Summary of

Money Laundering/Terrorist Financing Risk Assessment of Virtual Assets and Virtual Asset Service Providers Report

Hashemite Kingdom of Jordan
February 2023

Table of Contents

Executive Summary **2**

Introduction **4**

Objectives **4**

Methodology **5**

The assessment team **5**

First: Introduction to Virtual Assets **6**

1. The concept of Virtual Assets (VAs) 6
2. Virtual assets Service Providers 6

Second: Virtual assets landscape 8

1. At the level of regulation and legislation 8
2. Interaction between Vas activities and sectors under oversight and supervision 9
3. Interaction with informal sector 9

Third: The Risk Assessment Process **12**

1. Threats 12
2. Vulnerabilities 15
3. Inherent Risks 16
4. Mitigating Measures 17
5. Residual Risks 17
6. Predicate offenses associated with VAs and VASPs 17

Fourth: Key Findings and Recommendations **20**

1. Key Findings 20
2. Recommendations 20

References 22

Executive Summary

Recently, the spread of what is known as virtual currencies or assets has increased, and these assets have become the focus of attention for all users, regulators and decision makers, including the Financial Action Task Force, the global specialized standard-setter for combating money laundering and the financing of terrorism.

Following the recommendations of the Financial Action Task Force (FATF) and its amendments, especially Recommendation No. (15), which requires countries , among many things , to identify, assess and understand the ML/TF risks emerging from activities of virtual assets (VA) and the activities of Virtual Asset Service Providers (VASPs), the report contributes towards meeting these requirements, which was prepared by an assessment team composed of all relevant competent authorities, including the Central Bank of Jordan, the Anti-Money Laundering and Terrorist Financing Unit, and law enforcement agencies such as General Intelligence Department, the Special Branch/ Public Security Directorate, Criminal Investigation Department, and the Public Prosecution.

This report includes determining the prevalence of VAs and VASPs in the Kingdom, citing the global situation of those assets and the data available to the assessment team on the local context, which was used to identify ML/ TF threats associated with VAS and VASPs, and the vulnerabilities that can be exploited by those threats, and then combining these threats and vulnerabilities to determine the level of inherent risk in the activities of VAs and VASPs in the Kingdom.

The assessment team adopted the World Bank's methodology to identify threats and vulnerabilities, calculate the inherent risks, and determine the measures that can mitigate risks associated with VA and VASPs, and then identify the residual risks. Based on this methodology, and where the FATF determined that the ML/TF risks related to the activities of VAs and VASPs must be evaluated, the above methodology was relied upon to determine the activities that should be evaluated, whether those related to VAs or VASPs. The assessment team determined that there is one type of VASPs; the “Virtual Assets Exchange” service provider, which offers four main activities whose inherent risk levels are as follows:

VASP Type	Types of Services	Threat Rating	Vulnerabilities	Inherent risks
Virtual Assets Exchange	Peer-to-Peer	High	High	High
	Fiat-to-VA	High	High	High
	Virtual-to-Fiat	High	High	High
	Virtual-to-Virtual	High	High	High

The risk assessment that was conducted showed there is a clear weakness in the applied controls and mitigation measures, and in light of this weakness, the residual risks associated with VAs and VASPs are still high, as the overall level of risks associated with VAs and VASPs are as follows:

VASP Type	Types of Services	Inherent risks	Adequacy of mitigation measures	Residual risks
Virtual Assets Exchange	Peer-to-Peer	High	Very Low	High
	Fiat-to-VA	High	Very Low	High
	Virtual-to-Fiat	High	Very Low	High
	Virtual-to-Virtual	High	Very Low	High

Finally, some measures were recommended to the competent authorities in the Kingdom that could be taken into account to mitigate ML/TF risks related VAs and VASPs. These recommendations include defining a clear approach at the national level in terms of allowing or prohibiting dealing with VAs, providing the necessary legislative environment for that in accordance with international standards and practices, and the need to enhance and develop the capacities of the regulatory authorities and provide them with the necessary knowledge and experience related to the activities of VAs, by subjecting them to continuous and appropriate training related to the activities of VAs and VASPs, in order to enable them to track, monitor and investigate ML/TF operations related to these assets.

According to the evolving nature of VAs and the technologies that rely on them, the assessment team recommends the need to agree on an appropriate periodicity for re-assessment and in proportion to the size of the remaining risks that were monitored in each assessment process.

Introduction

Recently, there is much talk about the so-called Digital Currencies in all its forms and types, specifically Virtual Assets (VAs), particularly after those assets achieved exceptional records in an unnatural pattern within their trading and prices. At the end of 2017, the massive rise in the price of Bitcoin -one of the most famous of these assets– attracted the attention of the public and the media to the VAs. This currency, which was developed after the global financial crisis in 2008, is the oldest crypto VAs that can bypass the traditional banking system by relying on a completely anonymous, decentralized and therefore unregulated model that is processed over the internet without the need for a financial intermediary between transaction parties.

This lack of supervisin and the anonymity of the transaction parties led the regulatory authorities to research, understand and address potential money laundering (ML) and terrorist financing (TF) risks associated with them. Among these international bodies is the Financial Action Task Force (FATF), the authority concerned with setting global standards for combating money laundering and terrorist financing (AML/CFT). In October 2018, FATF adopted updates to its Recommendations to explicitly state that they apply to financial activities involving VAs; the FATF adopted two new Glossary definitions—"virtual asset" (VA) and "virtual asset service provider" (VASP). The amended Recommendation (15) requires that VASPs be regulated for the purposes of (AML/CFT), licensing or registering them, and subject them to effective systems for AML/CFT supervision or monitoring.

Objectives

This risk assessment stems from the Kingdom's commitments to the FATF Recommendations, specifically Recommendation No. (15), which requires countries to identify, assess and understand ML/TF risks emerging from the activities of VAs and VASPs. Subsequently, this risk assessment provides the basis for implementing a risk-based approach to ensure that the preventive and mitigating measures are commensurate with the ML/TF risks identified. It also aims to inform authorities on the prioritization and allocation of resources as well as actions to be taken at national and sectoral levels to prevent or mitigate the ML/TF risks identified, enhance the understanding of relevant authorities on ML/TF risks associated with VA/VASPs, and Inform the ML/TF risk assessment of regulated entities and their risk management approaches.

Methodology

The Kingdom relied on the World Bank's methodology to identify and assess ML / TF risks arising from the activities of VAs and VASPs in the Kingdom, beside the methodology of the International Monetary Fund, and the experiences of other countries in the same context. The methodology included evaluates the ML/TF threats and vulnerabilities of VA and VASPs activities in the Kingdom for the purpose of calculating the inherent risks in these activities, and determining the mitigating measures applied to reach the level of residual risks rating after taking mitigating measures into account. As a last step, recommendations were formulated to propose additional mitigating measures to be implemented at national levels.

In order to complete this assessment, the assessment team participated in several training workshops with the Global Facility for Money Laundering and Terrorist Financing (EU AML/CFT Global Facility), including a workshop that was held in the period (23-24/10/2022) in addition to a regional conference (13-15/12/2022), during this conference, the team was able to learn about the experiences of many countries to benefit from them, and several meetings were held with representatives of the private sector and companies specialized in analyzing data related to VAs, also, the team obtained technical assistance from the legal department of the International Monetary Fund, , and the assessment team relied on a wide range of quantitative and qualitative data for the purposes of implementing the evaluation process. These sources included reporting entities, entities subject to regulation and oversight such as financial institutions, the Ministry of Justice, Criminal Investigation Department, and Anti-Cyber Crimes Unit, Telecommunications Regulatory Commission, Securities Commission, Anti-Money Laundering and Terrorism Financing Unit, published statistics and reports, and information collected through publicly published survey questionnaires.

The assessment team

For the purposes of conducting ML/TF assessment for risks associated with VAs and VASPs, in a manner that meets the requirements of Recommendation (15), and in line with the methodology of the World Bank and the International Monetary Fund, a working group has been formed consisting of representatives of all relevant regulatory and competent authorities, including representatives from the Central Bank of Jordan (CBJ), and representatives from the Anti-Money Laundering and Terrorist Financing Unit, also, representatives of the Telecommunications

Regulatory Commission, the Securities Commission, the Anti-Cybercrime Unit, Criminal Investigation, General Intelligence Department, Preventive Security and the Ministry of Justice / Public Prosecution participated in the evaluation process.

First: Introduction to Virtual Assets

The global monetary system has witnessed radical developments in the past years, the most prominent of which is related to the emergence of crypto VAs, for the purposes of completing this assessment, it is necessary to define what is meant by each of the VAs and VASPs.

1. The concept of Virtual Assets (VAs)

According to the FATF, a VAs 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 that are already covered elsewhere in the FATF Recommendations [1]".

2. Virtual assets Service Providers

FATF defined VASP as "any natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conducts one or more of the following activities 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

Based on the World Bank's methodology, VASPs can be classified according to the activities they engage in as follows:

[1] Financial Action Task Force (2021), "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems", Page.189.

A. Virtual Asset Wallet Providers

Virtual Asset Wallet Providers provide storage for virtual assets or fiat currency on behalf of others. They then facilitate exchanges or transfers between virtual assets and fiat currency. They include a Custodian Wallet, and Non-Custodian Wallet.

B. Virtual Asset Exchanges

Virtual asset exchanges provide a digital online platform facilitating virtual asset transfers and exchanges. Exchanges may occur between one or more forms of virtual assets or between virtual assets and fiat currency. Exchanges can be, for example, online platform-based exchanges or in-person, such as trading platforms that facilitate peer-to-peer exchanges or kiosk-based exchanges.

C. Virtual Asset Broking

VA brokerage services facilitate the following:

- The issuance and trading of VAs on behalf of a natural or legal person's customers
- Order-book exchange services, which bring together orders for buyers and sellers, typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users
- Advanced trading services that allow users to buy portfolios of VAs and access more sophisticated trading techniques, such as trading on margin or algorithm-based trading

D. Virtual Asset Management Providers

An investment fund that focuses on cryptocurrencies as the underlying assets typically involve Fund management, fund distribution; and compliance, audit, and risk management.

E. Initial Coin Offering (ICO) Providers

ICOs typically involve issuing and selling virtual assets to the public. They might involve participating in and providing financial services relating to the ICO.

F. Virtual Asset Investment Providers

They provide an investment vehicle that enables investment in or purchase of virtual assets (that is, via a managed investment scheme or a derivatives issuer providing virtual asset options, or via a private equity vehicle that invests in virtual assets).

Second: Virtual assets landscape

VAs have grown significantly in recent years, since the emergence of Bitcoin in 2008, which is considered one of the most famous and largest VA in terms of market share, the number of VAs has increased to exceed the limits of 22 thousand currencies, and the virtual assets market has witnessed quantum leaps in terms of the rise in the price of assets or a sudden decline as a result of the collapse of one of those assets or platforms through which it is traded, as the case in Luna currency or even in the FTX platform and others.

1. At the level of regulation and legislation

The Central Bank of Jordan reacted towards VAs since 2014, when CBJ issued its first circular, according to which it prohibited banks and all other financial institutions subject to its oversight and supervision to deal with VAs in any way, exchange them for another currency, or open accounts for customers to deal with them, or sending or receiving transfers in return for them, or for the purpose of buying or selling them; being not a legal currency and there is no obligation on any central bank to exchange their value for money issued by governments or for global traded commodities such as gold.

In 2018, CBJ issued its second circular to all banks and other financial institutions under its oversight and supervision, through this circular, CBJ stressed the continuation of the ban on dealing with VAs, including all types of VAs. CBJ also confirmed its aforementioned circulars in its circular issued on 24/11/2019, which was due to the spread of the phenomenon of promoting a cryptocurrency known as (Dag Coin). In addition, a circular was issued at the end of 2021 confirming the continued validity of the ban on all entities under its oversight and supervision to include all forms and activities of VAs in the Kingdom and as stated in the FATF Recommendations.

CBJ also issued the Guideline "Work procedures, regulatory controls, and warning indicators for monitoring and preventing dealing in virtual currencies using electronic payment instruments and channels", which is directed to banks and electronic payment and money transfer companies, with the aim of enabling banks and companies to rely on it when reviewing their internal policies, work procedures, and regulatory controls, in a manner that achieves compliance with the CBJ's circulars related to the prohibition of dealing in VAs, and to prevent any risks related to ML/TF, or fraud related to dealing with VAs, in addition to contributing to improving their level of understanding and awareness in this regard.

On the other hand, the Telecommunications Regulatory Commission, and the Securities Commission issued circulars to the entities subject to their supervision prohibiting them from dealing in these assets, also in accordance with the Anti-Money Laundering and Terrorist Financing Law No. (20) of 2021, VAs were included in the definition of Fund.

2. Interaction between Vas activities and sectors under oversight and supervision

A form was prepared and sent to all entities that provide payment and transfer services activities, with the aim of collecting data about the transactions that were observed by those entities, as those entities provided the team with the financial transactions for the period (1/2019- 6/2022), which was found to the team after analyzing data the presence of growth in the volume and value of the transactions that were monitored.

3. Interaction with informal sector

The activity of trading VAs is considered one of the activities that are not clearly regulated, and despite the CBJ's ban on banks and financial institutions to facilitate their clients' access to these assets' platforms, citizens are still able to exchange these assets either directly (Peer to Peer), or through the platforms using accounts they hold in foreign financial institutions.

A. Statistical data from published reports

Among the data that was referred to, a report was issued by Chainalysis[2] Company. According to the general index[3], Jordan ranked number 68 overall on the index, 60 overall in terms of

---

[2] Chainalysis is the blockchain data platform that specializes in providing data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries. Its data powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely

3) Global Crypto Adoption Index is made up of five sub-indexes, each of which is based on countries' usage of different types of cryptocurrency services. We rank all 146 countries for which we have sufficient data according to each of those five metrics, take the geometric mean of each country's ranking in all five, and then normalize that final

Centralized Exchange activity, 68 overall in terms of P2P Exchange activity, and 88 overall in terms of Decentralized Exchange (DeFi) activity.

In terms of activities, Jordan's largest category of activity was Centralized exchange, which received 82.8% of all activities between 2021-09 and 2022-09, the second largest category in Jordan was DeFi, which received 15.7%, for the P2P marketplaces, total value received by in Jordan reached $5.33 million, making it the number 14 largest P2P market in the region.

In Jordan, the top platform used in terms of web traffic is the exchange named (Binance.com) and received 1.97 million visits between 09-01-2021 and 09-01-2022. The second largest platform was the exchange named (FTX.com) which received 0.81 visits in the same time period.

In terms of illegal activities, the report indicated that in MENA, Chainalysis identified $954.8 million worth of illicit activities, which represents approximately 0.3% of the total value received. This was lower than the global average share of illicit exposure, which was 0.33%.

The illicit activity identified in Jordan has varied over the past 12-months. The largest source of illicit activity came from the SCAM category, which received $5.64 million worth of cryptocurrency over the past 12-months. The fastest growing crime category was stolen funds, which grew 0.2% from the previous 12-months, reaching $1.89 million in total value received by stolen funds.

B. Statistical data from a publicly available survey questionnaire

With the aim of exploring the spread and use of VAs in the Kingdom; the assessment team prepared a questionnaire and published it to the public through social media and in some local universities, in order to collect correct and transparent data. This questionnaire contained (18) questions, consisting of a set of questions about the demographic information of the questionnaire fillers, and the other section targeted the person’s knowledge of these assets, his possession of them, and the justifications for having them or not having them, and an indication of whether he was exposed any risks while trading these assets.

number on a scale of 0 to 1 to give every country a score that determines the overall rankings. The closer the country’s final score is to 1, the higher the rank.

(1700) people responded to the prepared questionnaire, the age group (31-45) ranked first in the sample that filled out the questionnaire with a percentage of 36%, the largest category that responded to the questionnaire was from Jordanian residents, at a rate of 90%, and the vast majority was concentrated in the capital, Amman, at a rate of 68%, the number of those who heard about VAs reached the percentage 84% of the sample, a 35% indicated that they heard about it through a friend or family, 74% indicated that they do not own any VAs currently, while those who currently own VAs amounted to 9%, and those who owned VAs but currently do not own any of them, their percentage reached 3%.

In addition, a question was asked about the method in which the assets currently owned or owned in the past by those who responded to this survey were obtained, the percentage of those who obtained these assets through trading platforms was 70% out of (172) people, while 22% stated that they obtained these assets directly from other people.

As for the category of who do not own any VAs, which is (1261) people, they were asked about the reasons for not owning these assets, where (590) people stated that the reason is that they do not have sufficient information about them, and (411) people indicated that the reason is that they are high risks, also, among the questions asked during the survey, "what are the risks associated with VAs/ cryptocurrencies?" 31% of the sample identified that their fluctuating price is the greatest risk, the survey investigated the extent to which the sample was exposed to fraud through VAs, 96% determined that they had not been exposed to any fraud related to these assets, 4% of the sample (69 people) determined that they had been exposed to fraud through these assets.

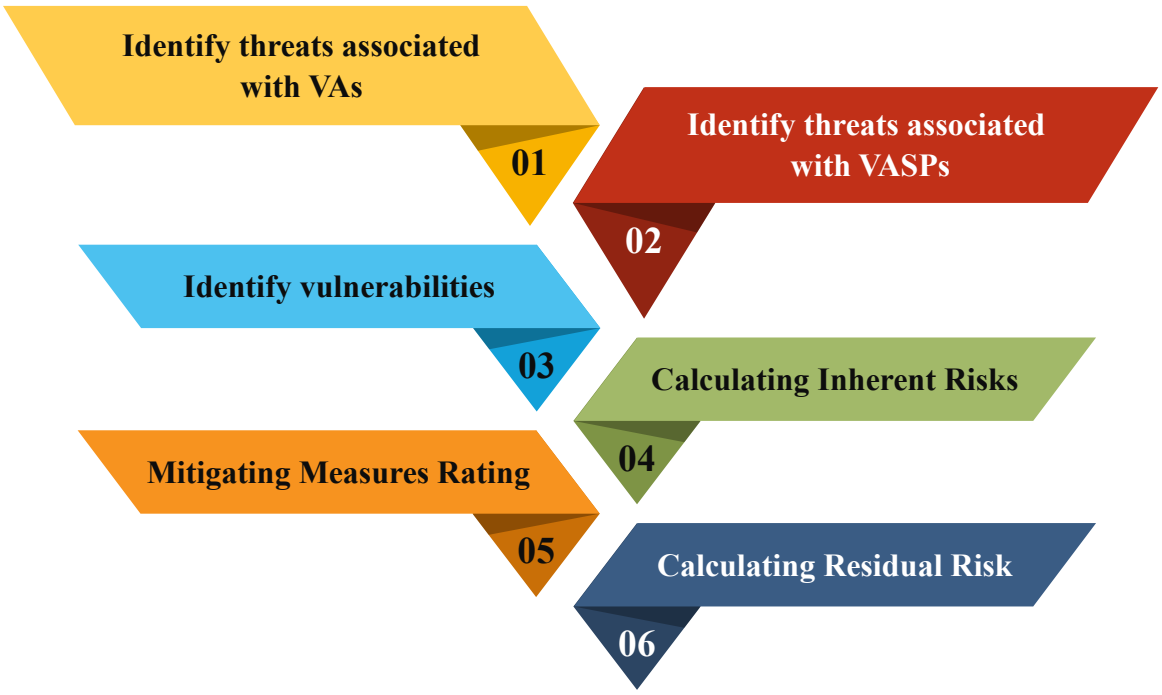
C. Open data sources such as the Internet and social media

By following up on virtual asset groups in Jordan through social media, the data published on the Internet and social media applications showed that there are buying and selling of VAs through a number of people, where the prices of these currencies are paid in fiat currency, and these people most of the time sell or buy the so-called currency (USDT) or Bitcoin and transfer it to one of the famous trading platforms to be converted into other VAs, through A personal interview between individuals, and paying for these assets using cash, or through electronic wallets, or by transferring through certain banks or through the CliQ system, Websites such as (BITCOIN-ATM) showed that there are no ATMs for virtual assets in Jordan.

Third: The Risk Assessment Process

In assessing risks, the assessment team relied on identifying threats and vulnerabilities for both virtual assets and virtual asset service providers, using an approach based on information collected from several sources previously referred to, in addition to the equations included in the assessment tool prepared by the World Bank, This assessment takes into account the input variables, which represent a set of characteristics and attributes through which threats and vulnerabilities in the activities of VAs and VASPs can be identified primarily from a local perspective, as well as on an international perspective, through the characteristics inherent in VAs that make it global, across borders, and without any restrictions.

The risk assessment process included a set of steps that can be described as follows:



1. Threats

Threats are defined as "The collection of illegally acquired assets that need to be laundered (in relation to money laundering) and the sum of funds collected for the purposes of committing terrorist acts (in relation to terrorist financing)". The threat assessment aims to determine the nature of predicate crimes and assess the exposure of VAs and VASPs to these predicate crimes, in

addition to determining the extent to which VAs and VASPs are exposed to threats related to fundraising for terrorist financing purposes.

A. VAs Threat Assessment

VAs threats were assessed according to Input Variables, which show the inherent risks before implementing any controls or mitigating measures, as shown in the tables below.

Intermediary variables	Input variables	Threat
VA Nature and Profile	Anonymity/pseudonymity	High Risk
	P2P Cross-Border Transfer and Portability	High Risk
	Absence of face-to-face contact	High Risk
	Traceability	Medium Risk
	Speed of Transfer	High Risk
Accessibility to Criminal	Mining by criminal	Low Risk
	Collection of funds	Low Risk
	Transfer of funds	High Risk
	Dark Web Access	High Risk
	Expenditure of funds	Low Risk
Source of funding VA	Bank or card as source of funding VA	Low Risk
	Cash transfers, valuable in-kind goods	High Risk
	Use of virtual currency	High Risk
Operational features of VA	Regulated	Does not exist
	Unregulated	High Risk
	Centralised Environment	High Risk
	Decentralised Environments	High Risk
Ease of criminality	Tax evasion	Very Low Risk
	Terrorist financing	Medium Risk
	Disguising criminal proceeds to VA not regulated	Low Risk
	Trace and Seize Difficulty	High Risk
Economic Impact	Underground economy – Impact on the country's monetary policy	Low Risk

Most of the VAs threats were assessed at a (high-risk) level, based mainly on the inherent feature of Vas, their nature, and characteristics in general. However, the rest of the other threats were evaluated at a (risk) and (low risk) level for a number of considerations and justifications, perhaps

the most prominent of which is not monitoring this threat on a large scale in the Kingdom, or monitoring cases of using VAs in some of the activities under assessment.

B. VAPSs Threat Assessment

Based on the methodology of the World Bank, it was determined that there is one prominent type of VASPs in the Kingdom; That is, Virtual Assets Exchange, depending on the definition of this type of VASP and the activities it provide.

Accordingly, the threats associated with all services and activities of the Virtual Assets Exchange service provider, namely P2P, Fiat-to-Virtual, Virtual-to-Fiat, Virtual-to-Virtual, were assessed, after intersecting with the input variables that were used in the assessment of VAs as aforementioned, so that its becomes as shown in the table below:

VASP Type	Types of Services	Threat Rating	Vulnerabilities	Inherent Risks
Virtual Assets Exchange	Peer-to-Peer	High	High	High
	Fiat-to-VA	High	High	High
	Virtual-to-Fiat	High	High	High
	Virtual-to-Virtual	High	High	High

It is clear from the above table that the ML/TF threats assessment for the VASP "Virtual Asset Exchanges" came with a (**High Risk**) level for all types of service provided, for several considerations, the most prominent of which are:

- That this sector is not licensed in Jordan, and is practiced mostly by natural persons; therefore, it is not possible to know the extent of the effectiveness of the regulatory controls that are applied by the service provider on the users of VAs, and that the services that are provided may be related to VASPs that are not licensed or registered, or VASPs that are located in countries that do not apply adequate measures to combat ML/TF, in addition to the lack of adequate regulatory controls from the competent authorities to reduce the risks of this sector.
- The possibility of conducting exchanges without revealing the identity of the user, as the most common VAs and stablecoins used by Jordanians are (USDT, BITCOIN, Ethereum), and these currencies have the advantage of (anonymity of the user) to a large extent, as was previously explained.
- Its global spread, as the activities of VASPs help criminals to commit money laundering and terrorist financing crimes across borders and without the presence of intermediaries.

2. Vulnerabilities

Vulnerabilities are defined as "gaps in AML/CFT systems or controls that are exploited from threats to carry out money laundering and terrorist financing operations in sectors and institutions." vulnerabilities may also include specifications or characteristics of a specific sector, financial product, or type of service that makes it attractive for purposes ML and TF.

Virtual asset vulnerabilities were evaluated for one type of VASP, which is Virtual Assets Exchange, with all the services and activities it provides, based on the variables below (Input Variables), which show the inherent risks of vulnerabilities before implementing any regulatory controls or mitigating measures as shown in the table below:

Intermediary variables	Input variables	Assets Exchange Virtual
Products & services provided ,and the types of VA	Nature, size and complexity of business	High Risk
	Products/services	High Risk
	Methods of delivery of products/services	High Risk
	Customer types	High Risk
	Country risk	High Risk
	VA (Anonymity/pseudonymity)	High Risk
	Rapid transaction settlement	High Risk
	Dealing with unregistered VASP from overseas	Very High Risk

Where the vulnerabilities of the above variables were assessed as ranging from high risks to significantly high risks, as several reasons and justifications contributed to this, most notably the following:

1) The lack of a regulatory framework in the Kingdom to deal with Vas, and the absence of licensed VASPs, which prompts those dealing with VAs to deal with VASPs in various countries, especially high-risk countries or countries on international sanctions lists or that do not have effective controls in combating ML and TF.
2) The rapid transfer of value via the Internet and the absence of a ceiling limit for the transactions.

3) The anonymity feature available in virtual assets makes it difficult for law enforcement and competent authorities to easily trace transactions.
4) Lack of sufficient information about the type of customer (Sender/beneficiary) and whether any of them belongs to the high-risk customer categories.

Accordingly, the assessment of the vulnerabilities of the VASP, after its intersection with the input variables according to each activity, becomes as shown in the table below:

VASP Type	Types of Services	Vulnerabilities Rating
Virtual Assets Exchange	Peer-to-Peer	High
	Fiat-to-VA	High
	Virtual-to-Fiat	High
	Virtual-to-Virtual	High

The overall vulnerability assessment of the Virtual Asset Exchange service provider becomes (High Risk).

3. Inherent Risks

The inherent risks in the activities of VAs and VASPs are represented by multiplying the total sum of ML/TF threat and the level of vulnerability inherent in ML/TF for each activity, which results in an overall classification of the risk level before the application of mitigation measures, which can be represented with the following equation:

After identifying the threats and vulnerabilities in the activities of the VASPs that were identified, it becomes clear to us that the level of inherent risks in this sector is **high** and can be detailed as follows:

VASP Type	Types of Services	Threat Rating	vulnerabilities	inherent risks
Virtual Assets Exchange	Peer-to-Peer	High	High	High
	Fiat-to-VA	High	High	High
	Virtual-to-Fiat	High	High	High
	Virtual-to-Virtual	High	High	High

4. Mitigating Measures

Within the procedures for assessing the risks associated with the activities of VAs and VASPs; the effectiveness and efficiency of the mitigating measures applied to combat these risks was measured, as the level of these controls was very low; due to the lack of legislative frameworks and tools to limit the exploitation of identified threats to the weaknesses in this sector.

The general weakness in the mitigating measures applied in the Kingdom can be explained by the following reasons:

1) The absence of a specific authority responsible for identifying and penalizing individuals who engage in VAs activity without a license or registration in light of the absence of a regulatory legal framework, as well as the absence of penalties for entities (legal persons) that are not subject to the supervision of CBJ, the Telecommunications Regulatory Commission, and the Securities Commission.
2) Weak legislative framework; the ban was not sufficient to mitigate the risks, being partial, and the authorities do not have sufficient tools, procedures and expertise to seize and confiscate the criminal proceeds of VAs.

5. Residual Risks

Residual risks are the risks calculated after applying the mitigating controls and measures. In this assessment and due to the extreme weakness in the applied mitigation measures, the residual risks are still high for the activities of VAs in the Kingdom, which can be summarized in the following table:

VASP Type	Types of Services	inherent risks	Adequacy of mitigation measures	Residual risks
Virtual Assets Exchange	Peer-to-Peer	High	Very Low	High
	Fiat-to-VA	High	Very Low	High
	Virtual-to-Fiat	High	Very Low	High
	Virtual-to-Virtual	High	Very Low	High

6. Predicate offenses associated with VAs and VASPs

According to the results of the National Risk Assessment (NRA) ML/TF, crimes (fraud, theft, tax evasion, drug trafficking and corruption) were classified among the highest predicate crimes in

terms of the value of criminal proceeds. In the context of assessing VAs risks, "fraud crime" was considered as the most important threat to VAs in the Kingdom.

A. Fraud

The significant increase in the value of Bitcoin from (10,600-67,000) US dollars during the period from 7/2019 to 10/2021, with the advantage of concealing the identity of dealers in virtual assets, contributed to the emergence of fraud crimes through criminals making false promises to investors with VAs and deceiving them.

The Anti-Money Laundering and Terrorist Financing Unit received, during the period from (2019-6/2022), (34) suspicious reports related to VAs, and the unit dealt with (16) report sent from various reporting parties (banks, exchange companies, electronic payment companies) on suspicion fraud through VAs at a rate of (47%) of the total number of reports. As for the remaining percentage, it should be noted that it related to trading in VAs without being linked to a predicate crime. There are also (11) cases with law enforcement agencies and one case with the judiciary all of them are fraudulent.

Case: Fraud

The Anti-Money Laundering and Terrorist Financing Unit received a number of reports stating that the suspects had received frequent money transfers in high amounts from the e-wallets of some people who wish to invest in digital currencies for the purpose of making profits. After receiving the transfers to the suspects' e-wallets, they made cash withdrawals in a short time.
The unit found that the nature of the financial transactions that took place on the suspects' accounts was inconsistent with the nature of their activity specified by the reporting authorities, as some of them are university students and others do not work.

Through analysis and investigation by the unit, it was found that the suspects are registered on Facebook pages that promote trading in digital currencies, and one of those pages works in the field of hierarchical marketing for selling and investing in the “DAGCOIN” currency and marketing it in Jordan and the Arab countries. Through research, it was found that the suspects are in a relationship with each other and they communicate with the visitors of the page for the purposes of selling (Dagcoin) currencies.

These notifications coincided with negative news published on the Internet and incoming complaints received by the Jordanian Public Security Directorate regarding fraud in digital currencies, and among the accused were the same suspects mentioned in the reports, as the unit found that the suspects follow a pattern similar to (Ponzi Scheme) in defrauding people, and based on the findings, the unit referred the case to the Public Security Directorate on suspicion of fraud.

B. Theft

Theft of VAs does not constitute a real threat since no cases in this regard have been registered with the competent authorities. However, the chainalysis's report considers the crime of stolen funds as the fastest growing crime (despite the low threat), as it increased by 20% for the year 2022 compared to the year 2021. The total value of stolen funds through virtual assets amounted to (1.89) million US dollars, although its percentage remains low compared to the value of trading, so it may pose a future risk.

C. Tax evasion

No cases related to tax evasion using virtual assets were detected in Jordan at the time of the assessment, and in light of this, the assessment team indicates that this crime constitutes a (very low) threat regarding the use of VAs for the purposes of tax evasion.

D. Terrorism financing

No cases related to the use of VAs for TF purposes were detected in Jordan at the time of conducting the assessment, and accordingly this crime was assessed as a low threat as previously mentioned.

It should also be noted that the assessment team did not find any evidence of the use of VAs for the purposes of drug trafficking and corruption in the Kingdom (which were identified as high-risk crimes in the national risk assessment), and therefore these crimes do not constitute a threat regarding the laundering of their proceeds through VAs.

Fourth: Key Findings and Recommendations

1. Key Findings

- This assessment represents the first assessment of ML/TF risks associated with VAs and VASPs activities. During this assessment, it was found that the general exposure to ML/TF risks associated with VAs and VASPs in the Kingdom is high risk. The exposure to money laundering risks is greater than the exposure to terrorist financing risks.
- There is a significant weakness in the system of legislation regulating combating ML/TF with regard to VAs. Where the Kingdom has not yet determined its position at the national level regarding VAs, but this was limited to circulars issued by some regulatory agencies such as e Central Bank of Jordan, the Telecommunications Regulatory Commission, and the Securities Commission.
- The activity of exchanging VAs is the most prominent activity in the Kingdom, through exchanging these assets with fait currencies or between them, and transferring them directly between users, and accordingly the risk assessment focused the "Virtual Assets Exchanges" service providers.
- Despite the existence of circulars that prohibit banks and all other financial institutions from dealing with VAs in any way, or exchanging them for another currency, opening accounts for customers to deal with them, or sending or receiving transfers against them, or for the purpose of buying or selling them; However, a significant number of transactions were monitored by banks and financial institutions, and they took the necessary measures in this regard.
- Due to the ban imposed on banks and financial institutions, the activity of VAs and VASPs is concentrated in the informal sector through direct buying and selling between people. This makes the process of controlling and monitoring the activities of VAs very difficult, most of this activity takes place through centralized platforms, and one of the most prominent of these platforms is (FTX), which has recently collapsed.

2. Recommendations

In light of the detected threats and vulnerabilities, and the absence of effective mitigation measures, the assessment team recommends some measures that can be considered to mitigate these risks by the competent authorities in the Kingdom and parties related to the activities Vas and VASPs, most notably the following:

- Defining a clear approach at the level of the Kingdom in terms of allowing or prohibiting dealing with VAs and providing the necessary legislative environment for this in accordance with international standards and practices.
- Developing the necessary procedures for seizing, confiscating and managing VAs associated with illicit activities.
- Adopt effective legislative texts and mechanisms to prosecute natural or legal persons who provide VAs services without a license and apply deterrent penalties against them in accordance with relevant laws and regulations.
- Enhancing cooperation with international agencies and organizations to benefit from the latest developments related to dealing with VAs, including in the legal, financial and judicial fields, and exchanging information VAs.
- Enhancing training and raising awareness among the competent authorities, regulatory and supervisory authorities, and law enforcement agencies of the concept of VAs and their risks, in a way that enables them to track, monitor, and investigate ML/TF operations related to these assets.
- Enhancing awareness among the private sector of the risks of ML/TF associated with VAs and VASPs.
- Reporting entities in the private sector should take additional steps to reduce the risks of ML/TF associated with the activities of VAs by including the outputs of this assessment in assessing the risks of customers and various financial products, and ensuring that their controls are effective in preventing the misuse of their financial services for the purposes of ML/TF through VAs, and cooperate with the competent authorities to understand and identify the risks in a way that ensures the existence of adequate controls to mitigate these risks and subject their related employees to continuous training.
- According to the evolving nature of VAs and the technologies that depend on them, it is necessary to agree on an appropriate periodicity for re-evaluation and in proportion to the size of the residual risks that were monitored in each evaluation process.

References

1) CBINSIGHTS (2019), "What Are Stablecoins?" , Available at: https://www.cbinsights.com/research/report/what-are-stablecoins/
2) Chainalysis (2022), "Chainalysis Country Analysis Report on Jordan".
3) Chainalysis (2022), "The 2022 Crypto Crime Report", Available at: https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf
4) Coincodex (2019), "Stable Coins", available at: https://coincodex.com/stablecoins/
5) Gov.UK (2019), Policy Paper on Cryptoassets for individuals, December 2018, Retrieved from: https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals
6) International Monetary Fund (2016), Virtual Currencies and Beyond: Initial Considerations, Retrieved from: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.
7) Natarajan, H., Krause, S., Gradstein, K., and Luskin, H., (2017), "Distributed Ledger Technology (DLT) and blockchain", World Bank Group FinTech note (1), Available at: https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
8) Mauritius (2022), "Money Laundering/Terrorist Financing Risk Assessment of Virtual Assets and Virtual Asset Service Providers", Available at: https://www.mra.mu/download/PublicReport2022.pdf
9) Republic of Seychelles (2022), "ML/TF Overall National Risk Assessment for VA & VASPS", Retrieved from: https://www.cbs.sc/Downloads/publications/aml/Report%20Seychelles%20ONRA%20ML-TF%20of%20VA%20and%20VASP%20-%2026.08.2022.pdf
10) Financial Action Task Force (2021), "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems", Retrieved from: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html
11) The Financial Action Task Force (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", Retrieved from: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
12) World Bank Group (2022), "Guidance Manual Virtual Assets And Virtual Asset Service Providers ML/ TF Risk Assessment Tool", Retrieved from: https://openknowledge.worldbank.org/handle/10986/37761

"END"