The Downsides of Digital Currency and the Limits of its Normative Regulation

TATIANA HAJDÚKOVÁ
Department of Informatics and Management
Academy of the Police Force in Bratislava
Sklabinská 1, 835 17 Bratislava 35
SLOVAK REPUBLIC

SAMUEL MARR
Department of Criminal Law, Criminology and Criminalistics
Faculty of Law
Comenius University in Bratislava
Šafárikovo nám. 6, P. O. BOX 313, 810 00 Bratislava
SLOVAK REPUBLIC

Abstract: The paper reflects on the consequences of the bankruptcy of the FTX exchange in the context of cryptocurrency volatility, as for the legal anchoring of cryptocurrencies in terms of *de lege lata* and *de lege ferenda*, especially in the context of the need for agile proactive state response to criminal activities connected to the use of cryptocurrencies. The nature of cryptocurrencies predisposes the commission of criminal activities related to crypto predominantly in the online space, resonating with the necessity to increase transparency and control of cryptocurrency transactions. The anonymity of coins and the limited ability to track them gives them a clear technological advantage over the efforts of law enforcement bodies to map them or check them by regulatory authorities. The subject of the empirical part of the paper is the analysis of a case study of a regulatory offense committed by a selected service provider in the field of performing exchange activities in the Slovak Republic.

Keywords: Cryptocurrency, Volatility, CyberSecurity, Money Laundering, normative regulation of virtual currencies

Received: March 27, 2023. Revised: February 9, 2024. Accepted: March 12, 2024. Published: April 16, 2024.

1. Introduction

The cryptocurrency market is becoming more and more successful in the financial sector. This is even though past results and investor behavior are in no way a guarantee of future results. The investor behavior is generally highly unpredictable, similar to the volatile market value of cryptocurrencies. The reasons for the increasing demand for cryptocurrencies could be perceived through their transparency, decentralization, censorship resistance, and, last but not least, decentralization. These are attributes that centralized banking institutions do not provide. The website of coin market cap gives the list of cryptocurrencies traded with their name, symbol, market cap, price, circulating supply, and volume [17]. The initial caution of investors is decreasing more and more, and companies have begun to buy crypto-currencies as reserve assets, which should allow them to avoid inflationary pressures better [7]. Bitcoin (hereinafter BTC) is the best-known and most popular virtual currency. One of the reasons for this fact is that in the longer-term horizon of

recent years, the bitcoin policy of regular BTC purchases achieved unrealized gains, despite periods when its price fluctuated sharply. Trust is rising not only among individuals, businessmen, and private companies but also in public administration. In December 2023, the city of Lugano, Switzerland, officially announced that the local government has launched the option of Bitcoin and Tether (USDT) cryptocurrency payments for taxes and all other community fees. The city chose the Swiss cryptocurrency platform Bitcoin Suisse as a partner in providing new services. The goal of cryptocurrency adoption in this city is to use Bitcoin technology as the basis for the transformation of the municipal financial system. It can be exchanged through reputable intermediaries or exchanges, and this is done non-cash, with a certain time delay [14]. Another variant is special Bitcoin ATMs, which quite often offer only purchases. As for Germany, Switzerland, and Slovenia, the conditions for the use of virtual currencies have been significantly opened by the introduction of zero tax. The Slovak Republic is not that progressive in this regard, however, since January 1, 2024, the so-called time test has been introduced, which means that after holding the cryptocurrency for more than 1 year, converting it to fiat currency or stablecoin is taxed at a rate of only 7% (for comparison, in the Czech Republic the profit tax is 15% regardless of the investment time). There is no common taxonomy of crypto-assets in use by
international standard-setting bodies. [12] The adoption of cryptocurrencies has a growing tendency in the population as well. It can be noticed that the legislative activity of particular member states, resulting from political, social, economic, and
environmental conditions, leads nowadays to reharmonization tendencies, which have not been analyzed in the literature on this subject so far [10]. The article does not aim to question the future of digital currencies, which, thanks to the high development dynamics and rapid adaptability, certainly have a promising future. Cryptocurrencies are still in their infancy, and it's difficult to state whether they're going to ever find a true mainstream presence in world markets [19]. The indisputable advantage of cryptocurrencies is the "transnationality" of cryptocurrencies and their flexibility to respond to any regulations. The greatest advantages from the perspective of a cryptocurrency owner are at the same time the greatest threats from the perspective of regulatory authorities. The benefit of this paper is pointing out the real ways of conducting unusual business transactions, which suggests the need to significantly increase transparency and control over entities engaging in business transactions with cryptocurrencies. The paper aims to, based on empirical data, highlight regulatory offenses committed in the provision of services in the field of performing exchange activities in the Slovak Republic.

2. Literature Review on Cryptocurrencies

According to [23], virtual currency means a digital medium of exchange that is not issued or guaranteed by a central bank or a public authority, is not necessarily tied to legal tender, and does not have the legal status of currency or money. However, it is accepted by some individuals or legal entities as a means of exchange that can be electronically transferred, stored, or electronically traded. In the context of the above, cryptocurrency is computer data with an objective economic value [5] with a significant potential to influence (both positively and negatively) the global financial system. To measure the worldwide recognition of cryptocurrencies correctly and to determine whether cryptocurrencies can provide a better concept of international fund transfers, it is necessary to deeply analyze different features of these virtual assets based on volatility, speed of transaction, transfer-related costs, security and privacy [6]. That is reflected in the proactive initiatives of central banks implementing the "Central Bank Digital Currency" into their product portfolio, which is a virtual currency issued by the entities in question. In addition to the fact that the aforementioned underlines the power of cryptocurrencies, it cumulatively depicts the difference between a virtual currency issued by a state authority, which is quite well normatively anchored, and standard virtual currencies, on the normative regulation of which opinions diverge. Extensive studies should be performed on the economic effects of Bitcoin on long-standing fiat currency performance and compare the results to countries that are starting to adopt state-sponsored cryptocurrencies [4], [1]. The apparent societal interest in creating more favorable conditions for trading with cryptocurrencies cannot be denied [8].

In April 2023, the European Parliament approved the Markets in Crypto-Assets (MiCA) Regulation, which regulates and unifies the rules for investing in cryptocurrencies in European countries. Different legal environments in European countries have limited several business activities with cryptocurrencies [20], [21], which should be changed by the new regulation. With the entry into force of MiCA Regulation, a unified regulatory framework should be provided for entities trading with virtual currency. The most important regulations will mainly concern entities that issue and trade crypto-assets (including asset-referenced tokens and electronic money tokens). The entities will be obliged to comply with increased transparency, publish authorization documents, or supervise transactions. They will have to publish all important information about risks, costs, and fees associated with their operation more clearly and transparently. Cryptocurrencies, considering the underlying Blockchain Technology, have the property of immutably storing the registration of all transactions. Blockchain Technology has brought an innovative way to exchange information [3]. Criminal activities using crypto tokens, cyber-attacks on electronic wallet providers, and money laundering are some examples [9].

3. Misuse of Cryptocurrency for Socially Undesirable or Criminal Activities

The nature of cryptocurrencies predisposes the commission of criminal activities related to crypto predominantly in the *online* space. The potential of cryptocurrencies in the plane of non lege artis is undeniable and the delay in reflecting the competent authorities as well as the legislator on the above-mentioned issue can therefore be undeniably considered as a shortcoming. [11] As an example, we will mention the insufficient regulation of the cryptocurrency exchange, which does not protect investors at a level comparable to securities law. Kraken crypto exchange belongs to the TOP 5 crypto exchanges in the world. In November 2023, it was accused of insufficient internal control and insufficient record-keeping, which was partly reflected in mixing customer money with its funds and paying operating expenses directly from customer funds [16]. A significant event in the context of the abstract of the anticipated content focus of this paper is the year 2022 and the November bankruptcy of the FTXT cryptocurrency exchange the collapse made it more insecure for people to hold their savings in a crypto bank leaving many customers and investors in a loss of billions of dollars,[15]. From both an economic and legal perspective, it is significant that this bank conducted a broad portfolio of operations (including those of a risky nature). Special mention should be made of investment operations through sophisticated structures in projects, the value of which significantly decreased in a certain time chain from the investment, as a result of which the clients' financial resources were at risk. The reasonable response to the above was the launch of a massive sale of cryptocurrencies issued by the FTX exchange through the exchange giant Binance. This signal determined numerous withdrawals of funds by FTX clients. FTX, like any financial house, only had a certain limited amount of funds that could be paid out immediately. As for massive withdrawals, the aforementioned logically exceeds the immediate capabilities of the financial entity. The depicted events *in fine* led to the bankruptcy of FTX and the related negative impact in the sphere of crypto volatility, causing a significant decline in its price [25]. We highlight the declines in the value of Bitcoin; centralized crypto tokens with an embodied subjective element of human decision-making were particularly affected. However, the question arises here from the perspective of *de lege ferenda* to adopt adequate legislative measures to prevent the above-mentioned cases. In our opinion, the tightening of regulatory activities towards cryptocurrency exchanges and the conditions for their establishment and operation is particularly necessary. In our opinion, these are insufficiently transparent. Here, as an example, we highlight the "healing" renaissance in the banking sector after 2008, which is currently at a significantly higher level. The undesirable reputational impacts on cryptocurrencies (hereby echoing the need for stricter normative regulation for crypto) stemmed from violations of the capital markets law and

fraudulent actions by Ton Kwan from South Korea. He is accused of the token collapse of *terraUSD* and L*una* in May 2022 amounting to 40 billion dollars. Due to his evasion, Interpol issued an international arrest warrant for him in September of that year. This significantly highlights the importance of the *stablecoin Terra* as well as its sister token L*una*.

4. Unusual Business Transactions

The rights and obligations of legal entities and individuals in preventing and detecting money laundering and the financing of terrorism (AML) and financing of proliferation (FP) are regulated by special laws in countries, specifically in the Slovak Republic by the so-called Anti-Money Laundering Law (AML). This provides an exhaustive legal definition in Section 2(1)a)-d), to which we refer for a more detailed understanding of the glossed issue. It is not our goal to cite legal standards in legal language, and therefore, about the issue of money laundering, we provide an inherently practical approach and state that illegal income (based on [22]) should be understood as a benefit in the economic sphere determined by committed or ongoing criminal activity, with the essential component of income being ownership in the form of property (including things). In money laundering, the perpetrator's effort to conceal the existence of income, mask its origin, and do so through various actions, is a significant characteristic. In simple terms, it can be said that it involves more or less sophisticated camouflage of the origin of the income, to make it appear lawful outwardly. Demonstratively, we can mention the concealment and hiding of items used in criminal activities, including their possible frustration in responding to requests for their surrender for criminal proceedings, as well as confiscation and/or forfeiture. The factual elements of the offense of Money Laundering in most European countries use legal features such as deposit, conceal, possess, store, consume, move, transport, import, lend, etc. By commenting on Section 2 of the AML Act, we state that money laundering means actions involving a change like assets, knowing that the property comes from criminal activity or participation in it, motivated by its concealment and/or masking, including its illegal origin, including the possibility of assisting a person jointly committing a criminal offense to avoid potential criminal consequences. Concealing and/or masking the origin of assets knowing that it is illegal, or acquiring or using it with such knowledge, cannot be omitted either. Any of the above-described actions committed in the form of conspiracy, incitement, inducement, aiding, as well as in the attempt stage should also be considered money laundering. Another significant aspect is the financing of terrorism, which is dealt with in Section 3 of the AML Act. About the provision in question, we state that gathering and/or providing of items, finances, and/or any other means to perpetrators of terrorism, such a group, and/or a member of a terrorist group, or to commit any of the 'package' of terrorist offenses, is a criminal offense. to the interpretation of the relevant conceptual elements, we define 'provision' (direct) as the direct provision of items, finances, and/or other means directly into the hands of the perpetrator of any terrorist offenses. Indirect provision, on the other hand, means carrying out the above-described activities indirectly, for example, through the use of foundations, thus masking the real purpose. As the legislator specifies means other than finances and items, these mean, for example, the provision of food aid, accommodation, etc. *In fine,* for a more detailed understanding of the issue of terrorism, we refer, among other things, especially to the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism of 22 October 2015, also known as CETS 217, and the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31/03/2017) by Act 297/2008. For the paper, it is necessary to clarify the content of the concept of an unusual business transaction (UBT), which, by the AML Act, means an act that suggests that its execution may lead to money laundering or the financing of terrorism. Given the diverse possibilities of execution, the characteristics of a UBT cannot be clearly defined,

and therefore, they are descriptively specified in the law. For example, transactions with an unusually high volume of financial resources that deviate from the usual framework or nature of a certain type of trade, or have no apparent economic purpose or clear legal purpose, are assumed. Another characteristic of a UBT is the refusal [1]of the client to identify themselves or provide the information required for due diligence exercised by the obliged entity. Similarly, the refusal to provide information about a planned transaction or the attempt to provide as little information as possible or information that the obliged entity can verify only with great difficulty or at high costs is evaluated negatively. The prevention and detection of money laundering (ML), financing of terrorism (FT), and financing of proliferation (FP) are in the interest of the state and are carried out at its level. For this purpose, the Financial Intelligence Unit (FIU) has been established. The FIU, as the central national unit, represents an independent authority responsible for receiving and analyzing information about unusual transactions and other information relevant to AML/FT/FP. The obligation to report to the FIU also applies to suspicions of predictive offenses, which the FIU forwards to law enforcement authorities based on the subject matter jurisdiction. The main tasks of the FIU include receiving and process reports on UBT from a wide range of obliged entities specified in the AML Act and supervising obliged entities in complying with obligations under the AML Act. In the context of this paper, the term "obliged entity" refers to a legal entity or an individual authorized to carry out exchange activities. Cryptocurrency exchanges are nodes through which cryptocurrencies are distributed and serve to deposit cash into the system, withdraw cash from the system, or transfer between currencies [18]. Furthermore, the obliged entity is required to prepare and update in writing a program for their activities aimed at preventing money laundering and the financing of terrorism, taking into account their organizational structure and the subject of their activities. During the year 2022, the FIU received a total of 2,185 reports on UBT from obliged entities, with the overall value of transactions amounting to more than EUR 1,160 million, of which 60 were related to the provision of services in the field of virtual activities [26].

5. Data and Research Methodology

The research methods used in this article are critical Analysis. Metrics and analysis have been prepared with the data provided by the FIU. The subject of the empirical part of the paper is the analysis of a case study of a regulatory offense committed by a selected particular service provider in the field of performing exchange activities in the Slovak Republic. According to [23], a virtual currency exchange service provider is a person who, as part of their business activities, offers or conducts transactions with virtual currency, the subject of which is the purchase of virtual currency for euros or a foreign currency or the sale of virtual currency for euros or a foreign currency. Cryptocurrency exchanges are nodes through which bitcoins are distributed and serve to deposit cash into the system, withdraw cash from the system, or transfer. The data used were extracted from the legally binding decision imposing a sanction by the FIU against the legal entity providing virtual currency exchange services[2]. By the procedure following the Code of Civil Procedure, it was convincingly proven and legally decided that a regulatory offense was committed during the conversion of funds worth almost 15 million euros during the audited period from 01/11/2020 to 28/02/2022. It involved repeated violations of obligations with the duration of the unlawful conduct lasting approximately 1.5 years. According to [23], the FIU can impose a fine on an entrepreneur for non-compliance or violation of any obligation stipulated by this Act. The fine can be up to twice the unjust enrichment if it can be determined, or up to 1,000,000 euros, whichever of these values is higher. When determining the amount of the fine, the FIU takes into account the

[1]For the purposes of the paper, a client means the final user of benefits, i.e. any natural person for whose benefit the exchange performs a transaction.

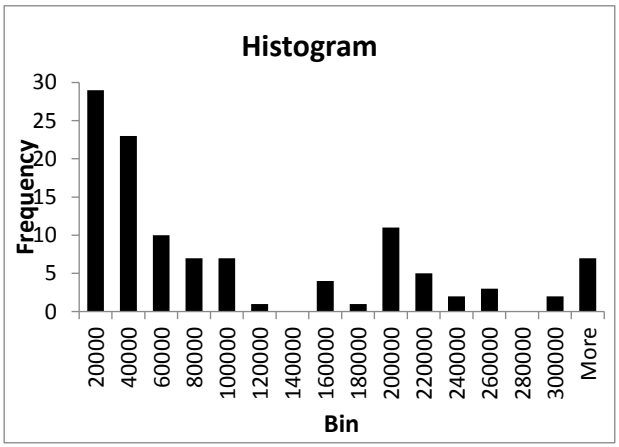
[2] The subject of the business activity is the purchase of virtual currency for euros or the sale of virtual currency for euros.

severity, duration, and consequences of the unlawful conduct, if determinable, the level of cooperation provided by the obliged entity during the inspection, the size and nature of the business activities of the obliged entity, and repeated non-compliance or violation of obligations stipulated by the Act or based on it.

6. Analysis of Selected Conversions in the Case Study

The most common regulatory offenses committed by the monitored obliged entity involved the failure to exercise due diligence about a client, failure to ascertain the origin of financial resources, failure to assess transactions for their unusual nature, failure to refuse to carry out specific transactions during the notice period despite suspicions of money laundering, and failure to report UBT to the FIU promptly. In one case, it involved a failure to provide the required cooperation to the FIU during the inspection. The histogram shows the frequencies of the particular conversions based on their amounts expressed in euros.

Graph1 Histogram of the Distribution of the Converted Amount in Euros



Source: Own processing from FIU data [24]

The intervals of the converted amount on the horizontal axis are linearly graduated in increments of 20,000 euros. The most common were individual conversions with the amount of up to 20,000 euros and up to 40,000 euros. Transactions with a low risk of money laundering or financing terrorism, based on risk assessment, have a designated maximum threshold amount of 15,000 euros according to [23]. Despite this limitation, more than 30 cases involved a one-time conversion exceeding the amount of 200,000 euros. A more detailed breakdown of conversion types is provided in Table 1.

Table 1 The Share of Individual Types of Conversions

Conversion	Amount	Percent
Among Cryptocurrencies	177640.23	1.19%
Into Cryptocurrency	1065374.57	7.11%
Into Euro	13736314.47	91.70%
Total Amount	**14979329.27**	**100%**

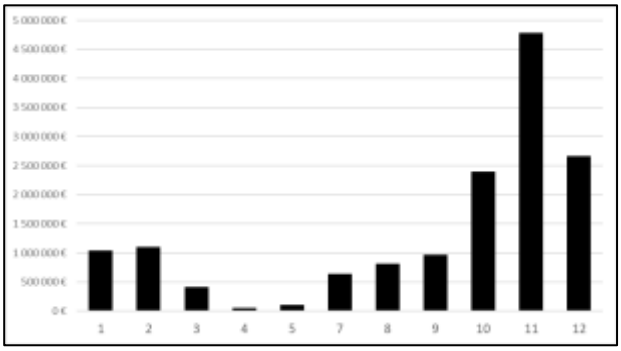
Source: Own processing from FIU data [24]

The conversion between different types of cryptocurrencies was quite rare, at approximately 1%. The exchange of euros for cryptocurrencies was marginal as well. The most significant, with a dominant share of over 90%, was the conversion of cryptocurrencies (BTC, USDT, and USDC) into euros.

6.1. Temporal Correlation and Origin of the Converted Amounts by Countries

In addition to the business transaction amounts, apparent signs of unusual business operations also include temporal correlations.

Graph 2 Conversion Distribution by Months of the Year

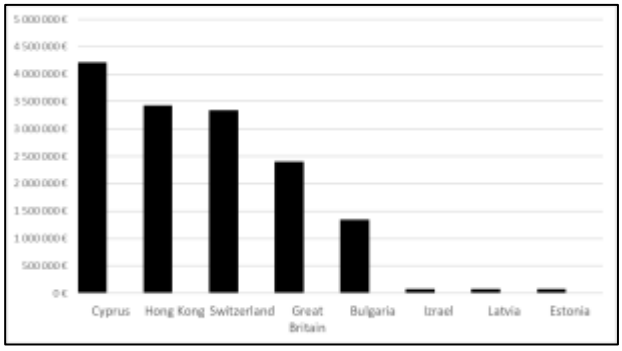


Source: Own processing from FIU data [24]

The horizontal axis on Graph 2 is time-based, distinguishing the months of the year, while the vertical axis shows the converted currency amounts. From the distribution in Graph 2, a significant temporal unevenness is obvious, with

approximately one-third of the conversion amount, nearly 5 million euros, carried out in November. Two-thirds of the conversions, totaling approximately 10 million euros, were carried out in the fourth quarter of the monitored years. The significant temporal disproportion of transactions for calendar months in the year confirms that UBT was carried out.

Graph 3 Origin Share of the Converted Amounts by Countries



Source: Own processing from FIU data [24]

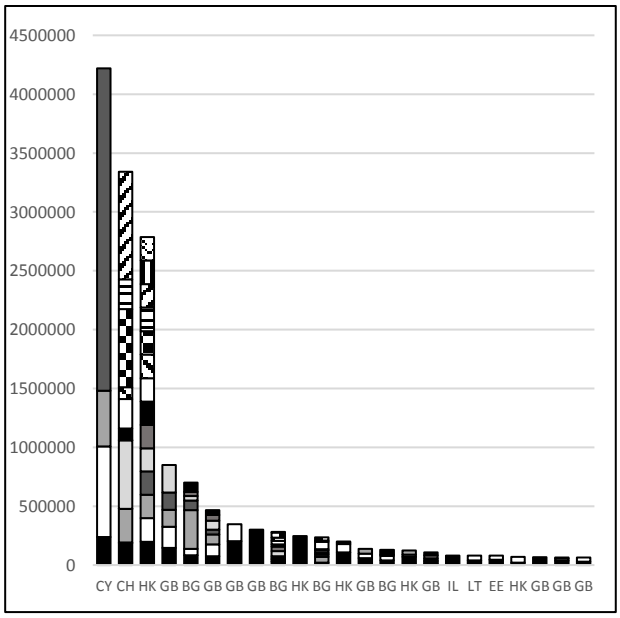
The total converted amount in euros is displayed on the vertical axis of Graph 3, and the horizontal axis there are the countries in which clients receiving the service by the obliged entity were identified. The inspection identified clients from eight countries. The largest share of the converted amount was identified among clients from Cyprus, Hong Kong SAR in China, and Switzerland, the countries considered tax havens. These countries are characterized by low taxation, which allows entrepreneurs and individuals to avoid and/or optimize tax obligations. In a smaller amount, almost 2.5 million euros, the conversion was carried out by persons whose accounts were held in the United Kingdom of Great Britain and Northern Ireland, and we will also mention the accounts held in Bulgaria with a conversion of more than a million euros.

The intensity of conversions may be related to inflation, where cash deposits in accounts held worldwide lose value. A larger supply of funds from foreign accounts held, for example, in Switzerland, Cyprus, etc., were subsequently used to purchase lucrative real estate in the Slovak Republic. As stated in [26], the origin of financial funds could not be unequivocally determined, but some investigations pointed to a possible connection with economic cases examined by law enforcement bodies in Slovakia in the past.

6.2. Repeated Conversions by Clients

Interest in the virtual currency exchange services may be repeated; however, in the case study we have examined, a one-time transaction occurred with only three clients, while all other clients carried out a group of transactions. The graph below shows the distribution of the converted amount by clients.

Graph 4 Distribution of Conversions of Each Client



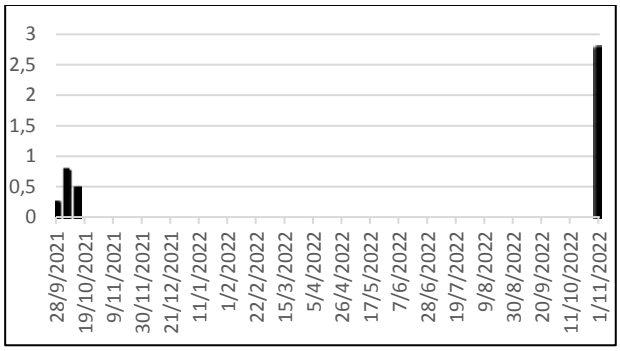
Source: Own processing from FIU data [24]

The horizontal axis of Graph 4 shows the country where the client's account was held (a total of 23 clients) and the vertical axis shows the converted amount for each client. The composition of the columns consists of individual transactions of each client. The clients on the horizontal axis are arranged in descending order from left to right based on the converted amount. The distribution of clients in Graph 4 draws attention to three clients with significantly high group transactions.

6.3. Details of Client Conversions with the Highest Transaction Amounts

We will analyze the actions of the two largest "investors" in more detail. The first client with cryptocurrency held in Cyprus carried out only four conversions but with enormous amounts.

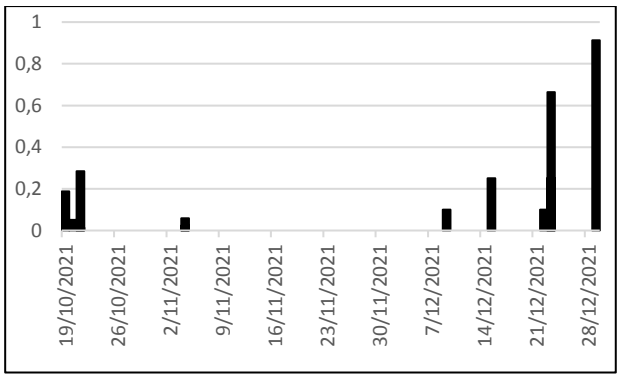
Graph 5 The Timeline and Amount of Conversions of a Client with Conversion from Cyprus



Source: Own processing from FIU data [24]

To highlight the temporal correlations, the horizontal time axis has intervals of 21 days. The vertical axis indicates the amount of conversion in millions of Euros. There is no time regularity in the monitored transactions. There is an apparent tactical approach in the client's actions, where the initial three conversions of cryptocurrency to euro were carried out to assess the 'reliability' of the service provider. The first conversions were carried out with "smaller" amounts worth several hundred thousand euros with quite short time intervals lasting a few days. The last fourth transaction was carried out after a break lasting more than a year (approx. 13 months) when a huge one-time conversion of almost three million euros was made in just one transaction. The transaction was traced based on the facts even after the period of the inspection when the decision on administrative proceedings had not yet been issued, and the obliged entity continued with its activities. The client took on enormous risks, but in this particular case, it was successful. A very similar tactic with a more cautious execution was implemented by another client, whose transactions are depicted in Graph 5. The chosen client converted cryptocurrency from an account held in Switzerland.

Graph 6 The Timeline and Amount of Conversions of a Client with Conversion from Switzerland



Source: Own processing from FIU data [24]

Compared to the case from the account held in Cyprus, there are several repeated initial trial irregular conversions with a 'smaller' amount in the range of tens to hundreds of thousands of euros, culminating in two huge conversions with the amounts exceeding half a million euros. Compared to the first case, the frequency of conversions is noticeably higher. The unanswered question remains: what was the reason that halted the 'investor' from continuing the unusual trading mediated by the monitored entrepreneur engaged in exchange activities. Greater certainty in distinguishing legal and illegal conversions and better anticipation of when and by whom money laundering/terrorism financing/proliferation financing occurs would significantly facilitate the work of regulatory authorities and law enforcement bodies. Considering the longer-term behavior, that showed a "willingness" not to prevent UBT. Both analyzed cases share a very easily recognizable feature, and that is the repeated conversion of high to very high amounts of cryptocurrency. As long as the obligation to report UBT is based on the honesty of a service provider with the subjective element of human-based decision-making, the temptation to 'earn extra' will remain a stronger motivator than fears of sanctions for a regulatory offense. Exchanges are a key partner for law enforcement bodies in collecting digital evidence related to payments made in cryptocurrencies [18]. With this paper, we illustrated the consequences of the failure to monitor processes in transactions involving cryptocurrencies at the level of an

obliged entity. Virtual currencies enable, despite clear identification of the asset, the anonymization of the owner, which, combined with the possibility of mutual substitution, constitutes an effective obstacle to tracing the flow of finances. Thanks to their easy convertibility, cryptocurrencies represent an ideal means for ML/FT/FP. The limited ability to track them gives them a clear technological advantage over the efforts of law enforcement bodies to map them or check them by regulatory authorities. Without active participation by all entities involved in virtual currency operations, success in the fight against money laundering and the financing of terrorism remains out of reach.

7 Conclusions

The Internet environment has open characteristics. [2] The possibility of exchanging virtual currency on various networks and the development of peer-to-peer exchanges through decentralized exchanges present a new, globally uncharted threat to the financial market. Reflecting on the Markets in Crypto-Assets Regulation in conjunction with MiFID II, we state that it is one of the focal tasks of the European Parliament, the Council, and the Commission to bring the issue of unified normative anchoring of cryptocurrency matters in the European area to the successful end. In our opinion, the issue of establishing mandatory registration of fractional non-convertible tokens with the regulator is imminent, while about ordinary tokens, we propose that their registration be decided *ad hoc* by the relevant national entity of the particular country. We consider the idea of the Markets in Crypto-Assets Regulation in the context of global harmonization of legislation in the anticipated direction within the common European framework (especially regarding the regulation of cryptocurrency issuers and service providers, including the transparent disclosure of information) to be positive. In response to the bankruptcy of the FTX exchange, we turn our attention to the activities of the International Organization of Securities Commissions (IOSCO), which harmonizes rules in the field of securities concerning G20 countries. The IOSCO advocates for the need for (more) adequate regulation of the crypto sector with a particular emphasis on conglomerate platforms. The IOSCO has already established certain principles for the regulation of stablecoins, and therefore, it is reasonable to expect efforts towards normative regulation of platforms offering crypto trading, especially exchanges, shortly. In this context, it is worth noting that the provision of services in cryptocurrency exchange activities in the conditions of the Slovak Republic is conditioned only by obtaining a trade license, with no influence of legal mechanisms on the part of the central entity represented, for example, by the National Bank of Slovakia or another responsible entity from the financial sector. In this context, we note that this results in a disproportionately higher proportion of registered entities in our territory compared to the neighboring countries in the European Union (for example, in France and Germany, there were several dozens of registered entities by the first half of 2020 compared to hundreds of registered entities in the Slovak territory). About the 'internal' expansion of the domestic territory, given the above, it does not make sense to comment on the same normative model determining the creation of legal authorization more deeply. The classification of these entities as obliged entities according to the AML Act does not change anything in the above-mentioned legal status either. In conclusion, we reiterate that, by the Markets in Crypto – assets Regulation, it is particularly important for cryptocurrency companies to possess the necessary license for the *lege artis* issuance and sale of digital currencies in the European Union. We are convinced of the substantive correctness of tightening regulations, leading to subsequent greater protection for investors. [11] We hold the same opinion about the need to possess a valid license. Although the criteria for the written development and updating of the program of the activities aimed at preventing money laundering and the financing of terrorism, taking into account its organizational structure and the subject of its activities, have been established in the conditions of the Slovak Republic, we have flagrantly pointed out their ineffectiveness. A less formal approach to the development of the program of own activities aimed at preventing money laundering and the

financing of terrorism by exchange operators, along with its more effective inspection, would undoubtedly better eliminate speculative attempts by perpetrators at various forms of fraudulent activities. One of the threats of ML/FT is the absence of technological solutions in virtual currency tracing. That does not refer to individual transactions. Every single activity conducted in the online environment leaves a trail [13]. The problem lies in the anonymity of investors and the origin of funds, which are exploited in various tax and money laundering schemes.

Based on the analysis of operations related to cryptocurrencies in the Slovak Republic, it can be assumed in the field of ML/FT that foreign 'investors' will continue to seek and exploit individual failures of virtual currency service providers. Current regulatory and control mechanisms are not sufficiently effective to stop the purchase and conversion of virtual currency, the use of electronic payment gateways, and products from foreign fintech banks to complicate the documentation of the flow of funds obtained through criminal activity. The new possibilities provided by anonymized tools used for transfers of virtual currencies, the use of mixers, etc., are trends defending against which is a significant challenge in the field of virtual currencies. To increase legal certainty and operational efficiency, it is necessary to strengthen the cooperation of relevant domestic and foreign authorities when exchanging and verifying financial information and financial analyses needed for the prevention, detection, investigation, and prosecution of serious criminal activities.

The paper was prepared with the support of the project APVV-19-0102 Effectiveness of preliminary proceedings – examination, evaluation, criteria, and the impact of legislative changes.

References:

[1] AKBANOV, M. et al., Wanna Cry Ransomware: Analysis of Inflection, Persistence, Recovery Prevention and Propagation Mechanisms, Warszawa: Journal of Telecommunications and Information Technology, 2019

[2] Chung-Chih Lee, Hsing-Chau Tseng, Chun-Chu Liu, Huei-Jeng Chou, "Using AES Encryption Algorithm to Optimize High-tech Intelligent Platform," WSEAS Transactions on Business and Economics, vol. 18, pp. 1572-1579, 2021, DOI:10.37394/23207.2021.18.143

[3] BONSÓN, Enrique and Michaela BEDNÁROVÁ (2019). Blockchain and its implications for accounting and auditing., Meditari Accountancy Research, Vol. 27 N.º5, pp. 725-740.

[4] DeVries, P.D. (2016). An Analysis of Cryptocurrency, Bitcoin, and the Future. International Journal of Business Management and Commerce,1(2), 1-9

[5] ČENTÉŠ, J. et al. 2022. Trestný poriadok (Code of Criminal Procedure). Veľký Komentár (Great Commentary). Updated Edition 5. Bratislava: Euro code, ISBN: 978-80-8155-109-3

[6] DURBIN, T.E. and J.G. RONC, (2015). U.S. Patent Application No. 14/215,473.

[7] IVANČIK, R. (2012). Security from the View of Economy Theory. In Political Sciences, 15(3), pp. 100-124. ISSN 1335-2741.

[8] IVANČÍK, R. and V. Andassy, V. (2023). Insights into the development of the security concept. In Entrepreneurship and Sustainability Issues, 2023, Vol. 10, No. 4, pp. 26-39. ISSN 2345-0282.

[9] KETHINENI, S. and Y. Cao (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review, 30(3), 325-344.DOI: 10.1177/1057567719827051

[10] KOZIEŇ, A., and N. KOZLOWSKA (2022). "Harmonization and Deharmonization of Excise Duty in the European Union as Contemporary Challenges of the EU Tax Law," WSEAS Transactions on Business and Economics, vol. 19, pp. 815-824, 2022, DOI:10.37394/23207.2022.19.71

[11] MARR, S. and B. SUCHOVSKÝ (2023). Právno-aplikačné problémy zaisťovania kryptomien (Legal-application problems of hedging cryptocurrencies). In: SAK Bulletin 5, pp. 24-29. ISSN 1335-1079

[12] MATAKOVIC, I. (2022) Crypto-Assets Illicit Activities: Theoretical Approach with Empirical Review, International e-Journal of Criminal Sciences,

[13] MIKLOŠÍK, A., KUCHTA, M., and Š. ŽÁK (2018). Privacy Protection Versus Advertising Revenues: The Case of Content Publishers. - In

Connectist: Istanbul University : Journal of Communication Sciences. - Istanbul : Istanbul University. ISSN 1302-633X, 2018, no. 54, pp. 117-140 online. 1-17-106-00
[14] PATZ, H. (2023). Swiss city Lugano accepts Bitcoin and Tether for municipal taxes. Available at https://cointelegraph.com/news/bitcoin-accepted-taxes-swiss-lugano
[15] Sidhartha Shukla and Emily Nicole. A Hedge Fund hit by FTX Colla pse Defaults on $36
[16] STEMPEL J. (2023). US SEC sues Kraken crypto exchange over failure to register [cit. 18. 11. 2023] Available https://www.reuters.com/business/finance/us-sec-sues-kraken-operating-crypto-trading-platform-without-registering-2023-11-20/
[17] Global Cryptocurrency Benchmark Study, 2017 by Cambridge Center for Alternative Finance [cit. 12. 12. 2023] Available: https://www.jbs.cam.ac.uk/facultyresearch/centres/alternativefinance/publications/global-cryptocurrency/
[18] UJVARY, K. and J. KUCHTOVÁ (2019). The specifics of clarifying financial transactions in connection with Bitcoin. - In: Current challenges of cyber security in the conditions of security forces, Bratislava: PF Academy, pp. 185
[19] UYDURAN, B. (2020). The Crypto Effect on Cross Border Transfers and Future Trends of Cryptocurrencies., Financial Internet Quarterly 2020 vol 16/no. 4, pp. 12-23, DOI: 10.2478/fiqf-2020-0024
[20] WOUTER, B. et al. Legal aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations. IMF Working Paper. WP/20/254
[21] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA
[22] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 8 November 1990, Strasbourg
[23] Act 297/2008 Coll. 297/2008 Coll. on Protection against Money Laundering and on Protection against Financing of Terrorism and on amendments and supplements to certain Acts (AML)
[24] Decision within the administrative procedure number PPZ-FSJ2-9/2022-KPO
[25] Million on Debt. Bloomberg. Available online: https://www.bloomberg.com/news/articles/2022-12-06/crypto-fund-orthogonaldefaults-on-36-million-debt-as-ftx-contagionspreads FTX opposes new bankruptcy
investigation as it probes Bankman-Fried
[26] Financial Intelligence Unit. Annual Report 2022 connections | Reuters

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.