RISK MANAGEMENT AND MONEY LAUNDERING SUPERVISION OF VIRTUAL CURRENCY SERVICE PROVIDERS

Kristina Trajković

Available at www.nbs.rs

Payment System Department

NATIONAL BANK OF SERBIA

Belgrade, 12 Kralja Petra Street

Telephone: (+381 11) 3027 100

Belgrade, 17 Nemanjina Street

Telephone: (+381 11) 333 8000

www.nbs.rs

Risk management and money laundering supervision of virtual currency service providers

Kristina Trajković

Abstract: Prevention of money laundering and other abuses in the digital assets sector is a major step in the preservation of financial system stability. Non-alignment of regulatory regimes in an environment of rapid market development creates a potential for abuse and illicit activities. Monitoring the market requires systematic analysis in order to define clear guidelines for mitigating identified risks. Regular implementation of risk assessment and the regulator's supervisory function facilitate the identification of the riskiness of the entire digital assets sector. In addition to an overview of regulations and standards governing the prevention of money laundering, the paper looks into the risks to which the digital assets sector is exposed, including the conduct of supervision and, in this sense, implementation of the risk-based approach.

Key words: regulation, digital assets, virtual currency, supervision, money laundering, abuse
[JEL Code]: E30, K20, K23, 010, G18

Non-technical summary

The nature of digital assets gives rise to the emergence of market changes and risks that may affect the overall financial system stability. Regulation and oversight of the digital assets sector requires the establishment of a comprehensive approach based on clear policies and procedures of supervisory bodies.

To achieve functionality and efficiency in the approach, regulators across the world are striving to establish legislative regimes and supervisory frameworks enabling them to respond to challenges in the market. Given the lack of a global regime that would govern the area of digital assets, alignment with international standards represents an important step. Though many countries have already made progress in implementing international standards and defining legislative regimes, only a small number of them have actually implemented a comprehensive regulatory framework governing this market.

As for the Republic of Serbia, the area of digital assets has been regulated in the part related to the prevention of money laundering and terrorism financing since 2018. The National Bank of Serbia (NBS), being the regulator and supervisor, regularly updates regulations in accordance with international standards, with the aim of improving its supervisory function. By adopting the Law on Digital Assets, the NBS started implementing a comprehensive approach. In addition to supervision in the area of the prevention of money laundering and terrorism financing, it also supervises other operations of virtual currency service providers.

In view of the global reach of digital assets, this paper provides an overview of risks, risk management and supervision in relation to all digital asset service providers, including virtual currency service providers which are subject to supervision by the NBS. At the same time, besides the money laundering risk, it also presents risks associated with other abuses.

Contents:

1 Introduction

Over the past several years, digital assets have become widely used. Digitalisation brings new possibilities for market development, and at the same significant risks associated with abuses that may affect the integrity of the financial system. The lack of a single approach to market regulation creates room for money laundering, terrorism financing, tax evasion and other more severe criminal acts.[1]

An increase in abuses, the rising market capitalisation and development of new types of digital assets[2] are driving the need to define reliable ways of managing risk and conducting supervision. To mitigate the identified risks a systematic approach is required, as well as a careful consideration of threats identified in the market. This is particularly important given the nature of digital assets that can be characterised by anonymity.

Though there has been progress in regulating this area, especially in the area of the prevention of money laundering and terrorism financing (hereinafter: ML/TF), many countries have still not implemented the standards of the Financial Action Task Force (hereinafter: FATF), or established a comprehensive legislative regime that would define clear rules of market supervision. Application of FATF standards requires the implementation of ML/TF risk identification and assessment associated with digital assets (hereinafter: DA), as well as the implementation of appropriate actions and measures to mitigate this risk. Inconsistent implementation of FATF standards hampers the creation of a single global approach to regulating the DA market.

Below we present a short overview of regulations and standards relevant for governing the prevention of ML/TF in the DA area, an analysis of DA market abuses – with an overview of relevant statistical data available in the market, management of the risk of ML and other misuses, with a separate insight into the geographic risk, transaction risk, client risk, DA type risk, and other risk factors that may bear relevance when assessing and mitigating risks in the DA market. Lastly, we present the supervision procedure over digital asset service providers (hereinafter: DASP) in the ML/TF area by applying a risk-based approach.

2 ML/TF regulations

To combat ML across the world, a number of laws and regulations have been passed. The differences in the adopted legislative regimes for ML/TF prevention mostly differ by country or region,[3] while their similarities are usually reflected in the constant creation and improvement of policies and procedures, as well as investment in technological resources, in their fight against financial crime. Below we provide a brief overview of goals and operating manner of FATF as an inter-government body, as well as systems for combating ML/TF adopted by the regulatory bodies of the European Union, the United Kingdom, the United States and Canada to better understand the

[1] Sesha, K.,Ying C., (2019). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity, available at: https://doi.org/10.1177/1057567719827051.

[2] Narain, A., Morreti, M., (2022). Regulating crypto, IMF, Finance and Development, available at: https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti.

[3] Ponamorenko, V., E., (2021). International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT). In: Ashmarina, S., Mantulenko, V., Vochozka, M. (eds) Engineering Economics: Decisions and Solutions from Eurasian Perspective, available at: https://doi.org/10.1007/978-3-030-53277-2.

risks and similarities in different approaches to ML/TF prevention. We also present the regulatory framework for combating ML/TF in the Republic of Serbia.

2.1 FATF

FATF is one of the leading creators of measures against ML/TF in the European Union (hereinafter: EU), founded in 1989 as an inter-government body. FATF's main goals are setting standards and promoting an efficient implementation of legal and operational measures for combating ML/TF. In addition to defining 40 recommendations, FATF has also developed other guidelines, such as the risk-based approach. In tandem with other international bodies, FATF works to identify vulnerabilities at a national level in order to protect the international financial system from misuse. FATF has 39 members, 37 member countries, and two regional organisations, the European Commission and the Gulf Co-operation Council. Accordingly, many laws and regulations across countries share common features which FATF promotes to its members. Its primary goal is to set up global standards for ML/TF prevention and to supervise the efficiency of their implementation. To this end, FATF regularly publishes updated recommendations for ML/TF prevention and closely cooperates with other organisations, including the IMF, the World Bank, the United Nations and FATF-style regional bodies (FSRB).

2.2 EU

The European Parliament issues directives on ML/TF prevention with the aim of offering the necessary guidelines to preserve the integrity and stability of its member countries' financial systems. The published EU directives are a set of rules for combating ML/TF and, among other, they indicate the current situation as to threats from ML/TF. Based on defined rules, member countries start improving their current laws and regulations to meet the defined requirements.

Directive (EU) 2018/843 of the European Parliament and of the Council – the fifth directive on anti-money laundering (AMLD5)[4] entered into force in 2018, while the deadline for member countries to align regulations ended on 10 January 2020. The AMLD5 is primarily concerned with regulating DA, including their legal definition, reporting requirements and regulations governing the area of DA. It also includes requirements, which imply that EU members regularly assess and update existing lists of high-risk third countries, taking into account factors such as corruption level and ML combating measures. In addition, it defines requirements pertaining to pre-paid cards, customer identification based on documents and also orders the inclusion of electronic identification which government bodies find acceptable. The AMLD5 also covers transactions associated with high-value goods and lists of politically exposed persons/officials.

In July 2021, the European Commission presented the sixth EU directive on anti-money laundering (AMLD6),[5] which still has not been formally adopted. The directive covers the alignment of the EU legal framework regarding ML prevention by defining a list of 22

[4] 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, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.

[5] Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0423.

criminal offenses associated with ML. It also defines requirements related to the expansion of criminal liability onto legal and natural persons (legal representatives of legal persons, authorised persons or persons tasked with conducted control within a legal person) based on the defined criminal offenses. At the same time, the directive is concerned with the issue of a dual criminal offense, specifying special requirements for the exchange of information between countries in order to enable cross-border criminal prosecution in member countries. Additionally, it defines stricter penalties for legal and natural persons, and harder prison sentences.

On 20 April 2023, the EU approved a revised Regulation on markets in crypto-assets (MiCa),[6] which should enter into force at end-2024. MiCa aims to develop a European approach encouraging technological development and ensuring financial stability and customer protection. The Regulation will amend the existing EU regulations, directives and rules that require financial institutions and DASPs to manage ML/TF risk. Among other, one of the goals of this document is to align the travel rule in the EU territory. Since the DA market is conducive to various forms of misuse, the Regulation will improve the existing structure, the market functioning system and the existing systems for combating ML/TF. According to many authors, the adoption of this Regulation is the first step towards the global regulation of the DA sector.

2.3 United Kingdom

The Financial Conduct Authority (FCA) is an independent non-government organisation tasked with regulating the financial market in the United Kingdom, including combating ML/TF. Since 10 January 2020, FCA has also been tasked with DASP supervision in the part related to ML/TF.[7] FCA's goals include consumer protection, as well as the preservation of financial system's integrity and stability. In terms of regulations and supervision, the FCA lays down legal guidelines for combating ML/TF aligned with FATF recommendations, and in the supervision procedure it verifies the implementation of defined guidelines, given that the United Kingdom is a FATF member.

2.4 USA

The Bank Secrecy Act (BSA) is the primary regulation against ML/TF in the USA, implemented by the Financial Crimes Enforcement Network (FinCEN). The BSA's main focus is prevention of ML, and as of recently its competence has been expanded to include other abuses. According to FinCEN, entities performing transactions associated with DA are subject to the BSA, regardless of the type of DA. FinCEN regulates all DA in order to prevent ML/TF, while the US Securities and Exchange Commission (SEC) regulates DA that can be considered securities. With the increase in DA-related criminal activities and abuses,[8] and in line with the USA's FATF membership, when

[6] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114.

[7] The Financial Conduct Authority, Cryptoassets: AML/CTF regime, available at: https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime.

[8] FinCen Advisory (2019). Advisory on Illicit Activity Involving Convertible Virtual Currency, available at: https://www.fincen.gov/sites/default/files/advisory/20190510/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

implementing its supervisory function FinCEN strictly adheres to FATF recommendations and requires DASPs to adhere to them as well.

2.5 Canada

The Financial Transactions and Reports Analysis Centre of Canada (Fintrac) is tasked with identifying and preventing ML/TF and other threats to Canada's security. Its goal is to facilitate the detection and prevention of ML/TF and issue measures to combat ML/TF. As an FATF member, Canada is also part of the Asian-Pacific Group (APG), a FATF-style regional body (FSRB)[9] which endorses FATF recommendations on ML/TF prevention. Fintrac regularly aligns its regulations and policies with FATF recommendations, including supervision procedures over obligors, such as DASPs.

2.6 Republic of Serbia

When adopting the Law on Digital Assets (RS Official Gazette, No 153/2020),[10] the Republic of Serbia also adopted amendments to the Law on the Prevention of Money Laundering and the Financing of Terrorism (RS Official Gazette, Nos 113/2017, 91/2019 and 153/2020)[11] on 29 December 2020, which are in line with FATF's revised recommendation 15[12] and AMLD5.

Pursuant to the Law on the Prevention of Money Laundering and the Financing of Terrorism, since 2018 the NBS has continually supervised virtual currency services providers, and on-site supervision is conducted based on the estimated risk and the adopted annual supervision plan. Virtual currency service providers are obligated to undertake all actions and measures to detect and prevent ML/TF in line with the Law on the Prevention of Money Laundering and the Financing of Terrorism, including due diligence, reporting suspicious transactions, internal control, records keeping, etc. The NBS may pronounce administrative sanctions to virtual currency service providers if they fail to adhere to regulations governing ML/TF prevention, and in cases of a more severe breach of obligations defined by these regulations, the NBS may also revoke the entity's licence.

In 2021 Serbia conducted an ML/TF Risk Assessment in the DA sector as a special risk assessment in the process of updating national ML/TF risk assessments.[13]

---

[9] Asia/Pacific Group on Money Laundering (APG), Members and Observes, available at: https://apgml.org/members-and-observers/members/details.aspx?m=39448e7e-b6a4-4abf-b803-3a6193c2beba.

[10] Law on Digital Assets (RS Official Gazette, No 153/2020), available at: https://www.nbs.rs/export/sites/NBS_site/documents-eng/propisi/zakoni/digitalna_imovina_e.pdf.

[11] Law Amending the Law on Prevention of Money Laundering and Terrorist Financing (RS Official Gazette, No 153/2020), available at: http://www.apml.gov.rs/english/legislation.

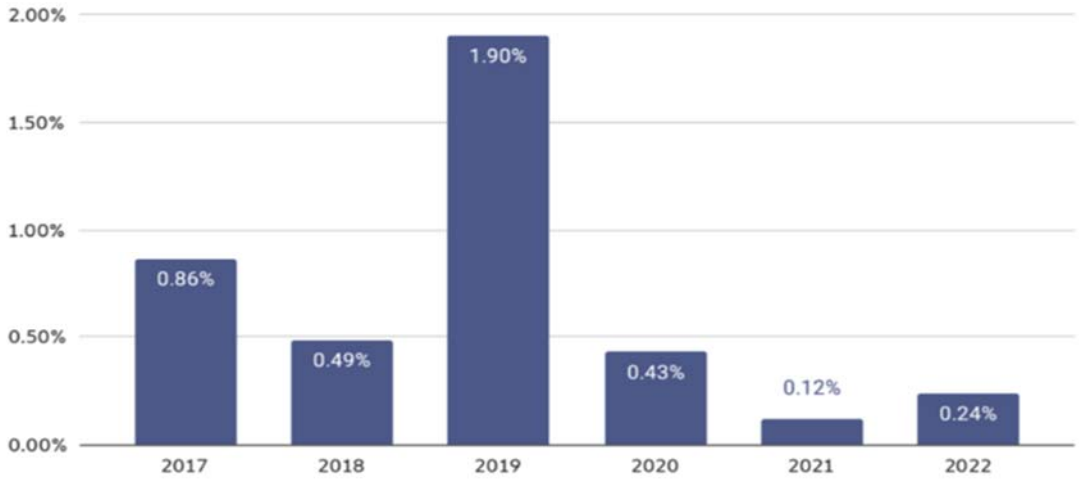
[12] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, available at: www.fatfgafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html.

[13] National Risk Assessment of Money Laundering and Financing Terrorism in the Digital assets Sector, in Republic of Serbia's National Risk Assessment (2021), available at: http://www.apml.gov.rs/uploads/useruploads/Documents/NRA%20novo%20skracena%20verzija-ENG%20FINAL.pdf.

3 Analysis of abuses in the DA market

Another indicator of the increasing use of DA is the overview of statistical data on executed transactions with DA. In 2021, the total transaction volume rose to USD 15.8 bn, which is 567% more than the total value in 2020. Criminal activities associated with DA also reached a record level in the same year. By way of illegal digital wallet addresses, usually associated with the dark web, around USD 14 mn was transferred – a significant increase from 2020 when this number equalled USD 7.8 mn. On the other hand, however, the percentage of transactions associated with abuses accounted for only 0.12% of total executed transactions with DA in 2021. According to the 2022 Chainalysis report, persons associated with cyber-crime laundered USD 8.6 mn through DA in 2021.[14]

Figure 1 **Share of transactions associated with abuses in the total volume of DA transactions (2017–2022)**



Source: Chainalysis.

Figure 1 shows the share of transactions associated with ML and other abuses in the total volume of executed transactions with DA in the period 2017–2022. In the observed period, the largest volume of DA transactions associated with abuses was recorded in 2019, when the share of these transactions in the total number of DA transactions amounted to 1.9%. Afterwards, between 2020 and 2021, these transactions contracted, dropping to 0.12% in 2021, only to edge up negligibly to 0.24% in 2022.

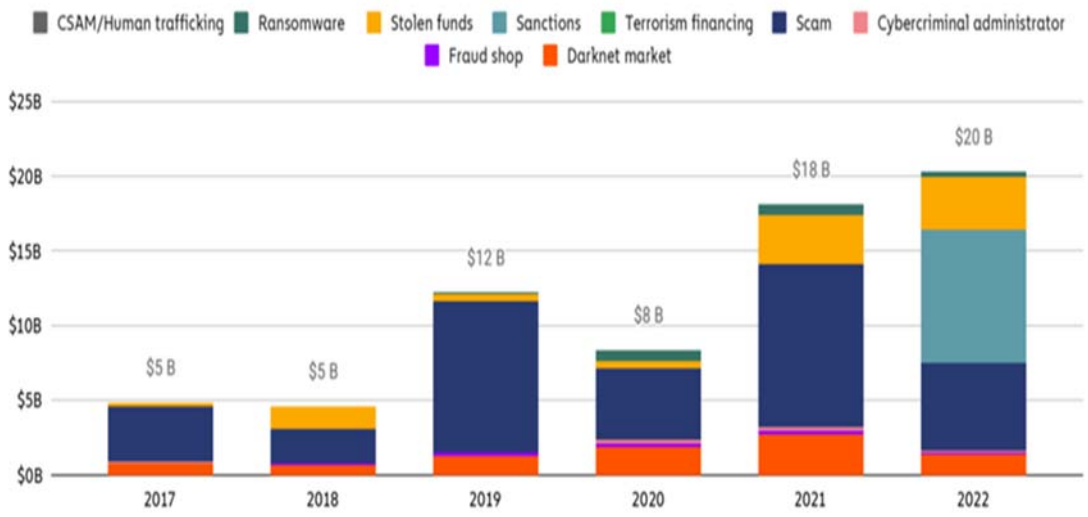
In 2022, ML activities associated with DA posted an increase worth USD 23.8 mn relative to 2021, when the figure stood at USD 14.2 mn. Of the total number of executed transactions, 43% of transactions associated with abuses in 2022 pertain to activities executed by sanctioned entities.[15] As Garantex, an organised platform for trading in DA, is associated with the majority of these transactions, in April 2022 OFAC launched a procedure to sanction the platform. However, Garantex being registered in Russia, it continued to operate with impunity. During 2022, the market was hit

[14] Chainalysis (2023)., Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity, available at: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

[15] Chainalysis (2023)., Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking, available at: https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction/.

by other turbulences, including the crash of several organised DA trading platforms, such as Celsius, Three Arrows Capital and FTX.

Figure 2 **Value of DA in dollars, used for various abuses (2017–2022)**



Source: Chainalysis.

Figure 2 presents the use of DA for various types of abuse in the period 2017–2021. During this period, we can conclude that DA were mainly used for scams, e.g. by promising profit from investing in a certain type of DA without any real basis, by posting false offers from organised DA trading platforms, advertising fake DA apps or mining networks that would attract potential investors, etc. Next, stolen funds are also considerably present as stolen funds, e.g. stealing DA by hacking digital wallets, as well as using DA in the darknet market. In 2022 a significant use of DA by sanctioned entities was noted.

The available data for 2023 indicate that criminal acts associated with DA have been partly mitigated. During 2023, the volume of transactions was generally declining, especially in the part of DA transactions associated with abuses, where a fall was recorded relative to the volume of legal DA transactions. Also, the value of DA channelled to digital wallet addresses, most often associated with dark web, and to risky entities declined by almost 42%.[16] The year 2023 also saw a fall in total revenues earned through fraud. By end-June 2023, entities engaged in DA-associated fraud earned 77% or USD 3.3 bn less than in June 2022.

The last several years saw an increase in ML abuse by decentralised exchange platforms because of their susceptibility to hacking, as well as an increase in darknet market activity. Also, some market participants tried to increase their profit and market share by advertising possibilities for earning high yields and investing in risky products.[17] Such business strategy is largely based on the continued increase in DA prices and value, that is, the inflow of new investments for settling current liabilities. Since a large increase in yields in a short period, as in traditional finance, always implies assuming

[16] TRM (2023)., Illicit Crypto Ecosystem Report, A Comprehensive Guide to Illicit Finance Risks in Crypto, available at: https://www.trmlabs.com/report#Money-Laundering.

[17] Financial Stability Board, (2022)., Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, available at: https://www.fsb.org/wp-content/uploads/P111022-3.pdf.

higher liquidity risk, this can lead to complex financial relations in the DA market, which are further facilitated by the anonymity and the high degree of volatility in DA prices.

Over time, as supervisory bodies improve and adjust their regulatory regimes for combating ML/TF to the circumstances in the DA market, to a certain extent we can see progress in the functioning of the global market in terms of preventing ML and other abuses associated with DA. This is also suggested by the above data, which testify to a certain improvement in decreasing the use of DA with the aim of conducting illicit activities.

4 Risk management

The complex structure of the DA market can be conducive to vulnerability and be susceptible to ML and other abuses in the market. The lack of a single global regulatory framework allows for a degree of independence in the conduct of market participants, and on those grounds it also leads to the emergence of new threats and risks from ML and other abuses. Data presented in FATF's latest report, published on 27 June 2023, also speak about the level of misalignment between regimes for combating ML/TF in the DA sector. Of the total number of observed countries, three-quarters are either not aligned or partly aligned with FATF requirements, three-quarters of countries (around 73%) do not implement adequate ML/TF risk assessments, and almost a third of countries have not defined the manner of regulating the DA sector, while around 10% have introduced a blanket ban on DA use. Although the travel rule is of key importance for financial crime prevention, the report states that more than 50% of observed countries still have not implemented it. As alignment with international ML/TF combating standards is a primary step in adequate risk management, the data presented indicate the need for countries to invest additional efforts in aligning their legal regimes to contribute to the improvement of existing ML/TF risk management systems.

Characteristics such as greater anonymity relative to traditional non-cash payment methods, the possibility of trading via online platforms and non-face-to-face customer relationships may permit anonymous transfer of funds if the sender and recipient are not adequately identified. Since there is no single, centralised global oversight system or software that would enable adequate tracking and identification of transactions, when monitoring risks and implementing supervision, supervisory bodies should monitor market changes that occur at a global level, having in mind the cross-border nature of DA. Due to the dispersion and global reach of DA, records on customers and executed transactions can be located with different entities in different countries, which requires continuous cooperation and an exchange of information between supervisory bodies.[18] According to international recommendations, when assessing the risk of ML and other abuses in the market, we need to take into account the factors such as geographic risk, transaction risk, client risk and other relevant indicators that may be important for determining the final risk assessment of an individual DASP and/or the DA sector.

[18] FATF (2014)., Virtual Currencies Key Definitions and Potential AML/CFT Risks, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

4.1 Geographic risk

Geographic risk can be considered individually, as well as when assessing customer or transaction AML risk. Indicators suggesting the presence of geographic risk, defined by regulators and other relevant institutions, are subject to change and have been on the rise over the past years.[19] Geographic risk is most often reflected in the possibility to transfer illegally acquired DA across the world in the absence of a single regulatory approach that would govern the area of DA. Different countries have different levels and types of risk, and factors underpinning the decision of whether a particular country carries a higher ML risk are the following: the presence of regulations on DA operations and obligation to licence or register DASPs, as well as the existence of supervision over DASPs; a country's alignment with amended FATF Recommendation 15; a country's legal and institutional framework in the area of ML/TF prevention; existence of sanctions, embargo or similar measures of the UN, the Council of Europe or another international organisation towards a particular country; these international organisations designating a country as an area failing to implement adequate ML/TF prevention measures and/or a country that funds criminal activities or organisations.

The results of geographic risk assessment can be used as a parameter for identifying more severe crimes, including ML, among other. To assess geographic risk, adequate systems need to be established that would determine the level of exposure to this risk. According to some recommendations, special attention needs to be paid to DA flows that originate (or are sent) from an organised DA trading platform not registered in the country, or to situations in which customers of a specific platform trade in DA in the country while having a permanent/temporary residence in another country with inadequate ML/TF prevention regulations, and similar. As in traditional financial flows, understanding and detecting geographic risk is necessary, and it is done by regular monitoring with the aim of protecting customers and DASP operations.[20]

4.1.1 Cross-border cooperation

Cross-border cooperation, which can have a world-wide reach depending on the case in question, partly leads to higher exposure to geographic risk in the sense of hampered risk monitoring, as well as oversight.[21] This primarily arises from the previously noted misalignment in regulations across countries. This is also supported by the fact that one and the same type of DA can be regulated and classified differently, or even non-regulated in some countries, which makes it easier to be transferred across borders. This leaves room for the occurrence of evasion, i.e. some market participants could be encouraged to dodge the implementation of strict regulatory requirements of some countries in this remit. As countries where the regulatory framework governing ML/TF prevention is lacking or is not aligned with FATF standards are fertile ground for criminal activities,[22] in this sense DASPs

[19] Data Derivative, (2022)., Geographic Risk Data, available at: https://www.dataderivatives.com/geographic-risk-data.

[20] Lemire A., K., (2022)., Cryptocurrency and anti-money laundering enforcement, Reuters, available at: https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/.

[21] Notabene, What Is Anti-Money Laundering (AML) & How Does It Apply to Crypto?, available at: https://notabene.id/crypto-travel-rule-101/aml-crypto.

[22] ComplyCube, How Crypto Businesses Can Spot Money Laundering Red Flags?, available at: https://www.complycube.com/en/how-crypto-businesses-can-spot-money-laundering-red-flags/.

need to increase surveillance of transactions from countries that have not implemented FATF recommendations.[23]

4.1.2 Geographic risk assessment

When assessing geographic risk, among other things, it is necessary to take into account the above-mentioned misalignment in the implementation of FATF standards across countries, which leaves room for the movement of illicit funds acquired through misuse.

Some indicators that may point to a high-risk profile of a country are the following:[24] the country is identified as an area associated with ML/TF; it is identified as an area with a significant level of organised crime, corruption or other criminal activities, including origin or transit countries for drugs, human trafficking, smuggling and illegal gambling; the country is an object of sanctions, embargo or similar measures issued by international organisations; the country has a weak regime of governance and law implementation, including countries identified in FATF statements as having a weak ML/TF prevention regime.

FATF conducts regular examinations of countries regarding deficiencies as to ML/TF risk or other threats that can affect the functioning of a country's financial system. It then publishes a list of high-risk countries where, depending on the detected deficiencies, a country can be included on the "Black List" or the "Grey List". FATF publishes lists of high-risk countries to encourage countries across the world to develop efficient procedures and regulations for ML/TF prevention, or improve the existing ones. Countries listed in either of these two lists generally fall short of adequate measures for ML/TF prevention, and are consequently susceptible to ML/TF, corruption and other abuses, therefore cooperation with them can pose a threat. In case of cooperation with high-risk countries, FATF requires the implementation of enhanced due diligence measures in order to protect the financial system from possible threats.

According to FATF's published report, as of June 2023, three countries have been blacklisted: Democratic People's Republic of Korea, Iran and Myanmar. The lack of efforts to combat ML/TF, proliferation of weapons of mass destruction and other illicit activities are the main reason for compiling this list.

Countries that are not assessed as high-risk in terms of ML/TF, but require increased monitoring due to strategic deficiencies in their regulatory regimes governing ML/TF prevention, are included on the "Grey List." Once a country is featured on this list, it implies that it is committed to working with FATF on resolving the identified deficiencies and that it is subject to additional oversight. As of June 2023, the "Grey List" includes the following countries: Albania, Barbados, Burkina Faso, Cameroon, Cayman Islands, Croatia, Democratic Republic of Congo, Gibraltar, Haiti, Jamaica, Jordan, Mali, Mozambique, Nigeria, Panama, the Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Uganda, United Arab Emirates, Vietnam and Yemen.

When assessing geographic risk, among other things, it is also important to underline the Basel AML Index which is the basis for ranking countries and assessing ML/TF risk at the Basel Institute

---

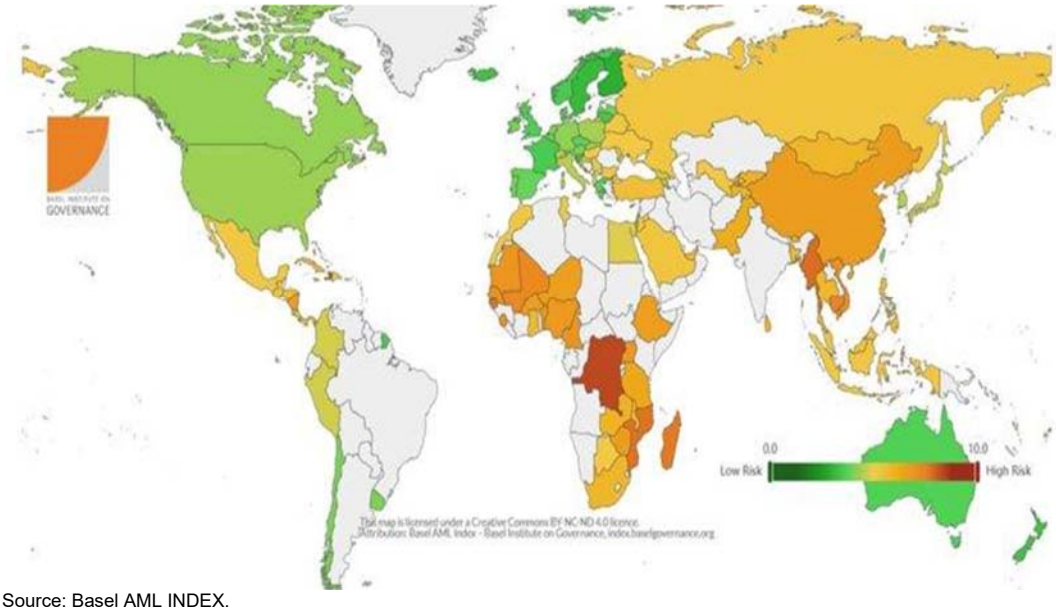
[23] Sanction Scanner, Examining the AML Risks and Red Flags of Crypto Exchanges, available at: https://sanctionscanner.com/blog/examining-the-aml-risks-and-red-flags-of-crypto-exchanges-258.

[24] FATF (2020)., Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets,

FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.

on Governance. Relying on data from publicly available sources, such as FATF, World Bank and the World Economic Forum, the Basel AML Index measures the total risk of ML/TF in countries across the world. The goal of the index is to establish and assess the regulatory exposure of a country to ML/TF, as well as its ability to respond to this. The Basel AML Index is based on five key factors, including: quality of the regulatory framework for ML/TF prevention (65%), exposure to bribery and corruption risk (10%), financial transparency and standards (10%), public transparency and accountability (5%), and legal and political risks (10%).

Figure 3 **Overall ML/TF risk assessment on a sample of 128 countries (2022)**



Source: Basel AML INDEX.

Figure 3 shows the assessment of the overall ML/TF risk during 2022 on a sample of 128 countries. According to the Basel AML Index, the overall risk was ten. High ML/TF risk was estimated in countries marked in red, with the Democratic Republic of Congo, Haiti and Myanmar having the highest score of the Index. Countries with an estimated low ML/TF risk are marked in green, with the highest score being that of Sweden, Andorra and Finland. Countries marked in orange and yellow are the ones where the risk is estimated as medium-high and medium-low.[25]

4.2 Transaction risk

According to FATF, some indicators that may point to a suspicion as to transaction risk that can indicate ML/TF are as follows: executing several high-value transactions in a short period; transactions that include multiple DA or several orders, without a logical business explanation; frequent transfers repeated over a certain period regarding the same DA to the account of more than one persons, from the same location or in relation to large transfers; transactions that involve

[25] Basel Institute on Governance, Basel AML Index 2022, 11th Public Edition Ranking money laundering and terrorist financing risks around the world, available at:
https://index.baselgovernance.org/api/uploads/221004_Basel_AML_Index_2022_72cc668efb.pdf

technologies unique to DA, such as P2P exchange platforms, mixer or tumbler services with the aim of increasing the anonymity of DA, and similar.

4.2.1 P2P transactions

P2P transactions may be potentially vulnerable to the risk of ML/TF, as they involve no intermediaries – DASP, i.e. an entity obliged to prevent ML/TF. P2P transactions may be used to conceal assets acquired by misuse or felony. On the other hand, it is often the visibility of P2P transactions on a blockchain that may contribute to conducting financial analyses or investigations for the purposes of law enforcement.

In one of its reports, FATF established, based on the input from blockchain analytic companies, that a significant amount of DA is transferred via P2P transactions.[26] In this regard, FATF defined a series of measures to be applied so as to mitigate the risk related to P2P transactions. Some of the recommendations are that countries should use risk-based approach when regulating P2P transactions and continuously adopt measures for reducing the risk of ML/TF, implement regular enhanced supervision over DASPs with a special focus on non-custodial wallet transactions, have additional AML/CTF requirements for DASPs suspicious of performing transactions with unregulated market entities, publish press releases to raise awareness of risks that P2P transactions pose, etc.

4.2.2 Travel rule

One of the main recommendations for reducing this risk is the implementation of the travel rule. In cooperation with other international regulatory bodies, FATF defined the travel rule, to improve the finances and DA market, fighting misuses. The travel rule is one of the FATF 40 recommendations which, inter alia, obliges DASPs to acquire data on all entities that participate in a DA transaction. If another DASP participates in a DA transaction, they are obliged to ensure that these data be delivered to the other DASP. In October 2018, FATF published that it will recommend to member countries to apply the travel rule, while in July 2022, the EU agreed with the implementation of this recommendation. The primary goal of the travel rule introduction is to assist supervisory bodies in detecting ML and other misuses.[27]

As the blockchain technology was not designed in a way that enables exchange of information concerning the transaction, DASPs, for the purpose of adequate implementation of the travel rule, should implement message exchange protocols, so as to obtain data about all participants in a transaction by means of safe exchange of information channels. The message exchange protocol is a set of rules for formatting, processing and exchange of information about the transaction principal and user. Some recommendations indicate the need for developing more than one protocol for exchange of information, because if a DASP is limited to exchange of information only with a DASP using the same protocol, information from other, different protocols applied by other DASPs will be inaccessible to them. On these grounds, many software development companies in the market launched an initiative for building the said protocols, to enable DASPs to meet the requirements imposed by the travel rule. This resulted in the appearance of numerous information exchange

[26] FATF (2021), Second 12-month Review Virtual Assets and VASPs, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assetsvasps.html.

[27] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.

protocols, while simultaneously raising the price and complexity of the application of the travel rule. Some of the better-known solutions are, for instance, Notabene and Trisa. Notabene established the first solution enabling DASPs to connect to the global network where 400 more DASPs are available to securely exchange information in different countries. On the other hand, Trisa is a P2P network enabling exchange of information necessary for the travel rule implementation.[28] The main goal of this network is to enable DASP compliance with the travel rule, without modifying the main blockchain protocols and increasing transaction costs. Nevertheless, Trisa, as many other solutions implemented in the market, facilitates the implementation of the travel rule only partially, bearing in mind that it partly depends upon available information of companies for blockchain analysis and for that reason many DASPs reject to implement this type of a solution, before it is widely used. These solutions in the market are available to all interested DASPs and to regulators for the purpose of exercising the supervisory function.

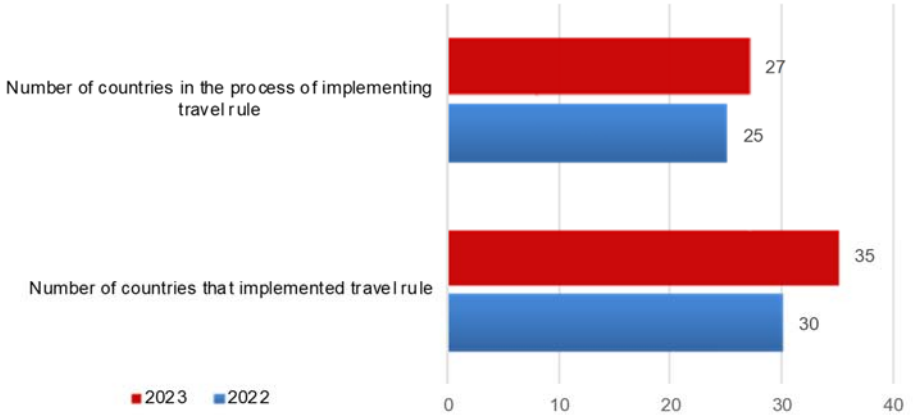
A risk-based approach is crucial for the efficiency of travel rule implementation. The travel rule is an efficient step in the international area which regulates AML. However, until uniform global regulations are adopted, some transactions will still be outside of the reach of supervisory bodies, given that this market allows some users to perform transactions without participation of licenced DASPs.

In June 2022, FATF published the report on travel rule implementation, stating that 98 jurisdictions observed[29] made limited progress in implementing and enforcing the rule. Namely, 29 out of 98 jurisdictions reported having passed the travel rule legislation, only 11 jurisdictions started enforcement and supervisory measures, while a quarter of jurisdictions started passing relevant laws and regulations. For comparison's sake, the progress reported in the fourth annual FATF report (2023) concerning the adoption of the travel rule and current challenges with its implementation, based on the voluntary survey that covered 151 jurisdictions, indicates again that most countries did not make sufficient progress with travel rule implementation. In this regard, in its report FATF pointed to the necessity of efficient action by countries and the necessity of travel rule implementation in supervision.

[28] Trisa, Decentralized Cryptocurrency Travel Rule Compliance, available at: https://trisa.dev/api/.

[29] FATF (2022), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.

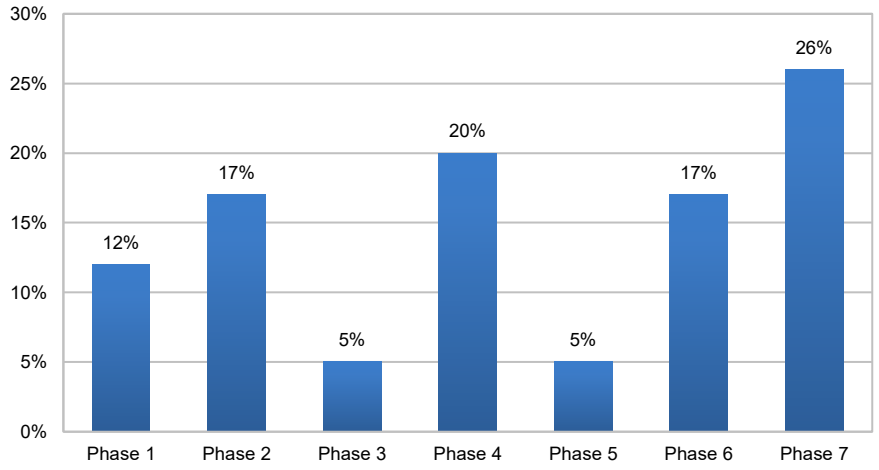
Figure 4 **Travel rule implementation (2022–2023)**



Source: FATF (2023), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France.

Figure 4 presents the number of jurisdictions which adopted or are in the process of adoption of the travel rule in the period 2022–2023. The 2023 report finds that more than a half of jurisdictions, i.e. 54%, took no steps toward the rule implementation. Of the total number of jurisdictions which adopted the travel rule, only 21% implemented and enforced it.

Figure 5 **Phases of travel rule implementation by countries (2022–2023)**



Source: FATF (2023) document, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France.

Note: The term "phase" (1-7) is used by the author with a view to simplifying the categorisation of the degree of travel rule implementation.

Figure 5 shows phases (1–7) which present in percentages to which degree jurisdictions across the globe implemented the travel rule, in the 2022–2023 period. Phase 1–12% of jurisdictions require from DASPs to implement the travel rule under certain circumstances only, such as the transaction value higher than the regulatory minimum; Phase 2–17% of jurisdictions enable DASP flexibility in terms of travel rule implementation, depending on circumstances related with the transaction; Phase 3–5% of jurisdictions require DASPs to perform transactions only with licenced, i.e. regulated market entities; Phase 4–20% of jurisdictions enable DASPs to perform transactions only with entities complying with the travel rule, Phase 5–5% of jurisdictions enable DASPs to perform transactions only with DASPs licenced under the laws of a certain jurisdiction; Phase 6–17% of jurisdictions enable DASPs to perform transactions with non-licenced entities that are not subject to

the regulations, but only in cases when measures are taken to reduce ML/TF risk; Phase 7–26% of jurisdictions enable DASPs to perform transactions with any DASP in the world, regardless of the licence/registration, respect of travel rules or other measures for reducing ML/TF risk.

The presented discrepancy between jurisdictions in terms of the implementation of the travel rule, may lead to more serious ML/TF-related misuse with DA and DASP.

Serbia, having adopted the Law Amending the Law on the Prevention of Money Laundering and the Financing of Terrorism[30] and harmonised with all international standards in the area of anti-money laundering and terrorism financing, implemented the travel rule.

4.2.3 Transaction monitoring

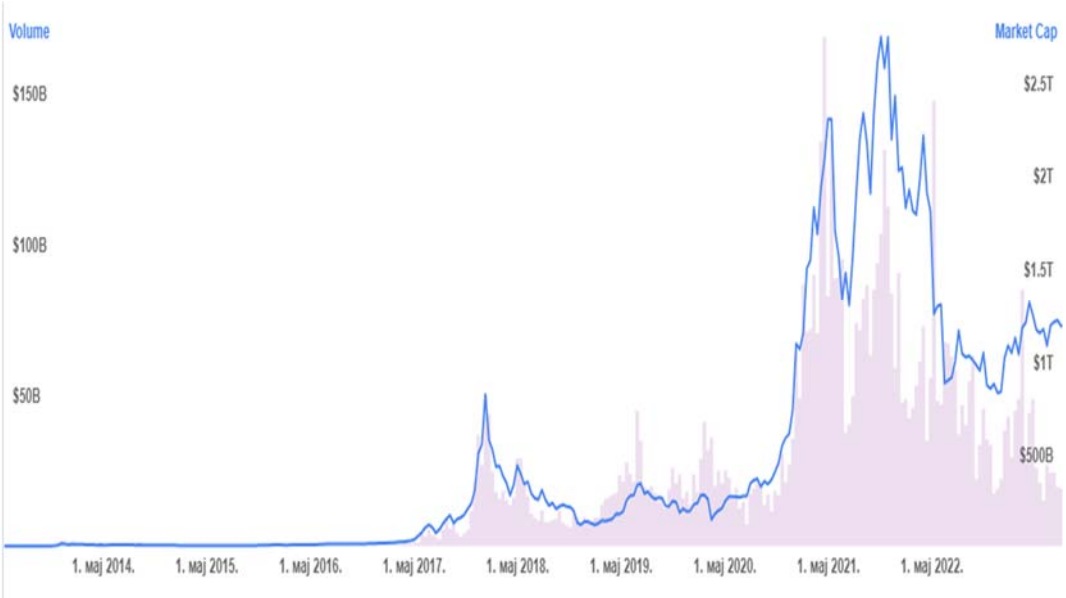
Monitoring transactions is one of the key steps in the fight against ML and other forms of financial crime. Except for the prevention of financial crime, monitoring of transactions at the same time contributes to compliance and harmonisation with regulations. The transaction monitoring process needs to be continuous so that transactions which do not fit the client behavioural pattern or deviate from usual transaction patterns are immediately recognised and further measures are taken. The transaction monitoring system may be manual or automated depending on the volume of transactions that the DASP performs in a business day. The level of transaction monitoring needs to be based on risk assessment by the DASP with enhanced monitoring conducted in situations with a higher risk of ML/TF. Systems for transaction monitoring used by a DASP need to be regularly revised and adjusted to the assessed risk of ML/TF.[31] Also, the recommendation is that transactions initiated by a third party, i.e. an entity in a business relation with the DASP, need to be considered and monitored under the same conditions as DASP-initiated transactions. Many companies in the market offer software solutions for automated transaction monitoring, both to DASPs and supervisory bodies for the purpose of exercising the supervisory function. Some of the most famous are Crystal Blockchain Analytics and TRM Labs, which at the same time offer solutions for travel rule implementation.

The importance and necessity of regular transaction monitoring are also indicated by many misuses in the market. One example is the case of organised platform for trade in digital assets BitMEX, accused in 2021 by FinCEN of performing the transaction worth around USD 209 mn on the darknet. At end-2022, organised platform Bittrex Crypto Exchange was fined with almost USD 30 mn by OFAC and FinCEN-a on account of violation of sanctions and obligations concerning AML. This platform was accused of participating in more than 116 thousand illegal transactions in the total value of around USD 260 mn. In addition to the said possible examples from practice which can arise daily, transaction monitoring is important from the view of constant changes in their volume and value, as well as the value of total market capitalisation.

[30] Law Amending the Law on the Prevention of Money Laundering and the Financing of Terrorism (RS Official Gazette, No 153/2020).

[31] The Financial Services Commission, British Virgin Islands, Virtual Assets Service Providers Guide to the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing, available at: https://www.bvifsc.vg/sites/default/files/vasp_aml_cft_guidance.pdf.

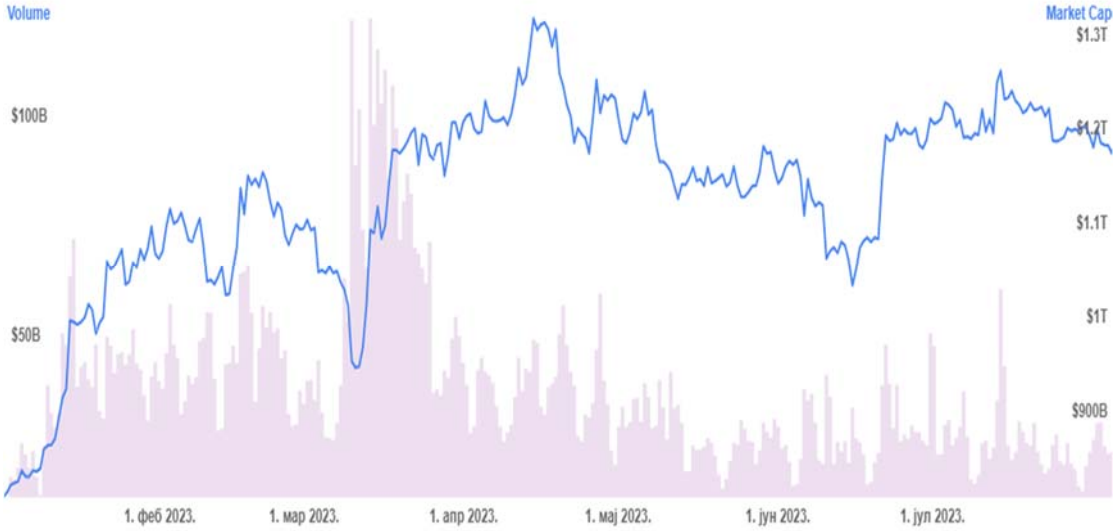
Figure 6 **Value of market capitalisation and volume of transactions (May 2014 – May 2022)**



Source: Live Coin Watch.

From May 2014 until May 2017, the value of market capitalisation and volume of transactions was almost unchanged. From May 2020 it recorded growth, only to reach more than USD 2.5 tn of market capitalisation and USD 150 bn of the value of the volume of transactions in 2021, after which it declined in 2022.[32]

Figure 7 **Value of market capitalisation and the volume of transactions (Fabruary 2023 – July 2023)**



Source: Live Coin Watch.

[32] Changes in the value of market capitalisation (May 2014 – May 2022), available at: https://www.livecoinwatch.com/crypto-market-cap.

From the beginning of 2023, the value of market capitalisation and the volume of transactions were on the rise, only to plunge at end-March, to below USD 1 tn of market capitalisation and USD 50 bn of the volume of transaction value, after which it recorded growth of over USD 1.3 tn of market capitalisation and USD 100 bn of the volume of transaction value. Afterwards it declined mildly in June 2023, and then increased slightly in July 2023 up to around USD 1.2 tn of the volume of market capitalisation and more than USD 100 bn of the value of transaction volume.[33]

4.3 Client risk

A higher exposure to the risk of ML and other misuses with the DASP in terms of client structure may be indicated by: the number of clients – legal entities with a complex ownership structure, a number of clients – off-shore legal entities or with off-shore legal entities in their ownership structure, the number of clients who are public officials; the number of clients with public officials in their ownership/management structure, etc; the number of clients non-residents; the number of clients non-residents – natural and legal entities from high-risk and off-shore countries, or countries with strategic defects in the area of AML/CTF; the number of clients performing activity that carries increased ML/TF risk; the number of clients that are subject to enhanced customer due diligence.

According to FATF, when assessing this risk, DASPs are obliged to pay attention to the behaviour of participants in the transaction, i.e. the sender or recipient of an illegal transaction:[34] creation of special orders under different names to circumvent limits of the DASP with a view to preventing ML/TF; transactions initiated from unreliable IP addresses, an IP address from a country under sanctions or an IP address previously marked as suspicious, incomplete or insufficient KYC information, or a client rejects requests for KYC (documents or queries concerning the source of assets); the sender/recipient of a transaction provides incorrect information about the transaction, source of assets and other party; a client provided forged documents. In addition, appearance of the address of the DA client in public fora connected with illegal activities, or reliable sources of information saying that the client has been involved in a criminal act or misuse require that DASPs take certain measures considering the high risk of ML/TF.

Suspicious client behaviour may be the consequence of using the client for the purpose of fraud. Victims may be misused by professional money launderers or may be victims of fraud with a view to transferring illegally acquired assets without the knowledge of their origin. Potential fraud victims may be indicated as follows:[35] a sender is not familiar with DA technology or solutions for keeping digital wallets; a client who is significantly older than the average platform user opens an account and participates in a large number of transactions, suggesting that older people are often used as victims of financial exploitation; a client is in dire financial straits often used by drug dealers for their misuses; a client buys large quantities of DA not in line with the real financial situation of that client possibly indicating a victim of fraud for the purpose of ML.

To reduce the said risks, according to FATF, the DASP must monitor the activities of all participants in a transaction related with DA with due diligence. Regular education and informing of

[33] Changes in the value of market capitalisation and volume of transactions (February 2023 – July 2023), available at: https://www.livecoinwatch.com/crypto-market-cap.

[34] FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.

[35] Ibid.

the public about new technologies and blockchain may help mitigate the said risks.[36] Better understanding of their advantages and disadvantages may reduce their use particularly in terms of the number of victims of misuses.

4.3.1 KYC (know your customer)

The KYC procedure is carried out during the identification and verification of potential customers, and the monitoring of their behaviour after the establishment of a business relationship. KYC is one of the steps in the fight against ML/TF. KYC procedures are aimed at establishing effective ML/TF risk management, monitoring customers' transactions and business operations, in order to ensure that customers with whom future business relations will be established will not affect the security and stability of DASP's operations.[37]

As part of the KYC, the customer/client identification procedure – CIP, involves the collection and analysis of information for the purpose of identifying the customer, and then verifying the obtained data (name and surname, address, date of birth and business licences/founding documents of the company) in relation to public information and blacklists in the prevention of ML/TF. The CDD procedure within the KYC process involves the assessment of a new customer/client, i.e. a potential business relationship. During the implementation of CDD, an additional analysis of the available transaction history is carried out with a view to determining the customer's potential ML/TF-related risk, and an analysis of the customer's market behaviour. EDD is a procedure within the KYC process carried out in cases when the customer is suspected of being at a higher ML/TF risk level, which requires additional collection of information.

There is still no global standardised system for the implementation and enforcement of KYC, but there are a number of software solutions which provide efficiency in its implementation. Moreover, there is a certain level of inconsistency between countries in terms of regulations and requirements for the implementation of the KYC procedure.

Given that this procedure can be expensive and time-consuming, all entities obliged to operate in accordance with the regulations governing the prevention of ML/TF, including a DASP, should apply a risk-based approach, which will allow them a certain degree of flexibility regarding the choice of procedure to be implemented. It is important to point out that the CDD procedure, after a detailed analysis of the customer with which the business relationship is established, further implies continuous monitoring of the customer during the established business relationship.[38] As the CDD procedure is a key part of the KYC process, it is described in more detail below.

4.3.2 CDD (customer due diligence)

CDD is a procedure that involves gathering information about customers in order to identify and mitigate the ML/TF-related risks and other abuses. The implementation of CDD helps the DASP in assessing the ML/TF-related risks regarding covert activities with digital assets, identifying

[36] Al-Amri, R., Zakaria, NH., Habbal, A., Hassan, S., (2019)., Cryptocurrency adoption: current stage, opportunities, and open challenges, available at: http://doi.org/10.19101/IJACR.PID43.

[37] CipherTrace Cryptocurrency Intelligence, (2020)., CipherTrace Geographic Risk Report: VASP KYC by Jurisdiction, available at: https://ciphertrace.com/wp-content/uploads/2020/10/CipherTrace-2020-Geographic-Risk-Report-100120.pdf.

[38] Sanction Scanner, Conducting Effective Customer Due Diligence, available at: https://sanctionscanner.com/blog/conducting-effective-customer-due-diligence-346.

suspicious customers or transactions exceeding the legal threshold.[39] The CDD procedure, among other things, includes customer identification, and where applicable, customer's beneficial owner, as well as the verification of the customer's identity based on reliable information.[40] Some of the primary information that the DASP should obtain in the CDD procedure about the customer are: proof that the DASP is regulated; proof that the DASP did not previously participate in a ML/TF-related crime; proof that the DASP operates in accordance with a legal regime harmonised with international standards for the prevention of ML/TF. The CDD process also includes understanding the purpose and intent of the business relationship, as well as obtaining relevant information about situations that indicate a higher ML/TF risk.

The FATF recommendations do not specify how this information is collected. Instead, they indicate that a combination of publicly available information and information collected directly from the DASP is sufficient to implement this procedure. According to FATF, a DASP should use all available data that would help it decide whether to carry out a transaction with a customer, that is, establish a business relationship with another DASP. In addition, when establishing a business relationship with a customer, the DASP should consider the level of ML/TF risk of that customer, as well as all the measures it could take to reduce the recognised risk.

Following the ML/TF risk assessment, the DASP further assesses whether it is necessary to obtain additional information related to the business relationship established with the customer. In the event of suspicion indicating a high ML/TF risk level, the DASP is obliged to obtain additional information and implement enhanced customer monitoring measures. In such cases, the DASP may apply some of the following actions:[41]

– obtain additional information from more reliable sources that can be used to determine the customer's risk profile;

– conduct additional searches (e.g. darkweb search), to determine whether the customer is in any way connected with possible abuses;

– undertake further procedures for the purpose of verifying the customer, or the customer's beneficial owner, in order to better understand the risk that the customer, or its beneficial owner may pose for the DASP's business.

DASPs are obliged to respond to the requests of supervisory authorities at all times, and in the case of using automated systems for customer verification or determining the customer's risk profile, use those that comply with legal regulations, which will not hinder the exchange of information with supervisory authorities or procedure of off-site/on-site supervision by supervisory authorities in any way.

Regardless of the nature of the business relationship or transaction, the country, i.e. the supervisory authorities play a key role in the application of effective procedures for the identification of the customer, risk profile or any other risk by the DASP, by means of their regular supervision

[39] IMF, (2021)., Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism: Effective AML/CFT Regulatory and Supervisory framework – some legal and practical considerations, available at: https://www.elibrary.imf.org/downloadpdf/journals/063/2021/003/article-A001-en.pdf.

[40] SWIFT, Society for Worldwide Interbank Financial Telecommunication, What is Customer Due Diligence (CDD)?, available at: https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd.

[41] FATF, 2021, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html).

procedures, guidelines for business compliance with relevant regulations and pronounced measures on the basis of implemented supervision procedures.

4.4 DA type risk

There are currently around 10,000 different DA types available in the world.[42] Depending on the regulatory framework and regulations in the DA area, their classification varies. Under the Law on Digital Assets, DA in Serbia include virtual currencies and digital tokens.[43] The NBS carries out the supervision of virtual currency service providers and the Securities Commission supervises digital token service providers.

Some countries enable the use of anonymous DA, which, as such, is prone to various types of abuse.[44] The use of anonymous DA is strictly forbidden in Serbia, as are the mixer and tumbler services that are most often used for ML/TF purposes, which partly limits the chances of market abuse.

The emergence of new DA types has resulted in robust development of the DA market in the past years. Bitcoin, as the best known and most widely used virtual currency, now shares the market with a large number of altcoins, but is still dominant. Many altcoins that have appeared offer a higher degree of anonymity. An anonymous DA is potentially susceptible to ML/TF as it enables the concealment of identity of transaction participants. The nature of blockchain is such that each transaction is recorded in the system, but the DA characterised by anonymity, alongside the use of additional tools contributing to anonymity, can "conceal" parts of blockchain. This opens room for persons related to criminal activities to illegally transfer the obtained funds more easily and without being tracked. Some types of anonymous DA include: Monero, Dash, Zcash, Horisen, Verge, Grin, Bytecoin. Monero is the most widely used anonymous DA, mostly on the dark web, such as, for instance, Hydra dark web market, which was closed in 2022.[45]

According to some authors, anonymous DA are a means used by organised criminal groups (OCG) to carry out illicit activities.[46] OCG may use anonymity features and the decentralised nature of some types of DA for ML/TF purposes and other misuses?. In such cases, illegally acquired assets are transferred directly from one digital wallet to another. Mixer and tumbler services reduce transparency and conceal DA financial flows to a greater extent. Each use of the existing anonymisation techniques, along with the use of software enabling anonymous communication across the world, such as, for instance, the Onion Router, can indicate abuse in terms of ML and other criminal activities.

Acting in line with regulators' instructions, many organised DA trading platforms removed from their offer of DA with anonymity features. Many platforms were accused by regulators of performing

---

[42] Statista, Number of cryptocurrencies worldwide from 2013 to August 2023, available at: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.

[43] Law on Digital Assets (RS Official Gazette, No 153/2020).

[44] Global Initiative against Transnational Organised Crime, Crypto, crime and control, Cryptocurrencies as an enabler of organised crime, (2022), available at: https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organised-crime.pdf.

[45] Office of Public Affairs, U.S. Department of Justice, (2021)., Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.

[46] Institute for Security and Development Policy, Organised Crime Groups, available at: https://isdp.eu/projects/organised-crime-groups/.

illegal DA transactions. Numerous supervisory authorities and AML/CFT agencies have developed adequate channels of monitoring suspicious transactions and abuses related to anonymous DA. Their role is important as they supress and mitigate this risk. The most important steps to be undertaken include the defining of unique market rules, regular education of the public, and strengthening the capacity for exercising the supervisory function.

"Stable DA" should be taken into account when considering the risk as to the DA type. "Stable DA" can be exposed to the ML/TF risk, with the degree of risk exposure depending on a number of factors, notably the legal AML/CFT system of a country, the degree to which the public accepts "stable DA", and the regulator's supervisory function.

According to FATF, the expression "stable DA" is not a clear legal or technical category of DA, but is primarily a marketing term used to promote this type of DA. FATF therefore uses the expression "so-called stablecoins". According to FATF, "stable DA" is by its nature very similar to other DA types, categorised as subject to ML/TF[47] due to potential anonymity and global outreach. Concerns may be raised that some types of "stable DA" may have the potential of broad use, which may increase ML/TF risks. Broad use is an important factor of ML/TF risk as the DA that is freely replaceable and used in the market is subject to a higher ML/TF risk and the risk of criminal abuse.[48] The reduced volatility of "stable DA" prices may help step up the pace of broader acceptance. On the other hand, a broad use of regulated and supervised "stable DA" in the segment of ML/TF prevention may provide insight to supervisory authorities into illicit market activities and mitigate ML/TF risks.

4.5 Other risk factors

In addition to the above risks concerning possible abuses relating to ML/TF, this market features many more various types of risk, such as, for instance, macroeconomic risks, DA price volatility risk, technological risks, operational risks, liquidity risk, data accuracy and reliability risk, and numerous risks that may impact a country's financial system. Below we give an overview of several risks that may be associated with ML/TF abuse.

4.5.1 DA trading

DA trading functions similarly as the traditional finance market. By mediating among stakeholders in the market, platforms enable DA users to be involved in various types of transactions. The main trade risks are comparable with traditional exchange risks, including malfunctions, trading abuse, and unsuccessful or untimely transaction execution and settlement. The materialisation of these risks may lead to market failure, a higher degree of misuses and liquidity risk. Several DA trading platforms failed due to poor capitalisation, risky trading and exposure to risky entities prone to misuses. The failure of these platforms significantly influenced numerous investors and brought to the fore potential risks that other market participants should be aware of. In terms of DA trading, P2P trading is commonplace – it implies transactions without intermediaries, i.e. without DASPs. The client identification procedure does not take place in such cases, increasing the risks of ML/TF

[47] Association of Certified Anti-Money Laundering, Understanding "Stablecoin" AML/TF risks, available at: https://www.acams.org/en/media/document/30786.

[48] President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, Report on Stablecoins, available at: https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

and other misuses. The direct contact between two stakeholders can also lead to contract termination and the sum agreed between users is not paid. However, in this domain, the use of smart phones for P2P trading ensures the identification of parties and transaction terms.[49] P2P market trading is mainly reserved for low-value transactions, while OTC DA trading has become popular for larger transactions. OTC trading is another method of direct exchange between two stakeholders without an intermediary. Stakeholders can specify the price as agreed, without exclusive reliance on the current market price. Professional independent brokers are also active in the market, while some organised platforms opened separate OTC trading sections with the aim of compliance with AML/CFT regulations.

4.5.2 Data accuracy and reliability

Due to their broad use, available data on DA-related activities may in some cases be unavailable to regulators or the public as non-regulated entities, exempt from the duty of regularly reporting to the regulatory body, can often implement those activities in practice. The lack of available and reliable data is a challenge for regulators that monitor and assess DA-related risks. Many authors believe that activities of DA market participants are fully transparent and reliable as they are available in public blockchain systems. On the other hand, according to some authors, a part of the activity can be "hidden" by using privacy enhancing technologies. Given potential imprecision, it is challenging for the regulator to assess and analyse data. This requires constant technological enhancement of data verification resources, including the verification of data reliability, so as to ensure that risk monitoring and the regulator's supervisory function yield proactive results.

4.5.3 Provision of combined services

The provision of different services not directly related to DA by a single organised DA trading platform may lead to risk occurrence. In some parts of the world, in addition to their primary activities relating to DA services, some platforms carry out trading in financial derivatives and similar products, which may create room for abuse. Similarly to the regulatory approach in the financial market, the recommendations to overcome this risk stem mainly from the fact that countries should consider banning the provision of combined services by organised platforms.

4.5.4 Digital wallet (custodial/non-custodial)

The digital wallet is an important segment of the protection of DA users. There are two types of digital wallets – custodial and non-custodial. The main difference between them is that in case of the custodial wallet, i.e. the provision of services of keeping DA / private keys of users, requirements prescribed by law must be met, such as: obtaining a license, implementing KYC procedures and complying with other relevant AML/CFT regulations, etc.[50] In most countries that have regulated the DA field, these services are provided by licensed DASPs. On the other hand, in case of the non-custodial wallet, the DA holder is fully responsible and independently manages his wallet, i.e. private

[49] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html.

[50] Legal Nodes, (2023), A Legal Guide to Custodial & Non-Custodial Wallets, available at: https://legalnodes.com/article/custodial-non-custodial-wallets.

key, and available DA. In that case, the DA holder, i.e. the user bears the risk of losing the private key or DA. However, the biggest risk that may arise in relation to the non-custodial wallet is that it is exempt from oversight, i.e. there is no obligation to obtain a specific license or to fulfil the AML/CFT conditions prescribed by law,[51] which may leave room for transactions with third parties, which are, for instance, linked to the dark web, or third parties linked to ML/TF abuses, without traceability. According to some reports, during 2022 and 2023, a higher usage of non-custodial wallets was observed.

4.5.5 Decentralised exchange platforms

In addition to non-custodial wallets and P2P transactions, decentralised exchange platforms may indicate a higher ML/TF risk. Some countries have taken measures to mitigate the risk, including the identification of natural/legal persons that perform transactions via these platforms, which is necessary given that they do not include intermediaries who are obliged entities under the AML/CFT law. According to available data for 2021, a larger quantity of DA was misused on decentralised exchange platforms than on any other organised DA exchange platform in the world. This may reflect the advancement of the AML/CFT system by DA trading organised platforms.[52]

The volume of transactions performed on decentralised exchange platforms increased by 912% in 2021. This implies the necessity of continuous monitoring of decentralised exchange platforms both by countries and FATF, so as to ensure adequate application of the defined guidelines.[53] According to the 2022 FATF report, trading on decentralised exchange platforms increased significantly, and that trend continued into early 2023. Consequently, decentralised exchange platforms require additional attention and interpretations from FATF.

5 DASP supervision

To ensure stable and safe functioning of the DA market, it is necessary to define a supervisory framework that will enable adequate monitoring of all market participants and the detection of potential abuses. Many countries face challenges in implementing effective supervisory regimes and a risk-based approach, which is one of the main FATF guidelines. The FATF recommendations provide supervisory authorities with flexibility in choosing the supervisory model to be applied, depending on the risks present in the DA sector.[54]

The transition from a rule-based to risk-based approach in the process of exercising the supervisory function requires certain changes in supervision, such as, for instance, additional investment in supervisory resources and training. The application of a risk-based approach, in the exercise of the supervisory function, contributes to efficiency in the ML/TF detection and prevention. The focus is on assessing current and future risks, as well as the vulnerability of DASPs from the

[51] FATF (2023), Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html.

[52] Chainalysis, (2022), Hackers Are Stealing More Cryptocurrency From DeFi Platforms Than Ever Before https available at: https://blog.chainalysis.com/reports/2022-defi-hacks/.

[53] FATF (2022)., Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, available at: https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.

[54] The Council of Europe, (2023), Money Laundering and Terrorist financing risk in the world of virtual assets, available at: https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4.

ML/TF aspect. Based on that assessment, supervision priorities are determined and resources channelled by the supervisory authorities, i.e. enhanced measures in circumstances when the risks are higher, and simplified ones when the risks are assessed as low. Risk assessment using this approach also requires the definition of procedures and methodologies by the supervisor, which will enable better understanding of the risk and the degree of exposure to this risk. The success of the conducted supervision also depends on the supervisor's understanding of the risks.

During the supervision procedure, supervisors should determine how much attention needs to be paid to some supervised entities, i.e. they should understand how the supervised entities are exposed to the ML/TF risk, in order to apply appropriate measures in respect to them. Supervisors' understanding of the ML/TF risk requires regular risk assessment and updating of earlier assessments, in order to obtain a broader picture of DASPs' ML/TF risk exposure. In addition, supervisory authorities, i.e. supervisors in the supervision procedure, among other things, check compliance of DASPs with regulations, as well as the actions taken in the fight against ML/TF. It is necessary to take into account all the risk factors that DASPs recognise in their operations, as well as the risk factors that are recognised by the supervisory authority, with a focus on the geographic risk, client risk, DA type risk, transaction risk, and other recognised threats and risks that may affect the safety and stability of DASP operation.

Some of the features of the DA market, such as DA anonymity, the possibility of establishing non-face-to-face business relations, transactions without DASP mediation, as well as the possibility for DASPs registered in one country to provide their services to clients in another country, whose AML/CFT regime is not aligned with the DASP's host country regime, or is not in place at all, contribute to a higher ML/TF risk. In such cases, it is necessary to undertake enhanced supervisory measures, especially in relation to the complexity inherent to cross-border transactions, involving multiple participants from different countries, with differently defined AML/CFT regimes. Moreover, the possibility of accessing services by clients of one country, provided by a DASP registered in another country, also indicates the unauthorised provision of DA services and entails additional examinations concerning ML/TF. Therefore, the supervisory authorities should consider the establishment of mechanisms that would enable, i.e. authorise a specific DASP to provide its services in other countries as well, but under the regulator's supervision.[55] Given the global reach of DA, DASPs and DA issuers should be subject to adequate supervision commensurate with their size, complexity and risks arising from their business activity.

Although there is an evident difference between the regulatory and supervisory regimes governing DASP operations across countries, most regulators, regardless of the country of origin, require DASPs to take all actions and measures to prevent and detect ML/TF, with a particular focus on due diligence, reporting of suspicious transactions, regular AML training of employees, implementation of internal controls, record keeping, regular updating of existing risk assessments, etc. Also, the criteria applied by DASPs as a basis for deciding on the intensity of monitoring various risks and threats are taken into account in the supervision procedure, and need to be clear and documented, so that supervisors in the supervision procedure gain a clear insight into how DASPs act in concrete situations. DASPs are obliged to regularly report to the supervisory authorities about all changes in operation, especially if there are changes in the business model based on which the/a? DASP provides its services. Based on the regular reports submitted by DASPs to the supervisory

[55] FATF (2021), Guidance on Risk-Based Supervision, FATF, Paris, available at: www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html.

authorities, they carry out risk assessment in accordance with the defined risk assessment methodologies and matrices, and based on the results, determine which DASPs require enhanced supervision and application of enhanced due diligence measures. Furthermore, the use of new technologies to improve AML/CFT compliance in the market, such as, for instance, advanced analytical systems for tracking transactions, brings new challenges for supervisors, requiring additional training and continuous improvement of supervisors' knowledge.

If, in the process of off-site and on-site supervision, the regulator ascertains that a DASP acts contrary to AML/CFT regulations, depending on the legal regime of the country, it may impose certain measures and sanctions in respect of the supervised entity, and in some circumstances revoke the license for the provision of DA services, provided the regulatory framework of the specific country also regulates the licensing procedure, as is the case in the Republic of Serbia.

According to the recommendations, international cooperation between countries is the key to the regulator's successful exercise of the supervisory function. In the process of licensing or supervision, the exchange of information with regulators from other countries where a DASP operates enables better understanding of its business model and activities in the foreign market, which is relevant from the aspect of risk assessment by supervisory authorities. Similarly, the exchange of knowledge and practical experience between supervisors can contribute to the advancement of supervision procedures and better understanding of market risks.

The quality of the conducted risk assessment and supervision by the supervisor also affects the implementation of the National ML/TF Risk Assessment (hereinafter: ML/TF NRA) in a country's DA sector. Understanding the risks to which the DA sector is exposed and how DASPs, as market participants, are exposed to the ML/TF risk, contributes to the final results of the ML/TF NRA.[56] In this complex procedure, it is necessary to exchange information between supervisory authorities, law enforcement authorities, the judiciary, customs, and intelligence services. Relevant information on ML/TF risk exposure can also be obtained through cooperation with the private sector, which is increasingly important for effective supervision, especially in the domain of innovative sectors such as the DA sector. However, the greatest contribution to the ML/TF NRA is the understanding of risks by supervisors conducting regular supervision and performing risk assessment on a daily basis. The implementation of the ML/TF NRA in the DA sector, among other things, implies an analysis of the sector size, the supervised entities operating in the sector, the scope and degree of their business activity, and their compliance with valid AML/CFT regulations. According to some of the recommendations, during the sectoral risk assessment, it is recommended to categorise the supervised entities within different types of risks.

Effective ML/TF risk management in the DA sector and supervision in that domain, at the level of a single country or legal person, requires the provision of sufficient capacities and resources, as well as a system of information exchange between supervisory authorities.[57] At the same time, international standards draw particular attention to the fact that prohibiting the provision of DA services, which include the use of anonymous DA, by the authorities, and which may lead to the impossibility of identifying the user, is of great importance for mitigating the ML/TF risk.

---

[56] FATF (2021)., Guidance on Risk-Based Supervision, FATF, Paris, available at: www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html.

[57] Financial Stability Board, (2022), International Regulation of Crypto-asset Activities, available at: https://www.fsb.org/wp-content/uploads/P111022-2.pdf.

6 Conclusion

The establishment of a comprehensive regulatory regime and the supervisory framework is imperative in the regulation of the DA market. Many countries have made progress in enhancing their legal systems and harmonising them with international standards. Still, the obvious differences in the approach to market regulation open up new possibilities for ?misuse. To provide support to countries, FATF intends to carry out public identification of countries in early 2024 with a detailed description of the steps they have taken in the process of harmonisation with international standards, so that these countries improve their legal regimes.

The risk of ML/TF and other abuses, with a clear upward tendency, implies the definition of an effective risk management system. The impact of risk of ML/TF and other misuses on a country's system largely depends on its efforts to establish an appropriate framework in response to threats. In addition to the necessity of monitoring, analysing and managing recognised risks, preserving the stability and security of a country's government system entails regular exercise of the regulator's supervisory function. The quality of the conducted risk assessment and supervision of DASPs is also important for the implementation of the National ML/TF Risk Assessment in the DA sector.

Regular risk monitoring and analysis, as well as the application of a risk-based approach in supervision procedures will ensure alignment with international standards. On the other hand, it will also open up the possibility of creating sustainable AML/CFT and anti-abuse systems which, with an adequate legal regime, strengthen consistency and efficiency in preventing potential abuses, with the aim of preserving stability.

References

Al-Amri, R., Zakaria, NH., Habbal, A., Hassan, S., (2019)., Cryptocurrency adoption: current stage, opportunities, and open challenges available at: http://doi.org/10.19101/IJACR.PID43.

Asia/Pacific Group on Money Laundering (APG), Members and Observes, available at: https://apgml.org/members-and observers/members/details.aspx?m=39448e7e-b6a4-4abf-b803-3a6193c2beba.

Basel Institute on Governance, Basel AML Index 2022, 11th Public Edition Ranking money laundering and terrorist financing risks around the world, available at: https://index.baselgovernance.org/api/uploads/221004_Basel_AML_Index_2022_72cc668efb.p.

ComplyCube, How Crypto Businesses Can Spot Money Laundering Red Flags?, available at: https://www.complycube.com/en/how-crypto-businesses-can-spot-money-laundering-red-flags/.

Chainalysis (2022)., Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity, available at: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

Chainalysis (2023)., Crypto Crime Trends for 2023: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking, available at: https://blog.chainalysis.com/reports/2023-crypto-crime-report-introduction/.

Chainalysis, (2022)., Hackers Are Stealing More Cryptocurrency From DeFi Platforms Than Ever Before https available at: https://blog.chainalysis.com/reports/2022-defi-hacks/.

CipherTrace Cryptocurrency Intelligence, (2020)., CipherTrace Geographic Risk Report: VASP KYC by Jurisdiction, available at: https://ciphertrace.com/wp-content/uploads/2020/10/CipherTrace-2020-Geographic-Risk-Report-100120.pdf.

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, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.

Data Derivative, (2022)., Geographic Risk Data, available at: https://www.dataderivatives.com/geographic-risk-data.

The Financial Conduct Authority, Cryptoassets: AML / CTF regime, available at: https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime.

FinCen Advisory (2019). Advisory on Illicit Activity Involving Convertible Virtual Currency, available at: https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

FATF (2014)., Virtual Currencies Key Definitions and Potential ML/TF risks, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FATF (2020)., Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.

FATF (2021)., Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, available at:

www.fatfgafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html.
FATF (2021)., Guidance on Risk-Based Supervision, FATF, Paris, available at: www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html.
FATF (2021)., Second 12-month Review Virtual Assets and VASPs, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assetsvasps.html.
FATF (2022)., Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.
FATF (2023)., Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html.
Financial Stability Board, (2022)., „International Regulation of Crypto-asset Activities“, available at https://www.fsb.org/wp-content/uploads/P111022-2.pdf.
Financial Stability Board, (2022)., Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, available at: https://www.fsb.org/wp-content/uploads/P111022-3.pdf.
The Financial Services Commission, British Virgin Islands, Virtual Assets Service Providers Guide to the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing, available at: https://www.bvifsc.vg/sites/default/files/vasp_aml_cft_guidance.pdf.
Global Initiative against Transnational Organised Crime, Crypto, crime and control, Cryptocurrencies as an enabler of organised crime, (2022)., available at: https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organised-crime.pdf.
IMF, (2021)., Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism: Effective AML/CFT Regulatory and Supervisory framework – some legal and practical considerations, available at: https://www.elibrary.imf.org/downloadpdf/journals/063/2021/003/article-A001-en.pdf.
Kethineni, S., Cao, Y., (2019)., The Rise in Popularity of Cryptocurrency and Associated Criminal Activity, available at: https://doi.org/10.1177/1057567719827051.
Lemire A., K., (2022)., Cryptocurrency and anti-money laundering enforcement, Reuters, available at: https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/.
Legal Nodes, (2023)., A Legal Guide to Custodial & Non-Custodial Wallets, available at: https://legalnodes.com/article/custodial-non-custodial-wallets.
Narain, A., Morreti, M., (2022)., Regulating crypto, IMF, Finance and Development, available at: https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti.
Notabene, What Is Anti-Money Laundering (AML) & How Does It Apply to Crypto?, available at: https://notabene.id/crypto-travel-rule-101/aml-crypto.
Office of Public Affairs, U.S Department of Justice, (2021)., Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.

Ponamorenko, V., E., (2021). International Organizations' Approaches to Digital Assets Legalization (Monetary Policy and AML/CFT). In: Ashmarina, S., Mantulenko, V., Vochozka, M. (eds) Engineering Economics: Decisions and Solutions from Eurasian Perspective, available at: https://doi.org/10.1007/978-3-030-53277-2.

President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, Report on Stablecoins, available at: https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A52021PC0423.

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114.

SWIFT, Society for Worldwide Interbank Financial Telecommunication, What is Customer Due Diligence (CDD)?, available at: https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/customer-due-diligence-cdd.

Statista, Number of cryptocurrencies worldwide from 2013 to August 2023, available at: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.

Sanction Scanner, Examining the AML Risks and Red Flags of Crypto Exchanges, available at: https://sanctionscanner.com/blog/examining-the-aml-risks-and-red-flags-of-crypto-exchanges-258.

Sanction Scanner, Conducting Effective Customer Due Diligence, available at: https://sanctionscanner.com/blog/conducting-effective-customer-due-diligence-346.

The Institute for Security and Development Policy, Organised Crime Groups, available at: https://isdp.eu/projects/organised-crime-groups/.

The Council of Europe, (2023)., Money Laundering and Terrorist financing risk in the world of virtual assets, available at: https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4.

The Association of Certified Anti-Money Laundering, Understanding „Stablecoin" AML/TF risks, available at: https://www.acams.org/en/media/document/30786.

Trisa, Decentralised Cryptocurrency Travel Rule Compliance, available at: https://trisa.dev/api/.

Law on Digital Assets. (2020), RS Official Gazette, No 153/2020.

Law Amending the Law on the Prevention of Money Laundering and the Financing of Terrorism. (2020), RS Official Gazette, No 153/2020.