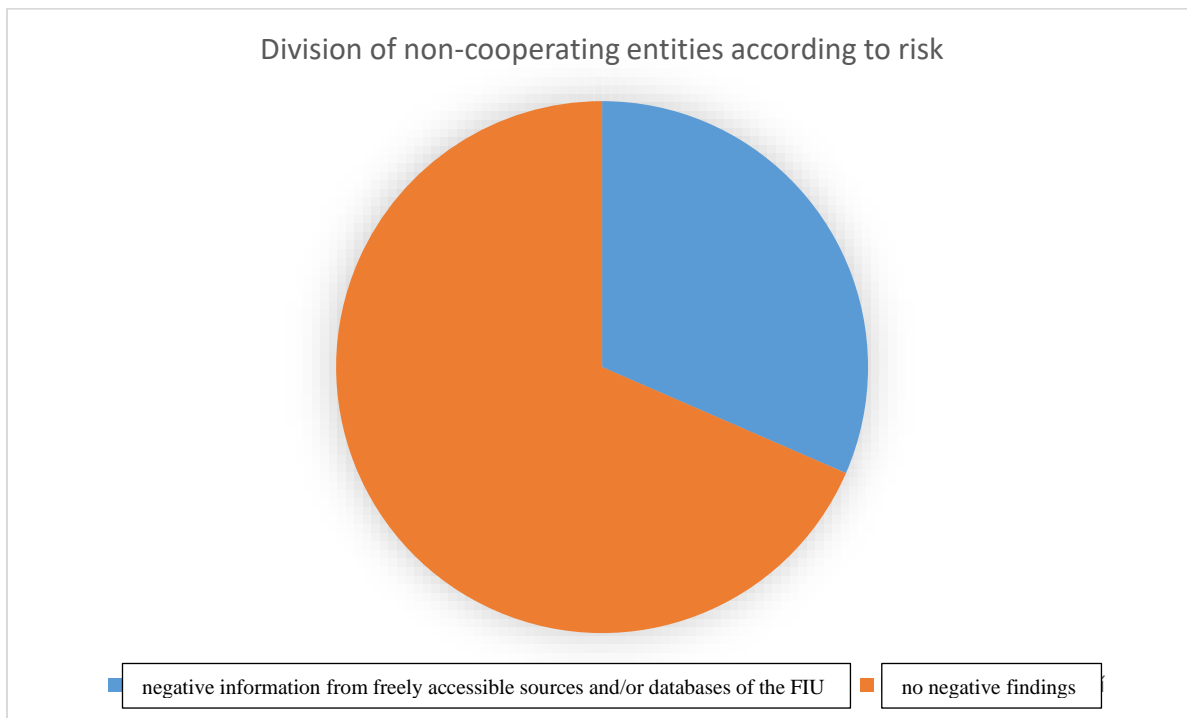


Chart No. 33



## 11. Conclusion of the questionnaire-analytical part of the VA/VASP sector

Influenced by the years marked by the pandemic, the entire financial sector has slowly but surely started to move into an online environment where national borders are blurring and AML/CFT supervision is becoming more challenging. This shift is noticeable both for entities established on the Slovak financial market and for newly emerging entities.

On the one hand, the rapid development and constant shift in the development of new technologically increasingly advanced tools allows the ordinary consumer to more easily manipulate and manage their finances, but on the other hand, it presents wide opportunities for criminals to conceal the criminal origin of funds, terrorist financing or commit other types of crimes.

Virtual currencies and virtual currency service providers represent a separate chapter within financial technology. These have certain specificities and, to some extent, bring new opportunities and advantages, as well as considerable transparency of transactions. However, the flip side of this is also the case, with rapid technological advances aimed at anonymising methods and technologies popular with fans of decentralised financial management, as well as with criminals.

Aware of the downsides of digital finance and virtual currencies, the Slovak Republic is slowly but surely trying to adapt to the new technologically more advanced environment of the financial sector. The complexity of individual processes in terms of finance, time and personnel combined with the progress that is growing day by day in the field of financial technologies, however, does not allow us to move forward at a pace that would be as efficient as possible and would help us cover the whole area. The steps that have been taken so far have mainly led to a familiarisation with the issue and to the identification of vulnerabilities, the gradual elimination of which will define the follow-up actions of the competent public authorities of the Slovak Republic in the coming period.

The analysis carried out in the framework of the evaluation of the responses received to the questionnaires distributed to the entities that had as of 30 June 2022 as their object of business registered the provision of virtual currency exchange or virtual currency wallet services, found that out of 340 responses received by the Financial Intelligence Unit, as many as 271 entities (approximately 80 %) indicated that they did not carry out the activity. Almost half of these respondents indicated that they had registered the activity of providing virtual currency exchange or virtual currency wallet services in the belief that this is a mandatory obligation if they wish to invest their funds, whether personal or from business, in virtual currency. These entities have real-world experience in purchasing and holding virtual currency for their own use and consider it a very safe and trustworthy means of return on investment or form of savings. They deal exclusively with their own funds and do not provide services to third parties. This fact together with other facts recorded in practice point to systemic shortcomings



in the registration process of business companies in the Slovak Republic, and shortcomings in the set-up of communication channels between the central government authorities and between the private and public sectors.

ATMs, which allow the deposit of funds without sufficient verification of their origin, represent a special chapter in defining the risk factors that new financial technologies bring in the context of potential money laundering. The risk is both deposit-taking ATMs introduced by banks and machines used to exchange cash for virtual currency (cryptocurrency ATMs). In the case of cryptocurrency ATMs, the potential risk of their use for the purpose of money laundering or terrorist financing is directly proportional to the possibilities of supervision and monitoring of these exchange instruments within the Slovak Republic.

## 12. The Slovak Republic and its approach to the issue of seizure of proceeds of crime

The General Prosecutor's Office of the Slovak Republic has been working on the issue of VA since 2016. On the basis of the knowledge gained from the European Union, the Council of Europe, the UN, the FATF and some states, the "Help for prosecutors on the issue of virtual currencies (especially Bitcoins)" was prepared in 2017 and updated at the end of September 2019. The next update is expected in 2023.

Based on the Irish experience shared within the ARO subgroup on virtual currencies, a leaflet - "Seizure of Virtual Proceeds of Crime" - Information for Law Enforcement Authorities - Identification of Bitcoin and other Virtual Currencies - was developed in cooperation between the Presidium of the Police Force and the General Prosecutor's Office of the Slovak Republic. This is available in paper format as well as in electronic format (for prosecutors on the prosecution Intranet).

The Prosecutor's Office participates in the activities of the European Judicial Cybercrime Network (EJCN), which was established in 2016. In and out of plenary meetings, the EJCN also cooperates with the private sector, including companies such as Chainalysis, Binance, Coinbase, etc. Specific issues related to virtual currencies are also presented by representatives of Europol (EC3). The EJCN also has a subgroup on virtual currencies which has developed a manual on the subject and at the same time organised two training events for representatives of judicial authorities in the EU on the issue of virtual assets in 2022. Prosecutors and judges are educated in this area within the framework of the activities of the Judicial Academy of the Slovak Republic, they also participate in international training events in this area (e.g. at the ILEA in Budapest, or training organised for Slovak prosecutors by the US authorities).

The General Prosecutor's Office of the Slovak Republic has long supported the introduction of the definition of virtual currency and the procedural institution of seizure of virtual currency into the legal order of the Slovak Republic. At the same time, it has participated in the development of legislation in this area.

### 12.1. Definition of virtual currency under the Criminal Code

According to the provisions of Article 131(7) of the Criminal Code, virtual currency is defined as follows:

"For the purposes of this Act, virtual currency means a digital medium of value that is neither issued nor guaranteed by a central bank or public authority, is not necessarily tied to legal tender, and does not have the legal status of currency or money, but is accepted by some persons as an instrument of exchange that can be electronically transferred, stored, or traded electronically".

## 12.2. Legal regulation of the virtual currency seizure process

The procedural procedure for the seizure of virtual currency is regulated in the provisions of Article 96d of the Code of Criminal Procedure as follows:

- 1) If the facts found indicate that the virtual currency is an instrument of criminal activity or proceeds of criminal activity, the presiding judge and in the pre-trial proceedings, the prosecutor may issue an order for the seizure of the virtual currency.
- 2) If the matter cannot be delayed, the prosecutor may also issue an order under paragraph 1 before the commencement of the criminal proceedings. Such an order must be confirmed by the pre-trial judge within 48 hours at the latest, otherwise it shall lose its validity.
- 3) The order under paragraphs 1 and 2 shall prohibit any disposition of virtual currency and shall order its surrender, including the surrender of the password, access code or similar data enabling the disposal of the virtual currency. Legal acts done in contravention of the prohibition under the preceding sentence shall be null and void.
- 4) The order shall be served without delay by the presiding judge and, in the pre-trial proceedings, by the prosecutor to the owner of the virtual currency or to the person who may reasonably be presumed to have access data to the virtual currency.
- 5) If the grounds for seizing the virtual currency have ceased to exist, the presiding judge, and, in the pre-trial proceedings, the prosecutor shall without delay order the revocation of the seizure of the virtual currency.
- 6) The order referred to in paragraphs 1 and 2 shall be in writing and shall state the grounds on which it is based. The order shall specify the address of the virtual currency repository of the authority which administers the seized property pursuant to a special regulation, the designation of the virtual currency and the number of units.
- 7) The owner of the virtual currency which has been seized or any other person from whom the virtual currency has been seized shall have the right to request that the seizure be revoked or limited. The presiding judge, and, in the pre-trial proceedings, the prosecutor shall decide on such an application without delay. A complaint may be lodged against that decision. If the application is refused, the owner of the virtual currency or any other person from whom the virtual currency has been seized may, unless they give other reasons, repeat it only after 30 days have elapsed from the date on which the decision on their previous application became final; otherwise it shall not be handled.

- 8) Where it is necessary in criminal proceedings to seize virtual currency to secure the victim's claim for damages, paragraphs 1 to 7 shall apply accordingly.

Prior to the adoption of the above-mentioned legislation, seizures were carried out on the basis of the provisions of Article 90 of the Code of Criminal Procedure (seizure of computer data).

In the context of the seizure activities, problems were identified in the transfer of virtual wallet assets from the police wallet to the wallet of the competent authority, which had not created one, and other problems were associated with the transfer, which were addressed at interministerial level.

The issue of virtual currencies/assets has been raised in various areas of crime, in particular ransomware, various forms of extortion, online fraud and, in particular, in cases of investment fraud.

The fact that virtual assets, as well as evidence, are primarily located with foreign VASPs places increased demands on prosecutors. A number of them do not have a physical seat, which makes it significantly more difficult to secure evidence as well as the eventual seizure of virtual currency.

Slovak legislation does not provide for direct cross-border contact between judicial authorities and private companies, and in cases where there is no physical seat of a VASP or where there is an avoidance of declaring a specific seat for the purposes of international judicial cooperation by the VASP, this causes difficulties in criminal proceedings. In the specific case, direct cooperation with Binance is being executed. This is a live case on which the General Prosecutor's Office cannot provide more information.

## 13. National Bank of Slovakia

The NBS does not currently regulate or supervise the VASP sector.

The information obtained is a combination of the results of a survey carried out in supervised entities and own expert knowledge, information and expertise in the VA/VASP area.

Based on the results of the survey of supervised entities within the financial market sectors, the entities' asset statements, and other information available to NBS, there is no information on record in the capital market and insurance sectors that would indicate that supervised entities in those sectors provide VASP services, have conducted VA transactions, or own VA assets.

The survey results indicate that VA/VASP -related activities were recorded in the banking and payment services sector.

The NBS notes that banks perceive the VASP sector as customers having higher to high risk. In the risk management process in relation to VASPs, they have identified specific ML/TF risks and have set AML/CFT measures in relation to them which can be considered as adequate. Banks that provide services to VASP customers are able to effectively mitigate the risks associated with these customers.

Banks that provide services to VASP customers have a very detailed understanding of the ML/TF risks arising from the business relationship with VASP. They apply a risk-based approach when providing services to these customers. In the context of providing VASP due diligence, they carry out a wider range of activities and measures compared to their approach to other customers. They also carry out more detailed transactional monitoring of VASP customers' transactions.

In particular, banks apply the following measures in the exercise of VASP customer due diligence:

- entering into a business relationship in the physical presence of persons acting on behalf of the VASP customer,
- designation of the VASP in the AML system in the "high risk" risk category,
- approval of the establishment of a business relationship with a VASP customer by the Compliance and AML department,
- conducting a thorough identification and verification of customer identification, taking action to verify information relating to the identification of the beneficial owner from multiple sources,
- the provision of VA services must be included in the objects of business of VASPs,
- a thorough review and verification of the ownership and management structure of the VASP,
- taking measures to establish the origin of the VASP's property and the origin of funds,

- ascertaining the origin of funds related to a specific transaction,
- they use a KYC questionnaire when entering into a business relationship, which contains questions specifically targeted at the VASP,
- they require detailed information on the future nature of the business relationship and the business model of the customers to ensure that they have obtained sufficient information on the nature and, in particular, the risks of VASP customers' business and also to ensure that they can effectively manage and mitigate the higher ML/TF risks associated with the VASP,
- during the course of the business relationship with VASP customers, banks carry out more detailed monitoring of transactions compared to other customers,
- they conduct enhanced transaction monitoring, especially for cryptocurrency-exchange-related transactions which they perceive as high risk.

From its survey of the banking sector, the NBS has identified in particular the following ML/TF risks identified at the time of entering into and throughout the duration of the business relationship with VASP customers:

- VASPs do not have adequate AML/CFT risk management systems in place, particularly in the area of identifying and verifying the identity of the customers to whom they provide services,
- insufficient identification/verification of the origin of funds used in VA transactions,
- high level of indicators supporting anonymity (VASP products, services),
- deficiencies in updating customer data,
- failure to check customers against sanctions lists and politically exposed persons list,
- risks related to cash operations (VASPs operating VA-ATMs make cash deposits from these devices into their payment account at the bank),
- difficulty in identifying the economic rationale for bulk transactions by VASPs,
- the unclear ownership structure of the beneficial owners of VASP customers.

The NBS has identified the following risks associated with the activities of customers operating in the VA/VASP sector from its survey of the payment services and electronic money sector:

- higher to high ML/TF risk,
- insufficient identification of customers and payments,
- risk of insufficient documentation (in connection with ICOs, insufficient token security),
- more difficult traceability of the origin of property for virtual assets (the possibility of multiple transfers, lower level of transparency),
- the possibility of anonymity (if the initial exchange was anonymous),
- inability to prevent the transfer of virtual assets to persons on the sanctions list and to jurisdictions with insufficient AML/CFT legislation,
- reputational risk (in terms of customers' failure to maintain integrity),
- cyber threats (exploiting loopholes/weaknesses in the financial system),
- de-risking by payment service providers in relation to VASP,

- lack of comprehensive regulation.

Supervised entities (banks and financial institutions) that have VASP customers in their portfolio have developed specific internal policies for the acceptance of VASP in relation to these customers, which are set up on the principle of a risk-based approach. Supervised entities exercise VASP customer enhanced due diligence. As a rule, the approval of the statutory body of the supervised entity is required to enter into a business relationship with a new VASP customer. Entities also use a number of independent and reliable sources of information to verify these customers (in particular their reputation, possible association with ML/TF risks, negative information from mass media, etc.).

In relation to VA/VASPs, the NBS has also reviewed consumer submissions to VA/VASP. Despite the fact that the NBS does not regulate or supervise the VA/VASP sector, consumers have contacted the NBS with negative experiences when buying/trading in/with VA/VASPs. However, the characteristics of the submissions do not indicate that they include AML risks. For the period 2021-2022, the NBS records 24 such submissions from consumers. Of that number, 12 of the submissions have some indication of VA fraud in their description, with the most common reason for a negative experience being that the consumer handed over their access codes to an intermediary during the actual VA purchase/trade, or the consumer contacted an unknown VASP whom they subsequently called fraudulent. Other submissions were related to consumers requesting verification of unknown VASPs or requesting technical assistance.

#### NBS Conclusions:

The NBS notes that the survey results, as well as the NBS's expert knowledge to date, have demonstrated that banks have an adequate understanding of the ML/TF risks associated with VASP customers and apply a risk-based approach to VASPs. Banks' cooperation with this clientele requires an increased demand on the staffing and professional capacity of banks' AML units. The scope of the measures taken by banks can be considered adequate at present.

It can also be concluded that the inherent risk to which supervised entities are exposed in relation to VASPs is adequately managed and mitigated by the entities' internal policies. The NBS considers that the residual risk in relation to VASP customers is the low level of awareness by the VASP community of AML/CFT obligations, particularly in the conduct of CDD in relation to its customers. In the near future, it will be necessary for the Slovak Republic to adopt a systemic framework of measures that will contribute to increasing VASP awareness of AML/CFT obligations (in particular education, training in the area of AML/CFT). At the same time, for the effective implementation of FATF Recommendation No. 15 in the AML/CFT system of the Slovak Republic, it will be necessary for VASPs to comply with the preventive measures (FATF R 10-R 21) and at the same time to adopt an effective system of AML/CFT control of VASPs.

## 14. Analytical part of the sectoral analysis

The Financial Intelligence Unit carefully perceives the growing trend of crypto adoption, not only at a global level but also at a local level. It is this global aspect of virtual assets that needs to be emphasised. Globality is their most costly and most native characteristic. Unlike other sectors, the virtual asset sector is the youngest, the least regulated and, thanks to its link with information technology, the most dynamic, not least the most flexible and the most responsive to any changes.

It is precisely these characteristics that have in most cases counteracted the traditional division between global and local in this sector. It is important to keep this in mind and view all aspects related to the crypto world at a global level. 99% of technology solutions are available to the majority of the population on this planet.

The societal acceptance of Bitcoin and the new technological horizons it brings with it, of course, create new types of crime and new opportunities for original crime types to use blockchain/virtual assets as one form of or channels for money laundering, terrorist financing or proliferation.

The speed and flexibility of the crypto world, unprecedented in the modern world, allows it to respond to any regulatory intervention in essentially the order of hours, days at most. An example can be the crypto world's response to regulatory intervention in the form of a ban on the Tornado.Cash mixer by the US OFAC in August 2022<sup>10</sup>. The reaction of the crypto community was almost immediate and the technological solution replacing the banned Tornado.Cash was available to users essentially within 24 hours.

---

<sup>10</sup> <https://home.treasury.gov/news/press-releases/jy0916>.



## 15. Taxation of proceeds from crypto-assets in Slovakia

The taxation of proceeds from crypto-assets in Slovakia is determined by Act No. 595/2003 Coll. on income tax, as amended, and amending certain acts - in connection with the change in the taxation of virtual assets.

The Slovak Republic introduced mandatory taxation of virtual assets only in 2018, in an amendment to Act No. 595/2003 Coll., as follows

- a) 19% if the annual income is up to EUR 37,981.94,
- b) 25% if the annual income is above EUR 37,981.94,
- c) 14% health insurance contributions.

The sale of virtual currency itself is defined in Act No. 595/2003 Coll., Article 2(ai) of the Income Tax Act as follows

- d) virtual currency sale shall mean
- e) exchange of virtual currency for property,
- f) exchange of virtual currency for another virtual currency,
- g) exchange of virtual currency for the provision of a service or transfer of virtual currency for consideration.

Since 1 January 2024, the new taxation has been applied at the following rate

- a) 19% in the case of income up to EUR 41,445.46,
- b) 25% if the annual income exceeds EUR 41,445.46,
- c) health insurance contribution 15%.

This taxation was one of the highest in the EU and often faced criticism from the professional community. The Financial Intelligence Unit has information that investors who made significant gains during the two significant growth periods in crypto markets in 2018 and 2020-2021 have often used tax optimisation structures, not only within the EU but also outside the EU, to minimise their tax burden. This trend highlights the need to rethink tax policy on virtual assets in order to promote fair and efficient tax regulation that takes into account the dynamic nature of these markets while stimulating innovation and growth in the sector. Extending legal and regulatory frameworks could help prevent tax avoidance while maintaining the competitiveness of the domestic market.

Some companies have even offered solutions directly on their websites to reduce tax using appropriate optimisation schemes.

The issue of taxation of cryptocurrencies is still in a developing phase in Slovakia and globally. Different countries, also within the EU, have adopted different tax arrangements in

relation to the taxation of crypto-assets. On one side of the spectrum we can find, for example, Malta, which is globally nicknamed “blockchain island”, where taxation varies between 15% and 35%, depending on the residency status of the payer,<sup>11</sup> or exotic or offshore, such as Panama, which has been used by several EU and Slovak citizens in order to optimise taxes. Panama has a very moderate tax policy, tax for companies is only of 10% and 0% for profits from taxes or capital gains.<sup>12</sup> A law is in the pipeline to apply the introduction of the tax.

Given the global spread of cryptocurrencies, tax authorities around the world face challenges in integrating them into existing tax systems. Cryptocurrencies bring new risks and obligations for investors, while their decentralised nature complicates the ability of tax authorities to collect tax revenue efficiently. With the increasing integration of cryptocurrencies into the global financial system, it will be important for regulators to adapt existing tax laws to reflect the unique characteristics and challenges that digital assets bring. This process will likely require international cooperation and innovation in tax approaches.

Table of tax revenues paid to the state budget:

Table No. 1

Year	Revenue from taxation of crypto (in thousands EUR)
2018	755
2019	451
2020	457
2021	4627
2022	645

Source: Internet

Based on the results of revenues from cryptocurrency profits paid to the Treasury, it can be assumed that there is a hypothetical relationship between the amount of taxation and the amount of taxes collected on cryptocurrencies, as in the case of the so-called Laffer curve.<sup>13</sup>

<sup>11</sup> <https://www.ccn.com/education/malta-crypto-tax-2023-everything-you-need-to-know/>.

<sup>12</sup> <https://fastoffshorelicenses.com/offshore-crypto-license/panama/>.

<sup>13</sup> <https://e-news.cz/nazory/ceta-lafferova-krivka-aneb-proc-nelze-dane-zvysovat-vecne/>.

## 16. Foreign FinTech companies and their overlap on the Slovak market of VASPs

The Slovak Republic, as an EU member state, has recently been enjoying the attention of the world's crypto professional community in a negative sense of the word. The primary reason for this is the absence of any oversight in the issuance of licences - in Slovakia it is just a form of registration by the Trade Register.

Certainty of granting a licence to do business in this segment (virtual assets), low cost, absence of a lengthy process as in other countries, no reporting requirements (except those under Article 5 of the AML Act, the introduction among obliged persons), the possibility to do business from a virtual seat and the possibility to register a company, to own a company as a foreign national are among the most frequently mentioned advantages of Slovakia as a suitable country for the registered office and activities of a VASP.

The absence of regulation and a separate licensing process with clearly defined complex requirements for the applicant and the resulting very easy access of domestic and especially foreign entities to the permit to do business in Slovakia in the segment of providing exchange and crypto wallet services leads to the fact that several foreign Fintech legal and consulting companies have begun to recommend Slovakia to their international clientele as a suitable place for the establishment and operation of a VASP.

Several countries and their regulators focus on the professional and work history of licence applicants, among other factors, in the licensing process. As part of the process, applicants' personal connections are also examined. This process is not carried out in Slovakia. The key requirements are age, completion of secondary education and the applicant must not have a criminal record.

Thanks to these facts, some foreign law Fintech firms are also focusing on the possibility to offer their customers turnkey solutions, which also allow for the staffing of the company through the so-called nominee - the installed director of the company and, if interested, the possibility of installing the shareholders of the company (in the case of a joint stock company) or the person of the partner/partners and the managing director/s in the case of a limited liability company.

The FIU has identified during its activities that a number of VASP entities in Slovakia have been established on purpose through foreign Fintech law firms and their local partners as a "turnkey" service. For a final price in the lower tens of thousands of EUR, the customer receives a complete turnkey solution along with the option to use local company staffing and an AML officer.

The simplicity of the process for setting up a VASP, the lack of mandatory due diligence on persons setting up a VASP, as in Germany for example, and the minimal or absent licensing

process, is perceived by the FIU as an extremely high risk for the establishment of schemes facilitating money laundering or terrorist financing.

The Slovak Republic is therefore increasingly promoted by foreign legal and B2B companies as an ideal location for their customers to do business in the crypto segment.

The simplicity of entity registration and very general definition of terms in its essence allows to create the so-called umbrella effect - covering by one company, one (or two, virtual wallet service provider and virtual exchange service provider) registered options, to cover the whole wide and very diverse possibilities that the crypto world provides, without the need to apply, pay and have additional permits (licences) for individual activities.

Fig. No. 12



Source: Website of a Fintech law consulting company

The photo above highlights just this simple opportunity to cover a wide and very diverse range of products and activities (e.g. NFT marketplace, ICO and ITO offerings, subscriptions, DeFi projects, FIAT to crypto conversions and vice versa) with a single registered trade in Slovakia, which is additionally called a licence and allows the entity to subsequently do business in the EU, on the global market, essentially without restrictions.

By comparison, in some countries, each single activity, set of activities is regulated separately and entities applying for a licence in a given segment have to apply for it separately, in an individual process, which of course increases the costs for the applicant and is also time consuming.

An equally important advantage for the establishment of a VASP in Slovakia is the possibility to nominate a managing director (director), a citizen of a European Economic Area country. Unlike in other countries, there are no specific requirements or criteria for the position of director.

In terms of AML/CFT issues, the ease of setting up a new company that can do business in the crypto segment is assessed as high risk in Slovakia and under a single market and unclear regulation, thus also in the EU. The absence of a licensing process, as mentioned several times in this sectoral analysis, leads to an unhealthy growth of the number of VASPs registered in Slovakia.

## 17. Definition of criminality

It is very important to be aware of the fact that criminality in connection with both modern technologies and crypto-assets is largely latent.

In Slovakia, law enforcement authorities are continuously focusing on improving their technological capacities for more efficient tracking of transactions on blockchain platforms. There is currently a strong focus on the development and integration of more sophisticated software solutions to enable better analysis and detection of illegal activities related to virtual assets. Although the process of introducing advanced technologies takes time, it is a key step towards increasing efficiency in detecting and preventing crime in the digital space.

As part of the sectoral analysis, the risks associated with crime latency in the crypto sector are quantified; they are caused mainly by the following factors:

- a) lack of regulation - due to the huge number of registered VASPs in the territory of the Slovak Republic and the absence of prudential supervision, it was and is very easy to get a permit to do business in this segment,
- b) non-fulfilment of obligations stipulated in the AML Act by VASPs - a number of entities do not consistently respect the status and obligations of an obliged person. In a number of cases, the Financial Intelligence Unit has imposed sanctions for non-compliance with the obligations under the AML Act,
- c) lack of technical and technological tools necessary for in-depth analysis and tracking of digital transactions - this stems from the absence of strategic infrastructure development, which takes time to implement and optimise within the supervisory authority, the absence of technical and technological tools.

## 18. Crypto community

The dynamism of cryptocurrencies is closely linked to the speed and agility of the crypto community, which often reacts to changes in the sector within hours or days. This rapid response reflects the adaptive and innovative nature of the community.

There is also a significant, though not numerous, group of adherents to so-called crypto-anarchism within the wider crypto world<sup>14</sup>. These groups promote maximum anonymity and seek to limit state control. Thanks to the growth of crypto-assets, these groups have powerful instruments at their disposal that act as internationally recognised values not issued by any state institution such as a central bank. These instruments are not under the control of any state authority and are created and developed by community participation.

In contrast, a much larger segment of the crypto community identifies with the original intent and meaning of cryptocurrencies, particularly Bitcoin. Bitcoin represents a form of electronic money that allows for flat and direct online transactions without the intervention of a financial institution on a peer-to-peer network<sup>15</sup>. The crypto community around the world returns to this original purpose and intended use. Sometimes with just a tinge of nostalgia, but sometimes with a proactive approach.

These two perspectives illustrate the diversity and dynamism of the crypto community that is constantly shaping the future of digital finance and defining new paradigms for the interactions between technology, economy and society. Each of these approaches contributes to the overall mosaic of the crypto ecosystem, ensuring its growth, adaptability and innovation.

---

<sup>14</sup> <https://paralelnapolis.sk/institut-kryptoanarchie/kryptoanarchisticke-manifesto/>.

<sup>15</sup> [https://blockchainslovakia.sk/wp-content/uploads/2018/06/bitcoin\\_whitepaper\\_sk.pdf](https://blockchainslovakia.sk/wp-content/uploads/2018/06/bitcoin_whitepaper_sk.pdf).

## 19.P2P in the crypto community

One such proactive approach in P2P is the Vexl.it application. Its meaning goes back to the original intent of cryptocurrencies and their use by the crypto community, or the community “without the right to transact freely we have no other rights”<sup>16</sup>, or as they say on their site: “Bitcoin has been in the hands of institutions for far too long. We want to make it accessible to everyone again.”<sup>16</sup> . .

The Vexl.it app itself claims to be a mobile app that provides its users with a simple, accessible and secure way to trade Bitcoin as intended - peer-2-peer and without KYC.

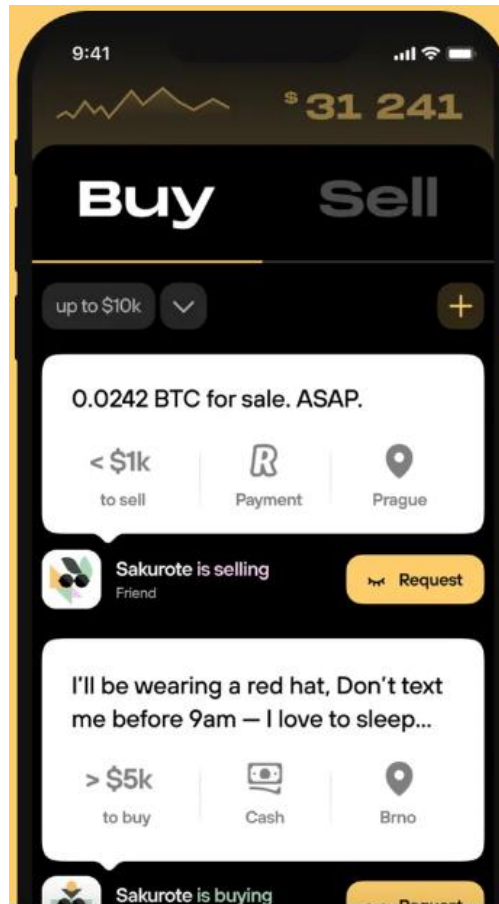
Its principle is based on an algorithm that, through phone numbers (first and second level contacts), a user-selected location, the trade value, the payment method preferred by the buyer/seller (FIAT currency bank transfer or cash, for example), finds a suitable counterparty or shows the selected circle an anonymised offer and, once a suitable offer is found, allows the person to contact the user via an online chat option to fine-tune the details. The app itself uses end - to - end encryption when chatting, so even the app operator does not have access to it. The app also allows you to delete the chat and then all conversations are irretrievably lost.

---

<sup>16</sup> <https://vexl.it/>.



Fig. No. 13



Source: website <https://vexl.it/>

An illustrative image from the Vexl.it website shows all the relevant details that are displayed to the buyer and filled in by the seller: the value of the deal, the way the transaction will be settled, the location and, finally, the contact request.

From an AML/CFT point of view, these are risky forms of converting crypto-assets into FIAT currency, where there are no KYC processes, no record of the conversion of each crypto-asset, no identification of the persons involved in the transaction or the origin of the funds. The fact that similar forms of conversion are carried out across borders or by foreign persons only increases the risk from an AML/CFT perspective.

The growth in the value of crypto-assets and the general increase in crypto adoption in recent years has led to a widespread acceptance of crypto-assets not only as payment instruments, but also as investment opportunities and, for a certain group of people, as store of value. This has created a demand for the possibility to exchange cash for crypto-assets instantly.

## 20. Communication tools in the crypto era

The development of crypto-assets and their adoption is inseparably linked to the development of the internet as a communication channel. On 11 February 2009, Satoshi Nakamoto presented a Bitcoin white paper at the P2P Foundation discussion forum.<sup>17</sup> The static forms of discussion forums have changed into the dynamic communication applications of modern times, such as WhatsApp, Signal or Telegram. The latter in particular enjoys great popularity in the crypto community due to its protectionist approach to user data and the reluctance of its creators to share it with law enforcement authorities anywhere in the world.

On the one hand, Telegram itself declares its willingness to cooperate with individual law enforcement authorities directly in its terms of use, where it specifies that it can reveal the user's IP address or phone number, but on the other hand, in the very next sentence, it adds or emphasises the information that it has never done so.

Photograph of Telegram's user terms and conditions, point 8.3 - cooperation with law enforcement authorities

Fig. No. 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>.

Source: <https://telegram.org/privacy>, 22 August 2023

It is because of this Telegram policy, which strongly supports anonymity and the protection of user data, that Telegram is held in great popularity by the crypto community worldwide. The Slovak crypto community is of course no exception and applies this trend to the fullest extent. Various channels dealing with issues related to cryptocurrencies often extend at least across borders and are often linked to Czech-Slovak communities and channels.

One of the trends is the use of this application and the channels operating on it to connect between various persons who offer an anonymous way to exchange cash for crypto-assets and vice versa. These individuals rely heavily on the app's strong encryption and its reluctance to release user data to anyone, including law enforcement authorities.

From an AML/CFT perspective, these forms of transfers and conversions of funds for crypto-assets, and vice versa, are extremely risky. As there is no record of them, there are no KYC processes and these conversions can be cross-border without any restrictions, it is possible to use these schemes to launder money or finance terrorism. An equally serious issue may be the use of these schemes to circumvent the trade sanctions imposed on the Russian Federation and its citizens following the launch of the invasion of Ukraine in 2022.

---

<sup>17</sup> <https://news.bitcoin.com/13-years-ago-today-satoshi-nakamoto-published-the-first-forum-post-introducing-bitcoin/>.

The Telegram app is often associated with the fact that it is used by various radical groups around the world due to its protectionist policies. In 2023, a Brazilian court ruled to ban the app in Brazilian territory due to lack of cooperation with Brazilian law enforcement authorities.<sup>18</sup> However, other countries around the world are also applying restrictive policies.<sup>19</sup>

---

<sup>18</sup> <https://www.nytimes.com/2023/04/26/briefing/brazil-telegram-ban.html>.

<sup>19</sup> <https://restoreprivacy.com/telegram-sharing-user-data/>.

## 21.ATS / Bots

Last but not least, the advantage of Telegram in terms of the crypto community is the fact that it allows connection to so-called trading bots.

Trading bots (on Telegram) are small automated programmes that can be implemented in Telegram, allow connectivity, most often to decentralised exchanges, and execute trade orders based on predefined criteria. This trend is rapidly increasing. Thanks to the fact that they are not yet constrained by any regulation, their number and, above all, their possibilities are enormous.

In terms of bot functionality, the most common features that are emerging are those aimed at

- a) Stop Loss / Take Profit - execution of orders associated with the termination of trading when the desired threshold is reached in the case of a profit, or a pre-set loss threshold in the case of a drop in value,
- b) Anti Rug-Pull Detection - prevention of rug-pull by the developer, in case the bot detects such something, it immediately tries to execute a sell order,
- c) Copy Trading - the user can choose to track a certain wallet and the movements on it (selling and buying certain tokens) are then copied to their account.

From a technical point of view there are basically no limitations, anything can be programmed as a bot algorithm and it is able to do it many times in extremely short time (the order of milliseconds).

Different bots can be encountered on low-liquidity small new tokens, with some crypto users deploying so-called Front Running Bots.

Front Running Bots are a type of software that aims to exploit latency in the blockchain. In doing so, it aims at trying to detect a large order (its size can be specified by the creator of the bot or set by the user using the software). Although Slovak legislation does not regulate the use of these bots, in the international context, or especially in developed countries, this method is considered insider trading - in the Slovak equivalent, the misuse of information in business dealings, which is a criminal offence.

The Financial Intelligence Unit points to the need to legislate and expand the issue of crypto-asset trading, not just regulation focused on the services of providers.

## 22.A.I.

Continuous developments in the field of technology and information technology allow for the systematic interconnection of different scientific and technical sectors. In the virtual asset sector, which is very young and dynamic by nature, the integration of technologies based on Artificial Intelligence (hereinafter referred to as “A.I.”) appears. The initial implementation of A.I. in this sector signals the beginning of a new era in the provision of virtual asset services.

The development of A.I. in a broader context is itself taking place in these years. The initial impetus for the public was the release of Chat GPT to the U.S. non-profit organisation Open A.I. in November 2022. Already during the first months there was a real boom of this technology and now the number of accesses per month exceeds 1.5 billion.<sup>20</sup>

In the first months, the number of interactions for registered users was limited and already in February 2023, a subscription version of ChatGPT Plus was introduced, for a monthly fee of USD 20 per month.<sup>21</sup> This package includes priority access to ChatGPT features, accelerated response time to questions asked, and access to news and edits before regular users. The world’s largest technology companies from the FAANG cluster<sup>22</sup> immediately responded to this new trend and implemented this type of technology in their solutions. In the case of Microsoft, this is the case of Office 365 and its A.I. superstructure called Copilot.<sup>23</sup>

But on the basis of the development of A.I. itself, its various other superstructures are also being developed. One of the most important and currently the most used is the so-called Large Language Model, known by the acronym LLM.

### 22.1. LLM

Large Language Model is a type of module that is based on machine learning<sup>24</sup> and can use statistical models to process large amounts of data, learn patterns between words and individual phrases used in supported languages<sup>25</sup>. To support their development and the learning process itself, it is important to “feed” this language module with as much data as possible, covering a large number of words, sentences, phrases, and a variety of words. The more data available to the module, the better it can generate new content.<sup>25</sup> Once a language module contains sufficient data, the creator or user can specify the conditions and parameters of the output content to be generated by the module.<sup>25</sup> These modules can also be used by other services and applications.<sup>25</sup>

The extremely dynamic development of A.I. and related technologies has come to the attention of national security forces, their regulators and, of course, the criminal environment.

---

<sup>20</sup> <https://www.similarweb.com/website/chat.openai.com/#overview>.

<sup>21</sup> <https://openai.com/blog/chatgpt-plus>.

<sup>22</sup> Facebook (now Meta), Amazon, Apple, Netflix, Google (now Alphabet).

<sup>23</sup> <https://blogs.microsoft.com/blog/2023/03/16/introducing-microsoft-365-copilot-your-copilot-for-work/>.

<sup>24</sup> <https://www.techopedia.com/definition/34948/large-language-model-llm>.

<sup>25</sup> <https://www.boost.ai/blog/llms-large-language-models>.

One of the first reactions was the temporary banning of the ChatBot GPT module from the American company Open A.I. by the Italian authorities.<sup>26</sup> One of the factors that the Italian authorities considered high-risk was their suspicion of violating privacy regulations.<sup>26</sup> In this case, the regulator referred to a security hole that allowed users to see the topics of other users' conversations.<sup>26</sup> Currently, regulation on A.I. is primarily being developed in the USA, China, and, of course, the EU, with each of these regions taking a rather different view of the issues and the key problems associated with artificial intelligence.<sup>27</sup>

## 22.2. A.I. and Europol

The issue of A.I. is, of course, also being addressed by law enforcement authorities, EUROPOL has published a short piece on its website which seeks to reveal the impact of A.I. on the criminal environment. Available at the following link:

<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 excels at providing the user with ready-to-use information in response to a wide range of stimuli. If a potential criminal knows nothing about a particular crime area, ChatGPT can greatly accelerate the research process by offering key information that can then be explored in the next steps. As such ChatGPT can be used to obtain information on a huge range of areas of potential crime without prior knowledge, ranging from how to break into a house, to terrorism, cybercrime and child sexual abuse. The identified use cases that emerged from Europol's workshops with experts are by no means exhaustive. Rather, the aim is to give an idea of how diverse and potentially dangerous LLMs like ChatGPT can be in the wrong hands. While all the information that ChatGPT provides is freely available on the internet, the ability to use the module to provide specific actions by asking contextual questions means that it is significantly easier for the criminal element to better understand and subsequently commit different types of crime.<sup>28</sup>

---

<sup>26</sup> <https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html>.

<sup>27</sup> <https://www.euronews.com/2023/05/23/what-can-the-eu-learn-from-chinas-generative-ai-regulation-before-it-adopts-its-ai-act>.

<sup>28</sup> <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>.

### 22.3. Deepfake

One of the latest trends with the biggest security threats, not only in terms of AML/CFT issues, but also in terms of security, is undoubtedly Deepfake. Deepfake branding was created by combining deep learning and fake and has its origins in the pornography industry.<sup>29</sup> Artificial intelligence and video, and more recently live streaming through programmes, allows photos and images to be combined, resulting in a final image of person A with a face and, most advanced, also voice of person X. This process can be used, for example, to elicit sensitive information from various individuals as well as legal entities. The aim may be to access data and information related to financial resources, bank login details or crypto seeds. An example is a recent deepfake call from a person pretending to be the CEO of a company and another one who presented themselves as a lawyer. The goal was to fraudulently elicit information about the company's finances.

More about the case at the following web link: <https://domov.sme.sk/c/23205010/umela-inteligencia-deep-fake-video-banky-slovensko.html?ref=njctse>.

However, the Financial Intelligence Unit also sees positive trends in the use of A.I. technology in the fight against money laundering and terrorist financing. One of the positive trends is the beginning of the use of artificial intelligence in segments demanding the processing of large amounts of data in a short time and at high speed.

### 22.4. Control of smart contracts through A.I.

In the cryptocurrency segment, such demanding data are, for example, the source codes of smart contracts.

A smart contract is a programme stored on a blockchain network, which executes automatically when the pre-defined terms and conditions are met. In a decentralised system, two parties can interact by replacing the intermediary that is usually needed to facilitate transactions, using a smart contract. Blockchains, including the Bitcoin network and Ethereum, use smart contracts to facilitate transactions and automate processes.<sup>30</sup> What makes smart contracts “smart”? These pieces of code automate processes and don't make human errors, ultimately reducing the time and cost associated with traditional contracts. In addition to overcoming human error, smart contracts have other advantages that make them important to the blockchain industry.<sup>30</sup>

Smart contracts determine exactly what will happen if a condition occurs. Because they are complex source texts, they are demanding in terms of the amount of data they contain. But at

---

<sup>29</sup> <https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise>.

<sup>30</sup> <https://www.binance.com/sk/blog/nft/v%C5%A1etko-%C4%8Dopotrebujete-vedie%C5%A5-o-smart-kontraktoch-nft-568745413587703085>.

the same time, any function must also be implemented with the execution conditions directly into the source code.

The figure shows the result of a smart contract scan using A.I. technology, the red boxes indicate possible threats with explanations.

Fig. No. 15



Source: <https://guardiannn.ai/bsc/token/0xcbb008773ebef8c527fc33a4382659b13c9e73f70>

A.I. checks the entire source code of an issue or smart contract in units of seconds and targets threats implemented in the source code. However, an implemented part of the source code does not necessarily mean that the project is a fraud. Therefore, A.I. only alerts about its presence, the actual buying/selling decision is left to the user, in the spirit of one of the key slogans of the DYOR crypto community - “Do Your Own Research”. It is therefore a precautionary type of scan, which aims to detect potential risks, such as scams in various forms (see the part on the possibilities of scams in ICOs in this sector analysis).

The disadvantage of A.I. is the fact that in order to learn a new scamming technique, the fraudulent or illegal features of that particular smart contract have to be fulfilled. Subsequently, A.I. can learn and then predict the threat based on data and behaviour patterns (e.g., token transfers, trading shutdowns, liquidity traps, proxies, and various others).

Another very interesting trend, especially in the compliance or control area, is the experimental deployment of artificial intelligence modules on decentralised exchanges. In the experimental phases that are currently underway, members of the community are trying to consolidate and then “feed” A.I. as much as possible with information and patterns associated with risky or explicitly illegal uses of cryptocurrencies, most commonly associated with the



purchase of illegal material such as child pornography or dark market purchases, support for extremist groups, and various others.

Last but not least, various forms of A.I. are also being tested and implemented in law enforcement authorities around the world. The Financial Intelligence Unit has information on countries for which A.I. has made them more efficient and enabled more sophisticated and faster execution of tasks.

The issue of A.I. development and deployment is one of the key aspects of the fight against money laundering in the crypto-assets sector and the Financial Intelligence Unit stresses the need to monitor this segment and to promote the deployment of this type of technology by law enforcement authorities in Slovakia in the future.

## 23. CEX vs DEX vs DEX Aggregator

In compiling its analysis of the VA/VASP sector, the Financial Intelligence Unit focused not only on the issue of centralised exchanges (CEX), but also, as part of its comprehensive data collection, on decentralised exchanges that are often used for cross-chain trading, decentralised autonomous organisations (DAOs), and advanced regulation in some parts of the world focused on the possibility of using blockchain technology in government, for example, in the establishment and management of companies. It is important to bear in mind the complexity of the issue and to quantify the risks associated not only with the conversion but also with the transaction itself.

In the issue of VASP and quantifying the threats, we also need to focus on the different main types of exchanges that enable the conversion or trading in crypto-assets.

### 23.1. CEX

CEX - Centralised Exchanges is a platform that allows you to exchange crypto for crypto and in addition to that, compared to DEXs, also buy/sell/exchange FIAT currency for crypto. Unlike DEXs, CEX exchanges must always take the form of a legal entity and the associated regulation.

In terms of AML regulation, for legal or natural persons that provide virtual currency wallet and virtual currency exchange services, the AML Act regulates their classification as obliged persons. The following are the conditions for fulfilling the definition of an obliged person under Article 5(1)(o) and (p) of the AML Act

- a) the relevant trade licence under the Trade Licensing Act,
- b) the provision of virtual currency exchange or virtual currency wallet services to customers as the object of the business activity.

The management of one's own assets is not considered to be the exercise of a business activity if it does not involve the exercise of a business activity.

Pursuant to Article 26(2c) and Article 29 of the AML Act, the control of the fulfilment and observance of the obligations of obliged persons under the Act is carried out by the Financial Intelligence Unit, which is the central national unit in the field of prevention and detection of money laundering and terrorist financing.

One of the primary essentials of crypto-assets, besides their decentralisation, their speed, is their globality. By globality we can understand the fact that basically anyone who owns a crypto wallet and has access to the internet can make a transaction, which will be executed (depending on the set fees in the case of BTC) essentially instantaneously. But we can also

understand by the term global that any crypto-user is not bound to a predetermined geographic location<sup>31</sup>.

Because of this global nature, it is natural for crypto users around the world to seek out offerings and services that suit their needs. The number of exchanges, whether DEX or CEX, is large, their service offerings diverse, and new exchanges and new services offered by them are continuously emerging.

Due to the global nature of crypto-assets, the regulatory approach is also very different. Due to continuous pressure from large regulators, especially in Western Europe, SEA and the US, mandatory KYC processes have been introduced for opening and verifying new accounts. On the other hand, it is important to stress that not all jurisdictions follow these trends. They have different views on AML issues and allow, under the supervision of their regulator, the establishment of VASPs that offer a so-called Non-KYC option for customers, where they do not require identification documents from their users to verify their account.

### 23.1. Non-KYC exchanges

Non-KYC exchanges themselves are also evolving and tend to offer several types of accounts for their customers, very often also divided according to the customer's willingness to accept the KYC process.

For unverified customers, certain limits or restrictions are often put in place. They most often take the form of a limit on withdrawals above/up to a certain amount for a specific, well-defined period of time. In practice, such a restriction for an unverified account takes the form of, for example, withdrawing funds up to 5 BTC / equivalent in another cryptocurrency, once every 24 hours.

Other CEX exchanges, on the other hand, have restrictions in place for unverified customers in the form of limited access to the services offered. Most often, in addition to the restrictions concerning the amount of funds withdrawn, it is also limited access to leveraged trades or derivatives.

Non-KYC exchanges are often reluctant to recruit customers from certain areas because they do not want to get into trouble with certain authorities. The most common example is restrictions on recruiting customers from the USA. However, as there is no KYC process in place, the only way such an exchange defends itself against customers from this area is by imposing restrictions based on IP addresses. It is very easy to show how weak this form of protection is by looking at the ability to purchase a VPN and use another country's IP address to access these services for any citizen (person) from almost any country.

---

<sup>31</sup> Of course, we can consider as an exception those countries that, at the time of writing this sector analysis, have in place restrictive measures on the purchase, sale and possession of crypto-assets, such as China, India. China not only has restrictive measures against crypto-assets, but also regulates the internet access.

The special kind are some specialised exchanges/traders where trading is carried out through an app, not a website. An example is an app that allows you to convert BTC to FIAT, with no restriction from the exchange, just a restriction from investor demand. The app reportedly does not collect any relevant data on users and does not require any form of verification of the customer and their account or the origin of the funds.

In addition to FIAT currencies, it also allows trading/conversion between cryptocurrencies themselves. In particular, trades associated with so-called Dark Coins - anonymous currencies, which are primarily aimed at not revealing the owners of the wallet and the transfer itself, must be considered high-risk. Because of these native characteristics of anonymous cryptocurrencies, it is almost impossible to trace them. The app states on its site that the cryptocurrency Monero and its market is among its largest.

All of these types pose a significant risk in the potential process of money laundering or terrorist financing, given the ability to trade crypto-assets without any process of verification of the origin of funds or without due diligence by the exchange against the person.

## 23.2. DEX

DEX - Decentralised Exchanges: this type of exchange is growing in popularity among users worldwide and is, at its core, the original intended way of trading crypto. With the increasing adoption of crypto, the popularity of these exchanges is also increasing. This is clearly supported by the two previous bull runs - bull market periods in 2018 and 2021 respectively. These bull market periods have had a significant impact on the amount of funds currently in the market.

Compared to CEX, the DEX processes transactions through smart contracts, peer-to-peer, or through a liquidity provider (LP). The transactions themselves are significantly more economically advantageous for users due to much lower fees (at the time of writing this analysis, they are around 0.13% of the transaction size).

Unlike CEX, the DEX does not allow trading in so-called FIAT currency (currencies issued by central banks or other state institutions) and only supports trading crypto for crypto. It may or may not be true for DEXs that they can only offer coins on one network. A number of DEXs already support bridging between networks and therefore inter-network trading.

DEX exchanges, unlike CEX exchanges, have no control over customer' funds; the customer logs into the DEX only through their private wallet and owns the private key to it. According to AML/CFT it is very difficult or almost impossible to identify a wallet with any particular person.

DEX exchanges do not hold any customer information (personal data), do not require any documents from the customer to perform KYC, no AML due diligence. Login to DEX is done through a non-custodial wallet and all transactions take place on the blockchain, making them

transparent and traceable, but also anonymous in terms of traditional identifiers such as name, date of birth, residence, nationality, origin of funds.

### 23.3. DEX Aggregator

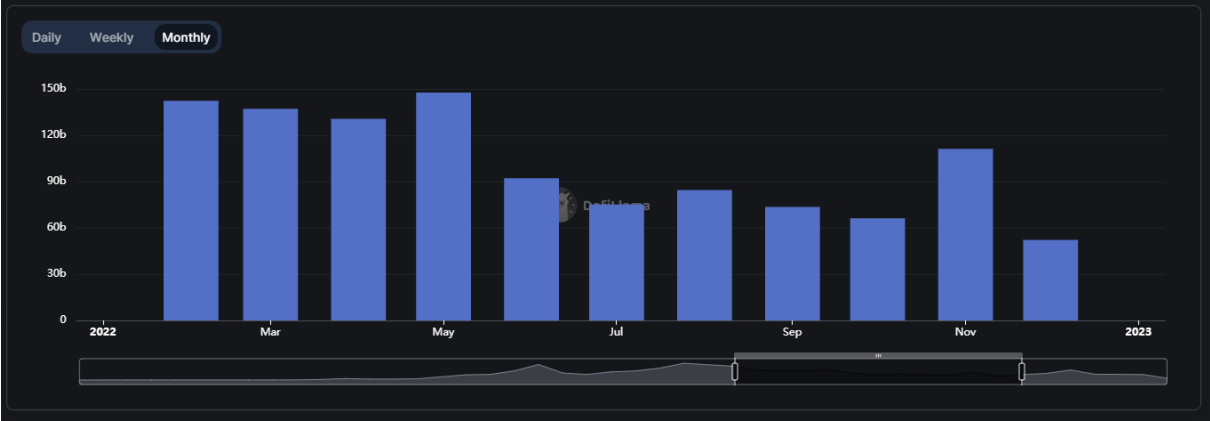
Recently, DEX aggregators, which operate on the principle of aggregation (grouping or accumulation) of offers of individual virtual assets traded on individual DEXs, have been gaining popularity. DEX aggregators offer, or try to offer, their users access to the best price and the greatest liquidity of a particular virtual asset. They also support the ability to split trades between multiple exchanges in order to provide the trader with the best possible price available.

With the growth of crypto adoption between 2017 and 2020 (see next), the pressure from regulators to introduce oversight tools on AML/CFT issues by exchanges has continuously increased.

Since 2020, when all major exchanges have started to introduce or have introduced oversight tools, the crypto community has responded with the development and massive popularisation of decentralised exchanges.

The following chart describes the individual monthly transactions executed on the decentralised exchanges in 2022, when the total volume of trades amounted to more than USD 1,100 billion.<sup>32</sup>

Fig. No. 16 Volume of trades: USD 1,100 billion for 2022



Source: <https://defillama.com/dexs>

Decentralised exchanges are a significant recent trend and a response by the crypto community to pressure from regulators to enforce mandatory KYC processes in centralised exchanges and oversight of AML/CFT issues by individual exchanges.

The absence of any customer verification process, the lack of a KYC process, or oversight on AML/CFT issues makes them very difficult to monitor and high-risk platforms for law enforcement authorities. Their ability to identify a wallet with the particular person is only

<sup>32</sup> <https://www.elliptic.co/blog/money-laundering-through-dexs-and-mixers>.

minimal and therefore in the future a technology solution will need to be purchased to enable blockchain tracking. Equally important will be international cooperation to regularly create and update wallets and addresses suspected of infringing activity.

#### 23.4. DEX & A.I.

The latest trend of the last months of 2022 is the making of advanced artificial-intelligence (AI) chatbot technology available to the public. After the initial enthusiasm, national efforts to open up the issue of A.I. regulation have begun to emerge, with Italy even moving to temporarily ban Chat GPT in April 2023<sup>33</sup>. The issue of A.I and its abuse for criminal cases is also addressed in a EUROPOL study available at the following link:

[www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf](http://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf)

Artificial intelligence technology also brings new opportunities related to ML/TF prevention, particularly in the VA and VASP markets. First information is emerging about the use of A.I. for the purpose of creating and then testing A.I. as a Compliance / AML / CFT module for some DEX exchanges. Pilot phases were started with smaller exchanges a few days ago and it will be important to monitor this trend. DEX exchanges themselves due to lack of due diligence, KYC implementation and other processes are rated as high risk in terms of AML/CFT.

---

<sup>33</sup> <https://www.cnn.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html>.

## 24. TradFi and DeFi convergence

Since its inception, developments in the crypto-asset market have been looking for technical and technological ways to connect the world of decentralised finance (DeFi) and the traditional world of finance (TradFi).

Until now, the concepts of DeFi and TradFi have been taken as two oppositional directions, each representing one evolutionary stage of the financial world. With the development of the blockchain, the increase in crypto adoption among users worldwide, the growth of the market capitalisation of crypto-assets in 2018 and 2020, the relevance of DeFi has also been growing. One of the directions of the crypto community development declared an effort to connect the traditional financial world and the world of DeFi.

The initial development, but not yet a literal link, was that several global brokerages started to add the ability to trade crypto-assets to their service portfolio. Examples include Saxo Bank, Interactive Brokers, eToro and various other international trading platforms.

Particularly large growth in the number of trading accounts and the value of the market capitalisation of crypto-assets is associated with the period during the coronavirus pandemic in the world. This trend is further amplified with the entry of the new Generation Z into the workforce and its relationship to innovation.

Last but not least, this development is linked to the so-called gamification of investing. The gamification of investing is linked to the development of the applications used to place the trading orders of a given broker. Gamification itself is most closely associated with the development of the American application or trading platform Robin Hood<sup>34</sup>, which was one of the first to focus more on making the process of investing more attractive to users by using the game method.

All of the above factors have had a positive impact on crypto adoption, whether in the form of the availability of buying cryptocurrencies in a user-friendly interface, trendiness within a generation, or purchasing as a game or experience for the user.

With the development of crypto adoption, and subsequently DeFi, came initial attempts to link DeFi and TradFi in various forms. TradFi can be thought of as an older sibling in terms of crypto-assets, which has influenced DeFi to a large extent.

Key elements of TradFi:

- it relies on a centralised system of authorities (regulators and supervisors),
- it is reachable by all persons who meet certain requirements or criteria (age, account opening, proof of origin of assets, agreement to trading conditions),

---

<sup>34</sup> <https://openiazoch.zoznam.sk/cl/223740/Inovacie-a-regulacia-Ked-je-obchodovanie-s-akciami-jednoduche-ako-hra/>.

- it is more user-safe in terms of central authorities and clearly defined processes overseeing the activities of entities and the rights of users.

#### Key elements of DeFi:

- it eliminates the presence of intermediary entities (e.g. a bank) as part of the chain necessary to execute the order,
- it guarantees access to anyone who has access to the internet and owns a wallet (hardware, such as Trezor, or software, such as MetaMusk),
- globality and immediate transaction execution - thanks to the absence of an intermediary and the globality of cryptocurrencies, each response is executed within units of seconds/minutes (only exceptionally longer, depending on the network on which the transaction is to be executed),
- peer-to-peer transactions - transactions between two peers, without the presence and need for an intermediary or oversight/supervision by a centralised institution,
- openness and transparency - public and transparent nature of the blockchain and its transactions.

The seemingly different worlds of TradFi and DeFi are gradually converging and complementing each other more and more, and to some extent even copying each other, see the different kinds of derivatives built on crypto-assets.

The latest trend is the penetration of the use of crypto-assets to buy traditional financial instruments. This process of tokenisation of assets such as stocks, financial derivatives (most commonly mentioned futures and options) and real estate is the next step for institutions in crypto adoption.

However, there are currently major uncertainties associated with this process, especially in the area of regulation and regulatory-licensing requirements by supervisory authorities. It is probably only a matter of time before this trend becomes more widespread and a similar pattern is replicated by other decentralised exchanges.

Leveraged tokens, which can be purchased on the Binance exchange, can be considered as a certain example of a fusion between TradFi and DeFi in terms of linking the capabilities of a financial derivative and the characteristics of a cryptocurrency in terms of tokenisation.

From a technical point of view, we can look at them as a “basket” of open positions of perpetual futures (derivatives) that are tokenised with leverage. The futures themselves reflect the prices of the underlying asset, in this case cryptocurrencies. It is important to note that there is a significantly higher risk of loss (but also profit) associated with this type of token than their underlying asset, which is of course due to the native leverage feature embedded in these tokens.



Quantifying the AML/CFT threats arising from this TradFin and DeFi linkage is very challenging. On the one hand, there is the complexity associated with the technologies required to route crypto-asset transfers on individual networks. On the other hand, there is a heavily regulated market for trading assets such as stocks and financial derivatives, with clearly defined rules and supervisory authorities.

In the event that individual law enforcement authorities (we can say that globally) do not have the technological solutions needed to route crypto-assets, international criminal organisations or terrorist groups could in the future create sophisticated schemes through instruments that link TradFi and DeFi for money laundering and terrorist financing. It is therefore necessary to monitor this trend from the outset and to keep a very close eye on the development of regulation in other countries in this segment.

## 25.DAO

The term DAO - Decentralised Autonomous Organisation - is a type of organisation that is run or operates without central authority, oversight or supervision, and many times without a clearly defined management structure. They are based entirely on blockchain technology and use smart contracts to operate. It should be stressed that the very concept of DAO is currently evolving dynamically and is not clearly established in the crypto world itself. From a legal point of view, they are not legal entities and operate exclusively in the online world, more specifically on the blockchain.

DAOs rely on the native properties of blockchains to operate, such as:

- 1) decentralisation - there is no specific person or institution that makes decisions, but decisions are most often made collectively, often on the basis of voting by its members/participants,
- 2) transparency - all decisions and transactions are visible to all other members due to the transparency of blockchain technology,
- 3) community - the priority of web3 technology solutions is community participation in the development, research and subsequent implementation of innovations into the system,
- 4) membership support - various supports for members and the participating part of the community to encourage development, increase the membership base and put into practice as many innovations as possible.

In some discussions in professional circles there are theories that the DAO itself does not need legal protection in law, because the source code itself clearly defines its functionality and capabilities, and therefore the idea of “Code is Law” is promulgated.<sup>35</sup>

It is very difficult to classify the local affiliation of a DAO, due to its decentralisation, lack of legal form and often anonymous network of founders. This makes the idea of some kind of regulation very difficult to implement at the moment.

### 25.1. DAOs in the world

Examples of exceptions, where the establishment of a legal form of DAOs has been based on a court decision, can be taken from court decisions from the USA, for example:

- 1) American CryptoFED - DAO recognised by a court as a legal entity, specifically by the court of the state of Wyoming, where the DAO was recognised as a “special form of LLC”.<sup>36</sup>

---

<sup>35</sup> <https://cointelegraph.com/magazine/legal-dangers-getting-involved-daos/>.

<sup>36</sup> <https://coingeek.com/the-first-legally-recognized-dao-in-the-usa/>.

American CryptoFED's goal is to begin operating fully without CEO management in the near future, where management of the entire organisation will be through Governance tokens held and used across the community<sup>37</sup>.

- 2) dOrg - DAO on the Ethereum blockchain network was the first company in the world to use its source code as its management system; its entire governance, property and ownership structure is managed through the blockchain.<sup>38</sup>

The legal system of the U.S. State of Vermont in Chapter 25, Subchapter 012 available at the following link:

<https://legislature.vermont.gov/statutes/section/11/025/04173>

specifies the establishment of Blockchain-based Limited Liability Companies. It is this legal status that dOrg uses for its activities.

## 25.2. Linking the DAO and traditional legal forms of business

It is the combination of DAOs and traditional legal forms that is one of the new industries being created by the penetration of blockchain into other segments.

BLLC - Blockchain-based Limited Liability Companies.<sup>39</sup> Overall, the entire management system now relies solely on blockchain technology, or smart contracts running on it.

This natural evolution of the fusion of the conventional legal system, represented by traditional schemes and forms of business, and new technologies that can replicate the clearly defined boundaries of the regulated business environment while innovating its elements through the implementation of new technologies and processes, is already beginning to emerge in some countries of the world. Again, however, those countries that are embracing these innovations often have very accessible business environments and make it possible for foreigners to set up such forms.

It is again important to emphasise one of the main aspects of the crypto - globality. In the modern world, which in many segments promotes the theory of globalism, the process of starting a business, i.e. setting up a company, is very simplified. Progressive entrepreneurial ideas and regulatory changes are spreading at great speed. Therefore, also from the point of view of the regulatory authorities, the changes implemented in the USA should be seen as an inspiration for improving the business environment in Slovakia.

## 25.3. DAO & Governance token

---

<sup>37</sup> <https://coingeek.com/the-first-legally-recognized-dao-in-the-usa/>.

<sup>38</sup> <https://www.coindesk.com/markets/2019/06/11/dorg-founders-have-created-the-first-limited-liability-dao/>.

<sup>39</sup> <https://legislature.vermont.gov/statutes/section/11/025/04173>.

However, DAOs without a legal entity are a unique example of the active use of governance tokens.

Governance token is defined very precisely on the website of the crypto exchange Kraken as follows: it is a type of cryptocurrency that seeks to democratize the governance of decentralised applications (dApps) and other blockchain-based protocols.<sup>40</sup>

Technically speaking, the owner of governance tokens has the right, opportunity, or literally the obligation to actively participate in the community running and decision-making of the DAO whose tokens the person or institution owns.

Of course, there are various forms of limitations on the usability of governance tokens, some of which may have only limited voting rights associated with a pre-specified area in which, for example, the holder can vote or exercise other rights.

Examples of “traditional” DAOs that clearly follow their decentralised function and operate solely on blockchain technology and, on the contrary, completely ignore traditional regulation are very numerous.

An example of a DAO project with a significant governance token function in the DAO routing and governance process is the MakerDAO project, which has issued its own stablecoin DAI<sup>41</sup>, and also has its own token, Maker (MKR)<sup>42</sup>, defined or functioning as a governance token, whose holders have voting rights in relation to the development and direction of the MakerDAO project. The DAO acts as a community-driven project, but at the same time the governance of tokens can be considered the equivalent of voting shares in the world of traditional finance.

The voting process itself is conducted through announced ballots available at <https://vote.makerdao.com/> and the number of votes is equivalent to the number of tokens held by individual owners. The parameters of the vote (whether 50% + 1 vote or 51% of all votes) are set in advance and then the voted change is implemented within a predetermined time frame.

In the case of governance tokens, there is a clear overlap, or inspiration, between the traditional world of finance and how shares and associated voting rights work. Of course, in this case, DeFi applies technologically convenient and time-flexible voting, without the need to call a general meeting, and the notarial record is the blockchain itself and the data written in it.

The Financial Intelligence Unit is closely monitoring the gradual development of DAOs that are linked to Slovak citizens, or DAOs that are popular in the crypto community in Slovakia.

---

<sup>40</sup> <https://www.kraken.com/learn/what-is-a-governance-token>.

<sup>41</sup> <https://coinmarketcap.com/currencies/multi-collateral-dai/>.

<sup>42</sup> <https://coinmarketcap.com/currencies/maker/>.

It is also important to quantify the threats associated with AML/CFT in the case of DAOs. DAO itself, already according to its name, operates as a decentralised organisation, without the need or necessity to collect any data or information about its users. It is this absence of data and any verification of the persons involved in their operation, management, voting and transfers that makes DAOs very suitable as a means<sup>43</sup> associated with the conversion of funds (insofar as the DAO in question allows it as a function) from crypto to crypto and thus complicating or making impossible the tracing of the transaction.

Outside of cases where the DAO also has its own legal entity, law enforcement authorities around the world do not, or if they do, only to a limited extent and in exceptional cases, have the means to compel any DAO to cooperate and share information necessary for procedural acts.

On the other hand, it is important to recognise that DAOs still operate in interaction with the outside world, their activities and direction being determined by specific individuals who may benefit financially. The running of the DAO itself is guided not only by the voting of the community, but also by the work of the developers themselves, who also take benefits, sometimes in the form of cryptocurrencies. And last but not least are the payments associated with running the servers, promotions and marketing events, and various other forms of project promotion. All these aspects could be taken as imaginary pebbles in the mosaic of a potential battle with AML/CFT in the case of DAOs.

---

<sup>43</sup> <https://compliancelatam.legal/en/decentralized-autonomous-organizations-and-money-laundering/>.

## 26.ICO

With the development of crypto-assets and increasing crypto adoption, new processes and concepts, often derived originally from the financial sector, have started to emerge. One such term, and also a newly emerging process, is the so-called ICO - Initial Coin Offering (in the sense of a crypto coin or crypto-asset).

The origin of the term and the whole process stems from the original one - IPO (Initial Public Offering), which refers to the process of the initial public offering of shares of a private company in a new share issue. An IPO allows a company to raise capital from public (private or institutional) investors.<sup>44</sup>

This process also inspired the crypto community and with the development of new networks and the altcoins running on them, it was necessary to standardise the process and terminology. The process that is taking place on different networks (chains) has been named ICO. The ICO process itself - the initial coin offering - is defined by the NBS on its website as follows: An alternative form of financing referred to as Initial Coin Offerings (ICOs) is an innovative and significantly growing way of raising funds from the public in order to finance the projects of specific individuals. This involves the creation of electronic “coins” or “tokens” and their subsequent offering and sale to the public in exchange for legal currencies (e.g. the Euro) or, more commonly, virtual assets (e.g. Bitcoin or Ether). Such offerings are most often made via the internet and social media.<sup>45</sup>

The AML Act further specifies the ICO process in Article 9(1) as follows:

“virtual currency shall mean a digital medium of value that is neither issued nor guaranteed by a central bank or a public authority, nor is it necessarily tied to legal tender, does not have the legal status of currency or money, but is accepted by certain natural or legal persons as an instrument of exchange which can be transferred, stored or traded electronically,”

ICO tends to be widely associated with strong marketing, particularly on modern platforms such as social media. Just as the globality or transnationality of crypto-assets is true in conventional trading, thanks to the internet, marketing is often not limited to one specific geographic area. Slovak citizens can therefore actively participate in the ICO process of a foreign entity very easily.

It is important to emphasise that ICO processes are often associated with the problem of so-called “scam ICOs”, commonly referred to in English as “scams”. The ICO process itself often becomes an abused process as a fraudulent method of eliciting funds from investors.

---

<sup>44</sup> <https://www.investopedia.com/terms/i/ipo.asp>

<sup>45</sup> <https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/>

Thanks to the extremely dynamic development of the various networks on which the individual cryptocurrencies or tokens run and the growing crypto adoption and, last but not least, the significant simplification of the process of creating a token on the individual networks, we can speak of a significant increase in the trend of abuse of ICOs in fraudulent schemes.

A large number of articles and YouTube videos are devoted to the issue of launching your own token, whether on the main network or on the so-called “testnet”. Thanks to the rise in popularity of cryptocurrencies, users no longer need a deep knowledge of programming or computer science to be able to find very precise instructions on how to run their own token running on some of the most well-known and common networks.

An example is this simple tutorial, including links to videos, available at the following link: <https://moralis.io/how-to-create-a-bsc-token-in-5-steps/>.

Thanks to the availability of a large amount of information, tutorials and the process where the whole crypto-scene has moved from IT enthusiasts to ordinary users, we can see the growth of the amount of fraudulent schemes on individual networks.

The NBS specifically addresses the ICO process directly on its website, in the financial market supervision section, available at the following link: <https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/>.

## 26.1. NBS and ICO

The NBS defines the ICO process on its website as follows:

An alternative form of financing referred to as Initial Coin Offerings (ICOs) is an innovative and significantly growing way of raising funds from the public in order to finance the projects of specific individuals. This involves the creation of electronic “coins” or “tokens” and their subsequent offering and sale to the public in exchange for legal currencies (e.g. the Euro) or, more commonly, virtual assets (e.g. Bitcoin or Ether). Such offerings are most often made via the internet and social media.<sup>46</sup>

### Information for consumers

The NBS draws the attention of the general public that the legislation of the Slovak Republic does not explicitly regulate or define crypto-assets and trading in them. The area of crypto-assets is not regulated and supervised by the NBS.

Products, services and activities involving crypto-assets, including Initial Coin Offerings (ICOs), are provided to persons in the Slovak Republic mainly via the internet, including by trading platforms from other countries. The law of these states may regulate crypto-assets and

---

<sup>46</sup> <https://nbs.sk/dohlad-nad-financnym-trhom/fintech/kryptoaktiva-a-initial-coin-offerings-icos/>.

the services related to them, and thus persons participating in may be subject to certain rights or obligations arising therefrom.

The NBS emphasises that crypto-assets do not have a physical counterpart in the form of legal tender. Exchanges or purchases of crypto-assets for other crypto-assets or officially recognised currencies (such as the Euro) are made at the own risk of the persons participating in such trades. There is no legal entitlement to compensation for any losses caused by such exchanges or purchases.

There are a number of significant risks associated with the products or services provided by trading platforms, also popularly referred to as “crypto exchanges” or “cryptocurrency exchanges”. These risks may include, in particular

- high price volatility, which can lead to the creation of a bubble and significant financial loss for participants in trades, including the loss of any funds invested,
- in most cases, the participants in the trades have no guarantee of receiving or enforcing the agreed remuneration or providing the agreed services or products,
- it may be difficult, if not impossible, for participants to sell or exchange the crypto-assets purchased for other crypto-assets or for officially recognised currencies,
- participants in trades may fall victim to misleading business practices, fraud or other illegal activities,
- limited function or complete malfunctioning of the technologies that enable trading crypto-assets, which may cause financial losses to participants in such trades.<sup>46</sup>

The NBS also clearly points out on its website that the ICO itself is not yet clearly regulated in Slovak legislation.

#### Legislation

The issue of crypto-assets, or ICOs, and the question of its regulation is a subject of discussion both within individual Member States and EU bodies, and globally. This is due to the growing importance of crypto-assets or ICOs and the increasing volume of funds in this area, as well as the need to address the risks associated with this alternative method of financing.

Currently, crypto-assets or ICOs are not explicitly regulated in the Slovak and European legislation, but some of their elements may be regulated therein.

In January 2019, the European Securities and Markets Authority (ESMA) issued a material (technical assistance) containing an analysis of the current crypto-asset market and a description of how crypto-assets and ICOs operate. The paper also addresses the question of whether the current legislation of the EU or its Member States applies to crypto-assets and ICOs respectively.



According to this analysis, some crypto-assets may be financial instruments, but most are not subject to EU regulation. If crypto-assets are considered in a particular case as financial instruments, ESMA considers that they (including their issuer or the firm providing the related investment services/activities) should be subject to the relevant EU regulation, in particular

- MiCA which takes the most comprehensive view on ICOs to date,
- the MiFID II Directive,
- the Prospectus Regulation,
- the Market Abuse Directive,
- the Short Selling Regulation,
- Central Securities Depositories Regulation,
- the Directive on settlement finality in payment and securities settlement systems.

The analysis notes that the assessment of whether a crypto-asset constitutes a financial instrument is based on the implementation of MiFID II into EU Member State law and is competence of the competent supervisory authorities, and the assessment should be based on the specificities of each individual case.

The European Banking Authority (EBA) has issued an opinion on the appropriateness of current EU regulation in relation to crypto-assets. The paper notes that some crypto-assets could be considered electronic money if they meet all the relevant definitional features, but the EBA's opinion also states that most crypto-asset-related activities are not regulated by the current EU legislation. In the case of crypto-assets that would be considered as electronic money, the application of the revised Directive on Payment Services in the Internal Market would also need to be considered according to the EBA.

The legislation within the scope of the NBS does not regulate crypto-assets, their mining and trading, nor does it contain a definition of crypto-assets. At the same time, the legislation does not provide for the obligation to obtain a licence to issue or trade in crypto-assets and, in this respect, does not regulate the requirements to be met for the purpose of carrying out such activities.

Authorisations to carry out regulated activities granted under the relevant NBS legislation (e.g. foreign exchange licence, payment service provider licence, electronic money licence) are not related to the issuance of or trading in crypto-assets, even if crypto-assets are bought or sold for Euro or foreign currency.

According to law of the Slovak Republic, crypto-assets cannot be considered as financial instruments under Act No. 566/2001 Coll. on securities and investment services. Nor can they be considered as securities as they do not meet the definition of a security, in particular the requirement to be registered in the form and manner prescribed by law.<sup>46</sup>

## 27. SCAM schemes

The Financial Intelligence Unit perceives an increase in the number of fraudulent schemes that use various fraudulent elements to elicit funds from users. With the development of smart contracts, there is also the development of potential opportunities to implement various variants of so-called backdoor in the source code of the contract, which may subsequently lead to abuse for unethical or even illegal purposes.

However, not all fraudulent schemes are necessarily linked to the implementation of backdoor directly into the source code for ICO. Many times it also involves misleading or deceiving people. Last but not least, deliberately manipulating a poorly liquid market/token and creating an artificial inflated price is also a common fraudulent scheme.

- 1) Pump n' Dump - a community action that artificially drives up the price of a token, mostly traded on a decentralised exchange (DEX), relying on the so-called FOMO (fear of missing out), where a high rise in the price of a token attracts other investors - speculators - and triggers an increased demand for the token and a consequent exponential rise in its price.

In the course of its activities, the Financial Intelligence Unit has detected the existence of special purpose groups run on the social network Telegram, which serve to bring people together and subsequently manipulate the market on purpose by creating artificial demand for crypto-assets.

This type of market manipulation is very often heavily investigated by regulators when it takes place in a regulated market such as stocks or financial derivatives; for crypto-assets that are still in the process of development and emerging regulation, these frauds are as yet without investigation or punishment for the perpetrators.

Fig. No. 19:

On the left, a call to create a “pump” - a demand for a designated token

On the right, thanking and informing the Telegram group members what the result of the artificially induced demand for the token was.

Fig. No. 17

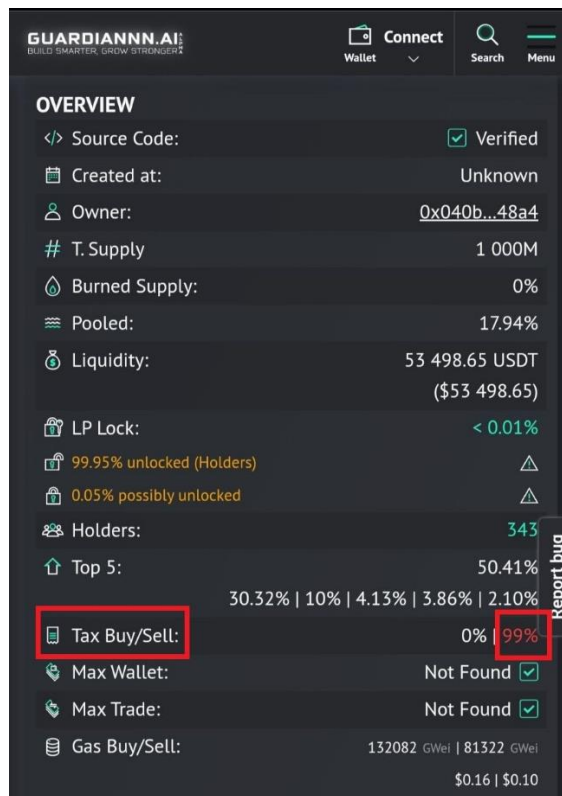


Source: The FIU's own activity

- 2) Honeypot - can take many forms, but most often it is deception linked to high yield or exclusive opportunities that are used as an enticement to investors. Subsequently, the scammer/smart contract programmed by them can cause unwanted activity, such as transferring to another wallet, preventing the ability to sell the token, or a loss right after the purchase.
- 3) Stop Trading - the creator of the token can implement a feature that allows them to stop trading the token and thus render it worthless.
- 4) Mint - the source code may include the ability to continuously issue new tokens and thus create a strong inflationary trend on the token price.
- 5) Hidden Mint - the above Mint, but extended with more complex features such as limiting trading through liquidity capping. Hidden Mint tends to be more difficult to detect because it is usually hidden more sophisticatedly in the source code.
- 6) Unverified Library - a library that cannot be verified may contain a type of code that may be harmful to token purchasers or token holders.

- 7) Forwarding to a predetermined address - after a user purchases tokens, the tokens are sent to the predetermined address in the contract, not the one specified by the purchaser when purchasing the tokens.
- 8) Sales Tax - when new tokens are issued, the creator tends to embed in the source code the option of a so-called sales tax, where a large (in the figure below up to 99%) tax is applied when the token is sold. Therefore, the buyer gets back less than 1% of the invested amount (after netting the network fees) after selling the mentioned / purchased token.

Fig. No. 18



Source: GuardiaNNN.ai

- 9) Rug Pull - a type of fraudulent behaviour where the developer tries to lure investors into buying an asset, most often a new token, by presenting the project as extremely profitable and then flees with their invested funds, leaving investors with often worthless tokens. Rug Pulls are a type of so-called “exit scams” most often on decentralised exchanges.

The most common types of Rug Pulls can be divided into 3 categories<sup>47</sup>:

- a) “liquidity stealing”,
- b) “limiting sell orders”,
- c) “dumping sale”.

<sup>47</sup> <https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it>.

10) Ponzi scheme - a scheme known and common in the traditional finance segment, where the token creator aims to lure as many investors as possible, who are paid above-standard returns. The system works up to the point where the inflow of capital from new investors is greater than the cost of the payout to existing investors, or to the point where the token creator decides to shut down the whole scheme.

The biggest Ponzi scheme in the cryptocurrency segment is the OneCoin case, which was presented as a “Bitcoin killer” and which ran from 2014 to 2019 on the principle of MLM - Multi Level Marketing and the total amount was close to USD 5.8 billion.<sup>48</sup>

OneCoin was also distributed in the Slovak Republic through MLM networks.

From experience we can say that this form of distribution is often abused to spread SCAMs in the crypto world.

11) Marketing Wallet - this is not a form of hidden / fraudulent extraction of funds from the project, but a form of abuse of funds to fund the lavish lifestyles of project creators. In order to attract as many mainstream retail investors as possible, project creators like to present an extremely successful and lavish lifestyle. Many times they draw funding for it from the project itself and the budget allocated for it by means of a marketing wallet. Some projects set aside up to 30% of revenue for this.

Fig. No. 19



Source: The FIU's own activity

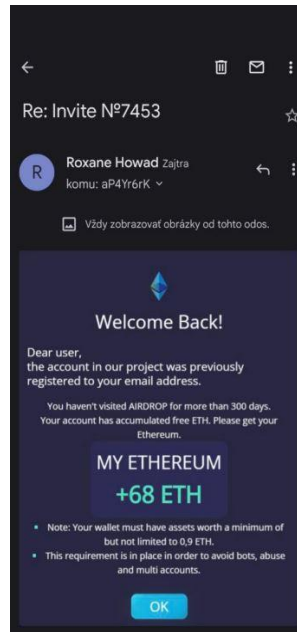
Among the most globally known and most used forms of fraud, which also threaten Slovak customers, are the following

<sup>48</sup> <https://coinmarketcap.com/alexandria/article/5-of-the-biggest-crypto-ponzi-schemes>.

- 1) fraudulent apps - fraudsters use well-known brands and their apps/websites to extort private keys, e-mails and passwords or other personal data from crypto-holders in order to gain access to their crypto-assets,
- 2) extortion - via e-mail or social networks, the victim is informed that there are recordings of them visiting pornographic sites or evidence of them visiting websites and downloading images, videos that contain child pornography. The attacker requires the sending of funds in the form of crypto-assets to a specified address or these records will be made public,
- 3) donation scam - scammers will announce via e-mail/social networks that they will send a higher amount, just for a smaller fee, or on the condition that the wallet, to which the funds will be sent holds a certain cryptocurrency and its owner will share e.g. a private key with them,
- 4) phishing scams - scammers send a link to a fraudulent site and try to elicit the necessary data from users, the aim being to get hold of their personal data, passwords or private keys,
- 5) fake notifications from companies - scammers will send a fake invitation to users, which may include a request to provide data on the grounds that their account has been hacked, or it may be a “pre-sale” invitation from a well-known global company that is about to release its own token and is offering the user an exceptional pre-sale purchase offer. The number of derivatives of these fake alerts is innumerable and new ones are created on a regular basis.

The figure shows a fraudulent email that announces a high accumulated amount and the information that the wallet to which it will be sent must have assets of a certain minimum value.

Fig. No. 20



Source: The FIU's own activity

Of course, there are dozens of other fraudulent schemes that aim to either extort funds from users or illegally take their personal or access data and then steal the funds.

Each of these schemes relies on a certain, often very short-term trendiness in crypto markets, and on a combination of low regulation and high risk acceptance by crypto-asset users. Last but not least, we can quote the well-known economist J.M. Keynes and his “animal spirit” - a mixture of emotions that can affect a person’s financial decisions.

One of the most effective ways to combat SCAMs in ICOs is through systematic education, financial literacy and prevention by supervisory and, where appropriate, law enforcement authorities, where new trends are regularly monitored and their threat actively communicated to the public.

## 28. Stablecoins

With the recent development of crypto-assets, the crypto community has been searching for effective solutions that combine the efficiency, speed and convertibility of cryptocurrencies while negating their biggest problem - extreme volatility. The initial response was the launch of so-called stablecoins, which have evolved into a separate segment within crypto-assets.

Stablecoins have been identified as a potential money laundering and terrorist financing tool. While the current use of stablecoins in money laundering appears to be small, there are concerns that the mass adoption of stablecoins could increase the risk of their abuse for illicit purposes. The global trend is that stablecoins and their providers are subject to increased scrutiny and oversight by government regulators and other oversight authorities. The US government also published a report on stablecoins and their potential risks, including money laundering and excessive leverage.

The Financial Intelligence Unit views the risk of stablecoins being used in laundering schemes associated with the purchase/sale of stablecoin to foreign entities through local VASPs while failing to exercise enhanced customer due diligence as highly topical.

Stablecoins are types of crypto-assets whose value is tied to an underlying asset, and depending on what that asset is, they can be divided into

- a) collateralised - with three most common forms and
- b) algorithmic.

### 28.1. Collateralised

Stablecoins with FIAT currency as the underlying asset - in this case, the value of the stablecoin is pegged to the amount of FIAT currency that is deposited in current banks, most often in the form of the currency itself e.g. USD, EUR, JPY and sometimes in the form of short-term financial instruments issued by central banks. However, the collapse of Silicon Valley Bank (March 2023), which was one of the main banks for USDC - Stablecoin on the Ethereum network, has shown that even this, so far globally much preferred system, is vulnerable to external influences.



Chart No. 34



Source: finance.yahoo.com, 13 April 2023

The chart above shows the reaction of the market, or rather the USDC stablecoin, fixed to the USD following the release of information about the problems of the SVB, which held about 8% of the reserves from the USDC stablecoin's total capitalisation<sup>49</sup>. The chart shows the moment when the analogy of a "run on the bank" was created, when the market was overwhelmed with requests to withdraw funds, and this in turn led to a significant drop in the value of the stablecoin. However, the FDIC (Federal Deposit Insurance Corporation) immediately (March 2023) said it would pay out deposits in full, which was received with great enthusiasm by the market and led to the stabilisation of the banking and financial sector in the USA.

Commodity-Backed Stablecoins, or stablecoins with an underlying asset in the form of commodities:

Commodity-backed stablecoins use individual commodities as collateral (security) and guarantee of their stability. Initial attempts were associated with oil as the primary underlying asset, but the trend has clearly shifted to precious metals as the most commonly used underlying asset. Such stablecoins are essentially blockchain-based representations of commodities and are backed by reserves held by a predetermined central entity. Some of the best examples are PAXOS GOLD (PAXG) or Tether Gold (xAUT). In the case of Tether Gold (xAUT), a single token represents 1 troy ounce of gold as specified by the London Gold Bar.

<sup>49</sup> <https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html>.

Crypto-Asset Backed Stablecoins - A crypto-asset backed stablecoin is a very popular type of stablecoin whose price is backed by either a single type of cryptocurrency - such as Bitcoin - or a basket of cryptocurrencies, most commonly those with the largest market capitalisation.

## 28.2. Algorithmic

Algorithmic stablecoins are a type of crypto-asset that are designed to maintain a stable value relative to another asset, usually a FIAT currency such as the US Dollar or more recently the Euro. Unlike crypto-asset backed stablecoins or those collateralised by reserves in FIAT currency, algorithmic stablecoins rely on highly sophisticated algorithms that essentially simulate the actions of central banks at high speed in their operation and control the amount of tokens in circulation based on a supply and demand relationship. When demand increases, to prevent the price of stablecoin from rising too much, they react by issuing new tokens; when downward pressure on the price is exerted in the form of an excess of supply over demand, there is a “burning” of tokens which reduces their supply in the market, and this in turn leads to an increase and subsequent stabilisation of the price. This whole process happens in a very short period of time and the objective of stablecoin algorithms is to achieve minimum volatility of stablecoins. Algorithmic stablecoins do not have independent assets in reserves to back the value of their stablecoins and rely entirely on sophisticated algorithms.

The latest development, which has so far had no precedent in the financial world and is likely to guide the world payments market in some way, is the decision by the US company PayPal to launch its own stablecoin,<sup>50</sup> initially for users in the USA, but with a view to expanding gradually to others outside the USA.

PayPal’s stablecoin, named PYUSD, runs on the Ethereum network and belongs to the group of stablecoins that are backed by assets. PayPal itself specifies that PYUSD will be backed by highly liquid assets.<sup>50</sup>

The PYUSD stablecoin was received with great enthusiasm by the crypto community, however, after analysing the source code, the first criticisms of the option emerged, which PayPal had reprogrammed. Some of them are, for example, that PayPal retained the option to freeze assets held in stablecoins or to delete a frozen wallet. PayPal calls these features by the single name “Asset Protection”.<sup>51</sup>

Slovak legislation does not currently address the issue of stablecoins separately, nor does it regulate them in any way.

The findings of the FIU show that there is currently one legal entity in the Slovak Republic whose owners and directors are from abroad and which is developing a stablecoin that will be pegged to the FIAT currency Euro. Its stablecoin runs on the Ethereum network and is of a



---

<sup>50</sup> <https://www.paypal.com/us/digital-wallet/manage-money/crypto/pyusd>.

<sup>51</sup> <https://blockworks.co/news/paypal-pyusd-stablecoin-centralization>.

type that is backed by assets in the form of FIAT currency and short-term financial instruments.

Fig. No. 21: List of the largest stablecoins in terms of market capitalisation

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	

Source: Coinmarketcap.com

Brevan Howard Digital in their study published an interesting comparison of the value of transactions between VISA, the world leader in electronic payments and the use of stablecoins on the blockchain.

The results of the comparison showed that there were USD 11 trillion in transactions on stablecoin networks in 2022 compared to USD 11.6 trillion globally via VISA.<sup>52</sup> An equally relevant fact, indicative of the growing crypto adoption in the stablecoin segment of the global market, is the amount of transactions being conducted.

Based on analysed blockchain transactions, the study shows that more than 5,000,000 wallets per week are active, of which ¾ of the transactions had an amount of less than USD 1,000.<sup>52</sup>

This data clearly points to a gradual crypto adoption by mainstream retail users in the stablecoin segment.

<sup>52</sup> <https://www.ledgerinsights.com/brevan-howard-digital-stablecoins/>.

The interest in stablecoins is evidenced by the fact that since the last bull run in 2021, the amount of stablecoin transactions has only declined by 11%, compared to decentralised and centralised exchanges, where the volume of transactions has declined by over 60%.<sup>52</sup>

The riskiness of stablecoins in terms of AML/CFT issues must be viewed broadly. The key risk factor for stablecoins lies not in their anonymity or pseudo-anonymity, as is the case with conventional cryptocurrencies, but in the mix of their native characteristics such as their low volatility, ability to generate profit on interest, cheap global transfer, easy interchangeability/convertibility for FIAT currency, increased acceptance by traders, but also high acceptance by decentralised exchanges (especially when trading on stablecoin/cryptocurrency pairs) and others.

## 29.Mixer

One of the most striking examples of the divergence in approach to cryptocurrencies between the crypto community and state authorities can be considered to be the attitude towards so-called mixers. Mixers are also a unique example of cooperation between the crypto community and the secret services of different countries on the other side.

A mixer is a service that allows a user to send crypto-assets through one or more transactions anonymously. It works on the basis of a combination of different sources that mix with each other and thus make it difficult to be identified on the blockchain. The aim of the mixer is to prevent other persons and software solutions (various forms of tracking software solutions) from tracking and potentially identifying the wallet address, with that particular person or user.

For the purposes of the VA/VASP sector analysis, we will discuss the technical capabilities and resulting risks associated with enabling legalisation of proceeds of crime, money laundering, and terrorist financing opportunities. Last but not least, we will highlight links to so-called APTs - state-sponsored cyber groups and their use of crypto-assets.

Sinbad.io - a software service and currently (at the time of writing this sectoral analysis - year 2023) the most used crypto mixer in the market. The crypto research firm Elliptic published a study that considers Sinbad.io to be just a re-launched version of the already banned Blender.io.<sup>53</sup> In May 2022, the U.S. Office of Foreign Assets Control (OFAC), under the U.S. Department of the Treasury, announced the first-ever sanctions on a cryptocurrency mixer service, namely Blender.io.

In a press release published on their website, OFAC informed <sup>54</sup> that Blender.io is being used by the Democratic People's Republic of Korea to support its malicious cyber activities and money laundering of stolen cryptocurrencies. On March 23, 2022, the Lazarus Group, a DPRK state-sponsored cyber group, carried out the largest virtual currency heist to date, worth almost \$620 million, from a blockchain project linked to the online game Axie Infinity; Blender was used in processing over \$20.5 million of the illicit proceeds. Under the pressure of robust U.S. and UN sanctions, the DPRK has resorted to illicit activities, including cyber-enabled heists from cryptocurrency exchanges and financial institutions, to generate revenue for its unlawful weapons of mass destruction (WMD) and ballistic missile programs.<sup>54</sup>

The press release further quotes the Under Secretary of the Treasury: "Today, for the first time ever, Treasury is sanctioning a virtual currency mixer," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests. We are taking

---

<sup>53</sup> <https://decrypt.co/121222/new-sinbad-bitcoin-mixer-is-sanctioned-blender>.

<sup>54</sup> <https://home.treasury.gov/news/press-releases/jy0768>.

action against illicit financial activity by the DPRK and will not allow state-sponsored thievery and its money-laundering enablers to go unanswered.”<sup>54</sup>

This unprecedented move by the US Treasury Department directly implies how much of a threat to national security funds can be when it is impossible to verify their origin, to identify the payment or its originator with a specific individual or legal entity. Blender.io itself, and currently Sinbad.io, is directly associated in professional circles with the Lazarus cyber group, whose members are associated with North Korean intelligence.<sup>55</sup>

Following the US Treasury’s move and the adding of Blender.io to the sanctions list, several other mixing services have appeared in short order as the crypto community’s immediate response to the sanctions.

OFAC re-imposed sanctions in August 2022 on the Tornado Cash service, which OFAC reports was used from its inception in 2019 until August 2022 to launder more than \$7 billion.<sup>10</sup> The Lazarus crypto group itself is credited with laundering funds in excess of hundreds of millions of dollars.<sup>10</sup>

The U.S. Department of the Treasury, in a press release associated with the Tornado Cash mixer’s placement on the sanctions list and on the mixer issue in general, goes on to say: “Virtual currency mixers that assist criminals are a threat to U.S. national security. Treasury will continue to investigate the use of mixers for illicit purposes and use its authorities to respond to illicit financing risks in the virtual currency ecosystem.”<sup>10</sup>

A typical monitored example of the use of the Tornado Cash crypto mixer in concealing the origin of illegally obtained cryptocurrencies by defrauding investors in an unnamed scheme.

---

<sup>55</sup> <https://www.fbi.gov/wanted/cyber/park-jin-hyok>.

Fig. No. 22

Txn Hash	Method	Block	Age	From	To	Value	[Txn Fee]
0xc2b2c840a175ea06e...	Transfer	16011914	500 days 5 hrs ago	0x91fbb5adf8d328eb690...	OUT 0xd990759720c4515c87	0.49191370848108 BNB	0.000105
0x0e2636fe349c8ee736...	Deposit	15131149	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	10 BNB	0.004838805
0x430d8e3d3733cca088...	Deposit	15131147	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	10 BNB	0.004864155
0x7fa7607f1859b72741...	Deposit	15131143	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	10 BNB	0.004864215
0x731ae590ac9ac913ab...	Deposit	15131140	530 days 22 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	10 BNB	0.00488925
0xb1c42748362802b731...	Deposit	12279089	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x3f0c42d81b336c9b2d...	Deposit	12279087	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864155
0xbc14d80e5d6497b11d...	Deposit	12279085	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004813395
0x2f0afcae8970fb64e2...	Deposit	12279084	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x3369ad9021c14b78e6...	Deposit	12279081	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x92f0afecb8e91a02287...	Deposit	12279080	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864215
0x28141f851bf68799c81...	Deposit	12278990	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x64d449f9ea2a9b3cfc...	Deposit	12278987	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864215
0xd2274817c8f836f4256...	Deposit	12278984	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864065
0xeeea212b87b3a2b253...	Deposit	12278981	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.00488925
0x65336dc4ea85ad44f...	Deposit	12278977	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004813339
0xcbc6662fb6d1a642ad...	Deposit	12278827	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x7a33931997d1a7e652...	Deposit	12278824	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0xbd04f4fcb1a1206e520...	Deposit	12278821	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864215
0xb8c3294650f8b9667...	Deposit	12278818	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x22b36ab043417fcb04f...	Deposit	12278802	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864215
0x3ea0f6b986ac85077...	Deposit	12278630	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864215
0xa57b9c55a0a66a144e...	Deposit	12278628	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004889585
0x5767592693983f2e7b...	Deposit	12278625	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004838805
0x9ac44327c6ca1efca3d...	Deposit	12278623	631 days 18 hrs ago	0x91fbb5adf8d328eb690...	OUT Tornado.Cash: Proxy	100 BNB	0.004864215

Source: The FIU's own activity

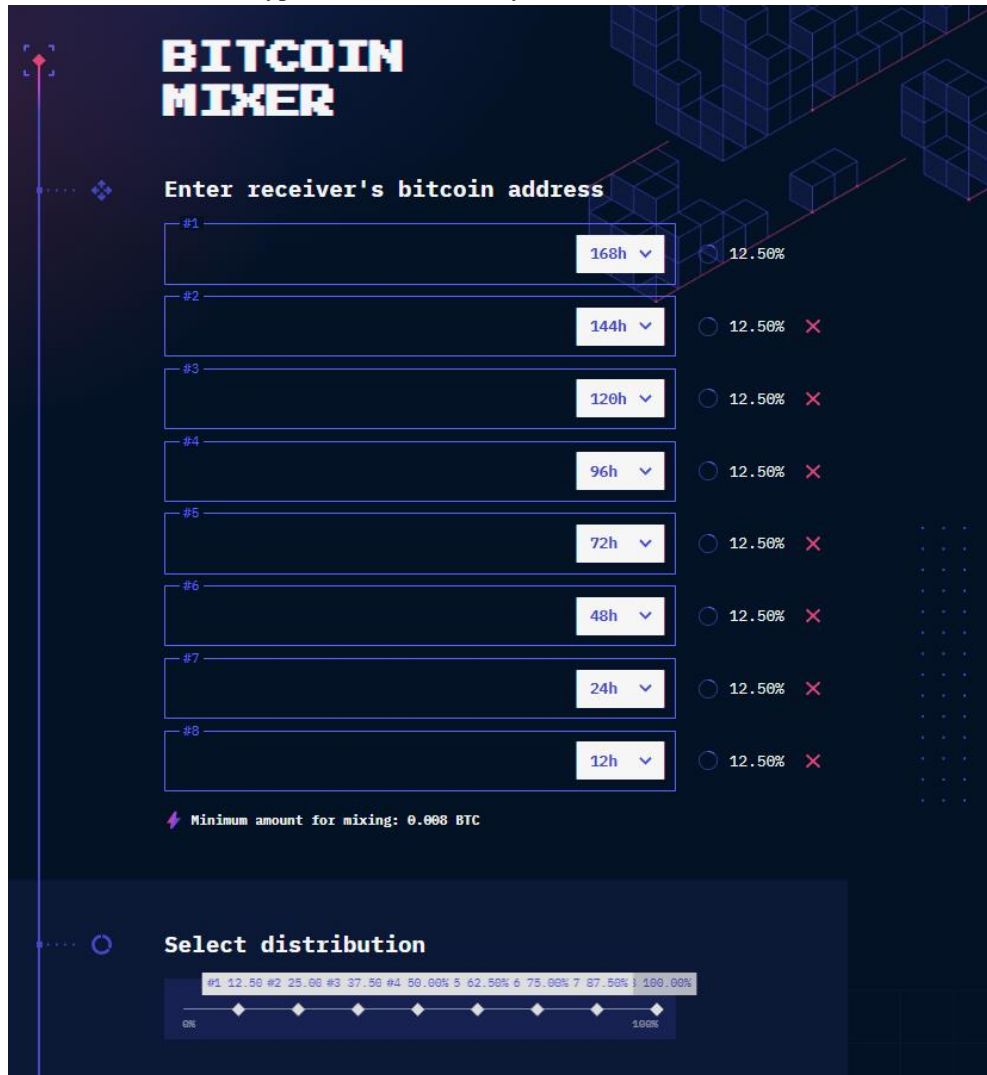
It is currently (summer 2023) perceived as the most technically sophisticated, and therefore most difficult to monitor in terms of AML/CFT issues, crypto mixer from arguably the original creators of Blender.io, Sindbad.io.

Expert sources point continuously to the Lazarus group's links to the Sindbad.io crypto mixer.<sup>56</sup>

New features, implemented in the Sindbad.io crypto mixer, allow you to split a transaction into up to eight addresses and set a separate transaction time for each address in the range of 0 to 168 hours.

<sup>56</sup> <https://crypto.news/stolen-crypto-from-atomic-wallet-traced-to-north-korean-linked-mixer/>.

Fig. No. 23 Photo of Sindbad.io crypto mixer functionality



Source: <https://sinbad.io/en>

OFAC published a list of new sanctioned entities on its website <https://ofac.treasury.gov/> on 29 November 2023, and among others, the Sindbad.io crypto mixer is sanctioned with its website [www.sinbad.io](http://www.sinbad.io), but also with its address available on Darknet or via the TOR network at the following link:

<http://sinbadiovklgdbafpqwfwjh2tfrisahtxmrskiovt62nirragcnkcad.onion>, e-mail addresses and a series of crypto addresses associated with this mixer.<sup>57</sup>

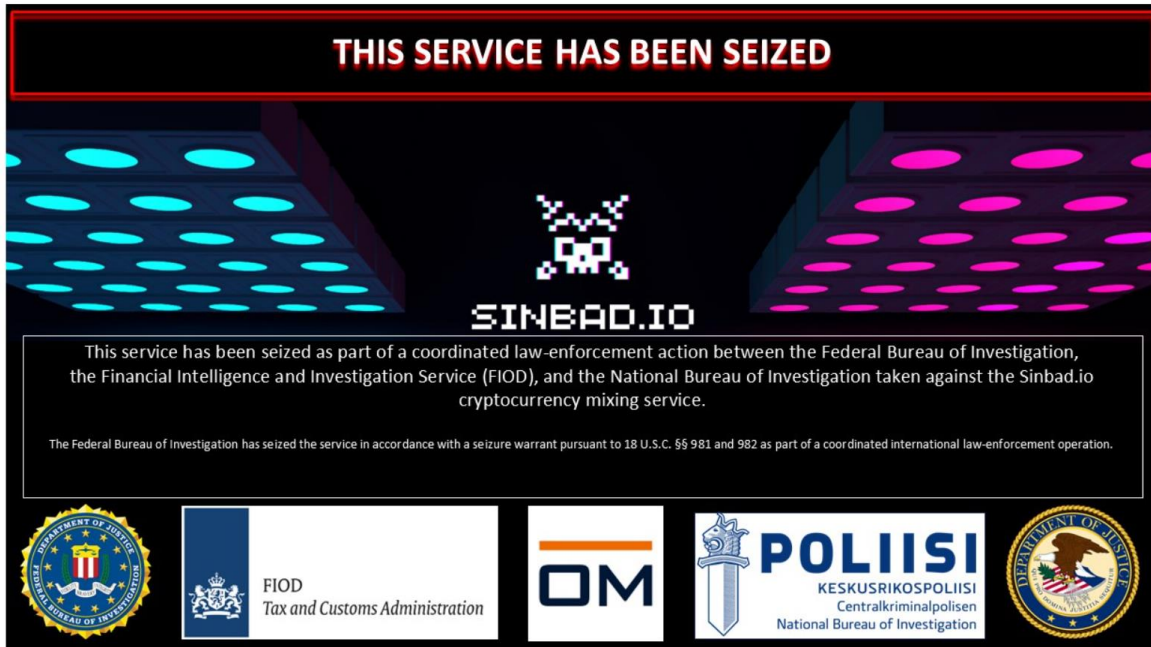
OFAC's rationale, provided on its website and in a press release, outlines the reasons for placing this service on the sanctions list as follows: "Sinbad is responsible for materially assisting in the laundering of millions of dollars in stolen virtual currency and is a preferred mixing service for the Lazarus Group. Sinbad operates on the Bitcoin blockchain and indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and

<sup>57</sup> <https://ofac.treasury.gov/recent-actions/20231129>.



counterparties. Sinbad is believed by some industry experts to be a successor to the Blender.io mixer, which OFAC designated for providing mixing services to the Lazarus Group.”<sup>58</sup> At the same time as the sanctions were imposed on Sindbad.io, the following message appeared on its website:

Fig. No. 24



Source: [www.sinbad.io](http://www.sinbad.io)

In terms of AML/CFT issues, crypto mixers are perceived as high risk services. Their explicit purpose is to obfuscate, make it difficult or impossible to identify the origin or original address of the funds, the destination of the funds, and the individual counterparties to a transaction that is executed through a mixer.

The U.S. Treasury Department’s attitude and individual actions toward mixers, noting their national security risks, clearly indicates the direction of its view on crypto mixers that should be inspirational to security forces around the world.

It is important to underline the fact that even if the issue of the use of anonymisation tools is viewed through the lens of supporting latent criminality, in the global geopolitical climate of radicalisation of society, the rise of support for dictators and the empowerment of the right or far right, these anonymisation tools offer an unprecedented and unique opportunity to support individuals, communities, structures, organisations or even states.

An example of this is Ukraine, which, following the launch of a full-scale invasion by the Russian Federation in February 2022, has prepared crypto addresses for the most widely used cryptocurrencies in cooperation with experts and state organisations: BTC, EHT and stablecoin USDT, available at: <https://standwithukraine.com.ua/donation/crypto>.

<sup>58</sup> <https://home.treasury.gov/news/press-releases/jy1933>.

It is worth noting that Ukraine accepts donations on three blockchain networks: BTC on the Bitcoin network, ETH on the Ethereum network and stablecoin USDT on the Tron network.<sup>59</sup> The element of diversification, so characteristic of financial markets, applies quite clearly to the issue of cryptocurrencies. OSInt reports that the equivalent of the total amount in FIAT currency collected during 2022 and 2023 was USD 225 million.<sup>60</sup>

Vitalik Buterin, the creator of ETH and one of the most influential people within the crypto community, has himself admitted to using Tornado.Cash to donate funds to Ukraine.<sup>61</sup> Jeff Coleman during a Twitter discussion with Vitalik Buterin pointed out: “Even if the government where you live is in full support, you might not want [the] Russian government to have full details of your actions”.<sup>61</sup>

It is precisely the issue of privacy and the efforts of state authorities to control that is one of the most prominent points of clash between the crypto community and the state authorities.

---

<sup>59</sup> <https://standwithukraine.com.ua/donation/crypto>.

<sup>60</sup> <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/>.

<sup>61</sup> <https://forkast.news/vitalik-buterin-says-used-tornado-cash-donate-ukraine/>.

## 30. Proposal for measures

The Financial Intelligence Unit, in cooperation with other institutions and authorities, has carried out a very extensive and in-depth examination of the Slovak market with virtual currency wallet service and virtual currency exchange service providers. Based on the findings of this analysis, the Financial Intelligence Unit organised a series of lectures and training sessions for partner institutions and organisations. These events provided a platform for presenting findings, relevant information and quantified risks associated with the domestic market. In addition, these trainings served as an opportunity to discuss best practices and strategic actions needed to manage the identified risks and to improve the links between the different market participants, public authorities and supervisory authorities. The overall objective of these initiatives was to raise awareness and improve preparedness for potential threats in the crypto-assets sector.

Based on its findings, the FIU proposes a series of measures aimed at mitigating the identified risks and vulnerabilities in the Slovak virtual asset market. These measures aim to strengthen market protection and improve the regulatory environment in order to address potential threats and challenges more effectively.

Proposal for measures:

- 1) Establish a regulatory authority - the establishment or designation of an institution to regulate, supervise and guide the entire sector and to carry out the licensing process itself.
- 2) Implement the licensing process - setting up a comprehensive licensing process during which each applicant would be examined in terms of the origin of capital, the intention to use the licence, the technical and technological equipment, the intended geographical scope and the staffing of key corporate positions.
- 3) Put in place technology solutions for monitoring and analysis - introduce more sophisticated software solutions that would enable better analysis and detection of illicit activities associated with virtual assets.
- 4) Increase international cooperation - given the inherent global nature of cryptocurrencies and crypto-assets, it is essential to broaden and deepen international cooperation in these segments.
- 5) Continue educational activities for VASPs and public authorities - continue efforts to increase awareness of the crypto-asset sector and its risks among public authorities as well as the general public.

## Conclusion

The entire virtual asset sector and the innovation and services associated with it, or that exist because of it, is entirely new and still taking shape for the world and society. As it has been pointed out several times in this sectoral analysis, we must forget judging in terms of locality/globality; we have to look at the overall market as primarily global, with instant payments, technological solutions available to all those who are currently operating on the blockchain.

Its complexity and interconnectedness to the world of information technology and the internet predisposes it to dynamic development and a propensity for rapid implementation of innovations. This speed and flexibility makes the cryptocurrency sector and its sub-segments very challenging for all state supervisory authorities, for law enforcement authorities and, last but not least, for national security services to keep pace with its dynamic changes.

It is the incorrect or ambiguous setting of legislation in Slovakia that we assess as the most significant risk. The absence of a proper licensing process has led to the rampant establishment of VASPs in Slovakia, some of which are likely to have been established as special purpose entities in international optimisation schemes.

Another high risk, besides the simple incorporation of VASPs, is the lack of any process for control of those associated with the VASP, whether as directors, beneficial owners or owners of the company.

These aspects are the most significant local risks directly related to the Slovak Republic as both the domicile of VASPs and as their regulator.

The global risks clearly arise from the very global nature of cryptocurrencies and their services and capabilities. Geographical borders play almost no role at all and because of them the threats faced by a user/investor/member of the crypto community are almost no different for a user from Slovakia, or Greece, or Australia.

The problem with these threats is, on the one hand, their latent nature and, on the other hand, their very difficult structure and often cross-border reach. What on the one hand is a native characteristic of crypto - globality and disregard for geographical boundaries - is on the other hand a major problem for law enforcement authorities around the world.

Last but not least, it is the fact that the problem of preventing fraud, SCAMs and scam structures in the world and in Slovakia is not yet properly understood by regulators or by individual law enforcement authorities.

The European Union expects the MiCA Regulation and its launch in the near future, and the Slovak Republic will clearly be one of several countries whose adoption of this regulation will help with market consolidation.

## Annexes

### List of Abbreviations:

A.I.	-	Artificial Intelligence
AML/CFT	-	Anti-Money Laundering / Countering the Financing of Terrorism
APT	-	Advanced Persistent Threats – groups linked to foreign intelligence services
ATS	-	Automated trading systems
CEX	-	Centralised Exchange
KYC	-	“Know your customer” - the process of customer identification by the obliged person, a concept encompassing Basic Due Diligence according to Article 10, Article 12 of the AML Act
DAO	-	Decentralised Autonomous Organization
DeFi	-	Decentralised Finance
DEX	-	Decentralised Exchange
EBA	-	European Banking Authority
FATF	-	Financial Action Task Force – international organisation
TradFi	-	Traditional Finance
VA	-	Virtual Assets
VASP	-	Virtual Assets Service Provider
MiCA	-	Markets in Crypto-Assets – EU Regulation
LEAs	-	Law enforcement authorities
OSInt	-	Open Source Intelligence
FIU	-	Financial Intelligence Unit
AML	-	Anti Money Laundering
OFAC	-	Office of Foreign Assets Control – USA institution
TOR	-	The Onion Router
ICO	-	Initial Coin Offering
FIAT		
currency	-	legal tender
P2P	-	peer-to-peer
MEKO	-	Interministerial Expert Coordination Body