Proposal

BOSNIA AND HERZEGOVINA

COUNCIL OF MINISTERS

Working group for the development of the Risk assessment of money laundering and terrorist financing in Bosnia and Herzegovina associated with virtual assets

RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING ASSOCIATED WITH VIRTUAL ASSETS IN BOSNIA AND HERZEGOVINA

Sarajevo, 2023

CONTENT

List of abbreviations

ML/TF: Money laundering/terrorism financing
FATF : Financial Action Task Force
VA: Virtual Assets
VASP: Virtual Asset Services Provider
DApp – Decentralized Application
DeFi – Decentralized Finance
DEX: Decentralized exchange
CEX: Centralized exchange
DNFBP: Designated non-financial businesses and professions
ECCD: Council of Europe's Economic Crime and Cooperation Division
FI: Financial institution
FIU (FOS): Financial intelligence unit or service
ICO: Initial Coin Offering
STR: Suspicious Transaction Report
ML: Money laundering
NRA: National Risk Assessment
P2P: Peer-to-Peer (mutual communication among equals)
PEP: Politically exposed persons
TF: Terrorist financing
BAM – Bosnian Convertible Mark

1. Introduction not notes

The Risk Assessment of Money Laundering and Terrorism Financing in Bosnia and Herzegovina related to virtual assets (hereinafter referred to as the Assessment) represents the first comprehensive overview of this sector by institutions at all levels of government in Bosnia and Herzegovina (BiH).

According to FATF[1], virtual assets (VA) are defined as "Digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." Virtual assets do not include digital representations of fiat currencies, securities and other financial assets already covered elsewhere in the FATF Recommendations".[2]

As virtual asset (VA) transactions are not restricted by geographical borders and remain unregulated in many countries, they pose an increased risk of Money Laundering and Terrorism Financing (ML/TF). Some jurisdictions have fragmented regulatory frameworks for VAs, while others advocate for their complete prohibition. In June 2021, El Salvador became the first country to adopt Bitcoin as legal tender, and others, such as Japan and Canada, are also moving towards embracing VA as a method of payment. However, other jurisdictions like China and South Korea are suppressing their use. The global acceptance of VA as a means of online payments, but also for investments, is increasing every day. The reasons for the mass acceptance of VA should be sought first of all in the fact that for their use it is not, as a rule, necessary to have a bank account or a bank as an intermediary in transactions, while on the other hand, transactions are very cheap, fast and simple. Anyone with an Internet connection can become part of that financial system without using the standard banking network. Furthermore, VA can be stored in their own, so-called unhosted crypto wallets allowing owners to maintain physical control over their funds, thereby enhancing their appeal.

At the same time, VAs have certain characteristics that make them vulnerable to abuse by criminals for money laundering and terrorism financing (ML/TF) activities. In particular, the virtual asset ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AEC), mixers[3], decentralized exchange platforms and other types of products and services that enable or permit less transparency and better concealment of financial flows, as well as the emergence of other models of electronic business or activity such as a cryptocurrency public offering (ICO) that poses ML/TF risks, including fraud and market manipulation risks. In addition, new illicit financing typologies continue to emerge, including the increasing use of layered transactions between different virtual currencies that attempt to further conceal transactions in a relatively simple, affordable, and secure manner.[4] The ability to make fast transactions allows criminals to move and store assets outside of the regulated financial system, and conceal the origin and destination of assets,[5] making it much more difficult to detect these criminal activities, as well as confiscate illicit funds.

[1] The Financial Action Task Force (FATF) is a global specialized body responsible for setting standards for combating money laundering and terrorism financing.

[2] FATF Recommendations - updated edition 2023, Chapter "Note for interpreting FATF Recommendation No. 15

[3] These are software tools designed for anonymizing transactions, enabling users to conceal the source or owner of digital assets in a way that prevents others from tracing the transaction and tracking it back to the source.

[4] FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

[5] https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf

Due to these and some other characteristics, VA has found itself in the center of attention of law enforcement agencies, regulators and decision makers, including the FATF. Specifically, in 2018, the FATF adopted changes to its Recommendations to explicitly clarify that they apply to financial activities involving virtual assets adding also two new terms and definitions to the Glossary, "virtual assets" (VA) and “virtual asset service provider” (VASP). The FATF has defined a VASP as "as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1) Exchange between virtual assets and fiat currencies;
2) Exchange between one or more forms of virtual assets;
3) Transfer of virtual assets;
4) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
5) Participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.

The amended FATF Recommendation 15 requires that VASPs be regulated for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes, that they be licensed or registered, and subject to effective systems for monitoring or supervision. In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 to further clarify how the FATF requirements should apply in relation to VAs and VASPs, in particular with regard to the application of the risk-based approach to VA activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, recordkeeping, and suspicious transaction reporting, among others; sanctions and other enforcement measures; and international co-operation.

The FATF also adopted Guidance on the application of the risk-based approach to VAs and VASPs in June 2019. This Guidance outlines the need for countries and VASPs, and other entities involved in VA activities, to understand the ML/TF risks associated with VA activities and to take appropriate mitigating measures to address those risks. The Guidance makes clear that VASPs, and other entities involved in VA activities, need to apply all the preventive measures described in FATF Recommendations 10 to 21.

2. Objectives

This Assessment is a strategic document whose preparation precedes the adoption of the Action Plan to combat money laundering and terrorism financing related to virtual assets in Bosnia and Herzegovina (hereinafter referred to as the Action Plan). The primary objective of the Assessment is a deeper understanding and detection of specific ML/TF risks in Bosnia and Herzegovina associated with the use of VA and the operations of VASPs, aimed at raising awareness and implementing appropriate strategic measures to prevent, mitigate, and eliminate the identified risks of misuse of VAs and VASPs offering their services in Bosnia and Herzegovina.

Furthermore, conducting the Assessment is of utmost significance for the entire society and economy of Bosnia and Herzegovina. It represents a crucial step in fulfilling the FATF recommendations and demonstrates Bosnia and Herzegovina's clear commitment to combating all forms of money laundering and terrorism financing.

This Assessment results from the obligations of BiH according to FATF recommendations, especially recommendation number (15), which requires countries to identify, assess and understand the risks of money laundering and terrorism financing associated with VA and the operations of VASPs. Additionally, this Assessment provides a basis for implementing a risk-based approach to ensure that preventive and mitigating measures are proportionate to the identified ML/TF risks. It also aims to inform the competent authorities and institutions on the determination of priorities, as well as the actions to be taken in order to prevent or mitigate the identified ML/TF risks associated with VA/VASP.

To initiate the execution of the aforementioned FATF recommendations, the Council of Ministers of Bosnia and Herzegovina, during its 57th session on November 9, 2022, adopted the Decision on the formation of a Working Group for the development of the Risk Assessment of Money Laundering and Terrorism Financing in Bosnia and Herzegovina associated with virtual assets[6] (hereinafter: the Working Group). The Working Group was established as a temporary, interdepartmental and expert body of the Council of Ministers of Bosnia and Herzegovina with the task of developing an assessment of the ML/TF risks in Bosnia and Herzegovina associated with virtual assets, and an action plan to combat money laundering and financing of terrorism in Bosnia and Herzegovina associated with virtual assets.

[6] Official Gazette of BiH: 1/23

3. Work methodology

The assessment was prepared by the Working Group[7] appointed by the BiH Council of Ministers in accordance with the Methodology of the Council of Europe for the sectoral assessment of the risk of money laundering and terrorist financing related to virtual assets and virtual asset service providers (hereinafter: Methodology) The Methodology itself consisted of a series of instructions, guidelines, tools and measuring instruments that enabled the Working Group to identify ML/TF risks associated with the VA and VASP sectors in Bosnia and Herzegovina. The Methodology also defined the process of data collection and analysis facilitating:

- analysis of the overall context of VA and VASP, including the extent of their use in BiH;
- identification of key characteristics of VA and VASP that are relevant to ML/TF risk assessment, including risks, threats, vulnerabilities, likelihood of negative events and consequences;
- formulating conclusions about the level and nature of various risks, including the main typology of ML/TF in relation to the identified risk factors.

The assessment was conducted based on data collected through statistical tables and questionnaires covering the period from 2020 to 2022, provided by: Financial Intelligence Unit (FIU), High Judicial and Prosecutorial Council (HJPC), Prosecutor's Office of BiH, Intelligence and Security Agency of BiH (OSA), Securities Commission of Republika Srpska, police, supervisory and regulatory authorities, private financial and non-financial sector, VASPs and tax authorities. Due to limited data currently available to the relevant authorities, determining the final risk assessment for each evaluated category takes into consideration international trends, analyses from blockchain analytics companies, publications from FATF, available assessments from other countries, as well as the prior experience of the Working Group members in this field.

The development of the Assessment was carried out with the support and cooperation of the Economic Crime and Cooperation Department (ECCD) of the Council of Europe.

[7] The Working Group consists of representatives of: the Ministry of Security of Bosnia and Herzegovina; Prosecutor's Office of Bosnia and Herzegovina; State Investigation and Protection Agency; Intelligence and Security Agency of Bosnia and Herzegovina; Ministry of Finance and Treasury of Bosnia and Herzegovina ; High Judicial and Prosecutorial Council of Bosnia and Herzegovina; Indirect Taxation Authority of Bosnia and Herzegovina; Ministry of Finance of the Republika Srpska ; FBiH Ministry of Finance; FBiH Tax Administration, RS Tax Administration, FBiH Securities Commission ; RS Securities Commission; Directorate for Finance of the Brčko District of Bosnia and Herzegovina; RS Ministry of the Interior; FBiH Ministry of the Interior and the Police of Brčko District of Bosnia and Herzegovina.

4. Country profile, materiality of *VA* and *VASP sectors* and contextual factors

4.1. General notes

Bosnia and Herzegovina (hereinafter: BiH) is located in the western part of the Balkan Peninsula. It borders Serbia and Montenegro to the east and the Republic of Croatia to the north, west and south. The area of BiH covers a total area of 51,209.2 km^2. According to the 2013 census, BiH has a population of 3,531,159 inhabitants.

Bosnia and Herzegovina is a democratic state that operates on the principles of the rule of law and through free and democratic elections, and administratively it consists of two entities: the Federation of Bosnia and Herzegovina (FBiH) and the Republika Srpska (RS) and Brčko District (BDBiH), a self-governing administrative unit of BiH. The Federation of BiH is further divided into 10 cantons. The country is politically decentralized, with a constitutional division of powers between the institutions of BiH and the entities, ensuring that each of them has its own constitution, president, government, flag and coat of arms, parliament, judiciary, police, tax authorities, postal system, financial regulatory bodies, etc. BiH is a member of numerous international organizations, and has candidate status for membership in the European Union.

4.2. Economic indicators

From the economic aspect, Bosnia and Herzegovina is a transition economy. The official currency is the Convertible Mark (BAM) and its approximate value is 1 BAM = 0.511292 euros. Nominal Gross Domestic Product (GDP) for 2022 amounted to 45.51 billion BAM, i.e. 13.26 BAM per capita, while the average net salary was 1,122 BAM. Coverage of imports by exports amounted to 62.8%[8], and direct foreign investments amounted to 1.44 billion BAM.[9] The results of the European Program for the Comparison of Prices and GDP showed that the GDP of BiH per capita in the purchasing power standard (PPS) for 2022 was 35% of the EU average, while the Real individual consumption per capita (PPS) for 2022 was 41 % of the EU average.[10]

It can also be noted that BiH does not constitute a significant regional financial hub. The total loans of financial institutions at the end of 2022 amounted to 22.3 billion BAM. Out of the total loans, 10.95 billion BAM or 49.1% were related to retail loans, 8.93 billion BAM or 40% were allocated to loans provided to private non-financial businesses, while loans to government institutions amounted to 792.7 million BAM or 3.6%.[11]

Due to its geographical location and poor road infrastructure, BiH does not represent a significant regional transportation hub. The length of European roads (E-roads) in BiH is a total of 995 km. E-roads in Bosnia and Herzegovina, on many sections, do not allow traffic to flow at the desired speed. Reasons include, among other things, small radii of curves, steep

[8] https://bhas.gov.ba/
[9] https://www.cbbh.ba/press/ShowNews/1526
[10] https://bhas.gov.ba/data/Publikacije/Saopstenja/2023/NAC_05_2022_Y1_1_HR.pdf
[11] Report of the Central Bank of Bosnia and Herzegovina on Financial Stability for 2022:

and frequent ascents, passages through settlements and cities, and inadequate road maintenance.[12]

4.3. Digital and online activity

According to data published by the Agency for Statistics of Bosnia and Herzegovina, 75.9% of households in BiH have internet access, 23.9% do not have access, while 0.2% of households are unsure if they have internet access. According to the same survey, 77% of women and 80.8% of men in BiH use the internet, while according to the employment status, internet is used by 53.3% retirees, 84.1% the unemployed, 95.2% the employed, with 100% usage among students.

The most common reasons for using the internet for personal purposes in BiH in 2022 are: seeking information about goods and services 75.8%, reading internet portals, online newspapers, and magazines 70.3%, sending online messages via Skype, Messenger, WhatsApp, Viber, etc. 84.5%; engaging in social networks 70.7%; making phone calls via the internet 93.6%; internet banking services are utilized by 20.1% of households in Bosnia and Herzegovina today, compared to 7.8% in 2019. Regarding e-commerce, the number of individuals who purchased/ordered goods or services online in the last 12 months was 43.1%, representing an increase of 10.5% compared to 2021. Individuals most commonly ordered products or services online in the following categories: clothing, footwear, or accessories (e.g., bags, jewelry) 52.7%; furniture, home accessories 23.2%; computers, tablets, mobile phones, or accessories 18.1%; sports equipment 18%; food or drinks from a store or delivery of prepared meals 16.7%; delivery from restaurants, catering services 14.5%; consumer electronics (e.g., TVs, stereo systems, cameras) or household appliances (e.g., washing machines) 13.8%.[13]

However, despite such a high internet usage rate, the general assessment is that financial literacy among the population of Bosnia and Herzegovina is at a low level, particularly concerning investments in VA. Nevertheless, access to and openness to using the internet create the possibility for the utilization of VA and services associated with VA and VASPs, thereby increasing the risk of VA market abuse.

On the other hand, the use of digital identity is facilitated by laws on electronic documents and laws on electronic signatures at the state and entity levels.[14] These laws regulate the right of administrative bodies, local self-government bodies, businesses, institutions, and other legal and natural persons to use electronic documents, electronic signatures, timestamp seals, electronic seals, and certificates for website authentication. Although there is a legal framework for its use, it can be observed that qualified electronic signatures are not yet widely applied in Bosnia and Herzegovina. However, an expansion of its usage can be expected in the near future. It is significant to note that domestic VASPs in Republika Srpska use an electronic identification system for their clients, which involves determining and establishing identity without the physical presence of the client.

[12] http://dep.gov.ba/dokumenti_politika/srednjorocna_razvojna_strategija/?id=28

[13] The use of information and communication technologies in Bosnia and Herzegovina in 2022.https://bhas.gov.ba/data/Publikacije/Bilteni/2023/IKT_00_2022_TB_1_BS.pdf

[14] Law on Electronic Document of BiH (Official Gazette of BiH, 58/2014); Law on Electronic Document of FBiH (Official Gazette of FBiH, 55/2013); Law on Electronic Document of RS (Official Gazette of RS, 106/15); The Law on Electronic Signature of BiH (Official Gazette of BiH, 91/06) and the Law on Electronic Signature of RS (Official Gazette of RS, 106/15 and 83/19).

4.4. Regulations and legislative framework for AML/CFT

Legislation regulating the area of anti-money laundering and combating the financing of terrorism (hereinafter AML/CTF) is governed by state, entity-level and BDBiH laws. At the level of Bosnia and Herzegovina, there is a consolidated AML/CFT law[15], as well as the Criminal Code of Bosnia and Herzegovina which criminalizes money laundering. The criminal codes of the entities and the Criminal Code of the Brčko District also include provisions criminalizing money laundering, ensuring that institutions and agencies at all levels of government are involved in the fight against ML/TF. The most significant roles are played by competent ministries, prosecutor's offices, the Financial Intelligence Unit (FIU), tax authorities, banking agencies, securities commissions, insurance agencies, police agencies, and other institutions/competent bodies at all levels of government.
Furthermore, it is important to note that the development of a new Law on AML/CFT is underway, aligning it with the Directives and Regulations of the European Union in the field of AML/CFT, as well as the standards and recommendations of FATF and MONEYVAL. With this law, among other obligated entities, VASPs are expected to be defined as obligated entities for implementing AML/CTF measures. Supervisory authorities overseeing the activities of VASPs in the AML/CFT field will be designated, and penalties for non-compliance with the prescribed AML/CTF measures will be established. In this way, VASPs will be brought in line with other obligated entities in Bosnia and Herzegovina regarding the obligation to conduct customer due diligence, enhanced due diligence, suspicious transactions reporting and other prescribed measures.

4.5. Establishment, registry, and supervision of VASP operations

When it comes to the establishment, registry, and supervision of VASPs, the most significant role, in accordance with constitutional competencies, should be exclusively held by institutions at the entity level and the level of the Brčko District of Bosnia and Herzegovina. Specifically, Bosnia and Herzegovina is in the initial stages of enacting regulations that govern the field of VA and VASPs. Currently, the operations of VASPs are only partially[16] regulated by law in Republika Srpska, while in the Federation of Bosnia and Herzegovina (FBiH) and the Brčko District of Bosnia and Herzegovina (BDBiH), there is no legislative framework regulating this area.

4.5.1. Establishment and VASP Registry in Republika Srpska:

The procedure for establishing VASPs in RS, like for any other company, is carried out in accordance with the Law on Companies of Republika Srpska.[17] The Law on the Securities Market of Republika Srpska specifies that the RS Securities Commission will oversee

[15] The Law on the Prevention of Money Laundering and Financing of Terrorist Activities (Official Gazette of BiH, 47/14 and 67/16).
[16] The Law on the Securities Market of Republika Srpska, Official Gazette of RS, 63/22, defines the concepts of VA and VASPs. It prescribes the obligation of registering VASPs, specifies the types of services registered VASPs can provide, designates the competent authority for monitoring compliance with laws and other regulations governing AML/CTF, and for taking necessary measures regarding these regulations concerning VASPs. The law also mandates the maintenance of VASP registry, establishes certain limitations on VASPs concerning the investor funds disposal, imposes the obligation to inform investors about the investment risk in VAs, and prescribes the authorities of the supervisory body and establishes the sanctions.

[17] Official Gazette of Republika Srpska, 127/2008, 58/2009, 100/2011, 67/2013, 100/2017, 82/2019 and 17/2023;

compliance with laws and other regulations governing the prevention of money laundering and the terrorist financing activities. It also has the authority to take necessary measures concerning these regulations regarding providers of services related to virtual currencies, as well as for establishing and maintaining registry of VASPs established in RS or providing services related to virtual currencies in RS through branches. In accordance with the provisions of the Law on the Securities Market of Republika Srpska, entities not registered with the RS Securities Commission cannot provide services related to virtual currencies.
The RS Securities Commission is not authorized to issue permits for the operation of VASPs, nor does it issue licenses for individuals employed by VASPs to perform these tasks. The Commission also does not set requirements for the registration of a business entity regarding the minimum share capital for conducting activities, it does not determine the staffing and technical equipment of service providers, nor does it give approval for acts adopted by the service provider.
In accordance with the Law on the Securities Market, a provider of services linked to virtual currencies is required to submit a notice to the Commission within 30 days from the date of establishment, providing a description of internal control measures established to fulfill obligations prescribed by regulations on the prevention of money laundering and the financing of terrorist activities. Additionally, the provider must submit a request for entry into the registry of service providers linked to to virtual currencies, along with the required attachments, in accordance with the Rulebook on the Registry of Service Providers Related to Virtual Currencies (hereinafter referred to as the Rulebook).[18] The Rulebook prescribes the manner of maintenance of registry, the content and form of VASP registry, conditions for entry into the registry, public disclosure of data from the registry, and changes to registered information.

Persons who were engaged in the provision of services related to VA before the Law on the Securities Market came into force were required to align their operations with the provisions of the law, as well as the provisions of the bylaws issued based thereon, within 120 days from the date this law entered into force. In this regard, these entities were obligated to inform the RS Securities Commission about the provision of services related to VA no later than January 31, 2023. This notification should have included a description of the internal control measures established to fulfill obligations prescribed by regulations on the prevention of money laundering and the financing of terrorist activities. Additionally, they were required to submit a request for entry into the registry of providers of services associated with VA with the required attachments.
According to the Rulebook, when submitting a request for entry into the registry of providers of services linked to virtual currencies, a VASP is obligated to provide the RS Securities Commission, within 30 days from the date of establishment, with:

- The decision of the registration court on the entry of a business company in the court registry, i.e. an extract from the court or other appropriate registry,
- Articles of incorporation or statute of the company,
- Unique identification number of the taxpayer (JIB) - certificate of the Tax Administration of Republika Srpska and notification of the identification number (MN) issued by the competent authority,
- Proof of identity of the owner, of persons authorized to represent the company and employees (ID card or passport or decision of the competent authority if the owner of the legal entity is another legal entity or multiple legal entities, proof of the identity of the owner, up to the ultimate owner, natural person),

[18] Official Gazette of RS, 4/23;

- Internal acts and other documentation proving the fulfillment of the obligations prescribed under the Law on AML/CTF and by-laws related to this law, with the aim of AML/CFT,
- Rules of business
- Data on the employee appointed for detecting and AML/CTF,
- Bank's verification of the account number designated for specific purposes.
- Confirmation from the competent court that the authorized person of the VASP or the appointed person authorized to enforce the AML/CFT law at the VASP has not been convicted by final judgments and is not subject to criminal proceedings in accordance with Article 41, paragraph (1), item b) of the AML/CTF Law.

The RS Commission has the legal authority to, during the processing of the application, request additional documentation deemed necessary for deciding on the specific request. When reviewing applications for entry in the registry of providers of services with virtual currencies, the RS Commission verifies the attachments submitted in accordance with the Rulebook.
The process of registering VASPs with the RS Commission began in January 2023. However, the RS Commission has been in contact with VASPs since the fourth quarter of 2022, providing them support through meetings and consultations to prepare the required documentation to be submitted in accordance with the Rulebook. Before being registered with the RS Commission, VASP is expected to understand the ML/FT risks, stipulate how they assess these risks in line with the specificities of their business activities, how they will act to mitigate these risks, etc. They are also required to provide all other evidence, documentation, and data proving their preparedness to comply with the AML/CTF regulations.
When processing applications for registration and verifying the submitted attachments with the request, it has been determined that five VASPs have adopted appropriate internal acts and prescribed internal control measures established to fulfill obligations specified in regulations on preventing money laundering and terrorist financing. These VASPs have been entered into the VASP Registry with the RS Commission.[19] Two companies that addressed the RS Commission with requests for registration provided untimely and incomplete documentation for registration. During the processing of one submitted request, the applicant withdrew the request, while the RS Commission rejected the other request due to failure to meet the requirements and deadlines for registration.

4.5.2. Supervision of VASP operations in RS

When it comes to supervisory bodies overseeing the operations of VASPs, as mentioned earlier, this area is only partially regulated in RS. Although VASPs are not recognized as obliged entities for implementing AML/CFT measures in the current Law on AML/CTF, they must take actions and measures in accordance with the Law on AML/CTF, in accordance with the amendments to the Law on the RS Securities Market. The effect of these amendments to the Law on the Securities Market is the application of preventive measures specified in the Law on AML/CTF to VASPs. In this way, all VASPs, whether established in RS or headquartered outside RS but providing services linked to virtual currencies through a branch in RS, are subject to the Law on AML/CTF as other entities under the jurisdiction of the RS Securities Commission. The same provisions of the Law on AML/CTF, bylaws, as well as the *Guidelines for Risk Assessment and Implementation of the Law on AML/CTF for Entities under the Jurisdiction of the RS Securities Commission* apply to all entities under the jurisdiction of the

[19] The RS Commission publishes information about registered VASPs on its website https://www.secrs.gov.ba/Ucesnici/PruzaociUsluga.aspx.

RS Securities Commission (published on the website of the RS Securities Commission in September 2015, as well as the Amendments to these Guidelines from December 2016)
The RS Securities Commission, since the entry into force of the amendments to the Law on the Securities Market and the acquisition of new competencies, has made efforts and undertaken activities to raise awareness among VASPs about their obligations stipulated by this law, bylaws, and Guidelines of the RS Commission.
Taking into account the timeframe of regulatory amendments, the stipulation of the competencies of the RS Securities Commission, the establishment, and registration of VASPs, supervising the operations of VASPs could not have been carried out during the assessment period.
When verifying the fulfillment of registration requirements, the RS Securities Commission, among other things, checks whether the VASP has adopted internal acts determining customer or group of customers' risk levels, their geographical area, business, business relationship, transaction, product, or service, and how these are provided to the customer. The Commission also verifies whether the VASP has an adequate policy for managing ML and TF risks, i.e., whether it has further defined: the purpose and objective of managing ML and TF risks and their connection to the business goals and strategy of the VASP, the areas and business processes of the VASP exposed to ML and TF risks, ML and TF risks in all key business areas of the VASP, measures to address ML and TF risks, and the role and responsibility of the management of the VASP in introducing and accepting ML and TF risk management. In addition, for all VASPs and in accordance with legal regulations, the Commission requested the submission of evidence (a court confirmation) that the authorized person of the VASP or the appointed person authorized to implement the AML/CTF law at the VASP had not been convicted by final judgments or that criminal proceedings were not initiated against them in accordance with the AML/CTF Law. In order to protect customers' funds, as with other obligated entities under the jurisdiction of the RS Securities Commission, the Commission has stipulated in the Rulebook on the Registry of VASPs that the VASP is required to open a special-purpose account for customers' funds at a business bank. The VASP must provide evidence of this when submitting the application for registration. Funds in the special-purpose account can only be used by the VASP for buying and selling virtual currencies and for the purpose of providing services related to virtual currencies. These funds in the special-purpose account are not the property of the VASP, do not become part of its assets, liquidation estate, or bankruptcy estate, nor can they be used to settle claims of VASP's creditors or be subject to forced execution in proceedings against the VASP.

In accordance with the regular supervision plan devised by the RS Securities Commission for each year, in accordance with Article 13 of the Supervision Rulebook, the Commission will control compliance with legal and other regulations, as well as the internal acts of VASPs regarding the implementation of AML/CTf measures in 2024. The control will be conducted as a targeted, comprehensive on-site inspection, assessing full compliance with prescribed obligations and the actions taken by the obliged entities under the AML/CTF Law regarding:

- Development/amendments/implementation of internal acts of the obligated entities (risk management policies and procedures for implementing AML/CTF measures).
- Creating a risk assessment (determining the level of risk of the customer or group of customers, business relationship, product, or transaction),
- Establishing indicators for the identification of customers and suspicious transactions,
- Applying measures for identification and monitoring customers,
- Verifying compliance with the obligation to appoint an authorized person and their deputy, and providing conditions for their work,
- Integrity checks during employment,

- Conducting regular internal controls and audits,
- Reporting and submitting prescribed data and evidence to the FIU,
- Ensuring data protection and record-keeping.
- Regularity of professional training and education of employees of the obligated party.

4.5.3. Powers of the RS Securities Commission

The legal framework for the supervision of VASPs by the RS Securities Commission is the same as for other obligate entities under the Law on AML/CTF under the jurisdiction of the Commission:

- The powers of the RS Securities Commission are stipulated in Article 80 paragraph (1) point h) of the Law on AML/CTF to supervise the work of obliged entities in connection with the application of the provisions of this law and other laws that prescribe the obligations of implementing measures to prevent money laundering and financing of terrorist activities, as one of the supervisory bodies, in accordance with the provisions of this and special laws regulating the work of individual obliged entities and competent agencies and authorities. Article 80 of the Law on AML/CTF defines the supervisory authorities (including the RS Commission) for the supervision of the compliance of the obliged entity's business with this law.
- The provisions of Article 81 of the Law on AML/CTF stipulate that the supervisory bodies are required, in accordance with the provisions of this law and the laws governing the business operations of individual obliged entities and supervisory authorities, to regularly monitor the on-site compliance with the business practices of the obliged entity.
- The powers of the RS Securities Commission are stipulated in Article 260 paragraph /---/ and paragraph (2) of the same Article of the Law on Securities Market./translator's note: the number of the paragraph is missing in the source document/

- In accordance with Article 263 paragraph (3) of the Law on Securities Market, supervised persons are obligated to grant authorized personnel of the RS Securities Commission access to their business premises, provide suitable facilities and staff, present and deliver the requested documentation and deeds, allow access to and inspection of electronic and other communication means installed at the supervised entity, provide statements and explanations, and ensure other necessary conditions for conducting supervision.
- Article 2 paragraph (3) of the Rulebook on the Supervision of Participants in the Securities Market stipulates that, in addition to the participants in the securities market referred to in paragraph (1), VASPs are also subject to the supervision of the RS Securities Commission. Article 3 of this Rulebook specifies that supervision includes, among other things, monitoring compliance with the Law on Securities Market and the Law on AML/CTF. Article 7 paragraph (7) of the Rulebook on the Supervision of Participants in the Securities Market stipulates the conduct of supervision (including types, methods, and procedures).

4.5.4. Sanctions:

Chapter XII of the Law stipulates penal provisions that lay down cases where legal entities (obliged entities) and responsible persons are sanctioned for the violations of these laws. Article 83 prescribes sanctions for legal entities and responsible individuals within a legal

entity for violations, while Article 84 regulates the sanctions of the supervisory body and responsible individuals within the supervisory body.
In accordance with the provisions of the AML/CTF Law, Articles 81, 83, and 84, the RS Commission may file a request to initiate misdemeanor proceedings if it determines that the obliged entity or responsible individual within the obliged entity has violated the provisions of the AML/CTF Law.
Additionally, the RS Commission may take other measures in accordance with its legal competencies:

- Article 265 of the Law on Securities Market stipulates that in case of identified illegalities and irregularities, the RS Commission will, by decision, order the undertaking of actions contributing to the establishment of legality and compliance with laws and other regulations, or impose an appropriate measure prescribed by this and other laws.
- Special measures that the RS Commission may order, relating to cases of violation of this and other laws and regulations, or in cases where the continuation of the business of the supervised entity is uncertain, are prescribed by Article 267 of the Law on Securities Market.
- Furthermore, Article 299 paragraphs (5) and (6) of the Law on Securities Market prescribe that the RS Commission may impose a measure of removal from the registry, lasting one year, or a permanent removal from the registry, on providers of services associated with virtual currencies who fail to take measures and actions defined by regulations governing the prevention of money laundering and terrorist financing.

4.5.5. Cooperation of RS Commission with other authorities

There is a clear legal framework that enables the RS Commission to exchange information and cooperate with other authorities and supervisors both domestically and internationally.

When it comes to cooperation with domestic authorities, it is regulated by a number of regulations, including:

- Article 262a of the Law on Securities Market prescribes that the RS Securities Commission is competent to cooperate and exchange data, information, and documentation with competent authorities regarding the implementation of laws and other regulations governing AML/CFT. Paragraph (2) of this Article defines that this cooperation also includes collecting information on behalf of the requesting competent authority, as well as exchanging the collected information.
- The RS Law on the Committee for the Coordination of Financial Sector Supervision (Official Gazette of RS, 49/09) regulates the manner of mutual cooperation and coordination between the RS Securities Commission, the RS Banking Agency, and the RS Insurance Agency. Article 8 prescribes that the RS Committee for the Coordination of Financial Sector Supervision is established to ensure complete coordination of the work of these supervisory bodies, adopt a unified strategy and guidelines for the development of supervision, and ensure the protection of the rights of users of financial services in the Republika Srpska.
- The Law on AML/CTF (Articles 61 and 62) regulates the cooperation between the FIU and other authorities.

The RS Securities Commission continuously consults with the FIU, the RS Ministry of Interior, and the RS Banking Agency of Republika Srpska on matters related to the procedures, operations, and records of VASPs.

Regarding measures taken to identify VASPs subject to supervision under AML/CFT regulations, the RS Securities Commission sent a letter to the FIU furnishing information regarding entities currently in the registration process or who have submitted requests within the designated legal timeframe. Consequently, the RS Commission informed the FIU that any other entities (legal or natural entities) potentially providing services associated with virtual assets, which are not registered or in the process of registration with the RS Securities Commission, cannot offer services associated with virtual currencies in accordance with Article 261 paragraph (3) of the Law on the Securities Market. In a specific case, information was exchanged about a legal entity suspected of providing services associated with virtual currencies in the territory of Bosnia and Herzegovina but was not registered in the VASP registry maintained by the RS Securities Commission.

When it comes to international cooperation, the Commission, in accordance with Article 260, paragraph (1), point n) of the RS Law on the Securities Market, is authorized to cooperate with related organizations abroad.
The RS Securities Commission has been a member of IOSCO (International Organization of Securities Commissions) since 2002 and a signatory to the IOSCO MMoU - Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information) since 2009, and a signatory to the IOSCO EMMoU – Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information since 2021. The RS Commission has undergone the verification and screening process by other IOSCO members to demonstrate that it meets all the conditions prescribed by IOSCO in order to acquire the status of a signatory to these international agreements on cooperation and exchange of information.
Scope of assistance includes, among other things, for example: providing information and documentation held in the files of the Requested Authority, delivering records identifying the ultimate beneficial owner or legal entity controlling another legal entity within the jurisdiction of the Requested Authority, taking sworn statements or testimonies, etc. These issues can also relate to VASPs.
As a member of IOSCO, the RS Commission adheres to IOSCO principles (specifically Principles 13, 14, and 15) relating to cross-border cooperation among regulators.
Furthermore, since June 20, 2019, the RS Securities Commission has also been signatory to AA - Administrative Arrangement for the Transfer of Personal Data between each of the European Economic Area (EEA) Authorities set out in the Appendix A and each of the non-EEA Authorities set out in Appendix B.
Moreover, the RS Commission is a signatory to various bilateral and multilateral agreements on cooperation and information exchange with counterpart institutions from neighboring countries.

So far, the RS Commission has not requested information, and information has not been requested from the RS Commission, regarding VAs or VASPs under the IOSCO MMoU/EMMoU. However, information has been requested from the RS Commission regarding one VASP by regulators from a neighboring country, based on a multilateral agreement on cooperation and information exchange with counterpart institutions from neighboring countries

4.6. VA and VASP sectors

As stated in the previous chapters, the operation of VASPs is currently only partially regulated by law in Republika Srpska (RS), while in the Federation of Bosnia and Herzegovina (FBiH) and the Brčko District (BDBiH), there is no legislative framework governing this area. According to the gathered data, the FBiH and the BDBiH have not taken any steps towards legal regulation regarding VA and VASP so far. However, it is expected that this area will be regulated after the enactment of the new Law on AML/CTF, which is in the final stage of development. However, the lack of regulation in the FBiH and the BDBiH does not hinder their citizens from making investments in VA, either through VASPs from Republika Srpska or through international VASPs. Specifically, it has been determined that investors from Bosnia and Herzegovina use the services of global VASPs in two ways. The first method involves direct deposits and withdrawals to and from foreign VASPs, with Binance and Coinbase being the most prominent platforms. This method requires that the customer's bank in BiH allows deposits and withdrawals to and from a foreign VASP. Although the majority of banks in Bosnia and Herzegovina, due to their internal policies, do not process transactions related to foreign VASPs, there are still a few banks that permit inflows and outflows in fiat currencies to/from their customers' accounts.[20]

The second method involves purchasing VAs through domestic VASPs and transferring them to wallets with foreign VASPs, where further trading takes place between individual VA pairs. However, when investors from Bosnia and Herzegovina want to exchange their VAs for fiat currency, they must transfer the VAs back to wallets with domestic VASPs and exchange them for the sole legal tender (BAM). This method is primarily used by investors from BiH whose banks do not permit transactions towards foreign VASPs.

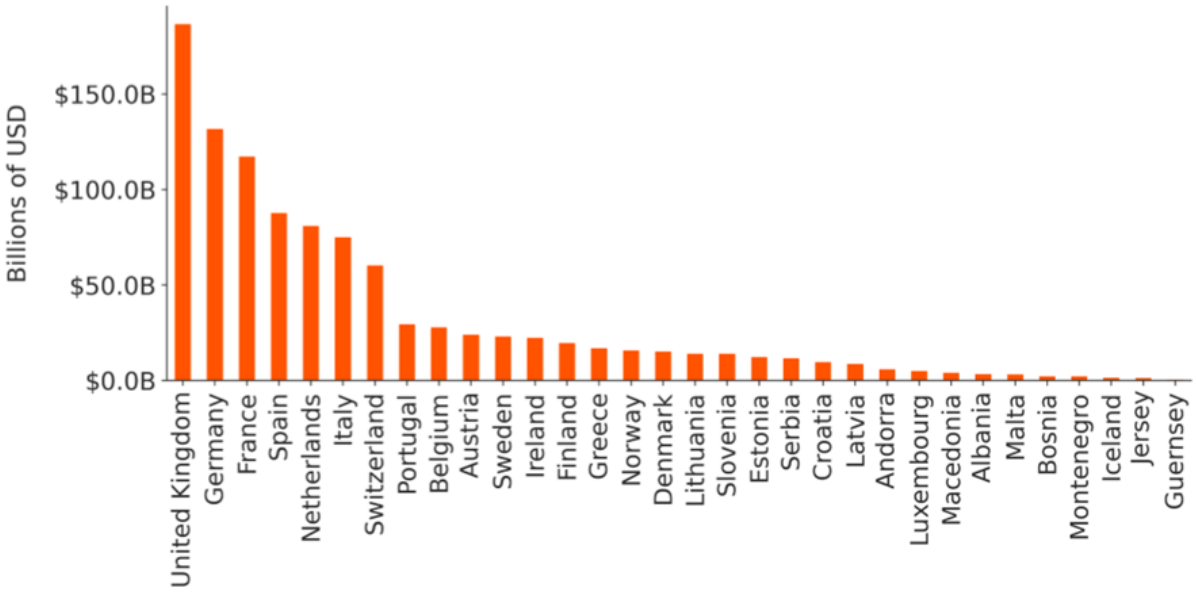
According to the Global Crypto Adoption Index compiled by the company Chainalysis[21], which covers 146 countries, BiH ranked 115th overall. This Global Index consists of several sub-indices that measure and rank various types of services, including centralized service scope; P2P trade volume, and DeFi trade volume. Bosnia and Herzegovina is ranked 113th overall in terms of centralized exchange activity, 65th in terms of P2P exchange activity, and 112th in terms of DeFi activity.[22] When it comes to ranking compared to Western European countries, Bosnia and Herzegovina holds the 28th position, with received values totaling 2.25 billion dollars (~3.96 billion BAM) in the period from October 2021 to October 2022[23].
Based on these indicators, it can be noted that the adoption of VAs in BiH is still at a low level. In comparison with the rest of the world, especially Western Europe, the volume of activities related to VAs is relatively low. The reasons for this can primarily be attributed to the low purchasing power of citizens, lack of trust and insufficient education regarding VAs, absence of adequate regulation, high risks, and similar factors.

[20] For more information, see Chapter 4.7 *VA and VASP related products and services in non- VASP regulated sectors*

[21] Chainalysis is a blockchain data platform specialized in providing data, software, services, and research to government agencies, exchanges, financial institutions, as well as insurance and cybersecurity companies in over 70 countries

[22] The closer the final result of the country is to 1, the higher the rank.

[23] The working group managed to collect data from Chayanalysis for Bosnia and Herzegovina covering the period from October 2021 to October 2022, which were predominantly used throughout the document for consistent comparison with data from domestic authorities during the same period.



Graphical overview of received funds in Western Europe according to Chainalysis for the period from October 2021 to October 2022

Although this amount may initially seem exceptionally large in the context of domestic affairs, it essentially represents the total volume of all transactions in VAs, the majority of which are not associated with deposits or withdrawals in currencies that constitute legal tender. For instance, every conversion from one type of VA to another or every transfer of VA from one crypto wallet to another is recorded as the overall turnover, even though, fundamentally, in the first case, it involves the conversion from one VA to another without converting to fiat currency, and in the latter case, it involves the transfer of VA from one wallet to another, often belonging to the same entity, i.e., from one personal wallet to another.[24]

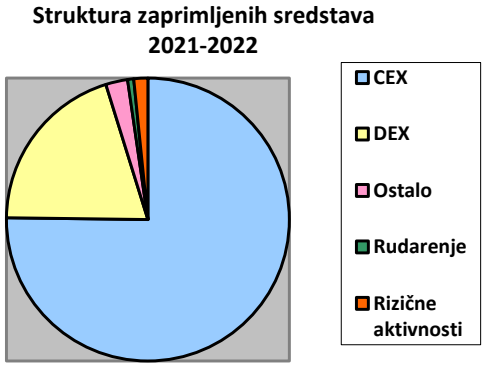
For comparison, the total transaction volume of both domestic VASPs during 2022 amounted to only about 20 million BAM, which is approximately 0.5% in relation to the overall recorded turnover of ~3.96 billion BAM. These findings are supported by data obtained from the Association of Banks of Bosnia and Herzegovina, indicating that the total amount of realized transactions related to VAs (inflows and outflows with domestic and foreign VASPs) for 2022 is 19,509,336.00 BAM. In this amount, the share of processed transactions in the domestic payment system of Bosnia and Herzegovina to and from VASPs within Bosnia and Herzegovina was 71.67%, or 13,981,975.35 BAM, while the share of transactions in the international payment system to and from VASPs outside Bosnia and Herzegovina was 28.33%, or 5,527,360.65 BAM, with inflow and outflow transactions in a relatively close ratio of 50/50%.[25]

[24] For security reasons, investors often have multiple different wallets where they hold VAs

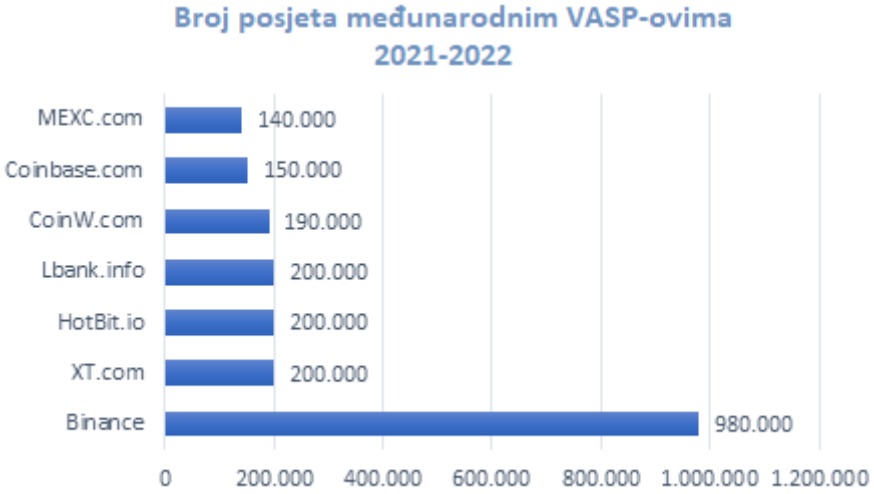
[25] The data were collected and provided by banks based on keyword identification and on a 'best effort' basis, and there is a possibility that not all transactions are included.

Comparing bank data with the data provided by Chainalysis inevitably leads to the conclusion that the majority of the turnover of ~3.96 billion BAM relates to the transfer of VAs between crypto wallets without conversion to fiat currency or the conversion of one type of VA to another, mainly through global centralized exchanges or decentralized exchanges. The following is a breakdown of the structure of received funds of ~3.96 billion BAM, where 75.2% is related to centralized exchanges (CEX), 20% to decentralized exchanges (DEX), 0.7% to mining, 1.6% to risky activities, while 2.5% is attributed to all other activities.[26]

From these indicators, one can conclude that investors from Bosnia and Herzegovina largely conduct transactions through global VASPs, which are predominantly centralized exchanges (CEX), but a non-negligible percentage also utilizes decentralized exchanges (DEX). Furthermore, analyzing the collected data led to the conclusion that residents who use domestic VASPs primarily use them to enter the world of VAs. After acquiring VAs, they transfer them to crypto wallets with global centralized VASPs or DEXs, primarily due to lower fees and a greater number of VA pairs available for trading. However, we should not rule put the possibility that there are those who transfer funds to DEX or global VASPs to mix them with illegally obtained proceeds, with the aim of concealing their origin and avoiding detection by law enforcement agencies. Nevertheless, according to available data, such proceeds represent a very small share of the total received funds.[27]



According to Chainalysis, during the period from October 2021 to October 2022, there were over 2 million visits to international exchanges from IP addresses in Bosnia and Herzegovina, with the majority being related to the platform Binance.com, which received approximately 980,000 visits during the same timeframe. The other significant exchanges are shown in the chart below.

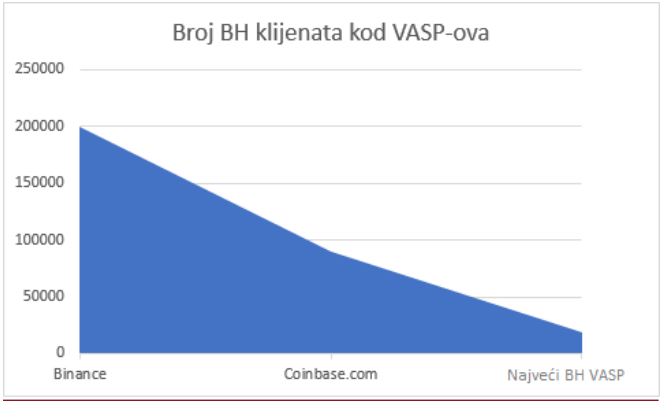


Significant numbers of visits were also recorded on pages related to online crypto gambling (Stake.com ~160,000 visits), cryptocurrency mining (2miners.com ~140,000), and

[26] Chainalysis Country Analysis Report on Bosnia 2021-2022, pg. 4

[27] For more data, see Chapter 5 of Risk assessment of money laundering through a predicate offense and risk assessment of financing terrorism for VAs/VASPs

cryptocurrency staking (ethermine.org ~170,000).[28] These data only indicate the number of registered visits to international exchanges from IP addresses in BiH over the course of one year, and it is not even possible to indirectly determine the total number of residents using the services of international VASPs or the number of transactions conducted. For example, one person may visit these platforms multiple times without making any transactions. However, these data are valuable as they show that residents visit platforms of global VASPs much more than domestic ones. Although there are no official data on the number of residents using the services of international VASPs, unverified information suggests that only two international VASPs have around 290,000 clients from BiH[29], namely Binance with approximately 200,000 clients and Coinbase with around 90,000 clients. This is significantly more than the number of registered clients held by the largest domestic VASP (approximately 19,000 clients).



By extrapolating this data and consulting external sources of information, along with the transactional activity of authorized VASPs in the Republika Srpska, it is estimated that the actual percentage of the population exposed to VAs is between 5-7%. The significant difference in the number of clients between domestic and foreign VASPs indicates the existence of a large number of residents who do not use domestic VASPs' services at all but exclusively trade through global VASPs via domestic banks that allow deposits and withdrawals to them. According to the data furnished from the banking sector during 2022, as much as 28.33% of all deposits and withdrawals (5,527,360.65 BAM) were related to foreign VASPs.

4.6.1. Virtual assets mining

According to the mentioned Chainalysis Report, "mining" as one of the ways to acquire VA, accounted for only 0.7% of the total volume of received funds by all VASPs during the period from October 2021 to October 2022. Although there are no official data on the number of miners, estimates suggest that there are currently around 2,000 active miners in BiH. In the earlier period, the number of miners was significantly higher due to cheap electricity. However, due to the increase in the price of electricity in BiH, there has been a significant reduction in the number of individuals engaged in mining.[30]

[28] Chainalysis Country Analysis Report on Bosnia 2021-2022, pg. 6
[29] These data were provided by a domestic VASP
[30] For more information, see Chapter 6. Risk assessment of ML/TF according to the customer/user profile, and Chapter 8.2.10 Miners/validators

4.6.2. Peer to peer (P2P) transactions

When it comes to P2P transactions, the total value received in BiH between October 2021 and October 2022 was 4.72 million BAM, representing only 0.12% of the total received value during the same period, ranking it as the 24th P2P market in Western Europe. The analysis of the number of transfers that moved to P2P platforms in BiH shows that there were an average of about 47 thousand P2P transfers per month during the mentioned period.[31] This number includes both P2P transactions between individuals within BiH and P2P transactions between individuals within BiH and abroad. However, it was not possible to determine the exact ratio between domestic and cross-border transactions. If we divide the total received value by the total number of P2P transactions (~556,000), it turns out that the average transaction amounts to around 8 BAM. The reasons for the lower use of peer-to-peer exchanges, compared to CEX and DEX exchanges, are primarily attributed to their technological complexity and the high potential for investor fraud.[32]

6.6.3. Domestic VASPs in Republika Srpska

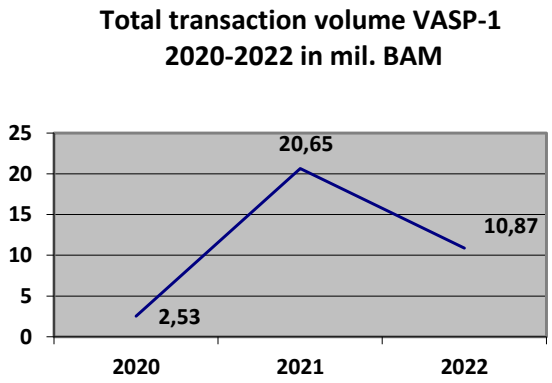
When it comes to domestic VASPs, according to the data from the RS Securities Commission, as of June 2023, six companies providing services linked to virtual currencies have approached the RS Securities Commission with a request for registration in the registry of providers of services associated with virtual currencies. Out of these, four companies have successfully completed the procedure with the RS Securities Commission and have been registered in the registry of service providers. Two other companies have approached the RS Securities Commission with incomplete and untimely documentation for registration. One company did not rectify and complete the request within the prescribed deadlines, resulting in the rejection of the application. The other company withdrew its request, leading to the suspension of the procedure. In October 2023, the fifth VASP was registered in the registry of VASPs with the RS Securities Commission.

According to legal provisions, VASPs in the RS can provide one or more of the following services:

a) Custody and management of virtual currencies on behalf of third parties (wallet depositary service provider)
b) Organizing a platform for virtual currencies trading,
c) Exchange of virtual currencies for the legal tender
d) Exchange of virtual currencies for another virtual currency
e) Transfer of virtual currency
f) Execution of the offer or sale of virtual currencies.

[31] Chainalysis Country Analysis Report on Bosnia 2021-2022, pg.5
[32] For more information, see Chapter 8.2.4.

In the period for which data was collected (2020-2022) in the territory of RS, a total of two VASPs provided their services. One of the VASPs (hereinafter referred to as VASP-1) is essentially a centralized exchange that offers users digital wallets for storing, receiving, and sending VAs. This VASP also manages a trading platform for VAs, an internet platform through which users register and verify their accounts, manage their digital wallets for VAs and legal tender (receive, transfer, and store VAs), and engage in VA trading. Through this platform, users can exchange VAs for other VAs or for BAM, the legal tender currency. VASP-1, after the amendments to the Law on Securities Market came into force in October 2022, informed the RS Securities Commission about providing services associated with virtual currencies and subsequently submitted a request for registration in the registry of VASPs with the RS Securities Commission. After verifying compliance with the conditions, VASP-1 was successfully registered.



The total volume of VASP-1 for the period 2020-2022 amounted to BAM 34,050,968.23 through 25,278 completed transactions. The total gross profit for the mentioned period was BAM 1,337,661.97. The chart illustrates that during 2020, the total turnover of VASP-1 amounted to 2.53 million BAM. In 2021, there was an increase in the trading volume compared to 2020, totaling 18.12 million or 716.21%. However, in 2022, there was a decrease in the trading volume by 9.78 million BAM or 47.35% less compared to 2021.
VASP-1 offers six different VAs, including five cryptocurrencies (Bitcoin, Ethereum, Litecoin, Bitcoin Cash, and Ethereum Classic) and one stablecoin (USDT - USD Tether). The table below shows the volume and structure of VA holdings by customers during 2022 at this VASP.

VASP 1 - Volume of VA holdings by customers

VA type	Volume of VA holdings in 2022	Natural persons	Legal persons	Anonymization	Unlawful use
Bitcoin	2,555,785.05			No	Unknown
Ethereum	3,030,438.45			No	Unknown
Litecoin	2,053,974			No	Unknown
BCH	58,533.15			No	Unknown
ETC	329,388.15			No	Unknown
USDT	2,811,194.1			No	Unknown
Total in BAM	**10,839,312.9**	**89.37%**	**10.63%**		

The second VASP (hereinafter: VASP-2) performed activities exclusively through crypto machines (5 pcs.) and had three types of VA in its offer (Bitcoin, Etherum and Litecoin) that could be both purchased and sold. In addition to these VAs, DOGE, BCH, and USD were also offered but solely for purchase, i.e., it was not possible to sell them via the crypto machines. VASP-2 provided its services from April 2021 to September 2022 when it suspended its operations pending completion of the registration procedure with the RS Securities Commission. This VASP resumed its activities in July 2023 after being officially registered with the RS Securities Commission. From April 2021 to September 2022, VASP-1 had a total turnover of 1,237,690.28 BAM through 807 transactions. Regarding the turnover volume by

VA type, 10% relates to Bitcoin, 5% to Ethereum, and 85% to Litecoin. They did not offer so-called 'Privacy coins' in their portfolio.

VASP 2-Extent of VA holdings with customers

VA type	Volume of VA holdings in 2022	Natural persons	Legal persons	Anonymization	Unlawful use
Bitcoin	403,029.76			No	Unknown
Ethereum	890.00			No	Unknown
Litecoin	833,770.52			No	Unknown
Total	**1,237,690.28 KM**	**100%**	**0%**		

4.6.4 Supervisory Activities of FBiH and BDBiH

FBiH and BDBiH have not reported the presence of registered VASPs in their respective areas, nor have supervisory authorities been established for their control. However, during 2023, in the cities of Sarajevo and Tuzla (FBiH) and the city of Brčko (BDBiH), one company installed crypto ATMs (one each in Sarajevo and Tuzla, and one in Brčko) allowing the exchange of cryptocurrencies to fiat currency and vice versa. Upon inspection, it was determined that these crypto ATMs were installed without the required operational permits, indirectly highlighting the unregulated status of this area in FBiH and BDBiH.
Additionally, it is noteworthy that at least one web portal for connecting buyers and sellers for a wide range of goods and services has been registered in FBiH. Among other things, this platform features a large number of advertisements for buying and selling VA. Buyers and sellers on this platform can arrange face-to-face meetings to conduct direct exchanges of VA for fiat currencies, where VAs are transferred between non-hosted wallets (so-called cold wallets), and the seller receives payment in fiat currency in hand.[33]

4.7. VA and VASP related products and services in non-VASP regulated sectors

With respect to other non-VASP regulated sectors, banks play the most significant role in the market as financial institutions. In accordance with the applicable regulatory framework in Bosnia and Herzegovina, banks are subject to the Law on AML/CTF. According to the collected data provided by the banks in BiH, not a single bank provides products or services in VA, that is, not a single bank is registered to provide these services or products.
The majority of banks in the BiH market do not process transactions related to VA. However, those banks that do engage in VA-related transactions (buying/selling VA) do so by executing inflows/outflows in fiat currencies to/from their clients' accounts. These transactions involve both domestic and foreign VASPs. However, there are differences among banks that process transfers to VASPs. The majority of them allow transfers only with domestic VASPs, while a smaller number permit transfers with foreign VASPs. Furthermore, some banks only allow transfers in BAM, excluding foreign currency deposits/withdrawals. Additionally, certain banks permit only deposits but not withdrawals to foreign VASPs. On the other hand, domestic

[33] For more information, see Chapter 8.2.6

VASPs cannot have bank accounts abroad, significantly complicating their business operations.

According to the data provided by the BiH Association of Banks, the total number of processed transactions related to VAs (inflows and outflows to/from VASPs) for 2022 is 11,805 transactions with a total value of 19,509,336.00 BAM. In this amount, the share of processed transactions in the domestic payment system of Bosnia and Herzegovina to and from VASPs within Bosnia and Herzegovina was 71.67%, or 13,981,975.35 BAM, while the share of transactions in the international payment system to and from VASPs outside Bosnia and Herzegovina was 28.33%, or 5,527,360.65 BAM, with inflow and outflow transactions in a relatively close ratio of 50/50%.[34]

Through analysis, it has been determined that there are no formal barriers in the domestic legislation for banks in BiH to provide services to VASPs. However, it is evident that some banks consider VAs and VASPs to be high-risk in terms of ML/FT, and, as a result, they restrict or prohibit transactions associated with them through their internal regulations. Some banks justify this by the fact that they are conditioned by their correspondent banks not to engage in business with VAs and VASPs and that they do not want to jeopardize their relationships with them. Due to such business policies, these banks are exposed to lawsuits from VASPs for refusing to establish a business relationship. There are already non-final court judgments in favor of VASPs from RS due to banks' refusal to establish business cooperation. Additionally, there is a decision from the BiH Competition Council from November 2022, where one bank in BiH was fined 250,000 BAM for an unlawful agreement under Article 4 paragraph (1), point (b) of the Law on Competition. The bank was ordered to change its internal regulation that prohibits opening accounts and doing business with VASPs.[35]

However, regardless of the fact that banks in BiH do not offer VA products/services to their clients, some bank clients use banking products and services to convert fiat currency into VAs and vice versa through VA exchanges. Banking products such as credit/debit/prepaid cards, bank transfers, payment service providers, and accounts are used for purchasing/investing in VAs. Due to the lack of VA tracking processes, banks may face counterparty risks when their clients interact with VASPs, due to insufficient visibility of transaction traces and decentralized virtual asset systems, making them particularly vulnerable to anonymity risks. The counterparty risk is further increased if clients interact with high-risk VASPs located in jurisdictions with weak AML/CFT regimes. However, despite these clear vulnerabilities, banks are considered to represent a moderate level of risk, primarily because they are well-versed in AML/CFT measures and have robust policies and procedures, operating under clear regulatory and supervisory frameworks. Additionally, all electronic transfers are supported by SWIFT messages that record the names of users and senders, in line with FATF requirements.

Other financial institutions involved in financial intermediation (e.g., insurance companies, investment funds, stockbrokers, etc.) cannot mediate or invest in VAs due to restrictions in current legal regulations in BiH. The inspection revealed that these are not clients of registered VASPs.

Regarding designated non-financial businesses and professions (DNFBPs), the Working Group collected data from supervisory authorities and professional associations of lawyers, notaries, and accountants, real estate agents, as well as from supervisory authorities for entities engaged in providing games of chance services, buying and selling precious metals and gemstones, and buying and selling high-value goods in BiH. At the time of the assessment, there were no

[34] The data were collected and provided by banks based on keyword identification and on a 'best effort' principle.

[35] https://bihkonk.gov.ba/hr/saopcenje-za-medije-sa-111-sjednice-konkurencijskog-vijeca-bih/

recorded cases indicating that there were instances of the use or misuse of VAs by DNFBPs, nor did they have interactions with VASPs.

5. Risk assessment of money laundering through predicate offenses and risk assessment of the terrorist financing for VAs/VASPs

The Supplement to the Money Laundering and Terrorism Financing Risk Assessment in Bosnia and Herzegovina for the period 2022-2024 (NRA), adopted in March 2023 by the Council of Ministers of BiH, assesses the overall money laundering threat in Bosnia and Herzegovina as 'medium/high,' with a trend of 'no changes,' and estimates that the 'National Money Laundering Vulnerability' in Bosnia and Herzegovina is 'medium' with a score of 0.55. This document also rates the terrorism financing risk in Bosnia and Herzegovina as 'medium' with a tendency to decrease.[36] As for criminal offenses generating the highest amounts of 'dirty' money, categorizing as 'high threat,' include: corruption-related crimes (with a trend of 'increasing'), tax-related crimes (with a trend of 'no changes'), and organized crime/association crimes (with a trend of 'no changes'). Criminal offenses related to unauthorized trafficking and production of narcotics (with a trend of 'increasing') and the criminal offense of Fraud (with a trend of 'no changes') are classified as 'medium/high threat'. Crimes of general nature (with a trend of 'decreasing'), other economic crimes (except tax-related crimes) (with a trend of 'decreasing'), and crimes related to human trafficking and smuggling (with a trend of 'decreasing') are assessed as 'medium threat'.

The threat taxonomy and the overall exposure of BiH according to the Supplement to the Risk Assessment of Money Laundering and Terrorism Financing in Bosnia and Herzegovina for 2022-2024.

Predicate offense	Exposure level
Corruption-related crimes	High
Tax-related crimes	High
Organized crime/association	High
Unauthorized trafficking and production of narcotics	Medium/high
Fraud	Medium/high
General crimes	Medium
Human trafficking	Medium
Human smuggling	Medium
Other economic crimes	Medium
Terrorist financing	Medium

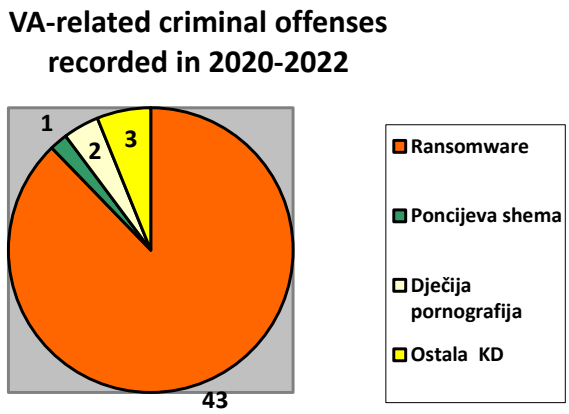
When it comes to the risk of misuse of VA for money laundering and terrorist financing (ML/TF) activities in Bosnia and Herzegovina, it is recognized in a larger number of strategic documents, primarily in Strategy of Bosnia and Herzegovina for the Prevention and Combating of Terrorism from 2021, Organized Crime Threat Assessment (OCTA) from 2021, and Supplement to the Risk Assessment of Money Laundering and Terrorist Financing in Bosnia and Herzegovina for 2022-2024. The listed documents generally recognized this threat, but they did not extensively address it nor determine the level of the threat posed by ML/TF. For

[36] The supplement to the Money Laundering and Terrorism Financing Risk Assessment in Bosnia and Herzegovina for 2021-2023 has been prepared in accordance with the World Bank methodology.

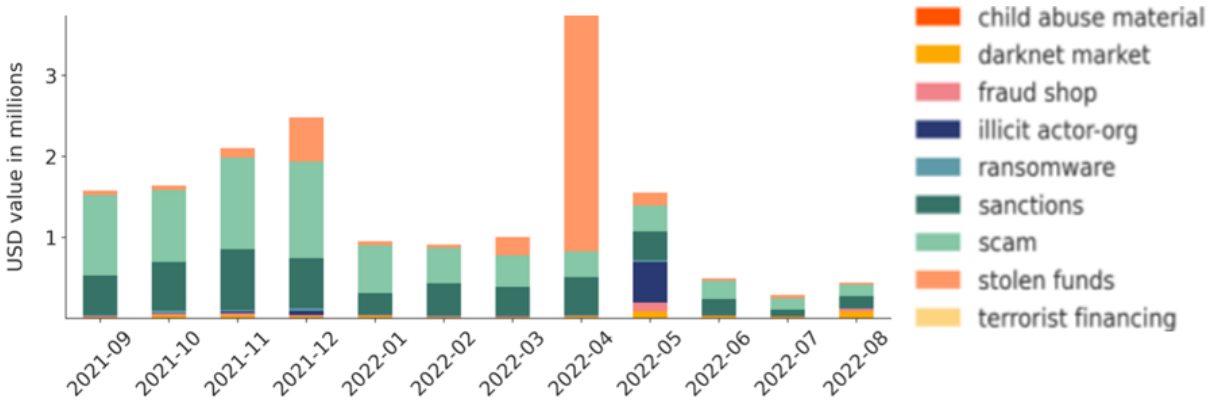
the mentioned reason, a special Working Group was subsequently appointed with the task of drafting a Threat Assessment of Money Laundering and Terrorist Financing related to virtual currencies.

According to the data collected by the High Judicial and Prosecutorial Council of Bosnia and Herzegovina (HJPC) from prosecutor's offices for the period of 2020-2022, there were no ongoing investigations or verdicts issued by courts for the criminal offenses of "Money Laundering" or "Terrorist Financing" related to VA in Bosnia and Herzegovina.

However, during the mentioned period in the territory of the Federation of Bosnia and Herzegovina and Republika Srpska, 49 other criminal offenses related to VA were recorded, with the most common being: (Ransomware), "Fraud" (Ponzi Scheme), "Blackmail," "Damage to Computer Data," and "Unauthorized Access to Protected Data Processing Systems and Networks," as well as "Illegal Goods Trading via the Internet (payment made in cryptocurrencies)," "Child Pornography," etc.[37] The structure of these criminal offenses is shown in the graph.



These data largely align with Chainalysis' findings, which identified that during the period from October 2021 to October 2022, the largest source of illicit activities stemmed from the fraud category, which received $6.77 million in cryptocurrency. As the fastest-growing type of crime identified, asset theft has increased by 2.6% compared to the previous 12 months, reaching a total value of $4.27 million received in stolen assets.[38]



Graphic overview of Chainalysis data on illicit activities for the period October 2021 to October 2022

When it comes to the methods of committing the recorded criminal offenses, law enforcement agencies in Bosnia and Herzegovina have noticed the following typologies:

[37] Data from the RS Ministry of Internal Affairs is missing.
[38] Chainalysis Country Analysis Report on Bosnia 2021-2022, pg.

- "Hacker" attacks are carried out on computers of individuals and legal entities, making certain electronic data on the server inaccessible for further use (files on computers are encrypted and unavailable for use). The victims of the attackers receive instructions to make payments from their crypto wallets in VA (most commonly in Bitcoin) in order to regain access to encrypted data.
- Access credentials for crypto wallets are hacked in various ways, leading to the theft of VAs, where victims often lose their funds irreversibly.
- Pyramid schemes are created where domestic individuals gather funds for "investments" in VA by presenting new users mainly with fictional, non-existent, or worthless types of VA, ultimately resulting in financial loss.
- Through internet forums, unauthorized international trafficking of narcotics is arranged, where the buyer makes payment via VA (most commonly in Bitcoin), after which the drug is delivered in a pre-agreed manner.
- Trading of illegal goods takes place via the internet (most commonly on the Darknet) with payment using VA (most commonly Bitcoin).
- Payments to crypto addresses potentially associated with websites containing child pornography have been detected.
- Investing and trading with VA on behalf and for the account of a third party are conducted:
- Some newly established single-member legal entities based in Republika Srpska, whose founders are citizens of an EU member state, are attempting to register as clients with domestic VASPs and engage in VA purchases in order to avoid paying taxes in their own country.

The majority of criminal cases are associated with ransomware, i.e., hacker attacks targeting domestic legal entities, demanding ransom payments to regain access to business data locked in the attack.
There is also a trend of abuse or fraud cases related to VAs, involving domestic individuals who, on behalf of foreign legal entities, recruit new members or gather funds for "investments." Considering that VAs are an attractive financial instrument, many such cases promote some form of VA as a secure investment, using a globally recognized individual or legal entity based in some of the global financial centers as a front. Specifically, these are complex so-called MLM (Multi-Level Marketing) schemes, which mostly originate from abroad, typically have some invented premise or basis, but are very effectively presented and promoted to portray themselves as legitimate investment opportunities to people who lack sufficient knowledge and experience. Most such schemes use VAs as proof of the concept's success and raise funds through VA investments. However, the product they offer to users is fictional, nonexistent, or worthless VA, thereby causing harm to end investors within such a pyramid scheme, while those higher up in the hierarchy profit directly from the losses of smaller investors, which is a classic *Ponzi scheme*.
There are several such cases in Bosnia and Herzegovina, and some of them include:

- Onecoin (the largest MLM scam) – no longer active, a multinational organization headquartered in Bulgaria, perpetrators identified by the FBI and Europol, some still at large, with damages estimated in the tens of billions.
- Zeniq - currently active, based in the UAE, involving many domestic individuals in the promotion, sales, and marketing of "investment packages."
- Lusate Balkan - a new scheme, headquartered in Africa.

Additionally, it has been found that drug traffickers continuously explore new avenues to avoid detection, including the use of technology and virtual space, with particular interest in utilizing social media and the Darknet. The annual sales of Darknet-associated drugs at the international

level amounted to nearly 800 million USD in 2019, representing a 70% increase compared to 2018.[39] Multiple online Darknet markets provide a virtual space for drug dealing. These web platforms ensure anonymity and facilitate peer-to-peer transactions. Although very few cases have been identified in BiH where drug dealers used VAs to purchase drugs on the Darknet, in the future, it can be expected that drug traffickers will increasingly use the Darknet and unregulated exchanges to avoid detection.

Furthermore, cases have been recorded in BiH where payments are made through the Darknet to crypto addresses potentially linked to websites containing child pornography or for trading products whose circulation is illegal or restricted.

Additionally, law enforcement agencies' assessments in Bosnia and Herzegovina largely correspond to registered predicate criminal offenses, as well as to the structure and modalities of the commission of these offenses described in relevant international sources and assessments from other countries. Based on the collected data, the Working Group assessed that the following predicate criminal offenses related to VAs have a high level of ML risk:[40]

- Frauds (pyramid schemes and ICO scams)
- Blackmail (ransomware)
- VA theft
- Unauthorized internet trading
- Trafficking in narcotics

Additionally, although there wasn't a significant number of reported cases of tax evasion using VAs/VASPs in BiH at the time of assessment, it was estimated that there is a high risk of tax avoidance on profits generated by investing in VAs. Specifically, based on documented typologies and trends, including FATF red flag indicators, there is evidence that VAs/VASPs are used for tax evasion on a global scale. Considering that investing capital in VAs is a relatively recent phenomenon, and that tax laws in BiH do not prescribe separate tax treatment regarding investment in VAs, this risk is further pronounced. Typically, these investments are recorded by legal entities as intangible assets (in the case of purchasing VAs) or as inventory (in the case of mining). In both cases, the sale of VAs is income subject to corporate income tax. In the case of individuals, the difference between the purchase and sale value is the individual's income, specifically capital gains, which are subject to tax obligations. Estimates suggest that there is a significant number of investors attempting to avoid paying taxes on investment income in VAs, resulting in substantial losses for budgets. Additionally, we should not overlook investors who are not even aware of this obligation due to the lack of regulation and reduced awareness.

The Working Group failed to determine the total extent of economic loss caused by criminal offenses related to VAs, as well as the amount generated in foreign and domestic jurisdictions, but it is estimated to be tens of millions of BAM. This estimate is based on a report from the specialized blockchain analysis company Chainalysis regarding Bosnia and Herzegovina, where it is stated that crypto wallets in BiH received funds totaling $29 million (~51 million BAM) during the period from October 2021 to October 2022, which were identified as illicit, representing only 1.14% of the total recorded amount received, and $53 million (~93.2 million BAM) identified as risky activities, representing 2.08% of the total received funds. Taking into account the way Chainalysis records the total volume of received funds, as explained above, it is difficult to estimate the actual amount of potentially laundered funds converted into fiat currencies. However, it is certain that it is multiple times lower than the amount stated in the Chainalysis report because criminals often transfer funds between multiple personal crypto wallets to obscure the trail and hinder detection by authorities, which evidently leads to an

[39] Chainalysis, *"The Chainalysis 2020 Crypto Crime Report" January 2020*, https://go.chainalysis.com/2020-crypto-crime-report

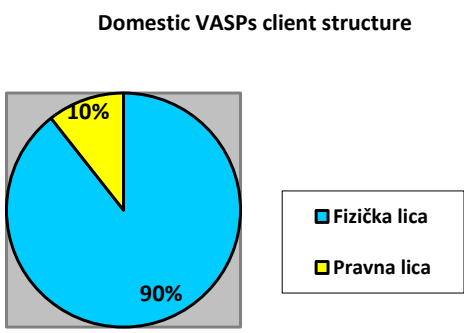
[40] The data and opinions were collected through the Questionnaire from the Methodology.

increase in the total volume of circulated funds. However, regardless of this, the Assessment supports the view that VAs are used for laundering proceeds related to the predicate criminal offenses identified above.

When it comes to the financing of terrorism (FT) associated with VA and VASPs, international typologies indicate that terrorist groups and their supporters are increasingly seeking "donations" in VA, and that terrorist organizations such as ISIS and Al Qaeda have received " donations" in Bitcoin.[41] No such cases were reported during the assessment in Bosnia and Herzegovina, but this certainly doesn't mean they didn't occur. An aggravating factor in detecting terrorism financing (TF) associated with VAs and VASPs is that, unlike money laundering, funds used in the majority of cases stem from legitimate sources, and financing occurs through transactions in small amounts of VAs, often through unregulated VASPs. In this regard, and despite the fact that at the time of the assessment in BiH there were no reported cases related to TF involving VA, it was still estimated that the misuse of VA for this purpose represents a medium level of inherent risk. This is primarily because there are certain risks of social media abuse for advertising and collecting 'donations' by organizations and individuals, often under the guise of humanitarian or charitable reasons.

6. Risk assessment of ML/TF according to customer/user profile

According to the collected data, it has been determined that VASPs registered in RS predominantly provide their services to natural persons (90%), while the number of legal entities using VASP services is relatively small (10%). The largest domestic VASP from RS (VASP-1) has around 19,000 registered clients.



When it comes to foreign VASPs providing services in BiH, there are no official statistical data on the number and structure of clients. However, according to unofficial information, Coinbase exchange had around 90,000 users from BiH in mid-2022, while it is estimated that the largest global exchange, Binance, has around 200,000 users from BiH.[42] The ratio of natural persons to legal entities using services of foreign VASPs is not known, but the assumption is that, similar to domestic VASPs, the majority consists of individuals who invest in VAs for profit, i.e., reselling VAs at higher prices compared to purchase prices.

Domestic VASPs from RS are obligated to assess the risk of ML/TF and complete the process of due diligence, applying a risk-based approach. The measures of customer due diligence should involve client identification and verification of client identity, identification of the beneficial owner and taking reasonable measures to verify their identity, assessment and understanding of the purpose and intention, and nature of the business relationship, as well as conducting ongoing customer due diligence of the business relationship, including monitoring transactions undertaken throughout that relationship. Additionally, domestic VASPs dealing with high-risk clients regarding ML/TF should conduct enhanced customer due diligence,

[41] Middle East Media Research Institute, "The Coming Storm – Terrorists Using Cryptocurrency", August 2019, https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency
[42] The data was provided by a domestic VASP.

which can also be triggered as a result of larger transactions, suspicious client activities, client names failing verification, for clients from higher-risk areas, when the client is a politically exposed person, or when there is any other risk factor. Both domestic VASPs (VASP-1 and VASP-2) that operated during the data collection period (2020-2022) state that they fully implement these procedures; however, this still needs to be confirmed by the competent supervisory authority (RS Commission) as there have been no on-site inspections conducted so far.

When it comes to foreign VASPs providing services in BiH, according to current regulations, they are not obliged to register their operations in BiH or establish a point of contact for communication with domestic authorities. Also, they are not obligated to submit suspicious transaction reports (STRs) for BiH residents to the domestic FIU but only have this obligation to the FIU of the country in which they are established. In this regard, it is significant to emphasize that the domestic FIU has been informed on multiple occasions by foreign FIUs about suspicious activities of BiH citizens, which they received from global VASPs registered in those countries. Through checks conducted by visiting the websites of foreign VASPs, it has been determined that all global VASPs providing their services in BIH implement customer due diligence procedures, and some of them even do not allow the registration of clients from BIH due to the inadequate regulation of ML/TF in BIH legislation. However, domestic authorities are not able to control whether and how foreign VASPs implement these procedures on clients from BiH, which inherently poses an elevated level of ML/TF risk both for natural persons and legal entities. Also, the lack of precise data regarding the structure and number of clients from BiH using foreign VASPs was an aggravating circumstance during this assessment. However, despite the mentioned challenges, the Working Group has conducted an assessment of the ML/TF risk level for specific categories of natural and legal persons, as explained below.

6.1. Natural persons

When it comes to natural persons, nearly all clients of VASP-1 are exclusively domestic users, specifically users who are citizens or residents of BiH. There is a very small number of users who are registered residents outside BiH, but they are still citizens of BiH. The number of foreign clients is negligible, mostly consisting of small investors who use domestic VASPs for trading as well as for storing VAs. For all natural persons, domestic VASPs are obligated to conduct procedures related to customer identification and monitoring, and managing ML/TF risks, which also entails collecting information regarding the source of funds. According to claims by VASP-1, the number of politically exposed persons using their services is negligible, and they are automatically categorized as high-risk, subject to prescribed verification procedures.

Speaking about the quantity and quality of suspicious transaction reports (STRs) received by the competent authorities in BIH, we can note that the cooperation with certain domestic VASPs is at a satisfactory level. Specifically, it has been established that the FIU has good cooperation with certain domestic VASPs regarding the submission of STRs and necessary documentation. On the other hand, the FIU also receives suspicious transaction reports from domestic banks during non-cash transactions between VASPs and clients from BiH, which are processed through the accounts of natural persons for the purchase or sale of VAs. Most of the money transfers were related to payments in favor of accounts of foreign cryptocurrency exchanges. Banks generally justify suspicion prompting the submission of suspicious transaction reports by stating that the area is unregulated in BiH. Considering that in the mentioned cases income was being generated, the FIU informed the relevant tax authorities,

while in cases of suspicion that cryptocurrency trading was linked to specific criminal activities, the competent police authority was notified.

Taking into account the overall situation concerning natural persons, it has been assessed that a particularly high-risk group regarding ML/TF consists of individuals engaged in online gambling and betting through internet platforms that accept VAs as a method of payment, as well as individuals who use the Darknet for trading illicit products. These client groups have been thoroughly addressed in Chapter 7 of this document, and they have been assessed as high-risk groups.
Additionally, it has been assessed that individuals who engage in direct exchange or payment in VAs using various online platforms for connecting buyers and sellers pose a high level of risk.

6.2. Legal persons

Regarding legal entities operating through the domestic exchange (VASP-1), four categories of clients have been identified:

1. Miners - clients, legal entities engaged in cryptocurrency mining.
2. Investors - clients, legal entities investing in the virtual asset market.
3. Occasional - mostly clients who have only had a need to acquire VAs for a specific purpose once.
4. Others - (e.g., merchants who enable the acceptance of payments in VAs for their goods and services).

In general, all legal entities without adequate financial reports, significant capital, and a clear intention and plan for investment, and whose founders and managers do not have adequate reputation are considered risky by VASP-1, and additional measures are taken to mitigate ML/TF risks. Below is an assessment conducted for all the mentioned categories of legal entities.

6.2.1. Miners

According to the assessment of one of the domestic VASPs, there are currently approximately 2,000 miners active in BiH. In the past, the number of miners was significantly higher due to cheap electricity. However, due to the increase in electricity prices in BiH and the decrease in Bitcoin mining speed, there has been a significant reduction in the number of individuals engaged in mining. According to the Chainalysis Report, the total volume of funds received in BiH originating from mining from October 2021 to October 2022 amounted to approximately 27.7 million BAM or 0.7% in relation to the total volume of received funds. It has been determined that miners, in order to cover mining costs, sell a portion of mined VAs mainly through global exchanges but to a lesser extent through domestic VASPs.
Mining is generally considered less risky than other methods of acquiring VAs because it is verifiable by VASPs. However, considering that identified abuse models of mining for ML/TF exist, primarily through investing dirty money to purchase mining equipment that further generates "clean" funds, and through so-called "mixing" of mined VAs with dirty crypto assets[43], it is assessed that miners represent a moderate level of ML/TF risk.

[43] For more information, see Chapter 8.2.10

6.2.2. Legal persons - investors

Regarding clients who invest in the virtual asset market through VASP-1 as legal entities, it is explained that they undergo enhanced due diligence regarding the source of funds being invested, and during the account verification process, the identity of the ultimate beneficial owner is mandatory to be verified in accordance with the applicable AML/CTF Law.[44] In cases of abuse by foreign legal entities, the assumption is that they use VAs to evade due dilligence and tax obligations when transferring money. According to VASP-1, there is a trend observed where certain newly established single-member legal entities based in Republika Srpska, whose founders are citizens of an EU member state, attempt to register as clients and conduct VA purchases. Since they are mostly legal entities that do not have regular income from their regular activities but are mainly used to provide certain services so that their owners can pay lower taxes in their own country, domestic VASP treat them as high-risk and thoroughly examine their sources of income and the purpose of investment for such cases.
Additionally, VASP-1 states that certain domestic legal entities have been identified whose purpose is "tax optimization," meaning the intention of the foreign owner to generate and tax certain revenues outside their domiciliary jurisdiction.
In relation to all the above, it is assessed that foreign legal entities - investors in VAs who invest through domestic VASPs represent a high level of ML/TF risk, while domestic legal entities - investors are rated as moderately-high risk, primarily due to the potential avoidance of tax obligations related to capital gains from investments in VAs.

6.2.3. Legal persons - sporadic clients

Legal entities that are sporadic clients are mostly victims of ransomware and typically acquire VAs only once to pay ransom, i.e., to regain access to encrypted data. There are no precise statistical data on the number and amounts of ransom payments, as they are often not reported to the competent authorities due to fear of permanent data loss, which is crucial for legal entities in most cases. It often happens that, even though the ransom is paid, the data remains encrypted, where the perpetrators disappear without a trace or may demand additional payments. Victims, upon realizing they have been deceived, decide to report the case to the authorities. According to the collected data, a total of 43 criminal offenses related to ransomware and demands for payment in VAs were recorded in the FBiH[45] between 2020-2022. There are no precise statistical data on how many of these extortion cases involve legal entities and how many involve natural persons, but the assumptions are that they mostly concern legal entities because they usually represent more solvent victims who can be extorted for larger amounts compared to natural persons. However, the fact is that among these clients, there are likely those who buy VAs for other reasons, such as tax evasion, etc. Considering all of the above, it is estimated that occasional clients, legal entities, represent a moderate level of risk of ML/TF.

6.2.4. Other clients

When it comes to other customer profiles, such as traders and caterers, it has not been established that there are legal entities in BiH that directly accept VAs for their services or goods. However, it has been found that there is at least one intermediary financial company

[44] Although VASPs are not explicitly mentioned as obligated entities under the current AML/CTF Law, VASP-1 states that it implements all legally prescribed measures for customer due diligence, as well as reporting on suspicious transactions.
[45] This applies only to FBiH as the RS Ministry of the Interior did not provide the requested data.

that, for a certain commission, enables its clients to pay for services and goods in VAs through an application (digital wallet), by converting the cryptocurrencies used for payment through the domestic exchange (VASP-1) into BAM as the sole legal tender. Payment/collection for goods and services is done by simply scanning a QR code using an application installed on a mobile phone, and the legal entity selling goods or services does not need to know what happens behind the scenes of the transaction, as it ultimately receives payment in BAM. According to available data on the website of this intermediary company, as of September 28, 2023, 83 legal entities from the entire territory of BiH accepted payments through this application at a total of 126 sales points.
Taking into account that all legal entities in BiH are obligated to conduct their payments and collections in BAM as the only legal tender, and that no legal entities have been identified as violating this obligation, it is assessed that there is currently a low level of risk of VA misuse for ML/TF purposes concerning traders and caterers. However, estimates suggest that VAs will become increasingly prevalent over time, and their usage will expand, so the possibility of misuse for ML/TF purposes should not be ruled out. This places a significant responsibility on VASPs to verify whether users or funds originating from VA applications are legitimate.

7. Assessing the ML/TF risk based on ties with various sectors of economy

It has been found that the majority of customers trade directly with VAs for their own financial benefit, using them as a form of investment to achieve short-term or long-term gains. Also, the majority utilize the services of centralized VASPs for this purpose and trade with VAs that have the highest market capitalization (e.g., Bitcoin, Ethereum, etc.).
Some users trade highly speculative assets (so-called altcoins) that are not widely available and whose value fluctuates enormously.
In terms of VA usage in other economic sectors not related to direct financial investments, according to gathered information, online betting via internet platforms that accept VAs as a method of payment is the most prevalent. Specifically, the betting sector is strictly regulated in most jurisdictions, sometimes explicitly prohibited, leading to the emergence of online casinos that relatively easily and simply facilitate betting. Given that access to financial services for such clients is difficult or restricted, especially for foreign clients, VAs emerge as a means to evade scrutiny and oversight when operating games of chance platforms in such jurisdictions.
According to the gathered information, there is no registered games of chance operator in Bosnia and Herzegovina that allows deposits/withdrawals or betting in VAs. However, globally, there are many online casinos and gaming establishments offering this service. Many of them are regulated and legally provide such services, but it is also certain that there are illegal operators, especially in East Asia, where gambling is prohibited in many jurisdictions but is prevalent among the population.
Also, considering that such a form of "international gambling," especially concerning the organization of so-called "poker tournaments," is gaining increasing popularity globally as it allows playing against participants from around the world, there are also participants in online gambling from Bosnia and Herzegovina. VASP-1 has identified several individuals with cryptocurrency transactions associated with online gambling. Considering the internal rules of the domestic VASP, such activity is categorized as high risk, and additional monitoring measures are implemented for such clients to gather information about the nature and extent of their engagement on these platforms.
Essentially, it is certain that this type of association between VAs and online gambling exists in BiH, but estimates suggest that it is not prevalent to a significant extent or scale. However,

given that it is a very dynamic activity, special attention should be paid to monitoring future trends.

The other risk for using VAs for illegal trading purposes involves using VAs to procure or sell illegal or strictly controlled products (drugs, weapons, pornographic content, medications, and the like). Most of these transactions occur either directly between the buyer and seller (P2P) or via the so-called Darknet, a hidden internet platform that enables communication and information exchange, as well as intermediation in trade between buyers and sellers. A particular risk is that such transactions can involve extremely small amounts, making it difficult to track the flow of money if the value is low. The monitoring and tracking system used by the largest domestic VASP to assess risk is capable of identifying transactions and addresses associated with such platforms or individuals, and such cases are reported to the Financial Intelligence Unit (FIU).

When it comes to designated non-financial businesses and professions (DNFBP), the Working Group collected data from supervisory authorities and professional associations of lawyers, notaries, accountants, real estate agents, as well as supervisory authorities for entities engaged in games of chance services, trading in precious metals and gemstones, and trading in high-value goods. The collected data indicate that there have been no recorded cases suggesting the use or misuse of VAs in the mentioned activities, which certainly does not mean that there are none or that there won't be any in the future. The key aspect in the mentioned sectors, generally concerning AML/CFT, is primarily the quality of work of supervisory authorities and their ability to recognize cases associated with ML/TF.

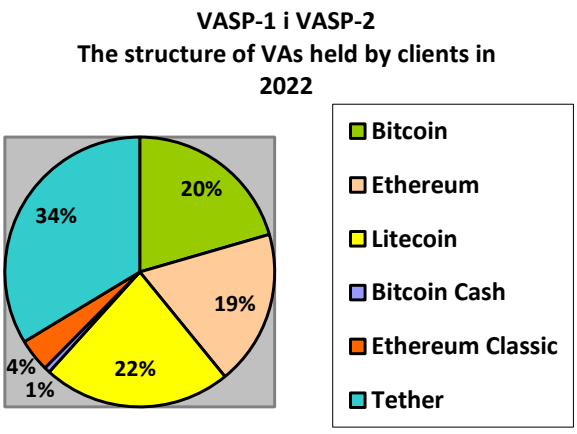
Considering all the above, international online gambling and betting, as well as trading via the Darknet where payment is made in VAs, are assessed as high-risk activities for the misuse of VAs for ML/TF purposes, while DNFBPs are rated as medium-risk.

8. Risk assessment of ML/TF by VA type / VASP services

8.1. Analysis of VA products and materiality of VASP services

As stated in Chapter 4.6, *Sector of VA and VASPs*, there were a total of two VASPs operating in the territory of RS between 2020-2022, specifically: ASP-1 as a centralized exchange offering users digital wallets for storing, exchanging, receiving, and sending VAs, and VASP-2 as a provider of cryptocurrency ATM services.

VASP-1 offered six different VAs, including five cryptocurrencies (Bitcoin, Ethereum, Litecoin, Bitcoin Cash, and Ethereum Classic) and one stablecoin (USDT - USD Tether). The total amount of VAs held by VASP-1 clients during 2022 was approximately 10.8 million BAM. VASP-2 conducted activities exclusively through crypto ATMs (5 of them) and offered three types of VAs in its services (Bitcoin, Ethereum, and Litecoin). In addition to these VAs, DOGE, BCH, and USD were also available for purchase, but exclusively, they could not be sold via crypto ATMs. VASP-2 provided its services from April 2021 to September 2022 and resumed operations after July



2023.[46] The total amount of VAs held by VASP-2 clients during 2022 was approximately 1.23 million BAM. In their response, both VASPs state that they do not offer VAs from the group of anonymous VAs, nor have they provided services or conducted offers for the initial sale of virtual currencies (ICO). However, it has been found that the majority of clients use the domestic VASP solely as an entry point into crypto, i.e., immediately after purchasing VAs through the domestic VASP, they transfer them to their accounts with international exchanges where they can trade a significantly larger number of VAs. Additionally, some banks in Bosnia and Herzegovina allow their clients to receive and send fiat currency transfers to/from accounts with foreign VASPs. There are no official data on the type and quantity of VAs held by clients from Bosnia and Herzegovina with foreign VASPs or on non-hosted wallets. However, it is a fact that clients from Bosnia and Herzegovina, through these means, are able to trade in all types of VAs, including anonymous, pseudo-anonymous, platform, and stablecoins.

Considering the large number of different VAs[47], it was not possible to conduct individual assessments for each VA. Instead, an overview of various types and subtypes of existing VAs is provided below, with descriptions and examples of each type. An assessment of the inherent risk of eight types and subtypes of VAs was conducted in terms of their anonymity, usability, and security features.

Table 1: Overview of VA types across the world

VA type	Subtype	Description	Prominent examples
VA exchange	Pseudo anonymous	• Mainly used as a means of exchange or store of value • Transactions can be linked to a specific sender	Bitcoin, Litecoin
	Anonymous	• Similar to pseudo-anonymous VAs, but transactions cannot be linked to a specific sender	Monero, Dash
	Platforms	• Provides access to digital markets and platforms • Primarily geared towards use on specific markets/platforms but often used for currency exchange	Ethereum, ERC20 tokens
	Stablecoins	• Strive to maintain price stability by being backed by reserve assets (e.g., fiat currencies)	Tether, USDC
Service-oriented VAs		• Funds that grant users access to a specific planned or operational service or product (e.g., exclusive user benefits) and generally resemble vouchers	FC Barcelona Fan Tokens
Security VA	Security VA	• Equivalent to traditional securities, providing owners with voting rights and dividend payments, but do not meet all the criteria of "financial instruments" under MiFID II/MiFIR.	Aspencoin
	Security-featured VA platform	• VAs presented by issuers as platform VAs, but with a built-in feature enabling revenue sharing with VA owners	Binance, Huobi

[46] After the amendments to the RS Law on the Securities Market came into force, this VASP suspended its operations pending completion of the registration process with the RS Securities Commission.

[47] According to data from the CoinMarketCap platform as of September 2023, there are over 23,000 different cryptocurrencies worldwide.

Closed virtual currencies	• Designed to be used as a means of exchange within closed ecosystems (e.g., video games)	World of Warcraft gold

All types of VAs are susceptible to the risk of ML/TF, particularly the anonymous ones. Anonymity for VA transactions can be facilitated by default due to their inherent technological properties or through second-layer solutions, such as anonymization tools. By default, anonymous VAs provide the highest level of anonymization to their users among all types of VAs. This means that they prevent external observers from seeing the balance of addresses or the amounts of transactions. Examples of such VAs include Monero and Zcash. It's apparent that such a product is designed to protect the privacy of its users, even if the intention isn't to enable illegal activity, thereby posing a higher risk of being used for ML/TF. While crime may not be the aim of these latter products, this is an obvious aspect that makes them more appealing for use by criminal elements. One study showed that over 70% of ICOs by value went to what was considered "quality projects," but over 80% of projects, by number, were identified as scams.[48] For this reason, anonymous VAs are rated as highly risky VAs in terms of AML/CTF.
Unlike anonymous VAs, pseudo-anonymous, platform, and stablecoins are types of VAs that are transparent, meaning that transactions and balances can be verified and tracked by any user. Therefore, addresses that have sent or received VAs of this kind can potentially be linked to a person's real-world identity. Furthermore, websites such as "blockchain.com" or "etherscan.io" allow public internet users to check the history of each address and transaction that has ever occurred on the VA network.
It's important to mention that in some cases, pseudo-anonymous and platform VAs can achieve a similar level of anonymity as anonymous VAs. Users can utilize anonymization tools or intermediaries to conceal transaction flows and significantly hinder the linking of identities to them. Such tools can include centralized mixers or specialized software solutions that enable users to mix funds with each other without a coordinating body.[49] Furthermore, recent trends in Bitcoin protocol development suggest that anonymization tools could become easier to implement in the future, making them more widely used.[50] For this reason, pseudo-anonymous and platform VAs are rated as highly risky in terms of ML/TF.

Stablecoin VAs offer less anonymity to their users compared to anonymous, pseudo-anonymous, and platform VAs. Stablecoin VAs are issued by a central governing body and are typically not designed to maximize anonymous characteristics.
From the perspective of usability for PN/FT purposes, it can be noted that pseudo-anonymous and platform VAs, as well as stablecoins, are most commonly abused due to their liquidity. Pseudo-anonymous VAs have the largest market capitalization, primarily driven by Bitcoin, which constitutes over 90% of that value. Pseudo-anonymous and platform VAs, as well as stablecoins, have trading volumes of over $1 billion each day. On the other hand, anonymous VAs have less than $100 million in daily trading volume across all global exchanges because only a few major exchanges offer trading with them. Therefore, potentially more funds can be laundered through pseudo-anonymous and platform VAs, as well as through stablecoins, than through anonymous VAs.[51] For this reason, stablecoins are rated as medium risky VAs in terms of ML/TF.

[48] https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ
[49] Coindesk, Binance Blockade of Wasabi Wallet Could Point to a Crypto Crack-Up
[50] Coindesk, An Army of Bitcoin Devs Is Battle-Testing Upgrades to Privacy and Scaling
[51] https://coinmarketcap.com/

Service-oriented VAs, security VAs, and closed virtual currencies have lower vulnerability to ML/TF activities compared to other types. Firstly, their anonymity is limited, as many of them require users to disclose personal information to VA issuers. Secondly, they lack significant transactional and exchange liquidity, which limits their usability. Thirdly, their security is also limited because the validation of transactions for these types of VAs is typically controlled by a central governing entity, which can impose certain restrictions. Furthermore, utility VAs are not designed for trading on exchanges, and the exchange usually occurs only between users and the application owner. Together, these factors make these types of VAs largely unsuitable for ML/TF purposes, and they are rated with a low level of risk.[52]

Below is an additional threat assessment based on additional characteristics of VAs, primarily: nature and profile, accessibility to criminals, source of funding, operational characteristics, crime facilitation, and economic impact
In this regard, the following table provides an assessment of the inherent risk for eight types and subtypes of VAs.

VA type	Subtype	Inherent risk
VA exchange	Pseudo anonymous	High
	Anonymous	Very high
	Platforms	High
	Stablecoins	Medium
Service-oriented VAs		Low
Security VA	Security VA	Low
	Security-featured VA platform	Medium
Closed virtual currencies		Low

It can be concluded that anonymous VAs have a very high inherent level of risk of ML/TF due to their anonymity, usability, and security features. For many of them, it is not possible to adequately monitor and assess transaction risk or identify the sender if trading occurs through VASPs that do not perform sender and receiver identification.
On the other hand, although there were no identified cases of ML/TF associated with VAs in Bosnia and Herzegovina during the period of 2020-2022, it is evident that when it comes to other criminal activities somehow linked to VAs, criminals in Bosnia and Herzegovina most often use Bitcoin for their payments and transfers, which falls under pseudo-anonymous VAs. However, considering the fact that a large number of altcoins can be easily exchanged for Bitcoin through VASPs without any difficulties, highlighting Bitcoin as highly risky VAs becomes irrelevant and unnecessary. Consequently, the general assessment is that almost all types of VAs can be used for ML/TF purposes, but the most common use of Bitcoin in the final phase is likely due to its ease and speed of exchange for fiat currency in larger amounts, as well as its relatively stable value compared to other types of VAs.

8.2. Assessment of inherent risk in relation to VASPs

[52] Vertical risk assessment of Luxembourg regarding ML/TF associated with VAs and VASPs

Risk assessment has been conducted both in relation to the type of services provided by VASPs and in relation to other methods and means of VA exchange (P2P exchange, brokers, crypto ATMs, centralized and decentralized applications, anonymization tools, miners, and validators).

8.2.1. Centralized exchanges (CEX)

Centralized VASP exchanges (CEX) are platforms for trading virtual assets (VA) controlled by a central entity and acting as intermediaries between cryptocurrency buyers and sellers. Centralized exchanges store digital assets on behalf of clients, establish trading terms and conditions, and hold their clients' wallet private keys, which is a critical component of cryptocurrency transfers. They also typically require platform users to undergo a Know Your Customer (KYC) verification process, which includes providing identity information, submitting documents for identity verification, and waiting for KYC document verification. Users are typically granted permission to fund their accounts and commence trading once these steps are completed.

From a global perspective, centralized exchanges are the most developed subtype of VASPs in terms of size and trading volume Only the top 227 centralized exchanges listed on the Coinmarketcap portal have a daily trading volume exceeding $150 billion[53]. Binance is the world's largest crypto exchange by trading volume, with $76 billion in daily trading volume on the Binance exchange since August 2022 and 90 million clients worldwide. On this platform, users can buy, sell, and store their digital assets, as well as access over 350 cryptocurrencies and thousands of trading pairs.[54] Different types of client profiles, high exchange volumes, and a large number of clients on centralized exchanges increase ML/TF risks.

CEX clients can be both individuals and institutional clients. Also, clients are often VASPs themselves, such as brokers or entities involved in ICOs looking to exchange raised VAs into fiat currency. CEXs typically offer activities with pseudo-anonymous or platform-based VAs, which have previously been assessed with a very high or high level of inherent risk. CEXs enable exchanges of virtual currencies for virtual currencies as well as virtual currencies for fiat currencies and vice versa. Therefore, from the perspective of ML/TF risk, CEXs are the riskiest type of VASPs because, unlike other types, they represent the entry and exit points for cryptocurrencies, i.e., they enable the exchange of VAs for fiat currencies. The process of purchasing VAs through CEXs involves the client first making a non-cash deposit in fiat currency. As the next step, when the buyer creates a market order to purchase VAs on the exchange, the exchange matches the order with listings from other users willing to sell VAs for fiat currency and facilitates subsequent trading. Once clients purchase VAs, they can store their funds either on the CEX itself or in private, so-called non-custodial wallets over which CEXs have no control. These wallets are mostly anonymous, and criminals use them by having multiple such wallets, fragmenting funds, and transferring them from one wallet to another in an attempt to conceal the recipient's identity. At the end of the money laundering process, criminals transfer VAs from non-custodial wallets, where the sender's and receiver's identities have been blurred, back to their wallets at centralized exchanges and exchange them for fiat currencies, which they further deposit into clients' bank accounts.

Each money laundering process involving VAs and VASPs consists of three interconnected phases: 1) placement of funds, 2) layering of funds, and 3) integration.

[53] https://coinmarketcap.com/rankings/exchanges/ as at June 9, 2023.
[54] https://coinmarketcap.com/exchanges/binance/

Placement refers to the initial entry of illicit gains into the financial system. Illegal money may already be in the form of VAs (for example, from selling illegal drugs on the Darknet for VAs or direct P2P purchases from another party) or in fiat currency. In the case of fiat placement, the criminal first needs to register with a centralized exchange and exchange fiat currency for VAs. In the case of direct placement of VAs, a criminal can send VAs either to wallets opened with any VASP or to non-hosted wallets under their exclusive control. It is important to emphasize that all types of VASPs can be abused during the placement phase if criminal proceeds are generated in VAs, but only certain types of VASPs can be used to launder proceeds generated in fiat currency (centralized exchanges).
In the second phase (the layering phase), criminals engage in activities aimed at distancing illicit funds from their source, or attempting to obscure the transaction trail, using various methods such as: fragmenting transactions in VAs and sending them to one or more VASPs, using anonymization tools (so-called mixers), employing decentralized exchange systems (DEX), peer-to-peer exchanges, and so on.
The final step in the money laundering process (the integration phase) involves withdrawing funds in cash or transferring them to a bank account. Therefore, the last step almost always involves centralized exchanges (domestic or foreign) that convert VAs into fiat and make payouts to a bank account.
According to the Chainanalysis report for Bosnia and Herzegovina covering the period from October 2021 to October 2022, out of the total received funds (~3.96 billion BAM), as much as 75.2% was exchanged via centralized exchange. From this report, it's not apparent what proportion of funds were exchanged through domestic versus international CEXs, but by simply comparing data received from domestic CEXs and domestic banks, it's easy to conclude that the vast majority of transactions (over 95%) occurred through international CEXs. Considering all the aforementioned, it is estimated that CEXs have a high level of inherent risk of ML/TF. During the risk assessment, there were opinions that domestic CEXs have a lower level of inherent risk compared to international ones. However, due to the fact that supervisory authorities have not had the opportunity to directly oversee the operations of domestic CEXs so far, the prevailing opinion is that they should also have a high level of inherent risk of ML/TF until further notice.

8.2.2. ICO/ IEO issuers

Initial Coin Offering (ICO) is a type of funding that utilizes cryptocurrencies as a means to raise capital for early-stage companies. Any cryptocurrency or blockchain company seeking to raise funds for developing an application, service, or new coin can use an ICO to gather those funds. In general, this means that investors can purchase the cryptocurrency at its initial issuance.
When it comes to Bosnia and Herzegovina, data indicates that there have been several attempts at ICOs in recent years, while one case even ended up in court due to a bank's decision not to engage in business with a company from the Republika Srpska (RS) that attempted to present mining VAs as its business idea. The foreign sister company had a business idea to mine VAs using special mobile facilities they called 'Mining Farms,' which would utilize renewable energy sources obtained from private solar and hydro power plants located in Bosnia and Herzegovina. The reason for choosing Bosnia and Herzegovina for the location of these mining facilities was significantly lower price of electricity compared to other countries in Europe. As a means of raising investments for their innovative business idea, they decided to conduct an ICO based on the Ethereum blockchain, utilizing ERC20 standard smart contracts, thus creating their own token, the BMF token. However, the bank terminated its business

relationship with the company from Republika Srpska, leading to the entire case ending up before the court, where in the first instance the bank lost the case, while in the second instance it won. Currently, the case is pending before the RS Supreme Court.[55]

Contrary to ICO, an Initial Exchange Offering (IEO) refers to an event in which token sales are conducted through a designated cryptocurrency exchange. This is a method through which newly established organizations raise capital by selling utility tokens that grant privileged status within the organization through a crypto exchange platform. Initial Exchange Offering provides a safer alternative for potential investors to purchase tokens during the fundraising phase directly from their exchange wallets. IEOs originated in January 2019 with the launch of the BitTorrent token (BTT) by Binance Launchpad.[56]

The issuer of ICOs and IEOs connects potential buyers with the company issuing VAs, and it's possible that they may also issue them themselves. Therefore, the primary activity of these issuers is similar to that of a centralized exchange. However, compared to centralized exchanges, ICO and IEO issuers are less vulnerable to ML/TF abuse due to several factors. First, ICO and IEO issuers typically offer VAs on platforms with lower risk ratings than pseudo-anonymous or anonymous VAs. Second, the value of such VAs is highly unstable, which is not conducive to criminals as they may lose their funds due to the market value of the newly issued VAs plummeting. On the other hand, there is usually a certain amount of time between the ICO/IEO issuance and the date when the newly issued VA becomes available for trading. Therefore, a criminal who bought VAs in an ICO or IEO would have to wait for a certain period before being able to exchange them for fiat currencies. Once the VA becomes available for trading on the exchange, its price could significantly drop from the issuance. So, the criminal's income potential could potentially be reduced, making ICOs or IEOs less suitable for ML/TF purposes. On the other hand, the ICO sector is highly vulnerable to ICO scams, and many companies are expected to seek funding through this method in the future. ICOs are estimated to represent a very high level of inherent risk of ML/TF, mainly due to the potential use of ICOs for committing fraud, as seen in numerous pyramid schemes registered in BiH.

8.2.3. Custodial wallets providers

Wallet custody service providers are vulnerable to misuse for ML/TF purposes as criminals can use them to store and transfer VAs. CEXs often also provide custody services, holding users' private keys. While this contributes to user convenience, it also means that users risk losing their assets if their profile is hacked. Globally, there are several wallet custody service providers that can offer custody over high-risk VAs, such as pseudo-anonymous or anonymous VAs. On the other hand, the broader acceptance of wallet custody service providers for ML/TF abuse is limited by their relative lack of security for criminals, as their operators can freeze accounts and impose censorship on their users' transactions. Criminals could use alternative solutions, such as specialized software solutions, to independently store their VAs and reduce their exposure to third parties. Additionally, there are wallet custody service providers in the market who exclusively offer their services to institutional investors. Such custodians typically have high financial barriers to entry, potentially reducing their vulnerability to ML/TF. For example, Coinbase Custody, the largest custody service provider in the world, accepts clients with a minimum balance of 1 million dollars.[57] However, this type of custodian is also unsuitable for criminals because it lacks anonymity. Criminals planning to use custodians for money laundering would have to undergo KYC checks. Therefore, criminals prefer self-

[55] https://brankopetrovic.blog/wp-content/uploads/2023/04/Studija-slucaja-Obaranje-dokaza-jednog-od-najvecih-kripto-sporova-u-istoriji-Neznanje-o-pravu-skodi.pdf

[56] https://cleartax.in/s/initial-exchange-offering-ieo

[57] https://www.coinbase.com/blog/coinbase-custody-acquires-xapos-institutional-business-becoming-the-worlds

custody solutions that do not require users to disclose their real identity to third parties. On the other hand, there is a recognized risk that wallet custody service providers often have very limited experience in KYC/AML procedures compared to banks. Considering all the above, wallet custody service providers are assessed to represent a medium level of inherent risk when it comes to ML/TF.

8.2.4. Peer-to-peer (P2P) exchange

The decentralized nature of peer-to-peer (P2P) cryptocurrency exchanges is highly appealing to criminals looking to launder illicit funds, as the transparency measures adhered to by numerous CEXs on P2P platforms are often not mandatory, creating a challenge for law enforcement efforts to track such activities. Criminals seeking to evade Know Your Customer (KYC) measures conducted by reputable cryptocurrency exchanges have begun to abuse legitimate peer-to-peer exchanges for the purpose of laundering illicit funds.[58] In essence, P2P exchanges are websites with advertisements where sellers and buyers can post their offers and have a cryptocurrency wallet to store assets. These platforms also have a chat for user communication and an escrow account to hold assets until the fiat payment is completed. Matching of trades is done using computer algorithms, and traders typically do not have to disclose their real identity, which can increase the vulnerability of peer-to-peer exchanges for ML/TF purposes. The role of a P2P platform is simply to connect buyers and sellers for a small fee, where clients transfer funds to personal wallets immediately after the transaction, without the P2P exchange holding them. Before initiating a sale, the seller must transfer their cryptocurrency to their wallet on the P2P exchange. To start trading on this platform, a user can either choose an existing offer or create their own advertisement. Once someone accepts the offer and the trade is initiated, the crypto is sent to an escrow account. It remains there until the buyer sends the agreed-upon amount to the seller through the agreed-upon payment channel. Payment can be made in cash, via mobile banking apps, using gift cards, but it's also possible to exchange it for other cryptocurrencies. After the seller confirms receipt of the payment, the asset is released to the buyer from the deposit. If the buyer and seller cannot agree on whether the payment has been made, the crypto remains in the deposit until an arbitrator resolves the dispute.

Given that sellers and buyers have the option of direct communication, they often meet face-to-face to conclude the transaction.

Since peer-to-peer exchanges often do not require KYC and do not have a central server, trading on them cannot be restricted. The Chainalysis report for 2020 on the state of crypto crime highlighted that these factors increase the acceptance of peer-to-peer exchanges by criminals for ML/TF purposes.[59]

On the other hand, peer-to-peer transactions also have some limitations when it comes to ML/TF. Unlike centralized exchanges, peer-to-peer transactions have high technological entry barriers. Users already need to have specific VA platforms to use them. Peer-to-peer exchanges can often only be accessed through specialized third-party software solutions. For instance, accessing peer-to-peer exchanges on the Ethereum network requires a specific browser extension. Consequently, it is inevitable to conclude that these services can only be provided by IT companies or highly IT-educated individuals. Given that some miners and VASPs in BiH have sister IT companies, there is a non-negligible risk that they could be used to create P2P platforms.

[58] KYC (Know Your Customer) is a security process in which companies, primarily financial institutions, verify the identity of customers to reduce the possibility of platform misuse.
[59] Chainalysis, 2020 Crypto Crime Report

Furthermore, although P2P exchanges are designed to protect both the buyer and the seller, there is still a high risk of fraud on them. For example, a seller may receive payment and refuse to release the funds from the deposit. This leads to a dispute, and in some cases, the fraudster could convince the arbitrator that they did not receive the deposit, thus retaining the cash and also the crypto. Resolving disputes on P2P platforms, especially when they face high trading activity, can sometimes take days.

However, a common scam is to prompt the seller to release their cryptocurrency from the deposit account before receiving payment. It is also common for fraudsters to make payments via bank transfers and then reverse the transaction after receiving the crypto. While fiat transactions can be reversed, crypto transactions cannot.

The technological complexity of peer-to-peer exchanges, along with the mentioned possibilities of fraud, lead to an overall lack of liquidity on them. Low trading volume makes it difficult for criminals to launder large amounts of VAs through them. The total value received by P2P markets in Bosnia and Herzegovina from October 2021 to October 2022 was 4.72 million BAM, representing only 0.12% of the total received value in the same period. However, although this amount is not significant in terms of the total received value, it ranks BiH high at 65th place in the Global P2P Exchange Index compiled by Chainanalysis. Analysis of the number of transfers that have moved from P2P platforms to wallet addresses in BiH shows that there were an average of about 47 thousand P2P transfers per month during the mentioned period.[60] This number includes both P2P transactions between individuals within BiH and P2P transactions between individuals from BiH and abroad. However, it was not possible to determine the exact ratio between domestic and cross-border transactions. If we divide the total received value by the total number of P2P transactions (~556,000), it turns out that the average transaction amounts to around 8 BAM, which may lead to the conclusion that this exchange method, although highly risky, still has limitations when it comes to ML/TF. According to current legal provisions in BiH, it is not possible to legally establish and register a P2P platform that would provide services without a mandatory identification process for the sender and receiver. However, considering that for P2P platforms, state borders pose no obstacle, the risk of ML/TF through P2P exchange becomes more pronounced and facilitated. This is particularly interesting because it has been found that there is at least one website in the FBiH area for connecting supply and demand for a wide range of goods and services. Although this portal cannot be considered a classic P2P platform, there are a large number of advertisements for buying and selling VAs on it, among other goods and services. The buyer and seller typically arrange a face-to-face meeting where they directly exchange VAs for fiat currencies or for other types of goods or services. If this payment is made through a bank account, it represents only a transaction between two individual clients, not between the client and the company providing P2P services, which poses a challenge for the banking sector in identifying suspicious transactions.

Although the Chainalysis report for BiH does not specify the amount of funds from P2P exchange that can be linked to criminal activities, the fact that transactions can be conducted without the identification of the sender and receiver is sufficient to classify P2P exchange as highly risky when it comes to ML/TF

8.2.5. Brokers

Brokers facilitate trading between individual buyers and sellers who cannot or do not want to execute transactions on the open market. Brokers typically serve institutional clients and globally enable trades worth billions of dollars. They are usually affiliated with the stock

[60] Chainalysis Country Analysis Report on Bosnia 2021-2022, pg.5

exchange but operate independently. VA traders often use brokers if they want to liquidate a large quantity of VA at a specific, agreed-upon price. One of the risks associated with brokers is nested accounts. Through these accounts, brokers aggregate clients under their main account, making it difficult to track inflows and outflows of funds for each individual client. Specifically, in order to conceal and obscure the source of funds, criminals use brokers to transfer their assets through their account to a centralized exchange, without the brokers being aware of it. Some exchanges have addressed this by requiring brokers to maintain separate wallets for each of their clients to facilitate easier tracking of the chain of inflows and outflows associated with a particular client.

Most nested services are legitimate businesses, and many prominent over-the-counter (OTC) brokers operate through this type of account. However, according to Chainalysis, the problem lies in the fact that while most brokers conduct legitimate business, some specialize in providing money laundering services to criminals. Brokers typically have much lower KYC requirements than the exchanges where they operate. Many of them exploit this leniency and assist criminals in laundering and cashing out funds, usually by first exchanging Bitcoin and other cryptocurrencies into Tether as a stable intermediary currency before likely cashing them out into fiat. Chainalysis has determined that the hundred most active brokers who knowingly laundered funds for criminals received over 3 billion dollars in 2019.[61] In Bosnia and Herzegovina, the existence of this type of brokers and their services is not registered.

Considering all the above, brokers are assessed to represent a medium level of inherent risk when it comes to ML/FT.

8.2.6. Cryptomats (crypto ATMs)

Cryptomats (also known as BTMs - Bitcoin Teller Machines) are devices that enable the purchase of VA using cash or debit cards and are continuously connected to the internet. They resemble ATMs designed for fiat currency, and the device itself consists of a scanner, cash slot, and transaction management computer. Additionally, some cryptomats also enable the sale of VA for cash using a scannable wallet address. In some cases, cryptomat service providers require users to have an existing account for transactions on the device. Globally, most cryptomats have predefined transaction limits below which identification is not required, potentially exploited by criminals for money laundering (ML). Specifically, to avoid any identification procedures, criminal depositors employ the technique of breaking down amounts below the identification threshold. Moreover, criminals often register on cryptomats using fake documents, after which they make cryptocurrency purchases, transfer them to non-hosted wallets, and later to centralized exchanges through which they cash out in fiat currencies.

When it comes to RS, it has been determined that VASP-2 provides services through five crypto ATMs. These ATMs are two-way, meaning they can dispense cryptocurrencies in exchange for local currency (BAM), and vice versa, they can dispense fiat currency (BAM) in exchange for cryptocurrencies. For each service, the ATM charges an additional fee percentage of 5% of the transaction value. The following cryptocurrencies can be purchased on these devices: Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Bitcoin Cash (BCH), and Dogecoin (DOGE), and Bitcoin (BTC), Litecoin (LTC), and Bitcoin Cash (BCH) can be sold[62]. It is important to emphasize that these crypto ATMs have daily (3,000 BAM), monthly (10,000 BAM), and yearly (100,000 BAM) limits, and identification is required when buying/selling VAs regardless of the transaction amount. The identification process involves registration via

[61] https://blog.chainalysis.com/reports/crypto-laundering/
[62] https://www.dcx.ba/usluge-bankomati.html

the crypto ATM based on a valid photo identification document, registration of a phone number to receive an access code, and completion of a PEP statement.
When it comes to FBiH and BDBiH, it has been determined that during 2023, in the areas of Sarajevo, Tuzla, and Brčko, one company, without authorization, installed crypto ATMs (one in Sarajevo and Tuzla, and one in Brčko) where VA can be exchanged for fiat currency and vice versa. It was found that the company provides its services without customer identification, with a limit of individual transactions set at 29,999 BAM.
Based on the foregoing, it is assessed that VASP-2 crypto ATMs represent a high level of inherent risk of ML/TF, while ATMs in Sarajevo, Tuzla, and Brčko are assessed as very high-risk primarily due to the fact that they operate without supervision and authorization, and do not implement customer identification and monitoring measures. Taking into account that there are two different levels of assessed risk, on one hand in the RS area and on the other hand in the FBiH and BDBiH areas, it is estimated that crypto ATMs in Bosnia and Herzegovina have an average high level of inherent risk of ML/TF.

8.2.7. Decentralized exchanges (DEX)

A decentralized cryptocurrency exchange (DEX) is an exchange built on a decentralized, non-custodial blockchain system that primarily supports direct peer-to-peer transactions. The largest and most well-known decentralized exchanges are: OKX, Uniswap, PancakeSwap, and others.
It's easy to confuse Peer-to-Peer (P2P) exchanges with DEX. However, they differ significantly in how they facilitate trading with VA, and even in how they are established, owned, and operated. A P2P exchange is founded, owned, and operated by a registered company. It's a website that connects sellers and buyers and facilitates the transfer of crypto from one wallet to another. A P2P exchange cannot exist without a legally registered entity behind it. The company behind a P2P exchange maintains and provides users with daily support. It also must continuously fulfill regulatory requirements such as requesting users to identify themselves by providing identification documents and their current addresses. However, the fact remains that a P2P exchange can easily go offline, as it is a portal or website hosted on a server.
On the other hand, a decentralized exchange (DEX) is a standalone application on the blockchain whose processes are governed by smart contracts. This approach eliminates the need for intermediaries. DEX does not require a formally registered company behind it. When trading on a DEX, one does not buy or sell directly from others. The trader never communicates with anyone other than the liquidity pool managed by the smart contract. The funds they send go into the liquidity pool, and what they receive also comes from the liquidity pool. So, essentially, trading is done via smart contracts. Due to its design, on a DEX, only one cryptocurrency can be exchanged for another, i.e., it cannot facilitate conversion between cryptocurrencies and fiat currencies. Regulators have little influence to compel DEX to follow their instructions because this form of trading is essentially just code executed on computer networks. Since DEX is on the blockchain, regulators find it difficult to shut down. Furthermore, decentralized exchanges do not require users to complete the KYC process. This allows for anonymous trading. Moreover, these applications enable users to maintain autonomy over their private keys unlike centralized exchanges that have control over their clients' wallets. Since decentralized exchanges facilitate direct transactions between buyers and sellers and operate without intermediaries, they have lower transaction fees compared to centralized exchanges. However, from the perspective of ML/TF, decentralized exchanges have several drawbacks, and one of them is that they often suffer from lower liquidity levels compared to centralized exchanges due to their typically smaller user base and trading volume. According to the Chainanalysis report for Bosnia and Herzegovina covering

the period from October 2021 to October 2022, out of the total received funds (~3.96 billion BAM), approximately 20% was attributed to centralized exchange.
Another drawback, compared to centralized exchanges, is that they are more technical in nature and require a certain level of understanding of blockchain technology to be used. For example, users must use compatible wallets for trading on the platforms and must manage their private keys. These steps, which can sometimes be challenging, can result in the loss of assets due to errors, especially for novice traders and investors.[63]
Furthermore, criminals are not favored by the fact that they cannot exchange cryptocurrencies for fiat currencies on decentralized exchanges.
However, despite these characteristics that reduce the level of vulnerability, it is assessed that DEXs represent a high level of inherent risk of ML/TF, primarily due to the established trading volume on them by clients from Bosnia and Herzegovina, anonymous trading, and the absence of customer identification and monitoring (KYC).

8.2.8. Mixers - tools for anonymization

Anonymization tools or "mixers" are online services used to conceal transaction flows and increase user anonymity. They have become a popular tool for those who want to keep their financial transactions private. Criminals often use unregulated decentralized mixers and the Darknet[64] to evade regulatory requirements for customer monitoring (KYC). Essentially, a mixer obscures the transaction chain on the blockchain by consolidating all transactions at the same Bitcoin address and sending them together through a complex, semi-random sequence of fake transactions, making it appear as if they were sent from another address, which greatly complicates linking specific addresses to specific transactions. Mixer services work by receiving instructions from users to send funds to a specific Bitcoin address, for which the mixing service provider charges a fee.[65] For conducting illicit activities using mixers, criminals typically use one cryptocurrency wallet located on the public internet (Clearnet) and two or more cryptocurrency wallets operating exclusively on the Darknet. For example, the attacker will send cryptocurrency from the wallet located on the public internet to the mixers. After mixing, laundered VAs are transferred to the TOR wallets of criminals[66].
According to a report by Chainalysis, a blockchain analytics company, Mixers processed a total of $7.8 billion in 2022, 24% of which came from illicit addresses, whereas in 2021, they processed $11.5 billion, only 10% of which came from illicit addresses. The data suggests that legitimate users have decreased their use of mixers, possibly due to law enforcement actions, while criminals have continued to use them. It's also worth noting that the vast majority of illicit value processed by mixers is made up of stolen funds.[67] According to a report by FATF, an intergovernmental organization that develops guidelines against money laundering, Bitcoin mixers are one of the biggest threats to anti-money laundering efforts in the cryptocurrency space. The report states that criminals primarily use mixers for money laundering and to avoid detection by law enforcement agencies.

[63] https://cointelegraph.com/learn/centralized-vs-decentralized-crypto-exchanges
[64] Darknet is a term referring to a specific collection of websites that exist on an encrypted network and cannot be found using traditional internet browsers. Nearly all sites on the Darknet conceal their identities using encryption tools.
[65] https://knepublishing.com/index.php/Kne-Social/article/view/1523/3612#content/citation_reference_3
[66] TOR wallets are anonymous wallets designed to keep their users' identities hidden. TOR functions by changing the user's internet address location and encrypting the internet address by routing the user's network through multiple remote servers.
[67] https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf

When it comes to the regulation of Bitcoin mixers in some countries, they are currently either illegal or operate in a legal gray area. For example, in the United States, the use of Bitcoin mixers is considered a violation of anti-money laundering laws, while in Japan, Bitcoin mixers can operate only if they are licensed by the government. Similarly, in the European Union, Bitcoin mixers are subject to anti-money laundering regulations and must comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.[68] As for Bosnia and Herzegovina, there are currently no regulations allowing the registration of mixer services, but there are also no regulations prohibiting their use, so it can be stated that this area is completely legally unregulated. During the analysis of cases, the working group did not identify specific cases of mixer abuse for ML/TF purposes, which certainly does not mean that they do not exist. However, it is significant to emphasize that cases of Darknet abuse for the purchase of illegal and prohibited substances have been identified, where VAs were used as a means of payment. This is important because these cases are often closely related to the misuse of mixers to conceal identity and transactions.
In light of the above, it is estimated that VA mixers have a high level of inherent risk of ML/TF.

8.2.9. Miners/validators

Mining is a term used to describe the process of validating transactions waiting to be added to the blockchain database for VAs that operate on the principle of blockchain so-called Proof of Work. There are numerous VAs that can be mined, but Bitcoin is certainly the most famous. A VA like Bitcoin has no centralized authorities that validate transactions. With Bitcoin, that work is done by miners. In the process, they create new Bitcoins. On blockchains that function on the principle of the so-called "Proof of Work" mining establishes a chronological order of transactions, which is essential to ensure that previous entries in the crypto "open ledger" cannot be altered. If a transaction is to be successfully confirmed and included, it must be packed into a block that must comply with strict encryption rules, and verified and validated by miners on the network. The process is called mining because of the many parallels with gold mining. Both scenarios involve the investment of a large amount of labor and energy into the production of a very valuable assets.
The most successful miners are rewarded with new Bitcoins if they successfully add a new block to the blockchain. In order to achieve greater computing power, miners join forces, creating so-called "mining pools". The reward is then distributed in proportion to the work done by each member of the group. Those with more computing power get a higher reward. There is an economic incentive to mine Bitcoin when the costs associated with mining Bitcoin (electricity and computer equipment) are lower than the value of the mining rewards. It it possible that the mining reward will not cover the mining costs. In that case, many people continue to mine, mostly because of the belief that Bitcoin will be worth more in the future. In Bosnia and Herzegovina, in recent years, there has been a multiple decline in the number of miners, primarily due to the increase in electricity prices and the decrease in the value of mined VAs. Estimates from one of the domestic VASPs indicate that there are currently around 2,000 miners in Bosnia and Herzegovina, compared to a peak of up to 20,000 miners.
By extrapolating this data and consulting external sources of information, along with the transactional activity observed by domestic VASPs in the RS, it can be concluded that the majority of mined VAs are exchanged through domestic VASPs. However, based on available information, a very small number of VAs are currently being mined, mostly Chia, primarily because Bitcoin mining has become unprofitable due to high costs and slow mining speeds.

[68] https://bravenewcoin.com/insights/why-bitcoin-mixers-are-a-double-edged-sword-for-anti-money-laundering

Newer blockchains typically use the so-called Proof of Stake and other consensus mechanisms, which do not need or allow mining. Today, this type of VA is dominant compared to those operating on the Proof of Work principle.
Miners (validators) can perform ML/FT in several ways. The basic way is for them to invest their dirty money in buying mining equipment, which will then generate VA for them. By exchanging mined VA for fiat currency, criminals get clean (laundered) funds.
Also, the specialized company Chainanalysis states that recently there is a noticeable trend of criminals "mixing" mined VA with crypto assets transferred from wallets associated with blackmail software (Ransomware) and scams. The process is that VA wallets linked to ransomware and/or scams send funds to mining pools where they are mixed with mined VA, from where they are transferred to VASPs to disguise the origin of the funds and create the illusion that these funds are mining revenue, not blackmail or fraud.[69] However, for all of the above, criminals need sophisticated technical knowledge about setting up the mining process and confirming transactions, as well as significant initial capital investments.
Although law enforcement agencies in Bosnia and Herzegovina have not reported cases of abuse of mining for AML/CTF purposes, due to the described modalities of abuse, miners are assessed to pose a moderate level of risk.

Table: Inherent risk in relation to VASP

VASP type	Subtype	Inherent risk
Exchanges	International centralized exchanges	High
	Domestic centralized exchanges	High
VA issuers	ICO/IEO	Very high
Custodians	Custodial wallets providers	Medium

VASP type	Subtype	Inherent risk
	P2P exchange	High
	Brokers	High
	Crypto ATMs	High
Exchange services and products	Decentralized applications	High
Other	Tools for anonymization	Very high
	Miners and validators	Medium

9. General risk assessment of ML/FT

Although there were no registered cases of ML/FT crimes associated with VA and VASP during the period 2020-2022, it has been determined that there is a general and specific exposure to ML/FT risks, where the exposure to money laundering risks is higher than the

[69] https://blog.chainalysis.com/reports/cryptocurrency-mining-pools-money-laundering/

exposure to terrorism financing risks. The average risk of ML in BiH is assessed as high, while the average risk of TF is assessed as medium.

10. Risk treatment

During the preparation of the assessment, a general and specific exposure to ML/TF risks associated with VA and VASP was identified. The treatment of identified risks was examined by the Working Group through an analysis of available resources and sectoral policies, as well as the legislative, institutional, regulatory, and supervisory framework for AML/CTF regarding VA and VASP.

10.1. Risks associated with resources

The most significant role in the AML/CTF system, when it comes to state authorities, is certainly held by: relevant ministries and prosecutor's offices, FIU, police agencies, banking agencies, securities commissions, insurance agencies, tax authorities, as well as other law enforcement institutions and supervisory bodies. Given the number of competent authorities, it is certain that investments in human and material-technical resources used in the fight against ML/TF are significant, but the question remains whether they are sufficient. Although this assessment is general, it also applies to investments in AML/CTF regarding the misuse of VA and VASP. Namely, the Working Group failed to gather enough data on the available resources and capacities of these institutions to combat ML/TF associated with VA and VASP, which would enable a more serious analysis. However, considering that ML/TF associated with VA and VASP is a fairly new phenomenon that requires both expertise and skills, as well as modern equipment and software, it is certain that all institutions require additional and continuous investments in resources, whether human or material-technical. This is particularly important due to the fact that the world of VA is very dynamic and changeable. In order to overcome the shortcomings of specialized equipment or required expertise, competent authorities are often forced to rely on free or inexpensive blockchain analysis software or external specialized blockchain analysis companies, and even VASPs themselves, within their investigations related to AML/CTF associated with VA and VASP. It has been found that some domestic VASPs possess satisfactory analytical tools for blockchain analysis and identification of transactions related to the Darknet, online gambling, mixers, and other high-risk platforms. Certainly, competent authorities would increase their efficiency if they had direct access to these tools. However, merely possessing tools is not enough; continuous education and training of officials are also necessary.

10.2. Legislative and regulatory risks

Weaknesses have been identified in the legislative framework regarding regulations concerning VA and VASP, primarily at the level of Bosnia and Herzegovina (BiH), but also at the levels of the Federation of Bosnia and Herzegovina (FBiH) and the Brčko District of Bosnia and Herzegovina (BDBiH). As previously mentioned, regulation exists only in Republika Srpska (RS), while at other levels, there is no legislative or regulatory framework governing this area at all. In RS regulations, the definitions of VA and VASP are provided, along with the requirements for maintaining registry of VASPs, specifications of the types of services that registered VASPs can offer, designation of the competent authority responsible for managing the VASP registry and supervising their compliance with AML/CFT laws and other

regulations, delineation of restrictions for VASPs concerning investor asset disposal, imposition of the obligation to inform investors about the risks associated with investing in VAs, and the establishment of supervisory authority's powers and potential sanctions. On the other hand, FBiH and BDBiH regulations do not explicitly prohibit the operation of VASPs, leaving room for the emergence of unregistered and unregulated VASPs. Furthermore, it is important to note that the development of a new Law on AML/CFT is underway, aligning it with the Directives and Regulations of the European Union in the field of AML/CFT, as well as the standards and recommendations of FATF and MONEYVAL. With this law, VASPs are expected to be defined as obligated entities for implementing AML/CTF measures. Authorities responsible for supervising VASPs in the AML/CTF domain will be appointed, and sanctions for failure to adhere to the specified AML/CTF measures will be outlined. In this way, VASPs will be brought in line with other obligated entities in Bosnia and Herzegovina regarding the obligation to conduct customer due diligence, enhanced due diligence, suspicious transactions reporting and other prescribed measures. However, even after the adoption of this law, this deficiency will not be fully eliminated until FBiH and BDBiH enact their regulations to govern the registration of VASPs. Due to the lack of adequate regulation in FBiH and BDBiH, there is a risk of the emergence of illegal VASPs, which are assessed to pose a very high risk for AML/CFT. This is further confirmed by the recent unauthorized installation of crypto ATMs in the cities of Sarajevo and Tuzla in FBiH, as well as in the Brčko District of Bosnia and Herzegovina. Authorities are taking certain actions to regulate the operation of these crypto ATMs in accordance with the regulations governing AML/CFT. Additionally, numerous advertisements for the purchase/sale of VAs have been identified on at least one platform in FBiH, which facilitates connecting individuals for the purpose of buying, selling, or exchanging consumer goods and services. Through such advertisements, private individuals engage in face-to-face contact and conduct the buying and selling of VAs, which is assessed as a high risk for AML/CFT. To reduce this risk, the Working Group believes that it is necessary to prescribe conditions under which such platforms can publish purchase/sale ads involving VAs, with mandatory implementation of customer and seller identification measures.

10.3. Risk management associated with VA and VASP

In relation to risk management associated with VA and VASP, it is clear that besides domestic ones, clients from Bosnia and Herzegovina can also use the services of foreign VASPs, which, in addition to CEX exchanges, also include the use of DEXs. It can be noted that, concerning domestic VASPs registered in RS, there is a satisfactory legislative and regulatory framework, as well as a supervisory authority responsible for monitoring the compliance of their operations with the laws and other regulations governing anti-money laundering and counter-terrorism financing. Domestic VASPs are required to assess the risk of AML/CFT and complete the process of in-depth analysis, applying a risk-based approach. The measures of customer due diligence should involve client identification and verification of client identity, identification of the beneficial owner and taking reasonable measures to verify their identity, assessment and understanding of the purpose and intention, and nature of the business relationship, as well as conducting ongoing customer due diligence of the business relationship, including monitoring transactions undertaken throughout that relationship. Additionally, domestic VASPs dealing with high-risk clients regarding ML/TF should conduct enhanced customer due diligence, which can also be triggered as a result of larger transactions, suspicious client activities, client names failing verification, for clients from higher-risk areas, when the client is a politically exposed person, or when there is any other risk factor. In addition to the above, they are required to fully cooperate with the authorities responsible for combating money laundering and terrorist financing and report suspicious transactions. Based on the gathered information,

it has been established that registered VASPs have prescribed internal procedures for the application of AML/CFT laws, as well as additional procedures related to identification, monitoring, and risk management concerning internal processes in transactions with VAs and clients. Furthermore, there is a designated person responsible for AML/CFT, and employees undergo mandatory seminars on AML/CFT.

VASP-1 has its own system specifically designed for monitoring, supervising, analyzing, and conducting forensics on all inbound and outbound transactions involving virtual assets (VAs). This system includes monitoring data from global databases concerning money laundering, terrorist financing, criminal activities, sanctions, enabling the creation of risk assessments for each VA transaction. This system also enables detailed analytics, visualization, and forensics for any virtual wallet address, transaction, or entity. Given that VASP-1 is a centralized exchange, all virtual assets as well as fiat currencies of investors on the platform are under their control and can be blocked at any time upon the request of official authorities.

Both domestic VASPs (VASP-1 and VASP-2) that operated during the data collection period (2020-2022), stated in their responses that they fully adhere to these procedures. However, this still needs to be confirmed by the competent supervisory authority (Commission of RS) since there have been no on-site inspections conducted so far.

Because of the particular nature of the VASP business sector, regulations mandate that VASPs must provide service users with information about the risks associated with virtual currency transactions, including the possibility of partial or complete loss of monetary funds or other assets, before initiating any transactions involving virtual currencies, as well as with the fact that regulations governing deposit insurance or the protection of financial service users do not apply to transactions with virtual currencies. VASPs must integrate these and other specified warnings into their internal policies, forming an integral component of the overall regulations governing the VASP. These regulations are accepted by the user upon registration on the electronic platform provided by the VASP. In order to protect clients' funds, as with other obligated entities under the jurisdiction of the RS Securities Commission, the Rulebook on the VASP Registry stipulates that the VASP is required to open a special-purpose account for clients' funds - cryptocurrency users at a business bank. Funds in the special-purpose account can only be used by the VASP for buying and selling virtual currencies and for the purpose of providing services related to virtual currencies. These funds in the special-purpose account are not the property of the VASP, do not become part of its assets, liquidation estate, or bankruptcy estate, nor can they be used to settle claims of VASP's creditors or be subject to forced execution in proceedings against the VASP.

According to the FIU report, cooperation with certain VASPs from RS is at a satisfactory level in terms of reporting suspicious transactions and providing requested documentation. Data related to the number of STRs submitted by domestic VASPs have not been collected because they have not yet been introduced into the electronic system for reporting suspicious transactions (AMLS), but they are submitted through other channels. Nevertheless, this shortfall will be remedied upon the entry into force of the new AML/CFT Law, which designates VASPs as obligated entities responsible for enforcing AML/CFT measures. Concerning the risks linked to foreign VASPs, it has been established that the FIU achieves the highest level of cooperation with foreign financial intelligence units and domestic banks. Foreign financial intelligence units mainly forward suspicious transactions reports received from VASPs registered in their jurisdiction to the domestic FIU, while domestic banks report suspicious transactions related to foreign and domestic VASPs. Banks commonly justify suspicions leading to the submission of suspicious transaction reports by stating that the area is unregulated in Bosnia and Herzegovina. The banks' approach suggests that they typically perceive investments in VAs as high-risk concerning AML/CFT, potentially resulting in undue strain on the FIU due to the influx of numerous low-quality STRs.

The Working Group is of the view that, in order to mitigate the identified risks associated with foreign VASPs providing services in BiH, it would be preferable to legally require them to register their operations in BiH and designate a contact person for cooperation with the relevant domestic authorities for AML/CFT.

11. Key findings and recommendations

11.1. Key findings

- Adoption of VAs in BiH is still at a low level. Compared to the rest of the world, especially Western Europe, the volume of activities associated with VAs is relatively low.
- The majority of recorded transactions (99%) involved exchanging one type of VA for another without conversion to fiat currency, mainly through global centralized or decentralized exchanges.
- There is a widespread perception that the VA/VASP sector is high-risk, but generally, there is limited direct understanding or experience regarding the specific risks of ML and TF in the VA and VASP sector by key stakeholders.
- There is a weakness in the legislative and regulatory framework concerning the VA and VASP sector, primarily at the level of BiH, FBiH, and BDBiH, where there is no legislative or regulatory framework regulating this area.
- The human and material-technical capacities of competent institutions are insufficient for an effective fight against ML/FT associated with VAs and VASPs
- Although there were no registered cases of ML/FT crimes associated with VA and VASP during the period 2020-2022, it has been determined that there is a general and specific exposure to ML/FT risks, where the exposure to money laundering risks is higher than the exposure to terrorism financing risks;
- The average risk of ML in BiH is assessed as high, while the average risk of TF is assessed as medium;
- The most significant predicate offenses for ML/FT associated with VAs and VASPs are identified as follows: Extortion (ransomware); Frauds (pyramid schemes and ICO scams); VA thefts; Unauthorized online trading; and Drug trafficking.
- The percentage of identified transactions associated with crime, ML, or FT, originating from or destined to BiH, is extremely small or negligible.

11.2. Recommendations

- To define a clear approach and ensure the necessary legislative framework for regulating VAs and VASPs at all relevant levels of government in BiH, in accordance with international standards and practices;
- To develop necessary procedures for the seizure, confiscation, and management of VA associated with illegal activities;
- To adopt effective legal texts and mechanisms for sanctioning individuals or entities providing VA services without registration and permit, and to apply deterrent sanctions against them in accordance with relevant laws and regulations;
- To intensify the implementation of measures for continuous monitoring and supervision of domestic VASPs by competent authorities;

- To enhance training and awareness-raising among relevant authorities about the concept of VAs and their ML/FT risks, enabling the identification, monitoring, and investigation of ML/FT operations related to this type of asset.
- To increase material and technical investments in competent institutions to access specialized tools and databases for monitoring the abuse of VAs for ML/FT and forensic intelligence data analysis, i.e., blockchain analysis;
- To improve cooperation with international agencies and organizations to leverage the latest developments regarding VAs and VASPs, including legal, financial, and judicial areas, and exchange information on VAs and VASPs.
- To raise awareness in the private sector about ML/FT risks associated with VAs and VASPs;
- Private sector entities filing STRs should take additional steps to reduce ML/FT risks associated with VA activities by incorporating the results of this assessment into customer risk assessments and various financial products, ensuring that their controls are effective in preventing the misuse of their financial services for ML/FT purposes via VAs, and collaborating with competent authorities to understand and identify risks in a manner that ensures the existence of appropriate controls to mitigate those risks and subject their employees to continuous training.
- Given the evolving nature of virtual assets (VAs) and the technologies associated with them, it is advisable to periodically reassess the remaining risks monitored in each evaluation process.

Conclusion

The misuse of VAs represents one of the contemporary methods through which criminals attempt to launder criminally acquired funds. Although there were no registered ML/FT crimes associated with VAs and VASPs during the period 2020-2022, it has been determined that there is a general and specific exposure to ML/FT risks, where the exposure to money laundering risks is higher than the exposure to terrorism financing risks. The average ML risk in BiH is assessed as high, while the terrorism financing risk is assessed as medium. The individual estimated threat level varies depending on the type of VA or type of VASP. When it comes to VAs, anonymous VAs are assessed as very high risk, while pseudo-anonymous and platform-based VAs are marked as high risk. All other types of VAs are rated as medium or low risk. In the majority of cases related to criminal activities, Bitcoin is used because it is the most accessible and easily exchangeable VA for fiat currency.

This Assessment has determined that in the territory of BiH, five VASPs were registered in 2023 (all in the RS territory), of which two were active during the data collection period (2020-2022). It has also been found that clients from BiH prefer to trade on international exchanges rather than domestic VASPs, primarily due to lower commission fees and a greater variety of VAs available for trading. According to the Global Crypto Adoption Index compiled by Chainalysis, covering 146 countries, BiH ranked 115th overall, or 28th compared to Western European countries. According to some estimates, about 300,000 inhabitants of BiH are or have been exposed to VA, which represents about 7-9% of the population.

When it comes to different types of VASPs or means and methods of VA exchange, the use of anonymization tools such as mixers is assessed as very high risk, while centralized exchanges, DEX applications, and P2P exchanges are rated as high risk. Centralized exchanges received this rating primarily because they are often the entry and exit points for funds targeted for laundering, while DEX and P2P exchanges received this rating due to their anonymity. Other types of VASPs or means and methods of VA exchange are assessed with a medium level of risk.

Additionally, drawing from an external analysis conducted by Chainalysis, a company specializing in blockchain transaction analytics, and considering data on the quantity and volume of VA transactions linked to Bosnia and Herzegovina, along with their ties to criminal endeavors such as money laundering and terrorist financing, the following conclusions emerge:

- There is a significant volume of transactions associated with VAs overall, but it is among the lowest in Europe.
- The majority of transactions (70%) are associated with centralized exchanges.
- The percentage of high-quality suspicious transactions associated with VAs is very small.
- The percentage of identified transactions associated with crime or ML/FT, with their origin or destination being Bosnia and Herzegovina, is extremely small.

In order to implement the recommendations from Chapter 11.2 and measures for the prevention and minimization of ML/FT risks associated with VA and VASP, the Working Group has developed an Action Plan to Combat Money Laundering and Terrorist Financing in Bosnia and Herzegovina associated with Virtual Assets for 2024-2027, which will be submitted to the Council of Ministers of Bosnia and Herzegovina for adoption along with this Assessment.

The Working Group will report to the Council of Ministers of Bosnia and Herzegovina at least once a year on the measures taken to implement this Action Plan.

REASONING

I. LEGAL BASIS

The legal basis for the adoption of this Decision is contained in Article 17 of the Law on the Council of Ministers of Bosnia and Herzegovina, which authorizes the Council of Ministers to enact decisions, conclusions, and resolutions, as well as to endorse drafts and proposals of laws, analyses, information, and other regulatory acts as part of its rights and responsibilities.
The legal basis for the adoption of this Decision is also Article 22, which provides for the establishment of permanent or temporary offices, directorates, services, committees, and other bodies to ensure the complete, effective, high-quality, and coordinated execution of tasks.

II. REASONS FOR ADOPTION

This Assessment results from the obligations of BiH under the FATF recommendations, particularly recommendation number (15), which requires countries to identify, assess and understand the risks of money laundering and terrorist financing associated with VA and the operations of VASPs. Additionally, this Assessment provides a basis for implementing a risk-based approach to ensure that preventive and mitigating measures are proportionate to the identified money laundering and terrorist financing risks. It also aims to inform the competent authorities and institutions on the prioritization, as well as the actions to be taken in order to prevent or mitigate the identified risks of money laundering and terrorist financing related to VA/VASP.

The Action Plan contains a series of measures to mitigate and counteract the identified risks of money laundering and terrorist financing.

The Economic Crime and Cooperation Division (ECCD) of the Council of Europe, during the MONEYVAL plenary meeting in May 2022, expressed readiness to support the process of conducting a Risk Assessment in the virtual asset sector in Bosnia and Herzegovina and to provide guidance on the application of the Council of Europe Methodology for assessing ML and TF risks associated with virtual assets.

To initiate the execution of the aforementioned FATF recommendations, the Council of Ministers of Bosnia and Herzegovina, during its 57th session on November 9, 2022, adopted the Decision on the formation of a Working Group for the development of the Risk Assessment of Money Laundering and Terrorist Financing in Bosnia and Herzegovina associated with virtual assets (Official Gazette of BiH, 1/23). The Working Group was established as a temporary, interdepartmental and expert body of the Council of Ministers of Bosnia and Herzegovina with the task of preparing an assessment of the risk of money laundering and terrorist financing in Bosnia and Herzegovina associated with virtual assets, and an action plan to combat money laundering and terrorist financing in Bosnia and Herzegovina associated with virtual assets.

Taking into account the aforementioned, the Working Group has developed a Risk Assessment of Money Laundering and Terrorist Financing in Bosnia and Herzegovina associated with virtual assets in accordance with the Council of Europe Methodology, and following the Action Plan.

Timely adoption of the Assessment and Action Plan is of great importance for the upcoming visit of MONEYVAL experts, scheduled for February 2024.

Furthermore, in accordance with Article 24, paragraph (1), Rules for Consultations in the drafting of legal regulations (Official Gazette of BiH, 5/17), and recognizing the urgency of the matter, the Working Group proposes an exemption from the obligation to conduct public consultations.

III. FINANCIAL RESOURCES

The implementation of this Decision will not require additional financial resources to be allocated in the Budget of the institutions of Bosnia and Herzegovina.