UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

EAG Eurasian group on combating money laundering and financing of terrorism

Countering the Misuse of Virtual Assets & Virtual Asset Service Providers for Terrorism Financing Purposes

Handbook Based on EAG Practices

Disclaimer

The opinions, findings, conclusions, and recommendations expressed herein do not necessarily reflect the views of the United Nations or any other national, regional, or international entities involved. This report is not intended to serve as a guidance document but instead take stock of current practices in place across the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) Member States when it comes to countering the misuse of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) for terrorism financing (TF) purposes. The designations employed and material presented in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area of its authorities, or concerning the delimitation of its frontiers or boundaries. The contents of this publication may be quoted or reproduced, provided that the source of information is properly acknowledged. The United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) requests to receive a copy of any document in which this publication is used or quoted. As modern technology evolves rapidly, more comprehensive systems aimed at preventing the misuse of VAs and VASPs for criminal purposes become available, international anti-money laundering, countering of the financing of terrorism and, countering proliferation financing (AML/CFT/CPF) standards are updated, and EAG countries continue to improve their legal frameworks. As such, the practices described herein are to be perceived as relevant at the time of writing. The practices described in the report are non-binding and do not override the purview of national authorities nor the Financial Action Task Force (FATF) guidance. This publication is intended to complement other ongoing work by building upon available research, including relevant FATF typologies reports, and the experiences of countries. It also accounts for the work being undertaken by other international bodies focused on addressing the risk of misuse of VAs and VASPs for TF purposes.

Acknowledgements

This report is the product of a joint initiative of UNOCT/UNCCT, the Federal Financial Monitoring Service of the Russian Federation (Rosfinmonitoring), and EAG. It has been made possible with the financial support from the Russian Federation. It is to be noted that the UNCCT Global Programme on Detecting, Preventing and Countering the Financing of Terrorism (CFT Programme) is also generously funded by the Kingdom of Saudi Arabia and the Republic of India.

---

uncct@un.org

@un_oct | #uncct

www.un.org/uncct

Contents

Foreword

The emergence of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) has brought significant positive changes to our world, driving innovation, enhancing efficiency, and promoting financial inclusion. However, certain characteristics of VAs also make them attractive to criminals, especially with the development of sophisticated digital tools such as mixers, tumblers, and anonymizers, which are designed to obscure transactional links to the original currency owners.

Criminal actors are increasingly exploiting the anonymity, speed, and borderless nature of VAs and VASPs to achieve their objectives. Although the number of proven cases of terrorists using these digital tools remains relatively low, evidence suggests that this number is steadily increasing.

Facing varying levels of risk posed by the exploitation of VAs and VASPs by terrorist entities, the nine Member States of the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) have made considerable and commendable progress in integrating digital financial technologies into their domestic systems, demonstrating a strong commitment to enhance their financial systems while ensuring compliance with relevant international standards.

The Financial Action Task Force (FATF) and the United Nations (UN) have established critical frameworks aimed at mitigating the risks associated with the use of VAs and VASPs for criminal and terrorist financing purposes. FATF Recommendation 15 provides a blueprint for implementing a risk-based approach to either prohibiting or regulating virtual assets, emphasizing the need to identify, assess, and manage specific risks in this domain. In its resolution 2462 (2019), the United Nations Security Council called upon Member States to enhance the traceability and transparency of financial transactions by assessing and addressing potential risks associated with virtual assets[1].

In 2023, to support the implementation of these frameworks, the United Nations Counter-Terrorism Center (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) partnered with the EAG Secretariat and the Federal Service for Financial Monitoring of the Russian Federation (Rosfinmonitoring). This collaboration aimed at conducting research to identify effective practices established by EAG Member States, using a consultative approach involving regional practitioners.

This report highlights the considerable achievements of EAG Member States in advancing laws, regulations, and effective practices designed to combat the financing of terrorism through virtual assets. It also acknowledges the challenges that remain, particularly as the rapid adoption of these technologies, coupled with varying levels of regulatory maturity and enforcement capabilities, has created an environment where gaps can still be exploited to fund terrorist activities.

Safeguarding the integrity of the financial system is crucial in denying terrorists access to the financial resources they require to carry out their activities. The EAG region's commitment to this objective, in line with international efforts, reflects a shared resolve to protect our societies from the scourge of terrorism.

It is our aspiration that this report will contribute meaningfully to ongoing efforts to suppress the financing of terrorism, thereby bolstering the security and stability of the EAG region and beyond.

Mr. Vladimir Voronkov
Under-Secretary-General
United Nations Office of Counter Terrorism

1 United Nations Security Council, 2019. Resolution 2462 (2019) Adopted by the Security Council at its 8496th meeting, on 28 March 2019 (S/RES/2462): United Nations. Available at: https://documents.un.org/doc/undoc/gen/n19/090/16/pdf/n1909016.pdf

Executive Summary

Terrorists continue to rely on "conventional" funding sources despite the rise of VA-based financing.

Terrorists continue to rely on "conventional" funding sources despite the rise of VA-based financing. However, the use of VAs and VASPs in the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) region presents significant challenges to domestic authorities mainly due to a lack of harmonization in Member States' practices and legal/regulatory frameworks. This report, supported by the United Nation Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT), aims to address these challenges by enhancing the understanding of practices established by EAG Member States and the need for harmonized approaches among the region, aligned with international and Financial Action Task Force (FATF) standards on VA/VASPs among EAG Member States.

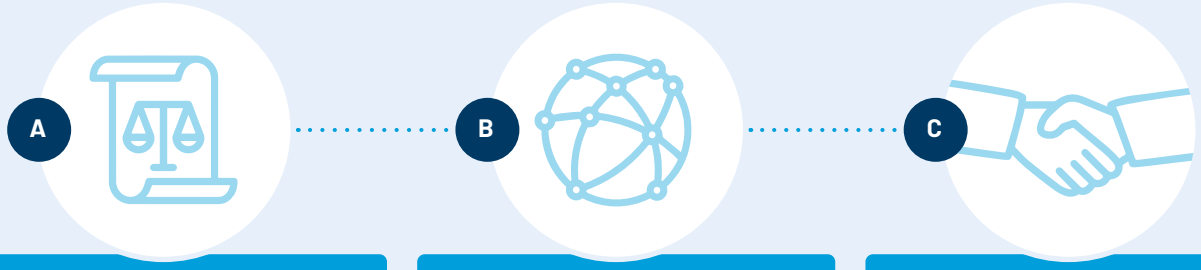
In addition to disjointed regulations, laws, and practices related to VAs/VASPs across the EAG region, VAs/VASPs are inherently borderless and flourish in anonymity adding a layer of vulnerability that terrorists can exploit, exposing the region to higher risks. Without enhanced coordinated efforts among EAG Member States, these vulnerabilities and risks will continue to undermine security and hinder effective counter-terrorism measures.

This report explores the characteristics of VAs and VASPs, the risks associated with their misuse for terrorism financing (TF), and the effectiveness of existing measures to detect, investigate, prosecute, seize, and confiscate VAs in the nine EAG Member States.

Additionally, the report assesses existing frameworks, legal and regulatory environments, and the effectiveness of practices across EAG Member States in combating TF through the use of VAs.

This report also provides an overview of practices that Member States are encouraged to implement to support the creation of a robust legal, regulatory and practical environment that can effectively counter the misuse of VAs for TF purposes in a harmonized way.

These practices entail:



Enhancing Implementation of Legal and Regulatory Frameworks

EAG Member States are advised to adopt and implement laws, regulations, and practices in line with international standards, including FATF recommendations, and in compliance with international law, notably international humanitarian law, international human rights law and international refugee laws.

Strengthening International Cooperation

EAG Member States are encouraged to collaborate among themselves and with the international community to facilitate the sharing of information and effective practices in combatting the misuse of VAs.

Encouraging Public-Private Partnerships

EAG Member States are invited to promote cooperation between the public sector and VA/VASP providers to enhance the understanding of risks and ensure compliance with regulatory requirements.

Additionally, it is critical to conduct capacity building and training programs to enhance the capabilities of regulators, law enforcement agencies, and other criminal justice officials. Developing specialized training initiatives will ensure that these stakeholders are well-equipped to monitor, investigate, and address VA-related activities effectively. Such programs are vital for staying ahead of the evolving threats posed by the misuse of VAs and for implementing the practices outlined in this report.

The effective regulation of VA/VASPs is imperative in safeguarding the financial systems within the EAG region from terrorist exploitation. By adopting harmonized practices in compliance with international law and, aligned with FATF standards, and by strengthening international cooperation, EAG Member States can significantly mitigate the risks posed by the anonymity and borderless nature of VAs. This report serves as a crucial step towards achieving a coordinated and robust response to the challenges posed by the misuse of VAs for TF.

01

Background

As acknowledged in UN Security Council Resolution 2462 (2019), "innovations in financial technologies, products and services may offer significant economic opportunities but also present a risk of being misused, including for terrorist financing."[2] Despite the ongoing recourse to traditional sources of illegal income, emerging methods are increasingly used to raise funds for terrorism, such as soliciting donations and instructing on digital wallets and cryptocurrencies. *"The increased utilization of digital methods in the form of electronic wallets, sale of prepaid cell cards, and cryptocurrencies is expected to become even more pervasive and significant."*[3]

The use of VAs to finance terrorism gained significant attention in 2017 with the increased use of cryptocurrencies by terrorists. In 2019, FATF introduced recommendations addressing the growing risk of money laundering and TF VAs/VASPs. Regulators worldwide are now scrutinizing this issue, though questions remain about the extent of VA use in TF.

As reported by experts during technical discussions hosted by the Counter-Terrorism Committee Executive Directorate (CTED), while traditional methods like cash and Hawala transfers remain the most common methods of financing terrorism, terrorists increasingly combine these with new payment methods. Terrorists have also abused mobile payment systems, VAs (including Bitcoin, lesser-known cryptocurrencies and privacy coins), and online exchanges and wallets.[4]

The scale and types of abuses vary by region and economic context, the means available, and TF goals.[5] Statistics on such crimes are often unreliable due to the anonymity of cryptocurrencies, their decentralized nature, and the lack of coherent standards to combat their misuse. Existing capacities often fall short in detecting, disrupting, and proving such crimes, and in preventing terrorists from exploiting VAs.[6]

Importantly, while VA legal regulation may vary from one jurisdiction to another, VAs are equally available in any jurisdiction where unrestricted Internet access exists. The findings from EAG's technical assistance activities, conducted as part of the project "Monitoring the Risk of Misuse of Virtual Assets for Criminal Purposes," [7] highlight a significant increase in the use of VAs in criminal activities, including TF. While there has been notable growth in the utilization of these assets, the cryptocurrency markets still face challenges related to harmonization.

2 United Nations Security Council Counter-Terrorism Committee, 2022. CTED's tech sessions: Highlights on "Threats and opportunities related to new payment technologies and fundraising methods". [Online] Available at: **https://www.un.org/securitycouncil/ctc/news/cted's-tech-sessions-highlights-"threats-and-opportunities-related-new-payment-technologies-0** [Accessed 13 June 2024].

3 United Nations Security Council, 2024. Letter dated 19 July 2024 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council (S/2024/556). Available at: **https://documents.un.org/doc/undoc/gen/n24/191/91/pdf/n2419191.pdf**

4 United Nations Security Council Counter-Terrorism Committee, 2022. CTED's tech sessions: Highlights on "Threats and opportunities related to new payment technologies and fundraising methods". Op. cit.

5 Ibid.

6 Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project.

7 **https://eurasiangroup.org/en/login?doc=1b52faf087e2171c46755802ea2694ee** (access rights are required)

02

Methodology

This publication was developed under the joint UNOCT/UNCCT, Rosfinmonitoring and EAG initiative launched during the 38th EAG Plenary (on 4-9 June 2023 in Almaty, Kazakhstan), in a session with over 200 participants.[8] Three regional consultations were organized under this initiative to gather feedback from academia, private and public sectors to further inform this publication:

Russian Federation AUG '23

The first consultation was organized in Moscow, the Russian Federation, on 24 August 2023. The event highlighted the challenges faced by both public and private sectors, including the tracking of anonymous-enhanced crypto assets for investigative purposes, and the necessary legal, regulatory and policy changes to ensure effective implementation. The event was attended by 1,200 people, representing over 20 countries, both online and in-person.

Kyrgyz Republic SEP '23

The second consultation took place in Issyk-Kul, the Kyrgyz Republic, on 4-5 September 2023. The objective was to gather expertise, good practices, and perspectives on the risk of and responses to the misuse of VAs for TF purposes. A total of 30 experts attended this in-person event.

Uzbekistan NOV '23

The third consultation was organized in Tashkent, Uzbekistan, on 13-14 November 2023, gathering further expertise, practices, and perspectives on the matter. 140 experts attended in person and the event contributed to the completion of a first draft of the document in Russian.

China DEC '23

The preliminary draft of the publication and the main findings were presented to the 39th EAG Plenary in Sanya, China, on 8 December 2023, to ensure all feedback and perspectives could be integrated into the final knowledge product. The Chair of EAG, multiple Member States and private sector entities commended UNOCT/UNCCT efforts with regard to VAs and counter-terrorism. A total of 200 people attended this in-person event.

8 ЕАГ, 2023. Итоги 38-го Пленарного заседания ЕАГ, PLEN (2023) 6 rev.2 (8 – 9 июня 2023 г). Available at: https://eurasiangroup.org/files/uploads/files/PLEN_(2023)_6_rev_2_rus_1.pdf

Additionally, this report is a result of analytical work based on the following sources:

- FATF Recommendations and guidance;[9] reports on EAG and CIS Heads of FIU working group projects; papers of the CIS Anti-Terrorist Center Academic Advisory Council; SCO working papers; and relevant reports of the United Nations;
- Laws and by-laws of EAG jurisdictions on the regulation and enforcement of rules regarding VAs;
- National mutual evaluation reports and sectorial evaluations from EAG jurisdictions;
- Open source (public domain) information, including practices of, and latest technology for, VASP customer identification, de-anonymization and tracing of parties to cryptocurrency transactions;
- More than 1,000 criminal case studies where misuse of VAs for criminal purposes was identified;
- Consultations with criminal intelligence officers, investigators, prosecutors, and FIU officers focused on TF and detecting and proving the misuse of VAs for criminal purposes;[10]
- Expert opinions of FIU officers, law enforcement officers, representatives of VASPs, crypto-focused NPOs, and academia from EAG jurisdictions.[11]

The findings presented in this report are based upon open-source desk-based research. This research also involved direct consultations with law enforcement agencies of EAG Member States, and private sector focused on countering use of cruptocurrencies for terrorist purposes.

The report also benefited from the expertise of the UNOCT/UNCCT expert consultant with practical experience in detecting and proving the misuse of VAs for TF purposes and tracing suspicious transactions. The three regional consultations mentioned on the previous page also provided valuable insight that is reflected in the report.

1,000+

criminal case studies misusing VAs for criminal purposes were identified

9 FATF, n.d. FATF Topics. Virtual Assets. [Online] Available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Accessed 02 August 2024].

10 Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project.

11 The analysis of data collected from participants at events held in the Russian Federation (August 2023), the Kyrgyz Republic (September 2023), the Republic of Uzbekistan (November 2023), and People's Republic of China (December 2023) under the project's framework. The findings provide a comprehensive understanding of the participants' perspectives and experiences, highlighting regional variations and commonalities in response to the project's objectives.

03

Characteristics of VAs, Blockchains & VASPs

Blockchain and VAs

Blockchain is a data structure, an ever-growing sequence of records created using cryptographic principles.[12] This enables the storage of data on all transactions and the balance of currency in each "wallet". In short, blockchain serves as a digital ledger where all participants record the details of each exchange. All transactions are documented in a single, sequentially numbered ledger, with each entry linked to the previous one. This method ensures transparency for all participants and makes it extremely difficult to alter any record, as it would require changing all subsequent entries. This ledger is known as a "blockchain," where each entry represents a "block", and the entire ledger forms the "chain". This system provides a secure and transparent way to track transactions, as all participants share a unified record, making it highly resistant to manipulation.[13]

As a technology, blockchain is:

Decentralized

A blockchain is typically distributed over a network of "nodes" (computers) that each keep its own copy of the blockchain and support the blockchain's operation.

Transparent

On an open blockchain, all transactions are public and can be freely visualized online.

Irreversible

Once a transaction is completed and added to the blockchain, it cannot be modified or deleted without compromising the integrity of the entire chain[14].

12 S. Nakamoto, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Accessible at: https://bitcoin.org/bitcoin.pdf.

13 UNOPS, 2024. Blockchain - Perspectives and Prospects for United Nations: United Nations.

14 L. Tredinnik, Cryptocurrencies and the blockchain, "Business Information Review" 31 (1), 2019. F. M. Teichmann, Current Trends in Terrorist Financing, "Journal of Financial Regulation and Compliance" 30 (1), 2022.

Therefore, blockchains allow transactions to be recorded securely and reliably in open-access ledgers that can be accessed transparently. Blockchains may be "open" (e.g. Bitcoin), "anonymity-enhanced" (e.g. Monero), or "hybrid". As of the time of writing, three generations of blockchain exist.[15]

Blockchain 1.0	Blockchain 2.0	Blockchain 3.0
Since 2009:	**Since 2016:**	**Present:**
It is the original and simplest form of a decentralized ledger recording transactions, which have to be verified publicly by users. Examples are Bitcoin, Litecoin, or MDASH.	It expands on and improves the capabilities of first generation-blockchain protocols into a new type of blockchain called Ethereum. It allows the development of decentralized applications and "smart contracts," [16] making possible, inter alia, the process of "initial coin offering." [17]	It is based on technology called Directed Acyclic Graph and makes it possible to deploy distributed-ledger applications and other software in sectors outside finance and payments.

Cryptocurrencies can be defined as convertible and decentralized VAs, relying on blockchain cryptography to ensure security in the transaction without the intermediation of financial institutions. Therefore, its feature can be attractive to cybercriminals to perform their fundraising activities. To detect blockchain-enabled crimes and preserve their traces as evidence, it is fundamental to know how blockchain works.

Virtual Assets (VA)

A digital representation of value that can be digitally traded and transferred and used for payment or investment purposes. VA are distinct from any digital representation of fiat currencies, securities, and other financial assets covered by the FATF Recommendations.

15 S. Nakamoto, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, op. cit.
16 A "smart contract" is a self-executing contract coded on a blockchain. It is automatically enforced once its terms and conditions are met.
17 An "initial coin offering" is a way of attracting investment by selling a fixed amount of newly "minted" cryptocurrency for subsequent trading.

Public (open) and private keys

A bitcoin transaction includes the following stages:

1. A transaction is created;
2. The originator "signs off" the transaction, effectively proving wallet ownership to the network;
3. The transaction is webcast to all operating nodes for the verification and closure;
4. The transaction is verified, closed, and added to the block history (this part is what miners are rewarded for);
5. The transaction is recorded in a public registry;

The cryptocurrency is credited to the beneficiary wallet.[18]

For a transaction to be successfully carried out on a blockchain, users are assigned both a public and a private key in the form of an alphanumeric string of characters. While the public key (which corresponds to the wallet's electronic address) is uniquely associated with the user and must be shared to receive a payment, the private key is not linked to any personal information and allows users to access their funds and execute transactions. Despite being linked to one another, it is nearly impossible to generate a private key from a public key, thus ensuring the integrity of transactions.[19]

Transactions themselves are publicly available online and anyone can use block explorers (such as localmonero.com, btc.com, or etherscan.io) to view a transaction. A block explorer normally shows open data, including transaction date and time, open keys of originator and beneficiary wallets, volumes of cryptocurrency sent and received, volume of commissions charged, and encrypted transaction identifier (also referred to as "hash" or TxID).[20]

TxID, an alphanumeric identifier assigned to each cryptocurrency transaction – effectively "the transaction number" – verifies that the transaction has happened and is publicly available. However, it only identifies the transaction, not the cryptocurrency owners. TxID is available in the transaction history.[21]

18 Doubloin, 2023. How Does a Bitcoin Transaction Work? [Online] Available at: https://www.doubloin.com/learn/how-bitcoin-transaction-work [Accessed 31 July 2024].

19 CoderCA Blog, 2022. A Byte of Blockchain – Week 20. Transaction Verification & Validation [Online] Available at: https://coderca.hashnode.dev/a-byte-of-blockchain-week-20-transaction-verification-and-validation [Accessed 31 July 2024].

20 Cointelegraph, 2020. How do you use a block explorer? [Online] Available at: https://cointelegraph.com/news/how-do-you-use-a-block-explorer [Accessed 31 July 2024].

21 Ethereum, n.d. Transactions [Online] Available at: https://ethereum.org/nl/developers/docs/transactions/ [Accessed 31 July 2024].

Types of cryptocurrencies

To combat the misuse of cryptocurrencies for criminal purposes effectively, it is crucial to consider their various types, as their different features influence the likelihood of tracking, ownership attribution, use as evidence, and confiscation.

Decentralized is the most prevalent type of cryptocurrency involved in criminal cases and financial investigations.[22,23] Decentralized cryptocurrencies are issued by a potentially unlimited number of entities engaged in a process known as "mining", and function without a regulator or any external entity exercising control. Peer-to-peer transactions in decentralized cryptocurrencies are impossible to freeze or roll back, and such cryptocurrency is difficult to confiscate. Most widely used decentralized cryptocurrencies are Bitcoin, Ethereum, Elastos, Tezos, IOTA, Chainlink, Zilliga, etc. For access to, and disposal of, decentralized cryptocurrency, a user needs a "private key." Transaction data in such cryptocurrencies are publicly available, but data on parties to the transactions are not.

Pseudo-decentralized cryptocurrencies are issued directly by the developers or commercial companies. The issuance depends on the exact cryptography algorithm in place and, effectively, on the will of people controlling the currency, i.e. developers or entrepreneurs. Transactions in pseudo-decentralized cryptocurrencies may be frozen or rolled back, and such cryptocurrency can be returned to the originator's wallet and, therefore, confiscated. Most pseudo-decentralized cryptocurrencies are issued in jurisdictions having a legal framework for regulating VAs.[24] Most popular pseudo-decentralized cryptocurrencies are Bitcoin Cash, XRP, EOS, Tron, etc.

Platform-based cryptocurrencies are payment tokens of electronic settlement units issued by online platforms – such as BNB, NEM, Waves, KuCoin, and others – to broaden their functionality and attract new users.[25]

Stablecoins are centralized digital assets whose value is pegged to other tangible or virtual goods such as fiat currencies, gold, oil, precious stones and metals, in some cases other cryptocurrencies, held, in most such cases, by a third party. Most stablecoins exist in regulated environments.[26,27]

Gaming cryptocurrencies are VAs used for settlements and payments in multi-user online videogames.

22 Chainalysis, 2024. 2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Randsomware and Darknet Markets See Growth. [Online] Available at: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ [Accessed 13 June 2024].

23 Europol, 2021. Cryptocurrencies - Tracing the evolution of criminal finances, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

24 BIS, 2022. Cryptocurrencies and Decentralized Finance, BIS Working Papers, No 1061. Available at: https://www.bis.org/publ/work1061.pdf.

25 Cryptocurrencies and blockchain. Policy Department for Economic, Scientific and Quality of Life Policies Authors: Prof. Dr. Robby HOUBEN, Alexander SNYERS Directorate-General for Internal Policies PE 619.024 - July 2018.

26 UNOCT & UNICRI, 2024. Beneath the Surface: Terrorist and Violent Extremist use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks: Turin, Italy; New York, US. Available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/dw_beneath_the_surface_update.pdf.

27 Chainlink, 2023. What Are Stablecoins? [Online] Available at: https://chain.link/education-hub/stablecoins [Accessed 31 July 2024].

How terrorist organizations can take advantage of VAs

VAs may typically be misused for TF purposes for the following types of actions:

- Travel expenses of persons leaving their country of residence for terrorist activity area;
- Terrorist attacks;
- Services of persons publicly inciting the commission of terrorist attacks on messenger apps, websites, and social networks;
- Services of terrorist recruiters;
- Fundraising campaigns;[28]
- Direct cryptocurrency transfers to wallets controlled by terrorist organizations;
- Financing of terrorist organizations and foreign terrorist fighters as their members;
- Financing of lone terrorist actors.

As noted in the 2023 FATF report "The collected funds are then used to finance a range of activities, including recruitment, training, procurement of weapons and supplies, logistical support, propaganda dissemination, and planning of terrorist attacks. The funds may also be directed towards supporting the families of deceased or imprisoned terrorists or providing humanitarian aid in an attempt to gain sympathy and support."[29]

As part of the consultations within this project, structured interviews and discussions were held with representatives from law enforcement agencies tasked with countering the financing of terrorism. These consultations revealed that cryptocurrencies are predominantly employed as intermediary tools in the financing process. Specifically, these digital assets are used to bridge the gap between the initial funder and the end-user, often in conjunction with traditional financial mechanisms.

- Funds are collected in cryptocurrency, then converted into fiat money and credited on accounts harvested from money mules, and finally made available to terrorists directly or through e-wallets;
- Funds are collected in cash or by wire transfers, then converted into cryptocurrency and used to finance FTF travel, pay to perpetrators of attacks, or create a reverse for further use by terrorist organizations;
- Funds are taken from organized crime proceeds, converted into cryptocurrency and later used for TF, with the overall objective to conceal their criminal origin and purpose.[30]

28 FATF (2023), Crowdfunding for Terrorism Financing, FATF, Paris. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf

29 Ibid.

30 Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project.

TF and cryptocurrencies in the EAG region

Cash is still prevalent across the EAG region as a way of moving terrorist funds. National and cross-border non-bank money transfers – incoming (from any part of the world) or outgoing (primarily to jurisdictions bordering terrorist activity areas) – are another important channel.

There is also a significant relationship between the volume of cryptocurrency mining and the shadow share of cryptocurrency activity in a jurisdiction. Three EAG jurisdictions are global leaders in mining.[31] This drives the crypto industry, stimulates general interest in cryptocurrencies among the public, and facilitates technological advancements, but at the same time increases the risk of criminal misuse of VAs.

Virtual asset service providers (VASPs)

A VASP is any natural or legal person that conducts any of the following activities on a commercial basis for, or on behalf of, other natural or legal person or persons:

- Exchanging between VAs and fiat currencies;
- Exchanging one VAs for another VA or more than one other VAs;
- Transferring VAs;
- Storing and/or administering VAs or instruments enabling control over VAs; and
- Issuing, or minting, or selling VAs, or providing financial services related to the same.

Governments should require VASPs to implement preventative measures to control and regulate such technology like decentralized blockchain. Without VASPs, they cannot suspend or cancel cryptocurrency transactions, nor can they return mistakenly transferred value if the transfer did not involve a VASP.

A centralized exchange or trader is a platform offering users a paid service to buy, sell, or exchange cryptocurrency within a computing structure controlled by the enterprise acting as the intermediary between a seller and a buyer.

On a centralized exchange, a user is expected to complete a "know-your-customer" (hereinafter referred to as "KYC") procedure before being allowed to transact, with personal verification in most cases taking the form of uploading a photo of their face with their passport open, and a questionnaire filled with their customer data. Large exchanges also typically collect and log geolocations, IP addresses, IMEI of devices used, and other data that may be instrumental in identifying parties to a transaction.[32]

Overall, centralised exchanges and traders can assist FIUs and law enforcement authorities in linking wallets to individuals, as they can identify wallet owners, as well as protect assets through services like password reset, support for "cold" crypto wallets[33] and two-factor authentication. Additionally, they provide users with access to fiat currencies, and maintain custody of their assets.

Decentralized exchanges or traders, collectively referred to as DEX, are platforms enabling users to exchange cryptocurrencies in a peer-to-peer fashion. In such platforms, transactions are typically "baked" into smart contracts. As DEXs do not identify their customers, they remain anonymous, which makes identifying wallet owners more challenging. This, in turn, makes DEXs more attractive for criminals.[34]

31 Statista, 2024. Distribution of Bitcoin mining hashrate from September 2019 to January 2022, by country. [Online] Available at: https://www.statista.com/statistics/1200477/bitcoin-mining-by-country/ [Accessed 22 July 2024].

32 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

33 A "cold wallet" is an offline device that stores the public and private keys. Most hardware wallets connect to devices (such as personal computers or smartphones) via a USB port. The private key is typically "baked" into a cold wallet; such a wallet cannot be controlled remotely. Seizure of cold wallets in most cases makes seizure and confiscation of cryptocurrency feasible.

34 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

When trying to detect cryptocurrency-enabled crime or conducting financial investigations, the following features of DEX transactions should be kept in mind:

- Users transact independently, without intermediation (value is transferred from one wallet to another);
- Owners of cryptocurrency remain anonymous as no customer identification is conducted, or data provided, which makes it impossible to order the VASP to assist in identifying parties to a transaction;
- Transactions nonetheless remain visible and traceable as they are enabled by distributed ledger technology irrespective of the type of VASP, just like any other transaction involving cryptocurrencies;
- Users have more freedom transacting with cryptocurrencies as there are no controls or regulatory policies in place;
- A wallet "private key" is the only way of proving ownership of cryptocurrency; loss of the private key makes regaining control over the wallet highly problematic.[35,36]

35 Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project. The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

36 Tisen O.N. Tracking cryptocurrency transactions in order to investigate crimes // Criminal proceedings. 2024. No. 2. pp. 54-60.

04

Existing Framework on TF & the use of VAs

In its effort to combat the misuse of VAs for TF purposes, the international community can find significant assistance in the robust framework and comprehensive guidelines established by international bodies like UN and FATF.

UN Security Council, Security Council Counter-Terrorism Committee and its Executive Directorate (CTC/CTED), and UN General Assembly	
UN General Assembly (1997) [37]	Calls upon all Member States "to counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations, whether such financing is direct or indirect through organizations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities."
UNSCR 1373 (2001)	Decides that all States shall [...] "criminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts."
UNSCR 1267 (1999)	Calls upon UN Member States to impose sanctions on assets belonging to persons involved in terrorist activities.
UNSCR 1989 (2011)	
UNSCR 2253 (2015)	

37 Cf. Paragraph 3(f), United Nations General Assembly, 1997. Measures to eliminate international terrorism (A/RES/51/210). Available at: https://digitallibrary.un.org/record/230747.

UNSCR 2462 (2019)	Underscores the need for effective implementation of terrorist asset freeze under UNSCR 1373 (2001), including as requested by other States.
UNSCR 2482 (2019)	Decides that all States shall, in a manner consistent with their obligations under international law, including international humanitarian law, international human rights law and international refugee law, ensure that their domestic laws and regulations establish terrorist financing as a serious criminal offense sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offense. Underscores a special role FIUs and financial investigations play in combating terrorism. Demands that Member States ensure that all measures taken to counter terrorism, including measures taken to counter the financing of terrorism, comply with their obligations under international law, including international humanitarian law, international human rights law and international refugee law; Urges States, when designing and applying measures to counter the financing of terrorism, to take into account the potential effect of those measures on exclusively humanitarian activities, including medical activities, that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law.
UNSCR 1617 (2005)	Strongly urges UN Member States to implement the comprehensive Standards of the Financial Action Task Force, i.e. Forty Recommendations on money laundering and Nine Special Recommendations on TF.
UN CTC Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes (28-29 October 2022)	Recognizes that "innovations in financial technologies, products and services, such as virtual assets and new financial instruments, including, but not limited to, crowdfunding platforms, may offer economic opportunities but also present a risk of being misused, including for terrorist financing;" Reaffirms that "Member States should consider and assess risks associated with specific products and payment methods, including value stored and prepaid cards, virtual assets and new financial instruments, including, but not limited to, crowdfunding platforms, and implement risk-based anti-money-laundering (AML) and counter-terrorist financing (CFT) regulations, monitoring, and supervision to providers of relevant services, and acknowledges the important work and the essential role of the Financial Action Task Force (FATF) in this regard."[38]

38 United Nations Security Council Counter-Terrorism Committee, 2022. Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes, New Delhi. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/outcome_document_ctc_special_mtg_final_e.pdf

FATF Recommendations

The Financial Action Task Force (hereinafter referred to as "FATF") is the global standard setter on combatting money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standards.[39]

FATF Guidance and Reports on VAs misuse for TF	
Virtual Currencies: Key Definitions and Potential AML/CFT Risks (2014)	The first international guidance paper focused on novel digital entities designed for financial settlements.
Guidance for a Risk-based Approach. Virtual Currencies (2015)	Describes the best ways to minimize the risks of VAs misuse for ML and TF.
Report on Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets (2020)	Outlines specific indicators suggesting potential misuse of VAs to strengthen the response to financial crimes involving VAs.
Report to G20 on So-called Stablecoins (2020)	Provides an assessment of the risk posed by stablecoins.
Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2021)	Aims at supporting countries in making sure that VASPs are subject to the same full spectrum of AML/CFT/PF obligations as financial institutions and designated non-financial businesses and professions. Clarifies that countries, based on their /, legal framework, or political considerations such as consumer rights protection, monetary policy stability, or national security, can decide to restrict or prohibit VA transactions or VASPs as businesses.
Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2023)	Further focuses on the special role of VASPs and the private sector in mitigating the risk of misuse of VAs for criminal purposes, stressing the need for them to put in place measures under Recommendation 15 (R. 15). Emphasizes the identification and assessment of risks related to "decentralized finance," non-hosted wallets, and P2P transactions.

39 For more information, please visit: www.fatf-gafi.org.

FATF Guidance and Reports on VAs misuse for TF	
Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity (2024)	Provides a snapshot in time of R. 15 implementation status of jurisdictions that are identified as having materially important VASP activities as well as jurisdictions that are FATF members.
Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs (2024)	Acknowledges the progress that has been made in the VA sector, especially in the registration/licensing of VASPs; however, it further stresses the need for global implementation of R. 15 and the Travel Rule, as gaps in AML/CFT regulatory systems persist.

According to the Interpretive Note to Recommendation 15 on New Technologies (INR. 15), FATF standards that are most directly applicable to VAs and VASPs are:[40]

- Understanding ML and TF risks the sector faces;
- Implementing risk-based approach to VAs and VASPs regulation and supervision for AML/CFT/PF purposes, in the same way as to other financial institutions;
- Licensing or registering VASPs;
- Ensuring that VASPs
  - Conduct the same preventive measures as financial institutions, such as customer due diligence, record keeping, and reporting suspicious transactions;
  - Obtain, hold and securily transmit originator and beneficiary information when making transfers.
- Engaging in international cooperation.[41]

The FATF Guidance underscores that VASPs should be subject to adequate regulation and risk-based supervision or monitoring by a competent authority, including systems for ensuring their compliance with national AML/CFT requirements.[42] Such competent authorities should be obligated to conduct supervision on the basis of risk and should be empowered to inspect their obliged entities, make compulsory information requests, and impose sanctions for non-compliance.

As an overarching R. 15 requirement, countries should conduct assessments of ML/TF risks as new products or practices become available.

40 FATF, n.d. FATF Topics. Virtual Assets. Op. cit.

41 FATF, 2019. Public Statement on Virtual Assets and Related Providers. [Online] Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Public-statement-virtual-assets.html [Accessed 18 June 2024].

42 The FATF Standards state that in this context, a "competent authority" cannot include a self-regulatory body (SRB).

Models of legal treatment of VAs

According to FATF Recommendations and Guidance, countries may decide to regulate, prohibit or limit VA activities or VASPs for those VA activities carried out by non-obliged entities based on their risk assessment of VAs and VASPs and their national regulatory context. Under FATF R.15 and INR.15, countries must either prohibit or regulate. Countries should subject VAs and VASPs to the full range of obligations under the above recommendations.

Most countries choose the latter option, prohibiting the use of cryptocurrencies as legal tender while allowing VASPs to operate, and their national persons to own VAs. This model equates to a balancing act: On the one hand, countries are ensuring the stability of national currency and intolerance to competition from decentralized assets, and on the other, they are preparing their country better prepared for investment in novel technologies or economic sectors and increasing state revenue, on the other.

However, some countries have not put in place any VA regulations or have limited themselves to formally providing only basic definitions related to VAs so far.

Failure of governments to regulate VAs may lead to challenges including:

- Prevalence of criminal cryptocurrency use increasing, including for money laundering and TF;
- Funds less likely to be monitored and risk-rated for the purposes of AML/CFT and combating crime in general;
- At the regional level, a further serious threat to be addressed would be the adoption of cryptocurrencies as a novel way of financing terrorist organizations.

A total prohibition on cryptocurrencies – compared to a controlled framework enabling their use mostly for investment purposes – is not only difficult to implement in practice, but it could also increase the risk of criminal use.

While many jurisdictions have already moved to put together a legal system for VAs, such as prohibiting or permitting their use as legal tender, property, or as an investment vehicle, most have been slower in making another critical step for effectively combating VA illicit use, namely ensuring that VASPs are fully covered as AML/CFT reporting entities.

05

Risk of misuse of Virtual Assets for Terrorist Financing

Highly anonymous and often underregulated, VAs are increasingly popular for concealing criminal activities and illicit proceeds.[43] By way of example, in the UN Security Council Al-Qaida Analytical Support and Sanctions Monitoring Team's Thirty-fourth report, Member States reported that "Detailed instructions to make payments through registering and replenishing digital wallets are routinely provided to transfer money through cryptocurrencies." Similarly, "the growing use of anonymity-enhancing cryptocurrencies (also called privacy coins) by ISIL and its affiliates" was noted. These findings indicate that the use of such digital methods is expected to become increasingly prominent.[44]

In the CIS and broader Eurasian region, advancements in information technology and the availability of VAs have introduced novel TF risks.

Cryptocurrencies facilitate anonymous funding of terrorist activities, communications via anonymous messaging apps, and payments to attackers. Social networks and messaging apps are used to recruit individuals for attacks, offering payment in cryptocurrency from abroad, complicating prosecution efforts. For instance, investigations on the Crocus City Hall attack in Russia on 22 March 2024 have confirmed the use of cryptocurrency by foreign organizers.[45,46,47] TRM Labs identified pro-ISIS groups in Tajikistan using cryptocurrencies for recruitment and funding, with notable arrests disrupting their operations.[48] Across the region, funds are sent to FTFs in conflict zones, with numerous convictions in Russia alone.[49,50] Gaming cryptocurrencies[51] are also leveraged for TF, while NFTs[52] are generally seen at risk of misuse for such purposes, highlighting the diverse methods terrorists use to collect and transfer funds.

43 FATF, n.d. FATF Topics. Virtual Assets. [Online] Available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Accessed 14 June 2024].

44 United Nations Security Council, 2024. S/2024/556, op. cit.

45 Следком, 2024. Председатель СК России провел оперативное совещание и заслушал отчет следственной группы о ходе расследования уголовного дела о террористическом акте в «Крокус Сити Холле» [Online] Available at: https://sledcom.ru/search/?q=крокус+сити&page=2&sort[Accessed 31 July 2024].

46 Известия, 2024. Цифровой силуэт: теракт в «Крокусе» финансировали криптовалютой [Online] Available at: https://iz-ru.turbopages.org/turbo/iz.ru/s/1673581/iana-shturma-roman-soldatov/tcifrovoi-siluet-terakt-v-krokuse-finansirovali-kriptovaliutoi [Accessed 31 July 2024].

47 РБК, 2024. В СК заявили о переводах с Украины для террористов из «Крокуса». [Online] Available at: https://www.rbc.ru/politics/28/03/2024/660581ec9a79477bc0fc74e1 [Accessed 01 August 2024].

48 TRM Labs, 2023. TRM Finds Mounting Evidence of Crypto Use by ISIS and its Supporters in Asia. [Online] Available at: https://www.trmlabs.com/post/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia. [Accessed 13 June 2024].

49 https://fedsfm.ru/activity/annual-reports

50 FATF (2016), Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris. Available at: https://www.fatf-gafi.org/en/publications/mutualevaluations/documents/mer-russian-federation-2019.html.

51 Council of the European Union - EU Counter-Terrorism Coordinator, 2020. Online gaming in the context of the fight against terrorism (9066/20), Brussels: Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf. Klein, M., 2024. Video Games Might Matter for Terrorist Financing. [Online] Available at: https://www.lawfaremedia.org/article/video-games-might-matter-for-terrorist-financing [Accessed 20 June 2024].

52 CNAS, 2022. Islamic State Turns to NFTs to Spread Terror Message. [Online] Available at: https://www.cnas.org/press/in-the-news/islamic-state-turns-to-nfts-to-spread-terror-message. [Accessed 13 June 2024].

Despite the rise of VA-based financing, terrorists continue to rely on "conventional" funding sources. Most funds from the EAG region ending up in terrorist hands still come from legitimate proceeds. The rest are for the most part criminal proceeds deriving from property crime such as fraud, corruption, and money laundering; trafficking in narcotics, arms and ammunition; or bulk cash and bearer negotiable instruments smuggled across borders.

Persons in the EAG region engaging in TF with the use of VAs and their motivations	
Active members of terrorist networks	■ Terrorist financiers; ■ Organizers of attacks; ■ Enablers collecting and diverting funds; ■ Terrorist organization members financially supporting FTFs and their families.
Terrorist sympathizers	■ Persons who, while not directly participating in terrorist activities, share terrorist objectives professed by the terrorist organization.[53] ■ Individuals who provide funds as a way of demonstrating loyalty and with a view to possibly joining the terrorist organization.
Family members and/or supporters of of FTFs or lone terrorist actors	■ Persons who support their everyday needs and use cryptocurrency deliberately, being aware of an inherently high risk of exposure.
Common individuals	■ Those manipulated into believing that their funds would be used for good works; ■ Persons who have ended up financing terrorism as a result of psychological manipulative techniques by terrorists to draw funds from as large and diverse base as possible.
Those who deliberately use VAs for criminal purposes are unlikely to use registered VASPs and highly likely to use ways to enhance transaction anonymity	■ At the same time, terrorists in the EAG region rarely attempt to publicly collect funds in cryptocurrency under the guise of religious donations. Religious communities in the region tend to regard VAs with mistrust.

53 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023). Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project.

Financial behavior patterns of VA-enabled terrorist financiers

Terrorism financiers and organizers have been found to use the following methods, separately or in combinations, to conceal their transactions:

- Cryptocurrency mixers/tumblers, browsing with IP address spoofers or multiple layers of trace erasers such as VPN41, VPS42, or TOR43;
- Secure online platforms, encrypted messaging apps;
- Anonymity-enhanced cryptocurrencies;
- Cryptocurrency exchanges and traders operating abroad, to make investigations as challenging as possible;
- Unregistered/unlicensed cryptocurrency exchanges and traders that do not require customer identification;
- Where a VASP is used, quickly withdrawing cryptocurrency to a personal wallet;
- Creating a new wallet for each transaction;
- Paying high transaction commissions;
- Using "burner" devices, including those operating with virtual e-SIMs;
- Using "burner" e-wallets and bank accounts that exist only to enable receipt of fiat money for cryptocurrency and cash withdrawal;
- Quick exchange of incoming cryptocurrency for other cryptocurrencies, at sizeable commisisons, with immediate crypto-to-fiat conversion;
- Anonymity-enabling crypto-ATMs;
- Over-the-counter cryptocurrency trading (or using over-the-counter desks if provided by the trader), engaging professional independent over-the-counter cryptocurrency brokers;
- Using "nested services" of registered VASPs to conceal criminal transactions in a much larger transaction pool;
- Anonymous accounts on e-payment platforms as receivers of cryptocurrency;
- Using DeFi and NFTs;
- Smurfing or "dusting" transactions;
- Transacting directly, without intermediation.[54]

The most prevalent means of disguise in the context of misuse of VAs for criminal purposes is a "cryptocurrency mixer,"[55] an anonymization service that splits originator's "coins," mixes them randomly with those belonging to third parties and sends the agreed amount to the recipient in a series of low-value transactions seemingly coming from various random parties, rather than directly.

Most cryptocurrency-enabled crimes involve online payment applications, with various techniques designed to spoof IP addresses or create dynamic or unrecognizable accounts.

The DarkNet is an Internet segment widely used by persons conducting illicit trade in prohibited or restricted goods or substances. DarkNet technology makes it possible to provide exclusive access for trusted users and exchange files anonymously. Nonetheless, law enforcement authorities in several EAG countries already have some track record in detecting and disrupting DarkNet-enabled crime.[56] [57]

54 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023). Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project.

55 Cointelegraph, 2022. What is a cryptocurrency mixer and how does it work? [Online] Available at: https://cointelegraph.com/explained/what-is-a-cryptocurrency-mixer-and-how-does-it-work [Accessed 31 July 2024].

56 РБК, 2019. ФСБ изъяла из даркнет-магазина 440 кг наркотиков на 650 млн руб [Online] Available at: https://www.rbc.ru/society/13/11/2019/5dcbad5f9a79472d74f9b3f9 [Accessed 31 July 2024].

57 UNOCT & UNICRI, 2024. Beneath the Surface, op. cit. EAG, 2022. Legalization (laundering) of the proceeds of cybercrime, as well as financing of terrorism from the said offence, including through the use of electronic money or virtual assets and the infrastructure of their providers. Available at: https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_eng.pdf.

06

Assessing & mitigating the risk of misuse of VAs for TF purposes

Countries need to understand and assess the risks related to the criminal misuse of VAs in order to effectively mitigate it by enacting AML/CFT legal obligations for VASPs and ensuring all VASPs are registered or licensed. However, this approach will only be truly effective if all countries designate VASPs as reporting entities and require their registration or licensing.[58] Since crypto exchanges or traders can operate from anywhere, criminals will continue to exploit gaps by resorting to unregulated service providers operating in the shadows.

To make cryptocurrency anonymity less of a challenge, some countries are working to create legal requirements to pass customer verification procedures and use only a specific bank account owned by the same person to buy and sell cryptocurrency for fiat money, effectively trying to put the same customer through customer due diligence (hereinafter referred to as "CDD") twice, by their VASP and by the bank.[59]

A step forward in this regard would be for jurisdictions to introduce regulations requiring VASPs to comply with the "travel rule," i.e. share relevant originator and beneficiary information alongside certain VA transactions. Under the latest FATF requirements related to novel financial technology, VASPs should accompany any transfer of VAs with originator and beneficiary data; receive and keep such records, making them available to all downstream counterparties and formally produce them upon request from competent authorities.[60]

58 FATF, 2024. Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity, op. cit.

59 IMF eLibrary: Schwarz, N. & Ke Chen. "Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (2): Effective Anti-Money Laundering and Combating the Financing of Terrorism Regulatory and Supervisory Framework - Some Legal and Practical Considerations," FinTech Notes 2021, 003 (2021), A001. Available at: **https://www.elibrary.imf.org/view/journals/063/2021/003/article-A001-en.xml**.

60 FATF, 2024. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs.

Challenges in assessing the risk of misuse of VA for TF purposes

In some EAG jurisdictions, VASPs are not reporting entities for AML/CFT purposes. Where they are, there is little experience supervising them, which makes effective information sharing difficult and, in some cases, impossible.[61] At the same time, on 28 July 2023, a report on the assessment of ML/FT risks in the sector of VAs and VASPs in Kyrgyzstan was approved.[62]

Risk assessments tend to rely on official data on the prevalence of VA-enabled crime, while - as discussed above – such statistics may not reflect the real situation as detecting VA-enabled crime is an inherently challenging exercise.

This may lead to an assessment that is, at best, hypothetical. Nonetheless, EAG jurisdictions lack clear and applicable guidance and manuals for such risk assessments.

Being a relatively new phenomenon, VAs are still understudied, and there are only few – if any – people with the appropriate expertise available for conducting government-ordered risk assessments of VA criminal misuse.

Risk-rating cryptocurrency wallets for CFT purposes in the EAG region

In the last few years, countries that have regulated VASPs for AML/CFT purposes have embarked upon assessing the risk of terrorist misuse of VAs. Due to the significant demand from private entities for checks on whether natural and legal persons' virtual assets (VAs) have been linked to criminal activity, many services now offer reports on the 'cleanliness' of wallets and potential connections of upstream and downstream transactions to ML or TF. The demand for such services is an indication that typical cryptocurrency owners not only want to be safe from getting their VAs blocked by a regulated VASP as a result of a sweeping anti-crime operation but are also becoming more conscious about legal jeopardy and are taking AML/CFT regulation of VAs more seriously.[63]

As developers and providers of such services typically warn their customers, automatic private risk-rating is inherently probabilistic. In fact, such "customer risk reports" often underscore that users make decisions at their own risk, and nothing in the report creates any legal obligation for the service provider or accountability for the consequences of the user's actions. The data informing these reports are indeed publicly available and collected online, which means some of the information derived may be fake, unreliable or prejudicial.

61 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

62 Кабинет Министров Кыргызской Республики, 2023. Отчет об оценке рисков финансирования террористической деятельности и легализации (отмывания) преступных доходов в секторе виртуальных активов и поставщиков услуг виртуальных активов. Available at: https://fiu.gov.kg/uploads/64d355f436421.pdf

63 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), Uzbekistan (November, 2023). Similar information was received from participants of the international scientific and practical forum "Topical issues of countering Money laundering and Terrorist Financing" (Russian Federation, 24-26 April 2024) from Belarus, Egypt, India, Iran, Kazakhstan, the Kyrgyz Republic, China, Cuba, Mauritius, Madagascar, the United Arab Emirates, Oman, Russia and Uzbekistan.

According to current cryptocurrency industry "conventional wisdom," the probability of a cryptocurrency wallet being associated with a crime translates mathematically into the following risk ratings:

Category	Probability (%)	Description
Low Risk	<35	Typically for general use wallets
Medium Risk	36-75	Often covering smart contracts with tokens pledged for liquidity purposes and wallets associated with VASPs that are not AML/CFT reporting entities
High Risk	>76	Typically for addresses associated with other addresses flagged as "DarkNet," "scam," "dark service," "dark market" etc., and with VASPs having a history of being associated with crime.[64]

Identifying the risk of VA misuse for criminal purposes in the EAG region

Identifying high-risk crypto wallets relies on the following sources of information, including, but not limited to:

- Open search on the internet ("content scraping" for a particular wallet address and surrounding context);
- Transaction records (blockchain browsing to find connections to previously compromised wallets);
- Association records (looking for connections to crime-related cryptocurrency exchanges and traders);
- Disclosures of national fius, law enforcement or supervisory authorities;
- Disclosures of foreign fius over secure international information sharing channels;
- VASPs;
- Bank compliance officers.[65]

Modern crypto search applications make it possible to find wallet addresses owned by the same person, cluster them and get all "target transactions" in a single query. Additional inputs such as IP addresses and open-source information may also be instrumental for clustering.

As a high-tech and rapidly evolving part of the economy, new technologies in the crypto industry, including effective tools to identify suspicious transactions and high-risk wallets, tend to be unique and costly products, proprietary to their developers and copyright holders.

Many governments have developed their own mechanisms for flagging fiat transactions related to cryptocurrency transactions, primarily utilizing business rules that automatically match records of incoming wire transfers with the dates, times, and values of cryptocurrency transactions.

64 The information was obtained as a result of an analysis of popular AML-verification services for cryptocurrencies in the EAG countries.

65 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), Uzbekistan (November, 2023). Similar information was received from participants of the international scientific and practical forum "Topical issues of countering Money laundering and Terrorist Financing" (Russian Federation, 24-26 April 2024) from Belarus, Egypt, India, Iran, Kazakhstan, the Kyrgyz Republic, China, Cuba, Mauritius, Madagascar, the United Arab Emirates, Oman, Russia and Uzbekistan.

Increasingly, banks are equipping their compliance services with tools that combine encrypted customer account data with data from crypto applications and look for date/time and value matches between crypto and fiat transactions.

Typically, these tools allow for a time gap of up to 30 minutes between a crypto and a fiat transaction and a crypto-to-fiat rate gap of up to +/- 15%. To identify details of VASPs and increase the sensitivity of such business rules, banks use "cryptocurrency mystery shopping." To tie a crypto wallet to a person owning a bank account, they may also match the IP, IMEI, and MAC addresses of online devices used by the bank customer to access their account to those used to access the VASP platform, and/or match the telephone numbers and email addresses of the bank's customers to those of the VASP.[66]

Secondly, regulators or competent authorities have developed indicators to identify a likely connection between fiat and cryptocurrency transactions. These indicators include a large number of incoming payments from natural persons within one banking day, incoming payments from known money mule accounts, the use of accounts opened shortly before the target transaction, and the "waking" of "dormant" accounts not used for a considerable length of time.[67]

Such indicators alone, while being relatively useful for purposes such as detecting tax evasion by self-employed individuals or incorporated professionals, tend to cast the net too wide. For instance, a large number of small-value transactions may indicate that a retail bank account is being misused to masquerade unregistered and untaxed business activity, a violation of the law, but a much more trivial one than this account being used as the focal point of an illicit crypto-to-fiat post-smurfing operation. Suspicion should be reasonably based on a combination of indicators. In isolation, there are no indicators unequivocally pointing to illicit activity, including TF.

As of the time of writing, there are no technical methods to reliably identify fiat transactions resulting from cryptocurrency conversion. However, technology continues to evolve in this direction, including in EAG jurisdictions.

Governments of countries where VASPs are still not reporting entities for AML/CFT purposes (a so called "sunrise issue"[68]) may try to put in place methods to detect suspicious crypto-to-fiat conversion transactions as a tentative risk-mitigating measure.[69]

66 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), Uzbekistan (November, 2023).

67 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), Uzbekistan (November, 2023). Similar information was received from participants of the international scientific and practical forum "Topical issues of countering Money laundering and Terrorist Financing" (Russian Federation, 24-26 April 2024) from Belarus, Egypt, India, Iran, Kazakhstan, the Kyrgyz Republic, China, Cuba, Mauritius, Madagascar, the United Arab Emirates, Oman, Russia and Uzbekistan.

68 FATF, 2022. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, Paris: FATF/OECD. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.inline.pdf.

69 For further information on their projects, see https://eurasiangroup.org/en/key-wgtyp-documents-and-on-going-projects

EAG measures to mitigate the risk of VA misuse for TF purposes[70]

- Regularly conducting comprehensive national assessments of the risks of VA misuse for money laundering or TF. Updating such assessments is of particular importance in the context of rapid development of financial instruments and technology
- Either formally prohibiting VAs or putting in place risk-based regulations, effective supervision of VASPs, making VASPs reporting entities for AML/CFT purposes;
- Adopting universal international standards for cryptocurrency industry and VASP operation;
- Putting in place effective mechanisms for detecting and disrupting unregulated VASP operation;
- Imposing CDD requirements on VASPs;
- Enforcing the "travel rule" for cryptocurrency transactions;
- Disseminating lists of national, if any, and foreign regulated/licensed VASPs among national competent authorities;
- Developing and coherently enforcing criteria for "red-flagging" suspicious cryptocurrency transactions;
- Flagging compromised wallets and VASPs and sharing such lists with competent authorities globally;
- Adopting government (FIU, law enforcement, other competent authorities) software solutions to trace suspicious crypto transactions, establish terrorist nexus and identify wallet owners;
- Promoting the development, adoption, and use of cryptocurrency transaction analytics by VASPs and credit institutions;
- Reaching out to crypto industry and IT executives, bank and VASP compliance units, NPOs, academia, and the general public for engagement in countering the criminal misuse of VAs, including flagging compromised wallets;
- Advancing forensic techniques to establish connections between fiat and cryptocurrency transactions and investigating the provenance of VAs freshly converted into fiat money;
- Systemically educating dedicated officers in cryptocurrency transaction tracing, wallet owner identification, and transaction de-anonymization techniques, and engaging in sharing practices on VA terrorist misuse risk mitigation;
- Engaging FIUs and law enforcement authorities in broader engagement with other stakeholders of AML/CFT systems;
- Raising Awareness across AML/CFT systems of the risks of misuse of VAs for TF;
- Developing academic knowledge and studies of countering VA terrorist misuse;
- Enhancing good practices and intelligence sharing on VA criminal misuse.

70 The findings presented in this table refer to the three regional consultations organized under this initiative. For more information, please refer to the initiative section of this report.

07

Measures in place in the EAG region

VAs legal framework in the EAG region

The Concept Note for the EAG typology project "Monitoring the risk of misuse of VAs for criminal purposes" underscores that the regional cryptocurrency markets are not harmonized, despite sizable growth in the criminal, including extremist and terrorist, use of VAs.[71]

All EAG Member States prohibit the use of cryptocurrency as legal tender. While three EAG Member States are in the top five globally for jurisdictions in terms of cryptocurrency owners, most members use "pilot legal regimes" for VASPs, allowing their activity only in specific geographically targeted areas. Cases in point are Belarus and Kazakhstan.

China effectively prohibited the use of cryptocurrencies from 2013-2017; Belarus, India, Kazakhstan, Kyrgyzstan, and Uzbekistan have put in place AML/CFT coverage for VASPs; the Russian Federation and Tajikistan are in the process of developing such regulations. Turkmenistan, while not having any legal framework for VAs or VASPs, stops short of directly prohibiting them, focusing on other contextual factors that, according to its NRA report, point at a minimal risk of the use of cryptocurrencies by Turkmenistan nationals.

71 For further information on their projects, see https://eurasiangroup.org/en/key-wgtyp-documents-and-on-going-projects.

EAG Countries' Regulations on VAs and VASPs[72]

Belarus[73]

Presidential Decree 8 (December 2017), "On the Development of Digital Economy"[74] outlines the conditions for economic operations based on blockchain other decentralized distributed-ledger technologies, ensuring their safety. In particular:

- Belarus citizens can freely buy and sell cryptocurrency from and to any traders, whether national or international.
- Legal persons, however, can transact only with residents of the High Technology Park (hereinafter referred to as "HTP").[75]
- Business activities involving digital tokens by non-HTP residents are prohibited (see Decree 8, paragraph 2.6).

VASP operations are regulated by the State HTP Administration, National Bank of Belarus, and State Control Committee. Key points include:

- Inspections of HTP residents require pre-approval by the State HTP Administration (see Decree 8, Paragraph 4.6).
- HTP-approved operations include crypto exchange, crypto trader, ICO organizer, mining pool.
- All VASPs residing in HTP are AML/CFT reporting entities and subject to all appropriate compliance requirements.

Republic of India[76]

The crypto industry in the Republic of India is currently regulated by the following authorities:

- Reserve Bank of India;
- Companies Register (Ministry of Corporate Affairs);
- Central Board for Direct Taxes (Department of Revenue, Ministry of Finance);
- Securities and Exchange Board of India.

Though not prohibited, VAs cannot be used as legal tender. Under Indian law in place since 2022, tokens are treated as taxable digital assets, with a 30% tax on any gains made from trading cryptocurrencies, NFTs, or any other VAs.

According to the Department of Revenue, Ministry of Finance of India Notification 244184[77] dated 7 March 2023, VASPs are subject to the Prevention of Money Laundering Act 2002, thus making VASPs obliged to comply with AML/CFT requirements - including the Prevention of Money Laundering (Maintenance of Records) Rules 2005 – reporting transactions to FIU India.

FIU India has also issued detailed AML/CFT guidelines covering both General Obligations of VASPs and specific obligations, such as KYC norms, CDD norms, EDD norms, Travel Rule implementation, sanctions screening. The guidelines also covered reporting obligations, which include filing of Suspicious Transaction Reports (hereinafter referred to as "STRs"), record retention, sharing of information, and prohibition of tipping off.

72 Given the rapidly evolving nature of this topic, these norms might undergo reviews or updates. Therefore, readers are encouraged to seek the most up-to-date information and sources to ensure accuracy and relevance.

73 The level of implementation of the requirements of R.15/INR.15 FATF was assessed by the EAG in course of the follow-up in November 2022. ЕАГ, 2022. Республика Беларусь: Первый отчет о прогрессе в рамках стандартного мониторинга (без пересмотра рейтинга). Available at: https://eurasiangroup.org/files/uploads/files/Follow-up_Report_Belarus_rus.pdf.

74 Президент Республики Беларусь, 2017. Декрет № 8 от 21 декабря 2017 г. [Online] Available at: https://president.gov.by/ru/documents/dekret-8-ot-21-dekabrja-2017-g-17716 [Accessed 31 July 2024].

75 HI Tech Park Belarus, n.d. Legal Framework. [Online] Available at: https://www.park.by/en/htp/legislation/ [Accessed 14 June 2024].

76 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by FATF in course of the mutual evaluation in June 2024. FATF, 2024. Outcomes FATF Plenary, 26-28 June 2024. [Online] Available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2024.html [Accessed 31 July 2024].

77 The Gazette of India, 2023. Notification 244184. Available at: https://egazette.gov.in/WriteReadData/2023/244184.pdf.

Republic of Kazakhstan[78]

Law 347 ZRK (June 2020): recognizes digital assets as property but prohibits their use as legal tender. Considering unsecured assets, cruptocurrencies can only be issued and traded within the Astana International Financial Center (hereinafter referred to as "AIFC").

Law 73-VII ZRK (November 2021): introduced AML/CFT obligations for digital asset issuers and traders. These entities must report their operations to the government maintaining a registry. The law also introduced taxes on digital asset mining.

Law 193-VII ZRK (February 2023): established state control, licensing, and more comprehensive taxation of digital assets.

AIFC Acts: regulate various DASPs and impose KYC and KYT procedures to prevent misuse for ML/TF, effectively checking not just every customer but their wallet too, having access to the full transaction history to look for possible traces of money laundering or TF.

AML/CFT Law of Kazakhstan, Article 3: introduced AML/CFT obligations for digital asset-related services and established red-flag indicators for suspicious transactions.

People's Republic of China[79]

China prohibits any transactions with cryptocurrency, with exceptions in its special administrative regions of Hong Kong and Macao. The People's Bank of China (hereinafter referred to as "PBC") launched its own digital currency project in 2014. However, then they have banned financial institutions from engaging with Bitcoin since 2013[80] and prohibited fundraising through ICOs since 2017[81]. The following regulations are in place:

- Cryptography Law (October 2019): established China's cryptography standards and procedures, and instituted the State Cryptography Administration (Article 5).
- Blockchain Information Management Regulations (January 2019): required registration for blockchain service providers.
- "Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation" (September 2021): reinforced the prohibition of cryptocurrency mining.[82]
- Other legal acts containing provisions on AML/CFT and VAs are "Counterterrorism Law" (December 2015)[83] and "Anti-Money Laundering Law" (October 2006).[84]

78 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by the EAG in course of the mutual evaluation in July 2023. ЕАГ, 2023. ОТЧЕТ взаимной оценки, Республики Казахстан. Available at: https://eurasiangroup.org/files/uploads/files/ME_(2023)_1_rus_rev1_2.pdf.

79 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by FATF in course of the follow-up in October 2020. FATF (2020), Anti-money laundering and counter-terrorist financing measures – People's Republic of China. 1st Enhanced Follow-up Report & Technical Compliance Re-Rating: FATF, Paris. Available at: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-china-2020.html.

80 The Central People's Government of the People's Republic of China, 2013. The People's Bank of China and five other ministries and commissions issued a notice on preventing Bitcoin risks. [Online] Available at: https://www.gov.cn/gzdt/2013-12/05/content_2542751.htm [Accessed 14 June 2024].

81 The People's Bank of China, 2017. Public Notice of the PBC, CAC, MIIT, SAIC, CBRC, CSRC and CIRC on Preventing Risks of Fundraising through Coin Offering. [Online] Available at: http://www.pbc.gov.cn/english/130721/3377816/index.html [Accessed 14 June 2024].

82 The People's Bank of China, 2021. Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation. [Online] Available at: http://www.pbc.gov.cn/en/3688110/3688172/4157443/4353814/index.html [Accessed 14 June 2024].

83 Standing Committee of the National People's Congress, 2018. Counter-Terrorism Law (as amended in 2018). Available at: https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/.

84 The People's Bank of China, 2006. Anti-Money Laundering Law of the People's Republic of China. [Online] Available at: http://www.pbc.gov.cn/fxqzhongxin/3558093/3558111/3561752/index.html [Accessed 14 June 2024].

Special administrative regions of China have their own provisions on VASPs.

- In Hong Kong, the AML/CFT Amendment Bill (December 2022)[85] sought to bring the "Anti-Money Laundering and Counter-Terrorist Financing Ordinance"[86] into compliance with FATF Recommendation 15. Hong Kong requires VASPs to register and obtain a license from the Securities and Futures Commission (hereinafter referred to as "SFC"), which regularly monitors licensed VASPs. The SFC may appoint an external auditor if it has reasonable cause to believe that the provider, or any of its associated entities, has failed to comply with any specified requirement.
- In Macao, the Financial System Act (1993) limits financial business only to financial institutions, credit institutions, and financial intermediaries were allowed to engage in financial business[87], meaning that VAs are not regulated. The Monetary Authority of Macao (hereinafter referred to as "AMCM")[88] issued several cautions against engagement with cryptocurrencies, emphasizing that they are not legal tender or supervised financial instruments.[89]

Kyrgyz Republic[90]

- Law 12 (July 2022)[91]: defines the legal status and requirements for businesses dealing with VAs, including VASPs, trading operators, cryptocurrency exchanges, and mining pools.
- Law 87 (August 2018)[92]: classifies VASPs as financial institutions and requires them to conduct CDD, report suspicious transactions to the State Financial Monitoring Service (Ministry of Finance), and comply with other AML/CFT requirements.
- Regulation 514 (September 2022): further regulates the circulation of VAs, folloqing Articles 16, 18, 25 and 28 of Law 12.
- Law 81 (August 2022): amended Law 87 to ensure VASPs comply with FATF Recommendations 10 through 21.

VASPs must be licensed by the Financial Market Regulation and Supervision Service (Ministry of Economy and Commerce) and can only operate as legal entities incorporated in the Kyrgyz Republic.

- Government Regulation 606 (December 2018): requires VASPs to follow the same KYC procedures as electronic payment systems.

85 The Government of the Hong Kong Special Administrative Region, 2022. Government welcomes passage of anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022. [Online] Available at: https://www.info.gov.hk/gia/general/202212/07/P2022120700263.htm [Accessed 14 June 2024].

86 Hong Kong Legislation, 2012. Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Amended 4of 2018 s.4). [Online] Available at: https://www.elegislation.gov.hk/hk/cap615 [Accessed 14 June 2024].

87 Macao Special Administrative Region, 1993. Decree-Law no.32/93/M of 5 July 1993 – Financial System Act. [Online] Available at: https://bo.io.gov.mo/bo/i/93/27/declei32_en.asp [Accessed 14 June 2024].

88 Autoridade Monetária de Macau. Available at: https://www.amcm.gov.mo/zh-hant/.

89 Government Information Bureau of the Macau SAR, 2014. Caution against Engagement in Bitcoin Transactions. [Online] Available at https://www.gcs.gov.mo/detail/en/N14FQ9bx3p;jsessionid=E815F0E3E733615115B98F1B19EC156F.app12. Monetary Authority of Macao, 2017. Alert to Risks of Virtual Commodities and Tokens. [Online] Available at https://www.iosco.org/library/ico-statements/Macau%20-%20AMM%20-%20Alert%20to%20Risks%20of%20Virtual%20Commodities%20and%20Tokens.pdf

90 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by the EAG in course of the follow-up in December 2023. EAG, 2023. Kyrgyz Republic: 5th Enhanced Follow-up Report (With Re-Rating). Available at: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Kyrgyz-Republic-FUR-2024.htm.

91 Закон Кыргызской Республики, 2022. О виртуальных активах, № 12 (В редакции Закона КР от 5 августа 2022 года № 81, 30 января 2023 года N 18). Available at: https://cbd.minjust.gov.kg/112346/edition/1220896/ru

92 Закон Кыргызской Республики, 2018. О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов, № 87 (В редакции Законов КР от 8 июля 2019 года № 83, 21 августа 2020 года № 139, 5 августа 2022 года № 81, 28 декабря 2022 года № 125, 7 февраля 2024 года № 38). Available at: https://cbd.minjust.gov.kg/111822/edition/2757/ru.

Russian Federation[93]

VAs are primarily governed by Federal Law 259-FZ (July 2020)[94]. Key points include:

- Digital financial assets (hereinafter referred to as "DFA") are defined as digitally represented rights, including pecuniary rights, rights to issued securities, and stakes in non-public joint stock companies.
- Investment platforms operators, information system operators, and DFA exchange operators are required to comply with AML/CFT obligations.
- DFA service providers must assess and mitigate ML and TF risks in compliance with AML/CFT obligations. As of the time of writing, legal frameworks for digital currency service providers are still in development.
- DFA providers must register as information systems operators or DFA exchange opertators. FIs and DNFBPs must evaluate and mitigate risks related to ML and TF.
- VAs are recognized as property, and international cooperation is guided by Russia's treaties and Article 1' of AML/CFT Law 115.[95]
- On 8 August 2024, the Russian Federation adopted a law classifying mining pools as AML/CFT entities,[96]and introduced an experimental legal regime for virtual assets.[97]

The Bank of Russia is the regulatory, controlling, and supervisory authority overseeing DFA service providers for AML/CFT compliance following a risk-based approach.

Tajikistan[98]

Tajikistan is still developing legal regulations for cryptocurrencies. The National Bank of Tajikistan has issued public warnings about the risks associated with cryptocurrency transactions and cautioned against investing savings in them. In April 2021, a working group on cryptocurrencies and blockchain technology was established.

Turkmenistan[99]

Despite the absence of specific legal acts regulating them, VAs can be recognized as property for AML/CFT/PF purposes. Individuals committing crimes using VAs are subject to criminal liability.

93 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by the EAG in course of the follow-up in December 2023. EAG, 2023. Russian Federation: 1st Follow-up Report (With Re-Ratings). Available at: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Russia-FUR-2024.html.

94 Президент России, n.d. Федеральный закон от 31.07.2020 г. № 259-ФЗ. Available at: http://www.kremlin.ru/acts/bank/45766 [Accessed 31 July 2024].

95 Президент России, n.d. Федеральный закон от 25.07.2002 г. № 115-ФЗ. Available at: http://www.kremlin.ru/acts/bank/18669 [Accessed 31 July 2024].

96 Российская Федерация, 2024. Федеральный закон от 08.08.2024 № 222-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Available at: http://publication.pravo.gov.ru/document/0001202408080023?ysclid=lzpltrbnzm9431578 [Accessed 12 August 2024].

97 Российская Федерация, 2024. Федеральный закон от 08.08.2024 № 223-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации." Available at: http://publication.pravo.gov.ru/document/0001202408080020?ysclid=lzpls67f58520364895 [Accessed 12 August 2024].

98 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by the EAG in course of the follow-up in June 2021. ЕАГ, 2021. Республика Таджикистан: Второй отчет о прогрессе в рамках усиленного мониторинга. Available at: https://eurasiangroup.org/files/uploads/files/Report_Tajikistan_2021_ru_1.pdf.

99 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by the EAG in course of the mutual evaluation in July 2023.

Republic of Uzbekistan[100]

- Presidential Decree 5120 (July 2017)
- Presidential Regulation 3832 (July 2018)[101]
- Presidential Regulation 3926 (September 2018) [102]
- Presidential Regulation 3150 (July 2017) [103]

The National Agency of Perspective Projects (hereinafter referred to as "NAPP") is in charge of developing and enforcing state policy for crypto assets, which prohibits the use of crypto assets as legal tender.

VASPs can offer services related to buying, selling, exchanging, custody, issuance, placement, and management of crypto assets. VASPs must be liceced as of 1 October 2018, and all transactions must be conducted only through registered VASPs as of 1 January 2023.

In addition to NAPP, VASPs are controlled by FIU Uzbekistan (Economic Crime Department, General Prosecutor's Office) for AML/CFT purposes and by other government authorities as appropriate.

- Law 660-II (September 2004): requires VASPs' compliance with CDD, record-keeping, suspicious transaction reporting, and internal controls.
- AML/CFT/PF Internal control rules: approved by NAPP and FIU in 2021 for persons engaging ni crypto asset circulation businesses,[104] amended as per the Updated FATF Guidance on RBA for VAs and VASPs.[105]

100 The level of implementation of the requirements of R. 15/INR. 15 FATF was assessed by the EAG in course of the mutual evaluation in August 2022. ЕАГ, 2022. Отчет взаимной оценки Республики Узбекистан. Available at: https://eurasiangroup.org/files/uploads/files/MER_Uzbekistan_2022_rus.pdf.

101 Президента Республики Узбекистан, 2018. О Мерах По Развитию Цифровой Экономики В Республике Узбекистан, № ПП-3832. Available at: https://lex.uz/ru/docs/3806048?ONDATE=04.07.2018%2000#3806419.

102 Президент Республики Узбекистан, 2018. О мерах по организации деятельности крипто-бирж в Республике Узбекистан, № ПП-3926. Available at: https://lex.uz/ru/docs/3891610.

103 Президента Республики Узбекистан, 2017. Об Организации Деятельности Национального Агентства Перспективных Проектов Республики Узбекистан, № ПП-3150. Available at: https://lex.uz/ru/docs/3280174.

104 National Project Management Agency under the President of the Republic of Uzbekistan, 2021. Resolution of the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan. [Online] Available at: https://static.norma.uz/documents/documents3/3309.pdf [Accessed 14 June 2024].

105 Департамент по борьбе с экономическими преступлениями при Генеральной прокуратуре Республики Узбекистан, 2022. Республика бюджетидан ажратилган маблағларнинг чегараланган миқдорининг ўз тасарруфидаги бюджет ташкилотлари кесимида тақсимоти тўғрисида. [Online] Available at: https://new-department.uz/ru/about/otkrytye-dannye/ [Accessed 14 June 2024].

VASPs supervision in the EAG region

As of 1 July 2024, five EAG jurisdictions have rules in place to address the AML/CFT aspects relating to for VASPs[106]: Belarus, India, Kazakhstan, Kyrgyzstan, and Uzbekistan.[107] While China prohibits VASPs and tokens, other countries are in the process of national consultations.

The lack of government regulation of VASPs does not hinder their operations; instead, it creates a favorable environment for the shadow economy. Many crypto exchanges and traders still operate outside legal frameworks by being unregistered in any jurisdiction, not identifying wallet owners, and failing to comply with legal requirements. As a result, terrorists can leverage this situation and exploit cryptocurrencies for illegal activities including ML and TF.

Under the AML/CFT internal control rules for VASPs in place since 2021 in Uzbekistan, VASPs are obliged to:

- Organize internal control and CDD systems;
- Assess their risks;
- Develop criteria, indicators, and detection procedure for suspicious transactions;
- Have measures and procedures in place for handling customers designated as terrorists/proliferators or terrorism/proliferation suspects;
- Have measures in place for complying with orders and requests of the authorized body;
- Have measures and procedures in place for documentation and storage and safeguarding of records.

These rules were enhanced as follows:

More requirements were introduced for founders of a VASP and for its internal controls officer;

Mandatory use of blockchain analytic software to identify other VASPs and wallets that customers have transacted with. The software should also include functionalities for risk-rating all customers' wallets based on the likelihood of their involvement in crime. For competition reasons, VASPs in Uzbekistan may choose any such software with the appropriate functionality.

In addition to a general rule that a commercial enterprise shall be registered in the country of incorporation, all crypto exchanges and traders are required to register or get a license in any country whose nationals use their services. This explains why centralized crypto exchanges tend to have multiple jurisdictional licenses.

106 VASPs in the EAG region include crypto exchanges, stores, traders, custodians, and mining pools.
107 The results of systematic monitoring of the effectiveness of national anti-washing systems provided by the EAG secretariat.

Detecting unlicensed/unregistered VASPs in the EAG region

EAG jurisdictions with registration/licensing requirements for VASPs, as well as law enforcement authorities, implemented various measures to detect shadow VASPs. These measures include conducting criminal intelligence operations (such as "controlled purchases") and acting on the back of FIU financial investigations. Additionally, provider details advertised either via websites, social media and/or anonymous messengers, should be matched with the known lists of licensed/registered providers. Lastly, fiat transactions should be analysed to uncover indicators suggesting a nexus with cryptocurrency transactions.

Kazakhstan

By way of example, in June 2023, an incorporated professional in Almaty, Kazakhstan, was fined for illicit trading in digital assets. The Financial Monitoring Agency (hereinafter referred to as "AFM") found him to have been offering cryptocurrency exchange services without a license between 2019 and 2022, extracting illicit proceeds roughly equivalent to USD 693,000.

Kazakhstan also takes action to detect unlicensed miners. In one such example, AFM together with the National Security Committee in Astana, terminated a major mining farm in February 2022, seizing 1,170 mining machines of four type.[108] The owners were indicted with illicit entrepreneurship (Article 214, Part 1 of the Criminal Code), the value of illicit proceeds (illegally mined cryptocurrency) was roughly equivalent to USD 2.5 million.

Uzbekistan

In Uzbekistan, a 2022 criminal intelligence operation of the FIU resulted in a successful apprehension of a person attempting to illegally sell bitcoins worth USD 224,000. The cryptocurrency was confiscated, while the person was indicted with, and later convicted for, illicit sale or purchase of currency[109,110] (Article 177 of the Criminal Code, Part 4, Paragraph A) and unlicensed business activity (Article 190 of the Criminal Code, Part 2, Paragraph A).

Belarus

In Belarus, the Investigative Committee together with the FIU (Financial Investigations Department, State Control Committee), disrupted operations of a major shadow crypto trader in Minsk in June 2023. Several persons were established to have created a criminal conspiracy in 2019 to buy foreign fiat currency and cryptocurrency illegally for the benefit of third parties. The organizers' illicit proceeds were reported as no less than BLR 9 million, roughly equivalent to USD 3 million. Illicit fiat and cryptocurrencies, as well as digital data carriers, were successfully seized at the suspects' residential and office properties. The suspects were then indicted for conspiracy to commit aggravated tax evasion.

The basic VAs restriction in Belarus is that natural persons can engage in cryptocurrency transactions only if they are HTP residents. The penalty for non-compliance is a fine of up to 100 "basic units" (1 "basic unit" = BLR 40 in 2024) and confiscation worth the entire turnover of the crypto wallet. According to a report for the first half of 2023, 27 Belarusian nationals were apprehended for illegally exchanging cryptocurrency for cash, having collectively generated illicit proceeds worth BLR 22 million, equivalent to USD 7.2 million.[111]

108 SBC Eurasia, 2023. The Financial Monitoring Agency of Kazakhstan To Investigate 1Win's Illegal Activities. [Online] Available at: https://sbceurasia.com/en/2023/08/24/the-financial-monitoring-agency-of-kazakhstan-to-investigate-1wins-illegal-activities/ [Accessed 31 July 2024].

109 Kun.uz, 2020. В Ташкенте правоохранители задержали незаконного торговца биткоинами. У него изъяли $400 тысяч. [Online] Available at: https://kun.uz/ru/33646214?ysclid=lz44fmk7lu196115164 [Accessed 01 August 2024].

110 Газета.uz, 2021. Двое мужчин задержаны при продаже криптовалюты в Ташкенте. [Online] Available at: https://www.gazeta.uz/ru/2021/03/05/bitcoin/ [Accessed 01 August 2024].

111 https://sk.gov.by/ru/news-ru/view/presechena-dejatelnost-krupnogo-tenevogo-kriptoobmennika-na-territorii-minska-12622/

Role of FIUs in countering the misuse of VAs for TF in the EAG region

Several EAG FIUs have specialized units focused on combating the illicit use of VAs. Additionally, EAG FIUs conduct parallel financial investigations leading to the detection of TF activities.

In Russia, according to the Joint CFT Communication Instruction adopted on 18 April 2024, law enforcement authorities are obliged to report all terrorist crimes to Rosfinmonitoring.[112] A copy of all related documentation must also be provided to enable the FIU to start a parallel financial investigation.

EAG-wide cooperation

EAG has the following objectives:

- Assisting its member jurisdictions in implementing the FATF Recommendations;
- Designing and conducting joint action against money laundering and TF;
- Performing mutual evaluations of its member jurisdictions' compliance with the FATF Recommendations and effectiveness of measures they take to combat money laundering and TF;
- Coordinating international cooperation and technical assistance programs with specialized international organizations, bodies, and interested jurisdictions;
- Analyzing money laundering and TF trends (typologies) and facilitating the sharing of best regional practices of combating money laundering and TF.[113]

The EAG Working Group on Typologies and Combating TF and Crime (WGTYP) focuses on systemic typology work, identifying key threats and vulnerabilities in the Eurasian region. It also drafts handbooks and guidance for competent authorities and red-flag indicators of suspicious transactions for the private sector.

EAG Plenaries have contributed to the progress made in addressing the risks associated with VAs and their misuse for criminal purposes. On 21 November 2022, the 37th EAG Plenary approved a final report on the project "Laundering of, and financing terrorism with, cybercrime proceeds, including through e-money, VAs, and provider infrastructure misuse".[114]

Subsequently, on 6 December 2022, the 37th EAG Plenary approved an interim report on the project "Monitoring the risk of misuse of VAs for criminal purposes" (project launched at the 35th Plenary). A further interim report on the same project was approved on 7 December 2023, during the 39th EAG Plenary. The report focused on the cross-border nature of VAs and the importance of international cooperation.[115]

112 Joint CFT Communication Instruction, approved on 18 April 2024, by joint order 89/290/149/195/61 of Federal Financial Monitoring Service, General Prosecutor's Office, Federal Security Service, Ministry of Interior, and Investigative Committee of the Russian Federation.

113 Agreement on the Eurasian Group on Combating Money Laundering and Financing of Terrorism. Available at: https://eurasiangroup.org/files/uploads/files/01_Agreement_16.02.2024_eng.pdf.

114 EAG, 2022. "Legalization (laundering) of the proceeds of cybercrime, as well as financing of terrorism from the said offence, including through the use of electronic money or virtual assets and the infrastructure of their providers." Available at: https://eurasiangroup.org/files/uploads/files/other_docs/WGTYP_(2022)_12_rev_1_eng.pdf.

115 https://eurasiangroup.org/d.php?doc=294385e683357e3d66820a48a7388314 (access rights are required)

08

Detecting & investigating TF with the use of VAs in the EAG region

Effective cryptocurrency crime detection relies on FIU's and law enforcement's blockchain expertise, understanding of VASPs, and ability to secure electronic traces.

Detection and investigation techniques vary among cryptocurrencies, necessitating tailored transaction monitoring and wallet owner identification procedures for effective investigation.

Understanding the unique characteristics of each cryptocurrency is also crucial for preserving electronic traces, identifying wallet owners, and facilitating confiscation efforts.

In addition, the introduction of standardized procedures for transaction monitoring and wallet owner identification across different cryptocurrencies are required alongside adjustments to legal frameworks, aiming for uniformity in investigative methods to improve efficiency and effectiveness.[116]

116 FATF, 2023. Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2023). [Online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

Challenges detecting and investigating TF with the use of VAs

Authorities detecting, identifying, and investigating such activity should consider the following challenges:

- Identifying criminal (mis)use of cryptocurrency;
- Identifying the true owner of a cryptocurrency wallet;
- Identifying, seizing and confiscating cryptocurrencies relying on VASPs, given that many VASPs are unregulated and do not comply with KYC/AML requirements;
- Determining the fair value of cryptocurrency in fiat currency at the time of the crime, in turn complicating the formal description and assessment of the harm caused;
- Retrieving transactions, or seizing, confiscating and recovering illicit VAs;
- VASP operations may physically be based anywhere and without a clear ownership structure;
- Criminals tend to use anonymization and encryption softwares, and may create a new cryptocurrency wallet for each illicit transaction;
- In most countries, there are gaps in formal procedures of detecting, securing and retaining electronic and other traces of crimes committed with the use of VAs.[117]

In most cases, the use of cryptocurrencies in the commission of a crime is established post factum during investigations of traditionally committed crimes. Timely detection of cryptocurrency-related crime typically occurs when VAs are stolen or misappropriated – such as in the case of fraud when victims report illegal losses of their cryptocurrency – or when law enforcement authorities undergo wallet monitoring already associated with criminal activity.[118]

Tracing cryptocurrency transactions

Criminals may use anonymity-enhanced cryptocurrencies that conceal all or part of transaction data on the blockchain, such as originator and beneficiary addresses and transaction value. At the time of writing, the most popular anonymity-enhanced cryptocurrencies are Monero, Dash, Zcash, SmartCash, Pivx, Verge, Horizen, Navcoin, and Komodo. However, to convert even such cryptocurrencies into fiat money, criminals may need VASPs, which may require customer identification, thus opening a possibility of identifying the owner of a wallet.

117 Tisen O.N. Proving crimes committed using cryptocurrencies // Criminological Journal. – 2023. – No. 2. – pp. 152-157.

118 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

Finding TxID

Sequence of actions to trace a transaction using a block explorer:

1. Access the block explorer website;
2. Open the bitcoin tracker;
3. Paste the TxID or wallet address in the query bar;
4. Press Enter; and
5. Copy the data on verified transactions.

Bitcoin explorers provide the following transactions data:

- Block ID;
- Originator and beneficiary addresses;
- TxID;
- Number of verified transactions, status of all transactions;
- Date of a specific transaction;
- Volume of the transaction in bytes;
- Incoming and outgoing aggregate amounts;
- Commissions charged by the exchange or trader;
- Whether Accelerate function was used for the transaction;
- Overall "transaction plus charges" amount.

General-purpose explorers lack advanced visualization capabilities, presenting transaction data in a complex text format that requires significant time and effort to parse manually. These tools do not facilitate regular monitoring of wallets and often lack support for directly matching wallets to VASPs, thereby complicating the identification of wallet owners. While enhanced explorers with these functionalities are available, they are typically offered on a subscription basis.[119] Furthermore, as with any open-source intelligence effort, it is crucial to conduct transaction research on a secured platform.

119 The results of the analysis of open blockchains. The information has been confirmed by the participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

Finding the transaction timestamp

Open blockchains show transaction timestamps typically in Greenwich Meantime (GMT).[120] However, to document the time of commission of the crime, it is important to keep in mind the time zone difference.

Timestamp misinterpretations may result in the wrong understanding and distortion of the actus reus, creating false alibis or ruining genuine ones and otherwise making proof of a crime more challenging.

Transparent Blockchain and its use by EAG jurisdictions

Many EAG jurisdictions analyze cryptocurrency transactions using 'Transparent Blockchain,' a blockchain browser developed by Rosfinmonitoring and offered on a free basis to government and law enforcement partners.[121] Transparent Blockchain provides means to trace cryptocurrency transactions and facilitates communication with VASPs when identifying wallet owners. It offers – at the time of writing – an extensive functionality among blockchain analytical tools accessible to most EAG users.[122] In addition to the more conventional functionality, Transparent Blockchain works on its own risk-rating model and runs its own database of wallets and their connections to cryptocurrency exchangers and traders. As an automatic crawler collects data from websites, social media, and the DarkNet, the analytical engine parses the data for wallet addresses and risk indicators.[123] As of the time of writing, Transparent Blockchain covers over 30 of the most popular cryptocurrencies.[124] [125]

The Transparent Blockchain database continuously updates its wallet-to-VASP and wallet-to-owner matches and risk rates. Each user can run their own filters to focus on a specific trader, wallet, or transaction – only visible to them – and generates reports tailored to the needs of law enforcement users. Correct transaction timestamps, matches to VASPs, and transaction values are important for correct documentation of the crime and determination of the value of assets used in the commission of the crime.

By the transaction (or wallet) address, a user can trace transactions upstream and downstream with analytically determined characterization of each transaction ("exchange," "payment," "transit" etc.). A Transparent Blockchain report can be the basis of a law enforcement intelligence-sharing request to the national or foreign FIU for more information on the wallet owner.

120 The time differences between GMT (also known as "Coordinated Universal Time" or UTC) and EAG time zones are Moscow / Minsk = UTC + 3, Ashgabat / Dushanbe / Tashkent = UTC + 5, New Delhi = UTC + 5:30, Astana / Bishkek = UTC + 6, Beijing = UTC + 8. Also, various countries and regions have their own complex and changing rules of "daylight saving time."

121 ЕАГ, 2023. Методические рекомендации ЕАГ по организации и проведению финансовых расследований в сфере ПОД/ФТ. Available at: **https://eurasiangroup.org/files/uploads/files/Public_typology_reports/FI_Guidence_rus.pdf**.

122 Tadviser, 2023. В Росфинмониторинге рассказали, как работает система «Прозрачный блокчейн». [Online] Available at: **https://www.tadviser.ru/index.php/Продукт:Прозрачный_блокчейн** [Accessed 01 August 2024].

123 ЕАГ, 2023. Методические Рекомендации ЕАГ по организации и проведению финансовых расследований в сфере ПОД/ФТ. Op. cit.

124 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

125 Forbes, 2020. Финразведка решила следить за сделками с биткоином с помощью искусственного интеллекта. [Online] Available at: **https://www.forbes.ru/newsroom/tehnologii/406797-finrazvedka-reshila-sledit-za-sdelkami-s-bitkoinom-s-pomoshchyu** [Accessed 01 August 2024].

Identifying the wallet owner in EAG countries

Given the lack of a central authority governing cryptocurrencies, there are two ways of identifying a cryptocurrency wallet owner:

A. Communicating with VASPs, mostly effective when cryptocurrency-related crime has already been established by the FIU or law enforcement authorities. However, this may be difficult if the target VASP operates in a country that does not regulate VAs and does not require its VASPs to verify customer information.

B. Seizing a private key as part of a criminal intelligence or public investigation (e.g. where private keys are retrieved from suspects' devices or premises in executing a search warrant).

EAG countries mostly use the following ways to identify the owner of a cryptocurrency wallet:

- Using heuristics, cluster and graph analysis to match different sources of information;
- Matching the activity history of the targeted cryptocurrency wallet to IP and MAC addresses of the suspect's devices, their social media account and DarkNet browsing histories;
- Analyzing digital fingerprints;
- Web crawling and using open-source intelligence to aggregate data;
- Obtaining wallet data from VASPs;
- Matching the wallet history to online buying history;
- Following the IMEI of the targeted devices.[126]

Proving cryptocurrency ownership

Law enforcement agencies of EAG Member States use the following factors to suggest cryptocurrency ownership:

- Possession of the private key (where such a private key was found on a suspect in the context of a terrorism-related investigation, or on their device, or on their premises in executing a search warrant or examining the scene of the crime);
- The fact that the person opened the cryptocurrency wallet and used a VASP that has their customer information (however, criminals may use the identification of a third person who may not be aware of the fact or of the fact that their identification was used for criminal purposes);
- The fact that the user's email address and telephone number match those provided to the VASP for wallet registration;
- The fact that an IP address matched to the suspect was used to access a wallet;
- The fact that the suspect's physical movements match geolocation stamps provided by the VASP;
- Possession of the device with IMEI recorded by the VASP as that of the wallet owner;
- Legal evidence documenting the suspect's access to a cryptocurrency wallet;
- Documented fact(s) that the suspect has posted online (on websites, social media, messaging apps etc.) the open key (address) of a particular wallet as owned by him/her;
- Witness testimony;
- The fact that the suspect used a wallet address to collect funds;
- The fact that the user's nickname (alias) coincides with a nickname identified as that of an suspect in the course of an investigation.[127]

126 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

127 Presentation by O.N. Tisen at events organized within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023). Tisen O.N. Identification of owners of crypto wallets, detection and seizure of private keys in the investigation of criminal cases. // Criminal process. 2024 No. 1. pp. 78-84.

EAG jurisdictions have a track record of proving cryptocurrency wallet ownership by submitting as evidence, including to criminal courts, notary executed paper documents reproducing the procedure of online data review.[128]

Getting user identification data from a VASP

In EAG jurisdictions regulating VASPs, law enforcement authorities typically have powers to obtain certain information from them directly as financial intermediaries or as part of their power to "request information from other natural and legal persons." Conversely, this is more challenging where VASPs are not regulated, as it requires involving criminal intelligence and/or resorting to FIU powers and resources. Some cryptocurrency exchanges and traders already comply with customer identification requirements even though particular jurisdictions where they operate may not yet have the appropriate requirements in place.[129]

FATF-compliant[130] VASPs are obliged to collect the following customer information:

- full name (given name, family name, patronymic where appropriate) and date of birth;
- date and number, and a copy of, the identification document;
- citizenship and postal address;
- photo;
- telephone number and e-mail address.

Most VASPs also collect the following customer data:

- IP addresses;
- VPN use and real IP address if an anonymizing application was used;
- geolocation;
- access device data;
- activity logs, statistics on preferences, etc.

In response to a law enforcement request or production order, a VASP should also provide:

- the beneficiary account number, date and time of creation;
- the transaction status (executed, closed, etc.);
- outgoing as well as incoming amounts for crypto-to-fiat currency transactions.

128 Judicial practice of the Russian Federation: Ruling of the Second Cassation Court of General Jurisdiction dated 05/26/2022 in case No. 88-11775/2022, 2-1291/2020; Rulings of the Third Cassation Court of General Jurisdiction of the Russian Federation dated 10/04/2023 No. 88-19394/2023, dated 06/03/2024 No. 88-11752/2024 (UID 11RS0010-01-2023-000042-56), from 06/26/2023 No. 88-11425/2023 in case No. 2-24/2022; Rulings of the Fourth Cassation Court of General Jurisdiction dated 12/06/2022 in case No. 88-37546/2022, dated 03/01/2023 No. 88-9876/2023, dated 07/04/2023 in case No. 88-19419/2023; Rulings of the Sixth Cassation Court of General Jurisdiction dated 07/11/2023 in case No. 88-12757/2023, dated 01/23/2024 in case No. 88-796/2024, dated 25.10.2022 № 88-22066/2022, 28.05.2024 № 88-12345/2024; Rulings of the Seventh Court of Cassation of General Jurisdiction dated 07.09.2023 in case No. 88-14946/2023, dated 05/24/2022 No. 88-7022/2022; Rulings of the Eighth Court of Cassation of General Jurisdiction dated 12.12.2023 No. 88-24608/2023, dated 08/02/2022 No. 88-15053/2022 in case No. 2-73/2022, etc.

129 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

130 FATF, 2021. Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers, op. cit. Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

Production of evidence in EAG countries

What qualifies as evidence?

In criminal trials within EAG countries, courts typically accept as evidence tangible objects, documents or testimonies relevant to crimes involving cryptocurrencies, including but not limited to:

- Formal report from forensic examination of electronic devices, "cold"/hardware crypto wallets, and cryptocurrency transactions history;
- Digital forensic reports identifying ownership and use of cryptocurrency, expert testimony on transaction nature and contents of seized devices, and responses from VASPs to law enforcement requests;
- Data from cellular carriers identifying owners of matched phone numbers, phone contacts suggesting complicity, geolocation/phone billing data, chat or call histories, and geo- and timestamps of access to online resources from a particular device;
- Forensic reports of group chats, exchanges between transaction originator and beneficiary, and records of interrogation of suspects or witnesses on circumstances pertaining to the crime;
- Testimonies on the suspect(s)' personality, behavior and views;
- Reports of search and seizure of material on private key (notebook, post-it, etc.);
- IP, IMEI and MAC addresses of accessed devices;
- Evidence from VASPs, or records of interrogation of their employees;
- Forensic reports from credit institutions on fiat transactions, suspect-owned account statements, and forensic accountants' analyses of fiat transactions, along with photo and video documentation of cash withdrawals and formal reports of data extraction from blocked devices.[131]

131 Presentation by O.N. Tisen at events organized within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

Detecting and preserving VA-related digital evidence in EAG countries

When investigating cryptocurrency-enabled crimes, close attention is paid to details, as losing crucial information can make solving the crime and seizing and confiscating cryptocurrency impossible. In TF investigations, it would be essential to locate and securely preserve all electronic devices by involved individuals, as well as all relevant electronic and physical traces, and any carriers of cryptocurrency wallet private keys.

To understand possibilities for freezing, seizing, and confiscating cryptocurrency obtained illegally or intended for use in TF or other criminal activities, an investigator would be expected have a clear idea of the types of wallets and exchanges or traders involved.

An important tactical step in a criminal investigation is planning measures to prevent device owners from deleting evidence. Modern software has numerous possibilities for remote data access and device control, thus allowing the transferring of cryptocurrency to another wallet controlled by an accomplice in just few seconds. It is therefore important to ensure that a suspect does not have the possibility to use their device even for short periods of time between start of action and physical device seizure, and to switch off the seized device or put it in the "flight mode" immediately after seizure.

Most personal devices are secured by PINs, patterns or swipes, face or fingerprint recognition. If there is no possibility to unblock the device on the scene, such a device may be sent to an electronic forensic unit to break through security and extract data.

Records of open and private keys to cryptocurrency wallets may be stored electronically on personal electronic devices or data carriers or in hard copy and can be found in a search or forensic review operation in a suspect's home, workplace or place of temporary stay.

Typical ways to store a wallet key include a computer file, a smartphone "note," or a line of characters written in a notebook or on a post-it stuck to a computer display or otherwise located in the vicinity. Investigators are mindful of all possible ways a private key can be stored and would be expected to identify all relevant objects and preserve them to the extent possible. If a private key, e.g. written on a post-it, is inadvertently destroyed, and there is no copy stored elsewhere, the wallet will be lost irretrievably, even if the suspect becomes cooperative.

EAG law enforcement authorities have a track record of using measures and devices to block internet connections, cellular and WiFi signals once search and arrest operations against organized criminal groups known to use cryptocurrency are initiated.[132]

It is also important to immediately preserve a seized device for fingerprinting to prove handling of the device and provide evidence against a suspect's possible statements, if they are aware the device would be established as a cryptocurrency wallet access point, that they do not own the device in question.

The accepted practice among investigators of cryptocurrency-enabled crimes in EAG countries is to seize any electronic devices found on the suspect, or in their home, or in the vicinity, and extract data from all of them as part of further criminal intelligence or public investigation.

If a review of an unsecured electronic device is deemed relevant, investigators should focus on high-level indicators of wallet/cryptocurrency service ownership and use. These indicators include emails from cryptocurrency exchanges or traders confirming access to and use of a cryptocurrency wallet, transaction records, and cryptocurrency-related search queries in browser history.

132 Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism. The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

Additionally, written exchanges with VASP customer support, and files containing passwords, and open and private keys are crucial. Similarly, websites and messaging app views confirming access to closed group chats and posts calling for fundraising or reporting transactions need to be taken into account as such indicators. Relevant pictures, videos, text, or archive files, as well as traces of applications providing access to cryptocurrency wallets – such as password files or activity logs – are to be examined. Other pertinent information that may be relevant to the crime or ensure the freezing, seizure, or confiscation of the cryptocurrency must be considered as well.

Preservation of electronic traces in such cases needs to be consistent with the basic features of blockchain, cryptocurrency wallets, and keys (see Chapter 5).

While a "cold" wallet seizure typically means a high likelihood of subsequent seizure and confiscation of the illicit cryptocurrency, a software-based "cloud" wallet makes it possible to access cryptocurrency from any smartphone, tablet, or computer. Traces of the latter type of wallets may be found by forensic examination.

To avoid overlooking hardware wallets and private keys, stored electronically or on paper, law enforcement officers are to keep in mind their possible types, shapes and traits (see Chapter 5).

Another object relevant to cryptocurrency-enabled crimes is a "seed phrase," typically a string of 12, 18, or 24 random English words that need to be reproduced in a particular sequence to recover lost private keys. A seed phrase helps get access to a wallet even if the owner is uncooperative.

Procedural action in EAG countries

According to FATF's updated guidance on VAs and VASPs, countries are expected to implement comprehensive measures to manage and mitigate the risks associated with VAs.[133]

All government actions performed vis-à-vis cryptocurrency need to be recorded in a step-by-step manner on paper, photographs or video records, with experts or witnesses present as needed. The record must include wallet and cryptocurrency data, the name and other details of the crypto exchange or trader, and transaction information. Records also include details about the involvement of the suspect in evidence collection, e.g. in disclosing private key(s) [see further below in 'Cooperative suspect/defendant in EAG countries'].

The record needs to detail the review process and findings of the electronic device, including the power-on status, security measures (such as passwords), main screen/desktop view and contents, relevant files and their contents, and actions taken to access these files.

If the device has a cryptocurrency software (application), the wallet balance and transactions history must be annexed to the record, ensuring time synchronization with the government agents' device for accurate data sharing. Copying data from suspect devices is crucial for preserving traces of cryptocurrency-enabled crimes, whether or not the devices are seized.

The make, model, type, and name of law enforcement device(s) are to also be recorded.

If written exchanges between the VA originator and beneficiary are found on devices or on social media or messaging apps, they need to undergo (psycho-) linguistic expert review to determine the possible intent-and-knowledge (mens rea) element of the crime. The review can be performed in any form (written or oral text), or combined material (e.g. video or audio recordings with static graphics) and may involve experts in various fields as appropriate (e.g. linguists, psychologists, religious scholars, or political analysts).

133 FATF, 2022. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, Paris: FATF/OECD. Available at: **https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.inline.pdf**.

Communicating with VASPs for evidence in EAG countries

Customers of a centralized cryptocurrency exchange conduct transactions within its infrastructure. Thus, these transactions will appear on the blockchain as those of the exchange. Most centralized exchanges operate in multiple jurisdictions, posing challenges for those EAG jurisdictions that do not yet impose AML/CFT obligations on VASPs.

In EAG countries with a legal framework for VASPs, both national and foreign VASPs with significant presence must register or obtain a license, providing opportunities to access information.

A. VASPs and crypto exchanges de facto conduct customer identification even if not required by the customer's country. Consequently, they usually provide customer data to law enforcement authorities pursuing a suspect.

B. If VASPs and crypto exchanges are an AML/CFT reporting entity in a partner jurisdiction, the FIU or a law enforcement authority in a jurisdiction without AML/CFT coverage for VASPs can request customer data through intelligence-sharing partners.[134]

EAG jurisdictions use the following methods to obtain information from cryptocurrency exchanges and traders:

A. Where VASPs are reporting entities, law enforcement can formally and directly request customer information, and compliance is compulsory. Depending on the legal framework, law enforcement authorities may need to send their request to a VAs coordinating body, which then relays them to the obliged entity.

B. Where VASPs are not reporting entities, authorities can still request information directly from the VASP, as many comply voluntarily. For uncooperative VASPs, authorities may conduct criminal intelligence operations or request it as part of an ongoing formal criminal investigation. Authorities can also request information from the FIU in the country where the VASP is registered or send a mutual legal assistance request to competent authorities of the country, though the latter typically takes longer.[135]

The FATF 2021 Guidance highlights the critical need for international supervisor-to-supervisor cooperation, in view of the cross-border nature of VAs businesses. To address the ongoing "sunrise issue," FIUs should enhance their international connections and use secure encrypted communication channels.

In the EAG region, government-to-VASP cooperation is not without promise. For example, FIU Kazakhstan signed an MoU with Binance in October 2022 to share information and block VAs obtained illegally or involved in ML/TF activities.

134 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

135 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

Cooperative suspect/defendant in EAG countries

In cryptocurrency-enabled cases led by EAG countries, defendants tend to be offered guilty plea deals. Examples of guilty plea deals include instances in which the plea agreement includes the defendant's commitment to disclose all facts related to the use of VAs in the crime, details of transactions and wallets, the VASP involved, types and volumes of VAs, and information on all conspirators and relevant electronic devices. Per these examples, a defendant could be expected to provide information on cryptocurrency wallets and keys, persons with access to them, crypto-to-fiat conversion mechanisms, and fiat money movements. Additionally, the agreement at times has obligated the defendant to prevent unauthorized disclosures, explain relevant transactions, cooperate in identifying and confiscating illicit cryptocurrency, and assist in controlled crypto-to-fiat conversions.[136] If cooperative, the defendant could participate in a joint examination of a fiat bank account statement with law enforcement and a bank officer to identify transactions related to crypto-to-fiat conversions.[137]

Interrogations

In addition to conventional information on the circumstances of crime, in cryptocurrency-enabled cases it is important to establish, for the record:

The fact of cryptocurrency wallet ownership;

- Type(s) of cryptocurrency used;
- Open and private keys;
- Type(s) of wallet(s) and access options;
- Electronic devices used for access to cryptocurrency;
- Places and ways to store cryptocurrency wallet passwords;
- VASPs used;
- Ways of crypto-to-fiat conversion used;
- Credit institutions and accounts used for such conversions;
- Any separate platform for crypto-to-fiat conversions, crypto-to-fiat exchange rates;
- Wallet address.

Pre-trial restrictions in EAG countries

When requesting pre-arraignment/pre-trial restrictions for suspects or defendants, investigators should consider that cryptocurrency can be easily accessed from any connected device, and private keys can be transferred electronically or through overlooked cold wallets, risking the dissipation of illicit assets. Therefore, simultaneous actions against all known members of a criminal group, including immediate searches and seizures of electronic devices and preservation of electronic traces, have been observed. For suspects not detained pre-trial, reasonable restrictions per the practice of EAG countries have included a general restraining order prohibiting electronic communication, no-contact orders with specific individuals, and temporary dismissal from office if the suspect is a VASP employee. In some jurisdictions, cryptocurrencies may be used as bail bonds, even if they are not considered legal tender.

136 Judicial practice of the Russian Federation: Appellate Rulings of the Moscow City Court dated 06/09/2022 No. 10-8888/2022, dated 03/01/2021 in case No. 10-573/2021; Appellate Ruling of the Second Court of Appeal of General Jurisdiction dated 02/07/2023 No. 55-21/2023; Ruling of the Sixth Court of Cassation of General Jurisdiction dated 05/14/2020 No. 77-668/2020 Appellate ruling of the Second Court of Appeal of General Jurisdiction from 11.12.2020 in case No. 55-592/2020; Verdict of the Sverdlovsk Regional Court dated 31.01.2019 in case No. 2-5/2019, etc.

137 Tisen O.N. Identification of owners of crypto wallets, detection and seizure of private keys in the investigation of criminal cases. // Criminal process. 2024 No. 1. pp. 78-84.

Forensic reviews in EAG countries[138]

(Psycho-) Linguistic review	In a TF case involving cryptocurrency, a linguistic review aims to determine if evidence suggests that the transaction originator was aware of the recipient's intent to use the assets for TF, and if the beneficiary's fundraising efforts indicated an intent of TF. This review of evidence assesses the content, form, and context of communications, such as posts or messages, to provide proof of intent, or lack thereof. Insights into the individual's behavioral patterns, interests, dispositions, and history may also be relevant to understand if they were aware of the true nature of their actions.[139] The Forensics Center of the Russian Ministry of Interior (hereinafter referred to as "FCMI") is an EAG example of use of linguistic reviews in TF cases, as it employs methodologies for such reviews, analyzing visual, audio, and textual evidence to ascertain possible intent or knowledge of TF activities.[140] Linguistic reviews can provide evidence relating to data on fundraising and fund movement, verbal cues of terrorist intent, indicators of conspiratorial activities, and the roles of criminal conspirators. Key questions for linguists include whether the text in evidence incites or justifies fundraising, the roles of interlocutors, and if the message conceals the true intent of transactions.
Device examination	To detect and preserve electronic traces evidence of VAs use in the commission of a crime, seized electronic devices should undergo a professional forensic review. This review should identify and preserve personal communication files (e.g. emails or chats), graphic, video and text files, cryptocurrency software, wallet data and transaction logs, alongside other relevant data.
Authorship attribution review	In a TF case involving VAs, an authorship attribution review can help determine if written texts can be linked to a specific person suspected of cryptocurrency management for terrorists. It can also identify if the text's author belongs to a particular group, like sex, age, or occupation, aiding in locating and identifying the suspect.
Phonoscopic review	A phonoscopic review (also known as "forensic voice comparison") can be valuable in TF cases to determine if a voice recording can be attributed to a specific person or if multiple recordings belong to the same individual. It can also identify features like specific accents or attempts to disguise the voice.

138 https://мвд.рф/вопросы/вопросы-по-линии-экц-мвд-россии?ysclid=lz47i30h4835117277
139 Tisen O.N., Gromova A.V. Appointment of expertise in cases of terrorism on the Internet // Criminal proceedings. 2022. No. 4. pp. 78-81.
140 https://мвд.рф/вопросы/вопросы-по-линии-экц-мвд-россии?ysclid=lz47i30h4835117277

09

Proving TF with the use of VAs in EAG countries

Object of proof in TF cases in the EAG region

In the EAG region, a TF investigation focuses on proving two main elements:

A. The ***actus reus***, which involves establishing the fact of providing financial or other support to a person involved in terrorist activity, the method of support, and its volume; and

B. The ***mens rea*** involves demonstrating that the person providing support knew it would be used for preparing or committing a terrorist act, benefiting a terrorist organization or its members, or aiding someone who provides services to a terrorist group. This applies regardless of the purpose, whether it be for terrorist acts or everyday needs.[141]

Proving mens rea: how to confirm intent to use VAs for TF

To confirm intent to finance terrorism, an investigation should establish that the suspect knew that the beneficiary of their support was involved in terrorist activity, i.e., including, but not limited to:

- Was a member or an active supporter of a terrorist organization; or
- Had participated in preparations for, or commission of, terrorist acts, or had committed terrorist acts before; or
- Was located in a terrorist activity area; or
- Intended to use the support to finance their travel (purchasing transport services and providing for other travel expenses) to a location where they would participate in terrorist activity.

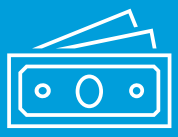
141 Tisen O.N. Features of the identification, investigation and qualification of crimes related to the financing of terrorism. Monograph. – M. Publishing House Pero, 2023. – 160 p.

In cases where cryptocurrency was transferred to wallets promoted through social media or messaging applications under the guise of charitable donations, judicial bodies have deemed the following types of evidence as substantiating the claim that the donor was cognizant of the funds being utilized for TF activities:

- Preserved screenshots (with stamps of time and location where the shot was taken) confirming that a charity call was posted in group, chat, or channel;
- Preserved screenshots (with stamps of time and location where the shot was taken) confirming that the group, chat, or channel systematically posted messages inciting the commission of terrorist acts;
- Preserved screenshots (with stamps of time and location where the shot was taken) of the comments under, or notes to, the post in question, confirming the mens rea of fundraisers and supporters;
- Records of written exchanges or audio records of telephone conversations between the originator and the beneficiary of funds, confirming the true intent of the latter;
- Records of cryptocurrency transfers made with captions confirming originator's knowledge of the true intent of the beneficiary;
- Records of exchanges between the originator and the messaging app group/channel administrator, confirming the true intent of the transactions;
- Data confirming that the originator's or beneficiary's wallet had been used for TF;
- Witness testimonies that the originator had been involved with TF.[142]

The current corpus of criminal case and criminal trial reports indicates that cryptocurrency-enabled TF in the EAG region mainly manifests in three ways:

1



Professional fundraisers within terrorist organizations orchestrate financing efforts.

2

Social media and messaging platforms are used to broadcast calls for cryptocurrency donations.

3

Criminal networks are established specifically to provide material support to terrorists, facilitated by cryptocurrency transactions.

142 Tisen O.N. Identification of owners of crypto wallets, detection and seizure of private keys in the investigation of criminal cases. // Criminal process. 2024 No. 1. pp. 78-84. Presentation by O.N. Tisen at events organized within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

These groups typically operate by posting appeals for cryptocurrency donations and wallet addresses on social media and messaging apps. They collect donations, transfer funds to facilitate access by terrorists, and convert cryptocurrency into fiat currency or use it directly to procure goods for terrorists.

Proving the beneficiary's involvement in terrorism and TF cases is crucial, but the use of third-party bank accounts or cryptocurrency wallets does not affect guilt. Online terrorist fundraisers often act as organizers within their groups.

Certain circumstances can provide reasonable grounds to initiate a TF investigation. For example, managing or participating in social media chats or groups that propagate terrorist content and solicit funds for terrorism can initiate investigations. Likewise, initiating or coordinating TF independently or through criminal networks aimed at supporting terrorism could be considered grounds for investigation. Convicted terrorist financiers have frequently been identified as supporters of particular terrorist organizations or of terrorism in a broader context.

These individuals have been known to allocate funds for various purposes, ranging from routine operational expenses to potentially facilitating the acquisition of weapons or conducting attacks. Notably, the Russian Federation has specifically criminalized the provision of financial support for travel aimed at joining terrorist groups since 2014. This legislative action underscores a targeted effort to curtail the logistical support provided to individuals seeking to engage with terrorist organizations.[143,144]

EAG courts consider as proof the originator's awareness that funds may be used for terrorism. Suspects often deny awareness, citing alternative reasons for transactions, but courts typically reject these defenses if comprehensive evidence, including witness testimonies and communications, indicates awareness.

The prevailing judicial formula is that providing financial support to a terrorist organization implies awareness that the funds could be used for terrorist crimes. This principle is commonly upheld in Russian courts, recognizing such actions as deliberate.

143 FATF (2016), Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, op. cit.
144 Tisen O.N. Tracking cryptocurrency transactions in order to investigate crimes // Criminal process. 2024. No. 2.

10

Seizing, confiscating & recovering VAs in EAG countries

The use of cryptocurrency in criminal activities presents significant challenges, sometimes hindering the ability to investigate and seize illicit proceeds. Based on their experience in detecting, investigating, and prosecuting such crimes, Belarus, India, Kazakhstan, China, the Russian Federation, and Uzbekistan have shared some practices relatively to seizure and confiscation, including during the workshops organized under the project to develop this report.

The terminology distinguishing seizure, freeze, and confiscation is crucial: seizure occurs during criminal investigations, freezing is a temporary measure under AML/CFT laws, and confiscation involves transferring ownership forcibly to the state. As VAs are recognized as funds or property, they become subject to these rules if they were found to be obtained as a result of crime or intended to be used in crime.

For cryptocurrency to be confiscated, a clear link must be established between a wallet and individuals convicted of crimes. Freezing orders on cryptocurrency are effective primarily through regulated VASPs or cooperative unregulated ones. Orders are executable technically if the VASP complies, highlighting the importance of VASP regulation for enforcement. Challenges remain where suspects use unregulated VASPs or engage solely in peer-to-peer transactions, necessitating cooperation or access to private keys for investigation.

While not all EAG jurisdictions legally recognize VAs as property for criminal justice purposes, practical measures are in place to prevent criminals from evading justice in the cryptocurrency domain. However, technical tools are needed to effectively control VAs held outside compliant VASPs, posing a continued challenge.

Procedures for cryptocurrency seizure and confiscation in EAG countries

Based on a review of confiscation practices in EAG jurisdictions where VAs are not universally recognized as criminal property, courts typically proceed with confiscation under two categories: seizing VAs as "other illegally obtained property" in cases involving charges like money laundering, or as "instrumentalities of crime" in cases involving activities such as narcotics trafficking or TF.[145]

In Belarus, Kazakhstan, and Uzbekistan, authorities seize cryptocurrency by transferring it to a government-controlled wallet.[146] Conditions for accessing suspects' cryptocurrency can vary cooperative suspects provide private keys; uncooperative ones may have their keys identified or cooperate with VASPs; complete non-cooperation can hinder seizure.

The feasibility of freezing and/or seizing cryptocurrency in a TF case depends on the type of the currency, wallet, and VASP used by the criminals (see Chapter 5).

As of the time of writing, identifying the owner of a cryptocurrency wallet typically involves two main methods.

- Firstly, authorities rely on communication with VASPs, although obtaining information can be difficult if the VASP operates in jurisdictions lacking stringent customer verification regulations. In all EAG jurisdictions, VASPs are legally required to respond to formal requests from investigators, prosecutors, judges, or other government enforcement agents. They must provide information as requested by law enforcement or competent authorities, such as the FIU where empowered. However, criminals often opt for foreign VASPs based in jurisdictions that disregard international requests.
- Secondly, government agents can gain physical access to cryptocurrency through hardware wallets or private keys, often obtained during criminal intleligence operations or public investigations.

Most cases of successful confiscations of anonymity-enhanced cryptocurrency in the EAG region became possible through seized hardware wallets, private keys or devices used by the suspects to access their cryptocurrency.[147] The actual sequence of events in such a seize-and-confiscate procedure may be as follows:

- A competent authority sends a formal freeze or seizure order to the VASP. In centralized VASPs, the actual cryptocurrency is kept by the VASP, rather than by its customers. Therefore, an AML/CFT compliant VASP will effectively enforce such a provisional measure;
- A government agent transfers cryptocurrency from the suspect's wallet to a wallet controlled by the law enforcement authority. In some EAG jurisdictions, law enforcement and judicial authorities have official wallets where cryptocurrency is kept when seized, confiscated, or used as the bail bond. In Belarus and Uzbekistan, cryptocurrency obtained as a result of crime or intended to be used in crime is transferred to the "police" or "court" wallets at the respective stages of the criminal justice procedure. Jurisdictions where such measures are not in place use wallets under effective control of authorities where cryptocurrency is converted into fiat money, fiat money is withdrawn in cash, the cash is physically presented to the investigator who proceeds with the formal seizure.
- A government agent transfers cryptocurrency from the suspect's wallet to a hardware wallet. In most EAG jurisdictions, such a process is formalized as a "record of crime reenactment."

145 Outcomes of the consultations, which included structured interviews and discussions with representatives from law enforcement agencies of EAG Member States tasked with countering the financing of terrorism, within this project.

146 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

147 Tisen O.N. Methodology of detection, fixation and seizure of electronic digital traces in cases of crimes committed using cryptocurrencies // Criminal law. 2024. № 3.

By way of example, in Russia a laptop was seized in a search of the home of a person indicted with bribery. The laptop had a pattern password. In a forensic examination, the password was disabled. A directory was found with open and private cryptocurrency keys. The wallet contained over 1,000 BTC. The cryptocurrency was seized by the court. A hardware wallet was bought and formalized as a piece of evidence. The seized cryptocurrency was transferred to that wallet. In June 2023, a district court in Moscow cited Russia's asset declaration law (Law 230-FZ of 3 December 2012 "On controls of consistency with the expenses of public officials and some other persons to their income") to confiscate the cryptocurrency and transfer the ownership to the state. The confiscation was enabled by a Rosfinmonitoring parallel financial investigation using the Transparent Blockchain software.

- The cryptocurrency remains in the same wallet. This option carries the risk of loss of cryptocurrency, even where the suspect appears cooperative. The suspect may change their attitude and successfully dissipate the cryptocurrency: it is easy to do if they are not under arrest before trial and more difficult – but theoretically possible – even if they are, since their co-conspirators or other persons having access to the private key may transfer the cryptocurrency away.[148]
- Physical seizure of a hardware wallet. See Chapter 10.
- Communicating with stakeholders other than VASPs[149].

EAG experience seizing and confiscating VAs[150]

Kazakhstan	The authorities of Kazakhstan (which regulates VASPs) have powers to freeze cryptocurrency as part of investigating unlicensed/unregistered business with VAs. According to reports so far, suspects kept cryptocurrency in custodial wallets operated by a licensed cryptocurrency exchange.[151]
Belarus	Belarus has a civil debt enforcement procedure with specific powers for seizing, assessing, and selling cryptocurrency (Justice Ministry Regulation 67 of 14 April 2022). A bailiff can seize cryptocurrency like any other property of the debtor and, if necessary, transfer it to a wallet owned by a government authority or a licensed operator. At this stage, the cryptocurrency is not formally assessed; its value as property can be accounted for only after conversion into fiat money, performed under a separate contract by a licensed operator. The debtor does not get their cryptocurrency back even if it remains unsold.
Russian Federation	In Russia, cryptocurrency is confiscated after controlled conversion into fiat money during a public investigation; cold wallets can be seized as evidence, or cryptocurrency can be transferred to a special hardware wallet also seized as evidence.[152]

148 Tisen O.N. Methodology of detection, fixation and seizure of electronic digital traces in cases of crimes committed using cryptocurrencies // Criminal law. 2024. № 3.

149 Krebs on Security, 2021. DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized. [Online] Available at: **https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/** [Accessed 17 June 2024].

150 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023) and China (December, 2023).

151 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

152 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

Recovery of illicit VAs in the EAG region

In the EAG region, efforts to recover illegally obtained cryptocurrency involve engaging with exchanges and traders, typically requiring detailed explanations of the assets' criminal origin or intent.

Identifying the current location of coins through blockchain explorers and tracking transaction details such as timestamps and TxID are initial steps. Investigations determine VASP involvement in transactions, crucial for recovery unless transactions were peer-to-peer. Controlled delivery operations and cluster analysis help pinpoint VASPs used, though recovery becomes less likely over time. Identifying VASPs' country of registration is critical, especially where unlicensed environments pose challenges. Requests for freeze and recovery are sent to identified VASPs, following detailed transaction data and legal grounds.

> The Russian Federation has some history of cryptocurrency recovery through communication with VASPs. In several cases, investigators requested assistance of private-sector experts who, upon their own analysis of the transactions, sent a crime warning letter to a known pool of compliant VASPs (large exchanges and traders).[153] In response to those letters, pool members upgraded the risk rates of the wallets involved, identified the wallets where the cryptocurrency was kept, froze them pursuant to a subsequent police order, and returned the cryptocurrency to the complainants' wallets.

153 The results of the analysis of information provided by participants of the events held within the framework of the project in Russia (August, 2023), the Kyrgyz Republic (September, 2023), Uzbekistan (November, 2023).

11

Practices in EAG jurisdictions on countering the misuse of VAs for TF purposes

Though innovative, new and emerging technologies could also have disruptive effects and introduce new challenges. VAs have the potential and are indeed being used for TF purposes, complicating law enforcement endeavors to counter the flow of funds to terrorist organizations.

To effectively address cryptocurrency-related crime, EAG jurisdictions need to take several comprehensive actions. These include adopting international standards for regulating VAs, ensuring VASPs comply with regulations, and establishing risk-based mechanisms for detecting suspicious transactions.

International cooperation in sharing information on criminal transactions and wallet owners is crucial. Legal frameworks for seizing and confiscating cryptocurrencies must be in place to overcome the challenges posed by their decentralized and cross-border nature. Additionally, efforts to de-anonymize ownership and counter cryptocurrency mixing would be important, alongside investments in training for government personnel to enhance their capabilities in combating digital financial crime effectively.

Implementing these practices presents significant challenges amid the complexities of today's global economy. The anonymity of cryptocurrency ownership, reliance on decentralized service providers, and the lack of cohesive prevention mechanisms underscore the heightened risk of VAs being exploited for criminal activities.

To effectively mitigate these risks, countries must invest in robust government-to-government and government-to-VASP communication channels and enhance information sharing capabilities.

At the national level, Member States may wish to establish multi-agency "fusion task forces" of experienced officers with the knowledge and skills required to counter cryptocurrency-enabled crime.

At the agency level, considering specific challenges posed by such crime, especially its nexus with TF, special units could be considered and supported by law enforcement authorities, financial intelligence units, and others.

This report was developed to support efforts in the EAG region in the fight against TF, by providing tangible examples of effective measures and ideas for technical support to Member States. With the preliminary results already presented at the EAG Plenary meeting in Sanya, China, 9 December 2023, the crucial feedback from multiple Member States was that there is a need to continue UNOCT/UNCCT's engagement with EAG member jurisdictions. This includes the potential for technical support, capacity-building efforts, and awareness-raising, subject to sufficient funds being made available by funding partners. UNOCT/UNCCT remains committed to supporting EAG member jurisdictions and other jurisdictions in this critical sector, and will explore further opportunities to support them in the coming years.

Acronyms

AIFC	Astana International Financial Center
AFM	Financial Monitoring Agency
AMCM	Monetary Authority of Macao
AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
BRICS+	Interstate group comprising Brazil, Russian Federation, India, China, South Africa, Islamic Republic of Iran, Egypt, Ethiopia, and the United Arab Emirates
CAC	Cyberspace Administration of China
CDD	Customer Due Diligence
CIS	Commonwealth of Independent States
CIS HoFIU	Member States of the Commonwealth of Independent States Heads of FIU
CTC	United Nations Security Council Counter-Terrorism Committee
DASPs	Digital Assets Service Providers
DEX	Decentralized Exchanges or Traders
DFA	Digital Financial Asset
DNFBP	Designated Non-Financial Business or Profession
EAG	Eurasian Group on Combating Money Laundering and Financing of Terrorism
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCMI	Forensics Center of the Russian Ministry of Interior
FIU	Financial Intelligence Unit
FTF	Foreign Terrorist Fighter
ICOs	Initial Coin Offerings
IMEI	International Mobile Equipment Identity
INI	International Network Institute for AML/CFT

IRAC	International Risk Assessment Center for Money Laundering and Terrorism Financing
ISIS	Islamic State in Iraq and Syria
ISKP	Islamic State in Khorasan Province
ITMCFM	International Training and Methodology Centre for Financial Monitoring
KYC	Know-Your-Customer
NAPP	National Agency of Perspective Projects
NPO	Not-for-Profit Organization
PBC	People's Bank of China
PF	Financing of Proliferation of Weapons of Mass Destruction
PRC	People's Republic of China
RBA	Risk-Based Approach
SCO	Shanghai Cooperation Organization
SFC	Securities and Futures Commission
STR	Suspicious Transaction Report
TF NRA	Terrorism Financing National Risk Assessment
TxID	Transaction Identifier
UNCCT	United Nations Counter-Terrorism Centre
UN CTED	United Nations Counter-Terrorism Committee Executive Directorate
UNOCT	United Nations Office of Counter-Terrorism
UNSCR	United Nations Security Council Resolution
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VC	Virtual Currency