STRATEGY

EU AML/CFT
GLOBAL FACILITY

THE EU GLOBAL FACILITY'S STRATEGY ON CRYPTOCURRENCIES

TOWARDS A SAFER WORLD USING VIRTUAL ASSETS

APRIL 2023

Funded by the European Union

EXPERTISE FRANCE
GROUPE AFD

IMPLEMENTED BY
NI·CO
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

This publication was developed by the EU Global Facility on Anti-Money Laundering and Countering the Financing of Terrorism (EU Global Facility) with funding from the European Commission's Service for Foreign Policy Instruments (FPI).

For further information, please contact:
info@global-amlcft.eu
www.global-amlcft.eu

EU AML / CFT
GLOBAL FACILITY

Contents

EU AML / CFT
GLOBAL FACILITY

1. Introduction

Funded by
the European Union

EU AML/CFT
GLOBAL FACILITY

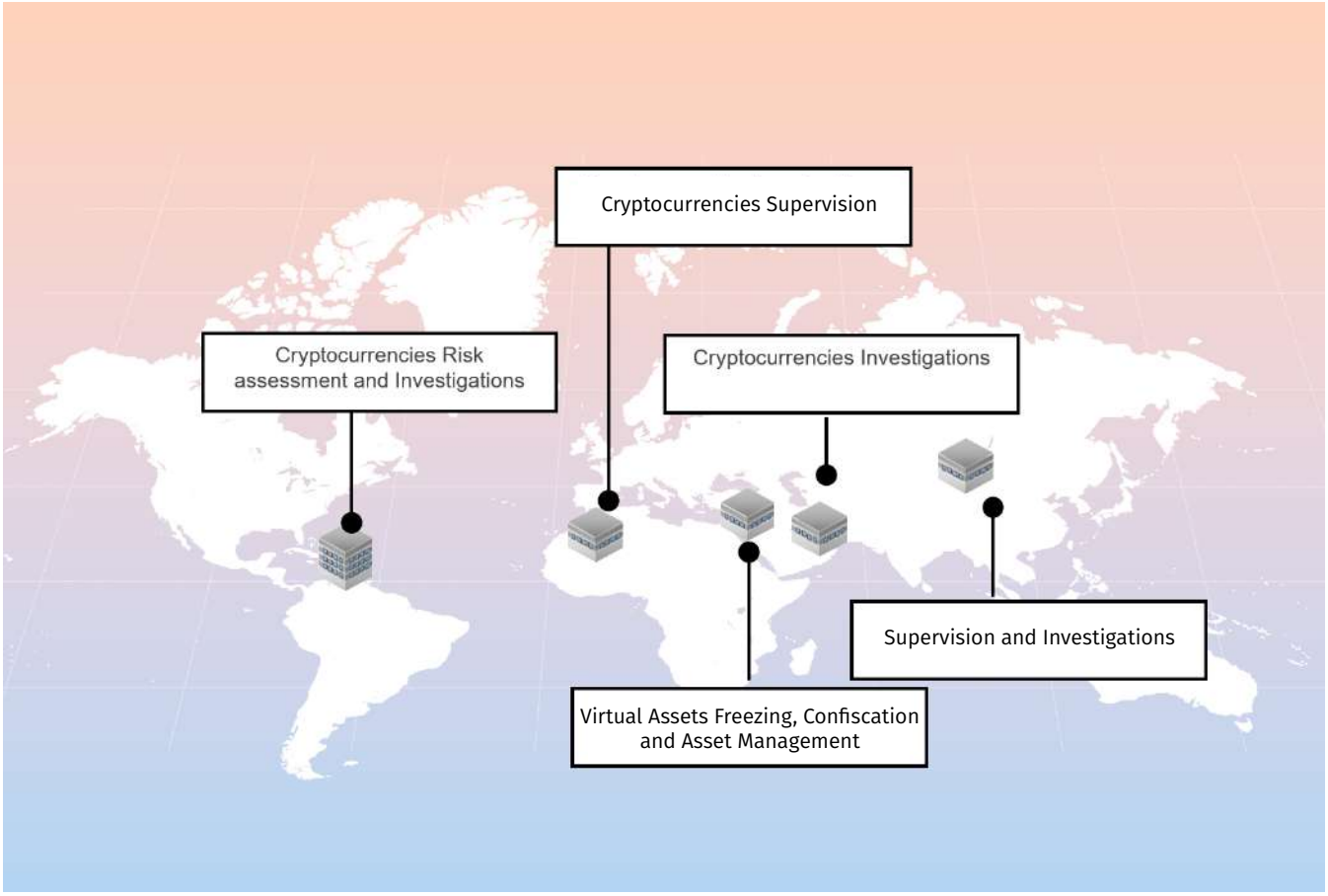
1. Introduction

Cryptocurrencies have drastically evolved in the past years, with their different types and models. In particular, the virtual assets ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralised platforms and exchanges, privacy wallets, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows. They also lead to the emergence of other virtual asset business models or activities such as initial coin offerings (ICOs) that present Money Laundering and Terrorist Financing (ML/TF), fraud and market manipulation risks.

Given the development of additional products and services and the introduction of new types of providers in this space, the Financial Action Task Force (FATF) recognised the need for further clarification on the application of the FATF Standards to new technologies and providers.

The effective global implementation of these standards by all countries will ensure **virtual asset technologies and businesses can continue to grow and innovate in a responsible way**, and it will create a level playing field. It will prevent criminals or terrorists seeking out and exploiting jurisdictions with weak or no supervision.

Strategy on Cryptocurrencies



EU AML/CFT
GLOBAL FACILITY

2. FATF's Approach on Regulating Virtual Assets

Funded by
the European Union

EU AML / CFT
GLOBAL FACILITY

2. FATF's Approach on Regulating Virtual Assets

The FATF has tackled the topic of virtual assets since 2014. In June 2014, the FATF issued *Virtual Currencies: Key Definitions and Potential AML/CFT Risks in response to the emergence of virtual currencies and their associated payment mechanisms for providing new methods of transmitting value over the Internet.*

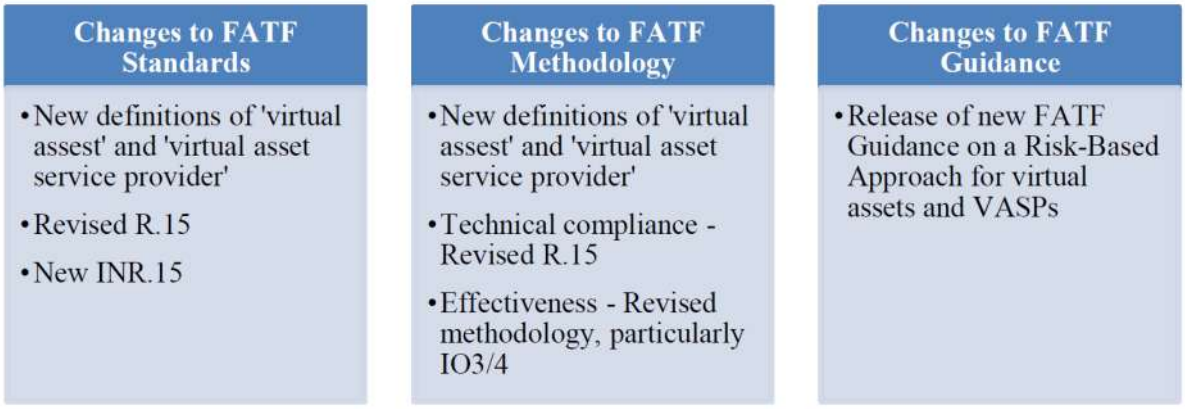
In June 2015, the FATF issued the *Guidance for a Risk-Based Approach to Virtual Currencies as part of a staged approach to addressing the money laundering and terrorist financing (ML/TF) risks associated with virtual currency payment products and services.*

In October 2018, the FATF adopted two new Glossary definitions "virtual asset" (VA) and "virtual asset service provider" (VASP).

- **Virtual assets** were defined as *"a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*
- **Virtual Asset Service Providers (VASPs)** were also defined as *"any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person (a) exchange between virtual assets and fiat currencies (b) exchange between one or more forms of virtual assets (c) transfers of virtual assets (d) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets (e) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."*

In 2019, the FATF issued an amendment to Recommendation 15 for the regulation of virtual assets and virtual asset service providers (VASPs). These recommendations are designed to help countries around the world develop regulatory frameworks that are effective in preventing the misuse of virtual assets for illicit purposes. One of the key elements of the FATF's recommendations is the requirement for VASPs to conduct customer due diligence (CDD) and implement anti-money laundering (AML) and counter-terrorist financing (CTF) measures. This includes verifying the identity of customers, monitoring transactions for suspicious activity, and reporting any suspicious activity to relevant authorities. Another important element of the FATF's recommendation 15 is the requirement for countries to ensure that VASPs are licensed or registered and subject to regulatory oversight. This includes requirements for VASPs to have appropriate governance structures, risk management systems, and internal controls in place.

The FATF's recommendations also call for enhanced international cooperation and information sharing to help combat cross-border money laundering and terrorist financing activities. This includes the development of common standards and best practices for identifying and sharing information on suspicious activity.



In addition to issuing recommendations for the regulation of virtual assets, the FATF has also taken steps to monitor and assess the effectiveness of countries' implementation of these recommendations. The organisation conducts regular assessments of member countries' AML/CFT regimes, including their regulation of virtual assets and VASPs.

Overall, the FATF's work in the area of virtual assets has been instrumental in helping to establish a more robust and effective regulatory framework for cryptocurrencies. By providing clear guidance and recommendations for the regulation of VASPs, the FATF has helped to ensure that virtual assets are not used to facilitate illicit activities such as money laundering and terrorist financing.

Moving forward, it will be important for countries to continue to work closely with the FATF and other regulatory bodies to stay up-to-date with the latest developments in the virtual asset ecosystem and to ensure that their regulatory frameworks remain effective in addressing evolving risks and challenges. By working together, regulators and industry stakeholders can help to promote the responsible use of virtual assets and to prevent their misuse for illicit purposes.

How could the EU Global Facility on AML/CFT help

As a result, there are four outcome areas that the EU Global Facility seeks in the development of cryptocurrencies framework. They are designed to identify and address specific issues in a particular context while also supporting processes of collective learning and problem solving in the face of common challenges.

The four main pillars are:

(1) Assessing the risks related to cryptocurrencies and their service providers;

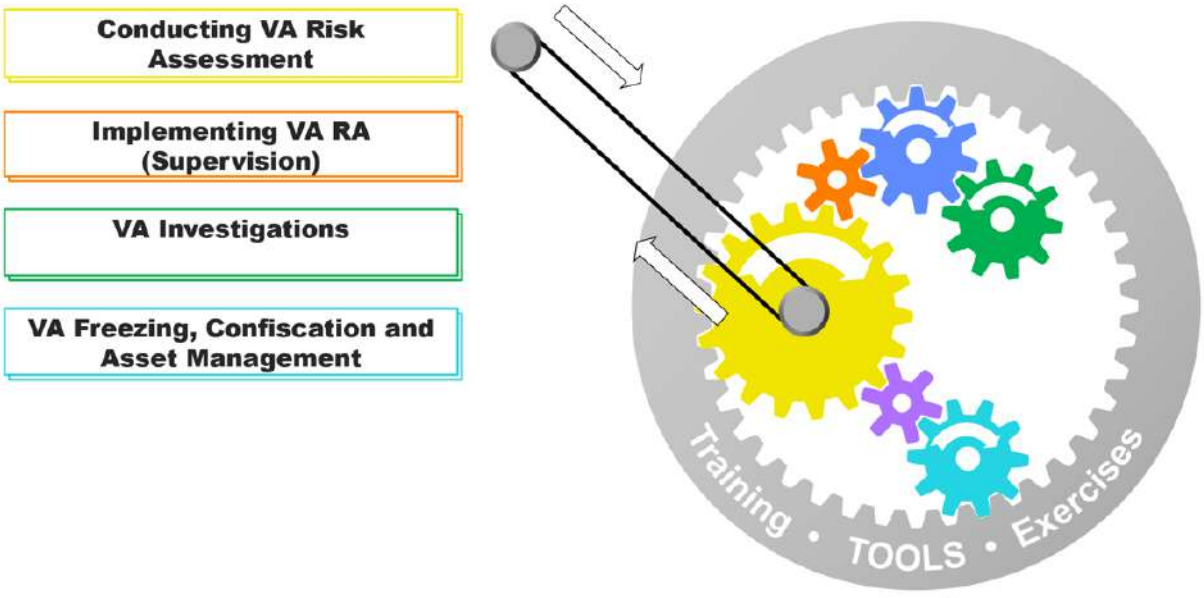
(2) Supervision regarding Virtual assets service providers;

(3) Investigating and tracing virtual assets; and

(4) Seizure and confiscation of virtual assets, and their management.

On middle-long term, the EU Global Facility will develop a methodology aimed at:

- Partnering with countries to better understand the VA environment and, ultimately, decide to either approve or ban VAs.
- Helping partner countries in identifying and equipping themselves with the tools to conduct their own Risk Assessment (RA) on VA.
- Supporting countries in their VAs investigations and eventually seizure and confiscation.



EU AML/CFT
GLOBAL FACILITY

3. To Ban or to Regulate: That is the Question!

Funded by
the European Union

EU AML/CFT
GLOBAL FACILITY

3. To ban or to regulate: that is the question !

Cryptocurrencies have been a hot topic of discussion in recent years, mainly because many countries have not decided on their strategic decisions, whether to ban cryptos wholly or partially or to regulate them like any other financial institution. While some see them as the future of finance, others view them as a threat to the stability of the global financial system.

Talking about regulating cryptocurrencies, the idea is to create a framework that allows for the safe and legal use of cryptocurrencies while addressing concerns about their potential misuse. Regulating cryptocurrencies can have a number of benefits, including:

1. **Consumer Protection:** Regulations can help protect consumers by preventing fraud and ensuring that exchanges and wallet providers adhere to certain standards.
2. **AML/KYC Compliance:** Regulations can help prevent money laundering and terrorist financing by requiring exchanges and wallet providers to comply with anti-money laundering and know-your-customer (KYC) regulations.
3. **Taxation:** Regulating cryptocurrencies can help governments collect taxes on cryptocurrency transactions, which can be difficult to track without proper regulation.
4. **Market Confidence:** Regulation can help boost market confidence by providing a clear legal framework for the use of cryptocurrencies.
5. **Implementation and development of enforcement legislation** to allow both regulator and LEA to conduct professional and independent investigations.

On the other end of the spectrum, some countries have chosen to ban cryptocurrencies outright. The reasons for this vary from country to country, but some of the most common arguments against cryptocurrencies include:

1. **Criminal Activity:** Cryptocurrencies are often associated with criminal activity, such as money laundering and drug trafficking.
2. **Lack of Regulation:** Some argue that cryptocurrencies are inherently unregulated and therefore pose a threat to the stability of the global financial system.
3. **Volatility:** Cryptocurrencies are known for their volatility, which makes them a risky investment.
4. **Environmental Concerns:** The process of mining cryptocurrencies requires a large amount of energy, which some argue is not sustainable.

Following the amendment of Recommendation 15, countries are required to either explicitly ban or regulate cryptocurrencies; while banning will involve proportionate dissuasive and effective sanctions, and regulation will entail copy-paste requirements for virtual asset service providers like the ones imposed on financial institutions and designated non-financial businesses and professions. in order for countries to reach this conclusion, they will need to conduct a RA on the virtual assets and virtual asset service providers sector.

Some countries may decide to prohibit or limit VA activities or VASPs, based on their assessment of risk and national regulatory context or in order to support other policy goals (e.g., consumer or investor protection, market protection, safety and soundness, or monetary policy). In such cases, some of the specific requirements of R.15 would not apply, *but jurisdictions would still need to assess the risks associated with covered VA activities or providers and have tools and authorities in place to take action for non-compliance with the prohibition or limitation.* In deciding whether to prohibit or limit VA activities of VASPs, countries should understand the ML/TF risks associated with VAs. A country should ensure that it has the technical capacity and resources to enforce such a prohibition or limitation.

Strengthening the public – private partnership information sharing and investigative protocols by early consultation with VASPs will be important to "design out" criminality. This will necessitate structures be put in place that protect the privacy of the private sector.

EU AML/CFT
GLOBAL FACILITY

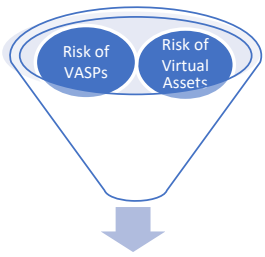
Assessing the Risks of VA and VASPs

Since the FATF has adopted the new standards and issued guidance on regulation and supervision of Virtual assets and Virtual Assets service providers, there is a requirement from all countries to conduct RA of virtual assets and virtual assets service providers. The objectives of the VA and VASPs risk assessment are to:

1. Identify, understand, and assess the overall money laundering and terrorist financing ML/TF risks related to VA and VASPs ecosystem;
2. Identify VA and VASPs products/services/ channels with high vulnerability;
3. Prioritise action plans to strengthen anti-money laundering and counter-terrorist financing controls in the VA and VASP ecosystem; and
4. Apply a risk-based approach to VAs and VASPs and effectively mitigate those risks. Countries are expected to identify, assess, and understand the money laundering and terrorist financing risks, and develop and implement a risk based national AML/CFT regime.

In this regard, and since countries have adopted different approaches to legislate and regulate these activities, there is no "one size fits all" for risk management, however, there are some broad guidelines/steps in order for countries and competent authorities should follow in order to properly assess the AML/CFT risks related to VAs and VASPs. Also, the assessment should be an opportunity for building the capacity and raising the awareness of competent authorities about the risks related to VAs and VASPs, as well as strengthening the interagency cooperation among them.

Countries should be able to identify and understand the different types and categories of virtual currencies and tokens that are in circulation within their jurisdiction, in order to assess the risks related to each type based on their properties. Also, they should be able to identify VASPs operating in their jurisdiction, if any, and understand their functions in order to be able to whether include them in their RA or not.



Virtual Assets/VASPs Risk Assessment

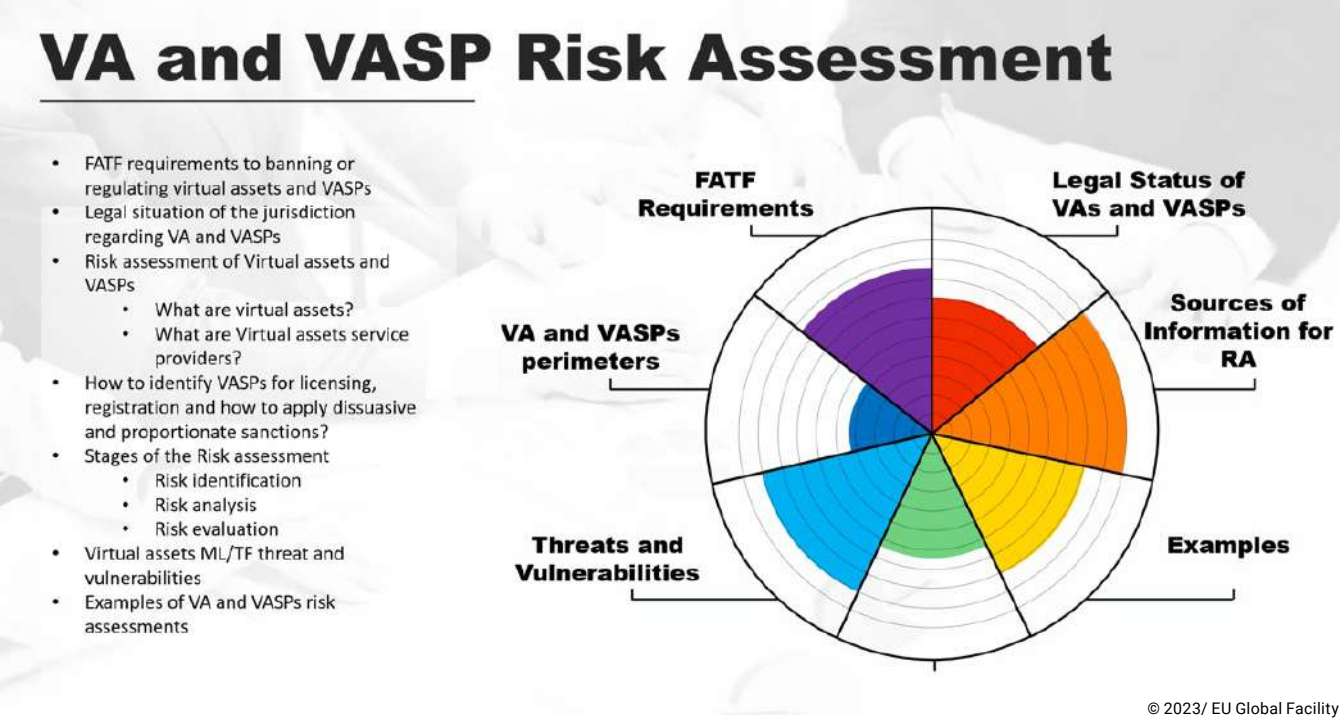
The collection of quantitative and qualitative data is essential element of the Virtual Assets RA. The ability to collect and analyse data about VA and VASP activities is crucial to assessing ML and TF risks. Mainly, there must be a number of sources in order to collect the information, such as cases from law enforcement agencies, cases from the public prosecution, STRs received by the FIU, open sources (such as reports from blockchain analytics companies), interviews, and international cooperation requests.

The systematic collection of quantitative data can play a crucial role in the effectiveness of the VA-RA as it may assist in facilitating discussion and assessment along with the competent authorities.

As a result, there should be a checklist in order to follow up with the RA which should include various components and steps, such as identifying the overall interaction of VAs, VASPs, and traditional obliged entities for ML/TF threat and vulnerability, identifying and assessing VA threat and vulnerability for ML/TF, and risk mitigation.

How could the EU Global Facility help?

The EU Global Facility is currently providing assistance to several countries regarding the VA Risk Assessment, including providing guidance on conducting VA/VASP Risk Assessment workshops, walk-through on their assessment and others. This is a snapshot of some of the contents of these VA RA workshops.



Supervising VASPs

As cryptocurrencies are new ways of doing things, supervisors, like all other stakeholders, should develop a deep understanding of the VASP market, its structure, and its role in the financial system and the country's economy to better inform their assessment of risk in the sector. This may require investing in training, personnel, or other resources that enable supervisors to gain the practical skillsets and expertise needed to regulate and supervise the range of VA providers and activities described in the VA services or business models.

According to the FATF recommendations, countries may prohibit or regulate virtual assets. In case of prohibition, countries should take action to identify natural or legal persons that carry out VASPs activities without the requisite license or registration, and apply appropriate sanctions to them. On the other hand, when a country decides to regulate VAs, there are a number of obligations, one of which is VASPs registration and licensing requirements, and also supervision on this sector.

Countries need to:

- Understand the money laundering and terrorist financing risks the sector faces
- License or register virtual asset service providers
- Supervise the sector, in the same way it supervises other financial institutions

To address these risks, many countries have begun implementing regulatory frameworks for VASPs. These frameworks typically require VASPs to register with regulatory authorities, implement robust anti-money laundering and counter-terrorist financing policies and procedures, and submit to regular audits and inspections.

Overall, supervising VASPs is a complex and challenging task, but it is critical to ensuring the integrity of the global financial system. Regulators, VASPs, and other stakeholders must work together to develop effective regulatory frameworks and supervisory approaches that promote the responsible use of virtual assets while mitigating the risks they pose.

Public Private Partnership

Public/Private partnership can help to (1) set clear expectations through the definition of a regulatory framework (2) exchange risks & typologies through the discussion of industry emerging trends; (3) learn & teach - discover new initiatives and product offerings, understand potential vulnerabilities, educate new players on industry best practices, risks, regulatory concerns; (4) build trust - identify relevant point of contacts and establish ongoing dialogue.

One key challenge in supervising VASPs is the constantly evolving nature of the virtual asset ecosystem. New technologies and business models are emerging all the time, and regulators must stay up-to-date to ensure that their supervision is effective. This requires close collaboration between regulatory authorities, VASPs, and other stakeholders in the virtual asset ecosystem.

Use of Technology in VASP Supervision

Technology has emerged as a critical tool for regulators to effectively and efficiently monitor VASPs and enforce AML/CFT rules. Technology can also play a significant role in the ongoing monitoring of VASPs. By automating certain tasks, regulators can monitor VASPs more efficiently and effectively.

Some examples of technology-enhanced ongoing monitoring include:

- **Blockchain analytics:** With the help of blockchain analysis tools, regulators can trace virtual asset transactions, identify suspicious patterns, and detect potential ML/TF activities. These tools can also be used to assess the effectiveness of VASPs' transaction monitoring systems.
- **Automated reporting:** VASPs can be required to submit periodic reports to regulators in a standardised, machine-readable format. This allows regulators to automatically process and analye the data, potentially highlighting concerning trends, risks, or patterns that warrant further investigation.
- **Risk-based monitoring:** By combining risk assessment data with ongoing monitoring information, regulators can adopt a more targeted and risk-based approach to supervision. This ensures that resources are allocated effectively and that higher-risk VASPs receive a greater level of scrutiny.

Technology can also facilitate greater collaboration between regulators, VASPs, and other stakeholders in the virtual asset ecosystem. By establishing secure data-sharing platforms, regulators can access a wealth of information from various sources, such as law enforcement, financial intelligence units (FIUs), and other regulatory bodies.

This collaborative approach not only enables regulators to leverage the expertise and resources of other stakeholders but also helps to create a more unified and effective AML/CFT supervisory framework.

How could the EU Global Facility help?

Solutions include workshops to regulators to help them understand the basics of cryptocurrencies and how to conduct risk based approach supervision on VASPs. This assistance can also include setting a framework for supervision on VASPs, including but not limited to supervision manuals.

EU AML/CFT
GLOBAL FACILITY

Investigating and tracing VAs

Cryptocurrencies have been a subject of investigation by law enforcement agencies and regulatory bodies around the world. The decentralised and anonymous nature of cryptocurrencies has made them attractive to criminals, who use them for money laundering, drug trafficking, and other illegal activities. Methods used for investigating cryptocurrencies can vary but they will hover around these techniques:

1. **Blockchain analysis** is a technique used to track the movement of cryptocurrencies on the blockchain. By analysing the blockchain, investigators can identify addresses associated with criminal activity and trace the flow of cryptocurrency from one address to another.
2. **Data Analysis:** In addition to blockchain analysis, investigators can also use data analysis tools to identify patterns and connections between individuals and transactions. This can help investigators identify and track down individuals involved in criminal activity.
3. **Cooperation with Exchanges:** Law enforcement agencies can also work with cryptocurrency exchanges to obtain information about users and transactions. This can include information about the identity of users, transaction histories, and IP addresses.

However, investigating cryptocurrencies can entail many challenges; one of the biggest challenges in investigating cryptocurrencies is the (pseudo)anonymity they provide. Transactions on the blockchain are pseudonymous, meaning that they are identified only by a public key (a string of numbers and letters denoting an account/address). This makes it difficult to identify the individuals behind the transactions. Secondly; the complexity of the cryptocurrency ecosystem can also pose challenges for investigators. There are thousands of cryptocurrencies, exchanges, and wallet providers, each with their own unique features and characteristics. However, investigators must not be experts in all of these types as much as gemologists must not be experts in seizing gems. Thirdly, cryptocurrencies are global in nature, making it difficult for law enforcement agencies to coordinate investigations across multiple jurisdictions, due to lack of training or use of appropriate technology or even political will.

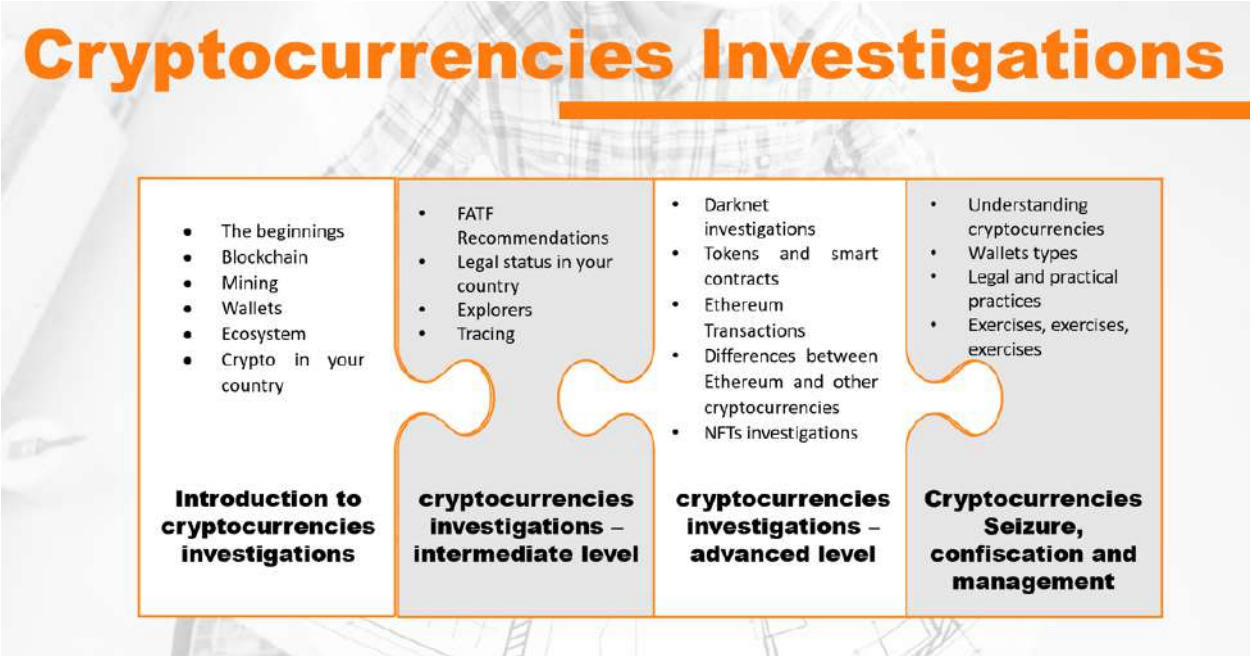
In conclusion, investigating cryptocurrencies is a complex and challenging task. Law enforcement agencies and regulatory bodies must use a variety of techniques and tools to identify individuals involved in criminal activity. While the anonymity and lack of regulation in the cryptocurrency industry pose challenges, there are ways to overcome them through cooperation and innovation. As the cryptocurrency industry continues to evolve, it is important for investigators to stay up-to-date with the latest tools and techniques for investigating cryptocurrencies.

How could the EU Global Facility help?

Solutions involve training and workshops in collaboration with leading blockchain analytics companies for LEAs and competent authorities to enhance their capabilities in tracing and investigating cryptocurrencies.

The requirement to utilise covert investigative methodologies, such as covert digital investigators, test purchases, and the use of various digital surveillance techniques will invariably increase as organised crime groups and terrorists conduct financial transactions online or in the metaverse.

Assistance can also entail providing financial investigations manuals. Summarized outlines for the different workshops EU Global Facility provides is shown below.



Seizure, Confiscation and Asset Management

There are many degrees of easiness in seizing and detecting assets related to money laundering, it may be fairly easy to link a fancy yacht belonging to a corrupt official in a money laundering case to a judge in court, but how can you show judges a fraction of a bitcoin? How can you trace bitcoins to prove the money laundering offence?

Understanding the blockchain with its inherent cryptography, the ability to carve addresses from computers and phones, and extracting private keys from wallets are all skills of the new age of cryptocurrencies, however, they need to be in the toolbox of investigators, prosecution agencies. There should be a guiding manual of how to detect, seize, confiscate and subsequently cash out crypto assets. This will help standardise the procedures for divesting criminals of this important and usually unnoticed source of criminal proceeds.

In fact, government seizures of cryptocurrencies are growing so rapidly. To give a flavor of this, "In fiscal year 2019, the US authorities had about $700,000 worth of crypto seizures. In 2020, it was up to $137 million. And in mid 2021, we're at $1.2 billion," Jarod Koopman, the director of the IRS cybercrime unit, told CNBC[1].

1. https://nationalpost.com/news/irs-seized-us1-2-billion-of-crypto-assets-this-year-to-be-auctioned-off

EU AML/CFT
GLOBAL FACILITY

One of the biggest concerns about the seizure of cryptocurrency is what to do with the coins once you have control of them. Do you "cash out" and convert the coins into fiat currency or hold them as they are? Having said that, government agencies must be well equipped with knowledge on how to deal with the seized cryptocurrencies; even if they have decided to outsource the seizing/confiscation to the private sector. There should be a great collaboration between the private sector and other government agencies to maintain custody of seized or forfeited crypto assets in criminal cases, and the subsequent monetisation of those tokens.

There are three key points to keep the chain of custody intact for seized cryptos. The first key point is the search and seizure of the asset, the second is the liquidation of the asset, the third is the deployment of the sale proceeds from the seized crypto asset.

In brief, detecting, seizing and confiscating crypto assets require a toolbox of awareness from the concerned government entities on the mechanics of crypto assets and blockchain, a standardised guideline and interagency cooperation.

How could the EU Global Facility help?

Solutions involve training and practical workshops for LEAs and competent authorities to enhance their capabilities in seizing and confiscating cryptocurrencies. Best practices are provided on how countries do seizure, confiscation and manage the assets afterwards.

THE EUROPEAN UNION'S GLOBAL FACILITY ON

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

www.global-amlcft.eu

@globalamlcft

Funded by the European Union

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the EU GF-AML/CFT and do not necessarily reflect the views of the European Union.