DEPARTMENT AGAINST TRANSNATIONAL ORGANIZED CRIME (DTOC)

ORGANIZATION OF AMERICAN STATES (OAS)

51 (VIRTUAL) MEEETING OF THE GROUP OF EXPERTS FOR THE CONTROL OF MONEY LAUNDERING
November 16-17, 2021
Washington DC – United States of America

OAS/Ser.L/LI. 4.51
DTOC/LAVEX/doc.2/21
November 17, 2021
Original: In Spanish

FINAL REPORT
RELEVANT CRYPTO ASSET CASES

Working Subgroup on Financial Intelligence Units and Criminal Investigation Agencies

2021

Overview of the mandate:

Under the 2021-2023 work plan that the GELAVEX plenary approved at its Asunción virtual meeting on November 10, 2020, the Working Subgroup on Financial Intelligence Units and Criminal Investigation Agencies would work on:

1. A study to identify, from a criminal investigation perspective, cases involving crypto assets, focusing especially on successful investigations in any member state, with a view to sharing relevant information and best practices;

2. A study on the laundering of proceeds of corruption, drugs and weapons smuggling, and tax fraud, with an emphasis on identifying typologies and reviewing laws in the countries of the group, with assistance from the Technical Secretariat and other areas of the OAS General Secretariat, such as MESICIC, along the same lines to be able to access court rulings;

3. Studies focused on analysis of end beneficiaries of money laundering, coordinated through the Technical Secretariat, with the work that other specialized organizations, such as GAFILAT and CFATF, may be conducting, and if appropriate, with participation from UINL;

4. Developing tools for strategic analysis in money laundering investigations: Country experiences with development and use of technological tools for improving operational and strategic analysis;

5. A study on the feasibility of implementing a consultation system for the region, with a view to implementing FATF Recommendation 12 regarding politically exposed persons (PEP), taking into account the legal limitations on information protected by personal data protection laws in member states; and

6. A study on money laundering tied to the illegal extraction of minerals, with emphasis on analysis of criminal and administrative laws for this sector, including identification of practical cases, typologies and existing measures to prevent illegal extraction, and management of assets associated therewith.

2021-2023 Work Plan

The Working Subgroup on Financial Intelligence Units and Criminal Investigation Agencies will be devoted to:

1. A study to identify, from a criminal investigation perspective, cases involving crypto assets, focusing especially on successful investigations in any member state, with a view to sharing relevant information and best practices; and

2. A study on the laundering of proceeds of corruption, drugs and weapons smuggling, and tax fraud, with an emphasis on identifying typologies and reviewing laws in the countries of the group, with assistance from the Technical Secretariat and other areas of the OAS General Secretariat, such as MESICIC, along the same lines to be able to access court rulings.

Mandate No. 1 was divided into two parts: Part 1 to be worked on in 2021, would focus on the collection of cases linked to cryptoassets in member countries; in Part 2, to be carried out in the second half of 2021, the results of the analysis of the cases collected would be presented.

OBJECTIVES

The objectives of this study are as follows:

1. General objective

To undertake a study of cases involving virtual assets, both in the institutions that participate in the preventive system and in the criminal prosecution system. This was commissioned by the Group of Experts to Control of Money Laundering (GELAVEX) at the plenary meeting in Asunción in 2020.

2. Specific objectives:

- To know the current situation of member countries as regards identification of possible control scenarios for virtual assets and cases in which activities involving them are recorded, given that we have noted significant differences in how this phenomenon has evolved in different countries in the region.
- To generate a database of best practices and problems identified in operations involving virtual assets.

Methodology

This study involved the consultation of cases provided by member states and permanent observers that have cooperated or are cooperating by furnishing information; open sources of information, such as studies conducted by the OAS and the Latin American Financial Action Task Force (GAFILAT), and instruments prepared by member states. Specifically, the Chilean and Paraguayan delegations will supervise the study and will review and systematize the information. The review will have three stages: first, detection and reporting by reporting entities; second, risk analysis and management; third, prosecuted and convicted cases.

The following table summarizes the information provided by the countries that cooperated in this report.

	Detection	Risk analysis and management	Prosecuted cases	Convicted cases
PARAGUAY	Work by the FIU has detected persons engaging in cryptocurrency activities. No suspicious transactions were identified.	The activities detected have given rise to low-risk reports that have not led to further analysis. No cases have been referred to the public prosecution service (Ministerio Público).	Based on consultations with the public prosecution services and a review of sources, no cases are being prosecuted.	No convictions have been recorded.
CHILE	Two STRs related to crypto assets were detected.	The reports were considered relevant and led to financial intelligence processes.	One case is being prosecuted.	No data
UNITED STATES	No data	No data	Access was provided to 67 investigated cases.	Access was provided to 67 in which convictions were obtained.
GERMANY	Germany reports that in 2018 and 2019 it received 1,330 reports associated with crypto assets.	More than half of the reports were linked to phishing and other fraud.	No data	No data
MEXICO	Mexico has provided a risk model and map based on reports of unusual activities involving virtual assets. It reports 1,479 unusual reports involving virtual assets	The risk model and map is an analysis of unusual reports involving virtual assets, which classify the risk level of those reported and generates a map of the use of those assets.	No data	No data
COSTA RICA	Costa Rica reports that in 2019 and 2020, it notified at least 5 reports of activities involving crypto assets.	It states that the reports are associated with a typology of transfers without justification.	No data	No data
ARGENTINA	Argentina has not provided any detection data.	No data	It reports a pretrial detention order in a case	No data

			involving a pyramid scheme carried out using a fraudulent virtual currency.	
GUATEMALA	Guatemala reports having received 40 reports of operations linked to crypto assets between 2018 and 2020.	It notifies that at least 3 reports have been sent to the public prosecution service.	No data	No data

CONCLUSIONS

Based on the information received, it was not possible to confirm the existence of any cases of suspicious transactions involving crypto assets that led to criminal investigations concluding in convictions.

Preliminarily, it could be concluded that, in terms of cases, countries were in an asymmetric situation from the point of view of suspicious transaction reporting and criminal investigations involving crypto assets.

In the Preliminary Report it was proposed, for a better analysis of the information received, to make a distinction between three stages in the prosecution process involving crypto assets: first, identification of cases of suspicious transaction reports relating to crypto assets; second, risk analysis and management of those reports; third, the prosecution, suppression, and, as appropriate, punishment.

The Preliminary Report expressed the need for information from member states and permanent observers. It also indicated that public sources would be used, along with any other information that might be appropriate for the purposes of submitting to the Gelavex plenary an interesting and beneficial analysis of relevant cases involving crypto assets from which useful lessons could be drawn.

As a result, information was received from the United States, Chile, Mexico, Paraguay, Germany, Costa Rica, and Argentina. The background information provided by those countries is very diverse, given the different situations that each face where crypto and virtual assets are concerned.

Having said that, in keeping with the criterion set out in the Preliminary Report of having three distinct stages, the information received, plus the review of open-source information, in

particular FATF guidance in this area,[1] an analysis of the information provided, and a brief description of some cases is presented as the final result, with elements of potential interest highlighted.

I. Suspicious transaction reporting and crypto assets

Crypto assets can be used in the three stages of laundering: placement, layering and integration. Placement is the stage at which fiat money from each State can be converted into crypto assets, and integration, the point at which crypto assets can be converted back to Fiat money.

These two stages are key to the flow of information, since, through companies that provide these services, it will be possible for intelligence agencies to access information on transactions that are then hard to trace on the network.

In terms of information provided by States, Chile, Germany, Mexico, and Costa Rica indicated having instances of suspicious transaction reports involving crypto assets.

- Germany reported that in 2018 and 2019 it received a total of 1,330 reports linked to crypto assets. The majority of those reports had to do with laundering activities following fraud, mainly of merchandise and phishing. In addition, many reports concerned fraudulent investments in fake crypto assets. It also said that most reports come from traditional financial entities and that there were few reports on transactions strictly involving crypto transactions.

- Mexico provided a report prepared by the FIU, titled Risk Model and Map, which states that 1,479 reports of unusual transactions involving virtual assets were received between May 2020 and May 2021.

- Chile reported two suspicious transaction reports related to cryptocurrency transactions.

- Costa Rica mentioned five reports associated with crypto assets in 2019 and 2021. It states that the underlying typology involves transfers without justification and opacity regarding the origin of funds. It adds that the regulation of virtual assets and providers is still under discussion in Costa Rica, and that it is an unregulated sector.

- Guatemala declared 40 reports in connection with crypto assets between 2018 and 2020. It also added that it had submitted three reports to the public prosecution service (Ministerio Público). It also provided an analysis of the reports, in terms of the persons reported and the reporting institutions, noting that they were regulated entities in the traditional financial system.

1. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs).

The information received shows the existence of notices and reports of activities involving crypto and virtual assets; however, the information provided is statistical and its confidentiality precludes the possibility of case studies. Nonetheless, a number of significant facts can be extracted:

- Of the reporting countries, four States reported having received reports involving crypto assets, but not necessarily originating from a cryptocurrency transaction, which is unusual among member states, except for the United States, as outlined in the FATF guidance.

- Virtual asset service providers should be subject to some degree of regulation and where possible be covered as regulated entities, or at least required to report to financial intelligence agencies.

- The background information provided by the United States shows the importance that virtual asset services provided by non-financial entities be reported to financial intelligence agencies.

- In the case of Chile, the aforementioned reports relate specifically to transactions carried out in virtual assets, generating the respective intelligence analysis.

- In its Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, the FATF recognizes the usefulness of virtual asset service providers reporting to intelligence units, and offers as an example a case that allowed the U.S. authorities to take action against a company operating with such currencies.[2]

- Also, although no information has been provided for this report, open sources note the existence of an incipient cryptocurrency ATM industry. The ATMs can be used to purchase virtual currencies by depositing fiat money, so it is important that companies that manage such services have a reporting obligation, and that the possibility exist to analyze the information of clients using the service in order to identify smurfing, for example.

II. Risk analysis and management

2. For example, STRs filed both by depository institutions and VASPs (specifically, exchangers) enabled U.S. law enforcement to take action in 2017 against BTC-e—an Internet-based money transmitter that exchanged fiat currency as well as VAs and facilitated transactions involving ransomware, computer hacking, identity theft, tax fraud schemes, public corruption, and drug trafficking—by helping them to identify VA wallet addresses used by BTC-e and detect different illicit streams of activity moving through the exchange. UPDATED GUIDANCE: A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, p. 68, footnote 51.

The report provided by Mexico is a good example of risk analysis and management in relation to virtual assets, offered professionally and on a regular basis by organizations other than financial institutions.

The review carried out by the Mexican FIU counts 1,479 reports of activities involving virtual assets and classified the risk level of the persons reported and distributes them geographically, allowing it to put together a map identifying the regions with the greatest use of virtual assets in unusual activities.

III. Investigation and convictions

As for the stage covering criminal investigations, whether or not they originated in from an FIU report, information was received from the United States and Argentina.

- The United States provided a list of 67 cases involving the use of cryptocurrencies on the darknet that were investigated and resulted in punishments.

- Argentina, for its part, provided background information on a specific case involving a pyramid scheme fraud carried out with fake crypto assets, including the court's pretrial detention order.

As can be seen, there is more information available on the investigation and punishment stage, than on the preceding, and the contribution of the United States, which has investigated and prosecuted a significant number of cases, is important.

- **Silk Road.** In 2013, several U.S. government agencies dismantled the Silk Road, a virtual marketplace used for illicit substances, weapons, and false identities , through an encrypted network known as Tor (The Onion Router), which allowed users to remain anonymous. Following the capture of the administrator and the dismantling of the market, several drug suppliers using the website were prosecuted.

- In 2014, a Baltimore District judge sentenced someone who sold drugs via Silk Road to six years in prison. The convicted person received orders for drugs via Silk Road and took payment in Bitcoin. This case is apparently the first in which federal agents confiscated the Bitcoin that the convicted felon used to buy his drug supply and received in payment. It should be noted that the network was global, with sellers and suppliers located in several countries.

- In 2018 a joint operation between the United States and Europol led to the arrest of 170 traffickers, as well as the seizure of drugs and US$6.5 million in cash and virtual currencies. The operation brought down the Wall Street Market, one of the world's largest illegal markets operating on the darknet.

- **Onecoin**. A group of people in the city of Córdoba banded together to orchestrate a series of scams using a proven scheme consisting of offering a high-return, low-risk investment to acquire a particular cryptocurrency that required a certain minimum investment. The cryptocurrency in question was known as Onecoin, which do not actually exist.

A computer expert report stated that Onecoin existed in virtual wallets, but in reality it was not tradable and was impossible to exchange for fiat currency.

Based on the above cases, there are a number of relevant elements to be borne in mind by this working subgroup:

No.	TYPE OF NEED	REQUIREMENT	RATIONALE
1.	MATERIAL	Virtual wallets for system operators	This requires that criminal prosecution agencies or courts have an appropriate location to keep virtual assets after they have been identified. In the same way that a person acquires crypto assets and has a virtual wallet to do so, States, through their institutions, should use such technologies to have the capacity to seize such assets and keep them safe.
2	MATERIAL	Hardware and software to enable tracking on the darknet	Technological capabilities of criminal prosecution agencies. As the cases provided by the United States show, it is important to be able to trace transactions on the darknet
3	REGULATORY	Working guidelines agreed upon by different operators	The consultations made and cases analyzed show that the type of expertise in these areas is very diverse, among both countries and institutions. For this reason, it is proposed that, at a minimum, CIAs and FIUs develop working guidelines as a basic framework for action.
4	REGULATORY	PROCEDURE OR GENERATION OF PROTOCOLS FOR USE	Considering that cryptocurrencies are growing increasingly commonplace and are used in different licit and illicit activities, it is necessary for authorities to have clarity on how they to operate in relation to virtual assets.
5	REGULATORY	Information, reporting and record keeping obligations	Given the explosive nature of the virtual-assets phenomenon and the latest modifications to international standards, it is

No.	TYPE OF NEED	REQUIREMENT	RATIONALE
			necessary to assess who should become a regulated entity.
6	OPERATIONAL	Protocols or agreements between institutions	The cases reviewed show that proper supervision and, potentially, punishment of the use of virtual assets requires the intervention of several agencies.
7	STRATEGIC	Linkage to other criminal phenomena	Cryptocurrencies can also be part of traditional scams, as the Onecoin case showed, in which a significant number of people were offered the possibility of purchasing tokens that could be converted into a cryptocurrency; however, it was simply a front for a Ponzi-type pyramid scheme. This reinforces what was previously stated, in that virtual asset service providers should be registered.