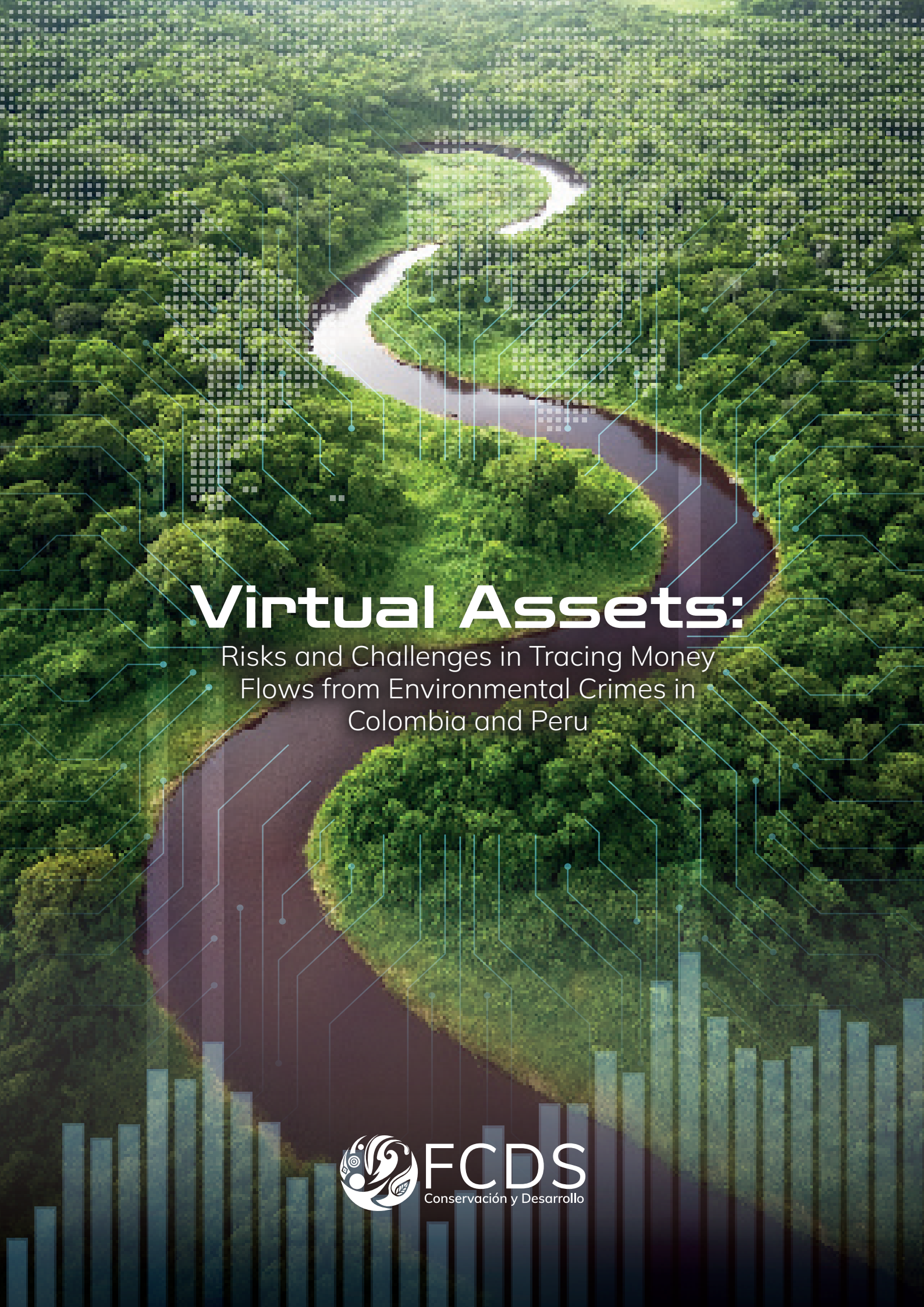




Virtual Assets:

Risks and Challenges in Tracing Money
Flows from Environmental Crimes in
Colombia and Peru



FCDS
Conservación y Desarrollo

VIRTUAL ASSETS:

Risks and Challenges in Tracing Money Flows from Environmental Crimes in Colombia and Peru

Autor:

Foundation for Conservation and Sustainable Development / Peru

Elaboration and analysis

Katherin Alfonso

Technical review, FCDS Perú:

Manuel Zapata

Coordinator for Binational Projects

Executive Director FCDS Peru:

Andrea Buitrago

Copy editing:

Jorge Cornejo

Design and layout

Fernando Pano

Photographic credits

FCDS Peru

Cover photo: AI generated.

Unless otherwise explicitly stated, credit belong to FCDS Peru

Suggested citation:

Foundation for Conservation and Sustainable Development / Peru
(2025). *Virtual Assets: Risks and Challenges in Tracing the Flow of Proceeds from Environmental Crimes in Colombia and Peru*. Lima: FCDS Perú.

Total or partial sale of this publication is prohibited; however, it may be used provided that the authors are properly cited.

Foundation for Conservation and Sustainable Development

www.fcds.org.pe

www.fcds.org.co

Fiste digital edition. October 2025

This publication is available for free download at:

www.fcds.org.pe/publicaciones

Virtual Assets:

Risks and Challenges in Tracing Money
Flows from Environmental Crimes in
Colombia and Peru

Presentation

In the digital age, environmental protection has taken on new dimensions and challenges. Environmental crimes are no longer confined to the physical realm of forests, rivers, or the atmosphere: today they also lurk behind screens, servers, and virtual transactions. Cryptocurrencies, tokens, and other digital assets—legitimate instruments of economic innovation—have become, in the wrong hands, vehicles for laundering money from illegal logging, illicit mining, wildlife trafficking, and other activities that destroy the planet’s ecosystems.

This report stems from the concern and commitment of the Foundation for Conservation and Sustainable Development (FCDS Peru) to the comprehensive protection of the environment and the Amazon in the 21st century. We understand that the fight to protect the environment cannot be limited to ecosystem restoration or denouncing extractive practices; it must also encompass the new dimensions of crime and the digital economy that threaten the progress made in protecting and ensuring the sustainability of the Amazon biome.

Through rigorous and specialized analysis, this research explores the relationship between virtual assets and environmental crimes, showing how emerging technologies—while offering opportunities for transparency and traceability—can also be exploited by networks operating outside the law. The text invites reflection on the need to strengthen regulatory frameworks, promote international cooperation, and foster a culture of technological responsibility.

Our organization embraces the challenge of articulating knowledge and technical evidence to inform decision-making in a field where technology, law, and the environment intersect. From the outset, this report is therefore a tool for raising awareness and promoting action. We aim to help public institutions, the financial sector, technology developers, and civil society understand that protecting the Amazon also plays out in the digital realm; because defending nature today also means understanding the language of code, blockchain, and new forms of value.

Only in this way can we ensure that technological innovation does not become a new instrument of impunity, but rather a powerful ally for environmental justice in the pursuit of conserving the Amazon.

Andrea Buitrago

Executive Director

Foundation for Conservation and

Sustainable Development FCSD / Peru



Contents

1.	Presentation	04
2.	Acronyms	06
3.	Introduction	08
4.	Guide to Understanding the Crypto World. Basic Concepts	11
	• Uses of Virtual Assets • What are the main elements of the crypto ecosystem?	
5.	Discussing virtual assets in the context of environmental crimes.	18
	• Amazonia, environmental crimes, and money laundering in Peru and Colombia • The role of illegal armed groups	
6.	Using Virtual Assets for Illicit Financial Flows Linked to Natural Resources. Trends and Typologies	31
	6.1. Using VAs in Illegal Mining (especially gold)	
	• Repatriation of resources from trade-based money laundering (TBML) and fraudulent commercial invoicing (revenues from exports and imports) • Payments for services, suppliers, and products in the illegal mining chain • Money flows from human trafficking • Creation of cryptocurrencies or use of virtual assets to launder resources from illegal mining	
	6.2. Illegal Wildlife Trafficking	
	• Methods to pay for trafficked species and money laundering in connection with illegal wildlife trade	
7.	Conclusions on alerts and major risks identified	47
8.	Regulation in Colombia and Peru: A Path Yet to Be Taken	52
9.	General conclusions and recommendations	56



Acronyms

Acronym	Description
AML	Anti-Money Laundering
ATM	Cajero automático <i>Automated teller machine</i>
ATF	Anti- terrorism financing.
ASSM	Artisanal and Small-Scale Mining
BF	Beneficial Owner
CBDC	<i>Central bank digital currency</i>
CDD	Customer Due Diligence
DDOT	Departamento contra la Delincuencia Organizada Transnacional. / Department against Transnational Organized Crime
DeFi	<i>Decentralized finance</i>
DIAN	Dirección de Impuestos y Aduanas Nacionales. / National Directorate of Taxes and Customs
DIJIN	Dirección de Investigación Criminal e Interpol. / Criminal Investigation Directorate and Interpol
EIA	Environmental Investigation Agency
ELN	Ejército de Liberación Nacional. / National Liberation Army
EMIC	Electronic Money Issuing Companies
FARC-EP	Fuerzas Armadas Revolucionarias de Colombia – Ejército del Pueblo. Revolutionary Armed Forces of Colombia – People’s Army
FATF	Financial Action Task Force
FCDS	Foundation for Conservation and Sustainable Development

Acronym	Description
FinCEN	Red de Control de Delitos Financieros Financial Crimes Enforcement Network
FIR	Financial Intelligence Reports
KYC	<i>Know your customer</i>
LAC	Latin America and the Caribbean
LBMA	London Bullion Market Association
ML/TF	<i>Money Laundering and Terrorism Financing</i>
NFT	<i>Non-fungible token</i>
OAS	Organization of American States
OFAC	Oficina de Control de Activos Extranjeros. / Office of Foreign Assets Control
P2P	<i>Peer to peer</i>
SFC	Superintendencia Financiera de Colombia. / Financial Superintendence of Colombia
SPLAFT	System for the Prevention of Money Laundering and Terrorist Financing.
STR	Suspicious Transaction Report
TBML	<i>Trade-based money laundering</i>
UIAF	Unidad de Información y Análisis Financiero. / Financial Information and Analysis Unit
UIF	Unidad de Inteligencia Financiera. / Financial Intelligence Unit
USDT	Tether
VA	Virtual Assets
VASP	Virtual Asset Service Provider



Introduction

In recent years, Latin America and the Caribbean have seen a steady increase in the use of virtual assets. Cryptocurrencies and other digital assets are used by thousands of people in the region as a means of investing, saving money, and making payments. Due to its decentralized structure, the world of virtual assets, sometimes known as the “crypto universe,” offers a chance for financial autonomy and independence, but it is also becoming a significant conduit for the transfer of illicit funds linked to various crimes across the globe.

The increasing use of cryptocurrencies, including bitcoin, which has become one of the most popular over the past ten years, has led to the implementation of monitoring, inspection, investigation, and control measures for virtual asset service providers (VASPs) and users who transact within this ecosystem, according to a number of international organizations. This is because of the dangers of anonymity and opacity it may provide, which may make it easier to commit financial crimes including money laundering from illegal enterprises like drug trafficking, human trafficking, migrant smuggling, and, more lately, environmental crimes¹.

The use of cryptocurrency to transfer illegal funds from environmental crimes, especially those that originate in the Amazon, as not received much attention². Because of this, this report aims to investigate potential links between illegal mining, illegal logging, and wildlife trafficking, among other crimes, and the use of virtual assets as conduits for money laundering and financing in nations like Colombia and Peru. In addition to being suppliers of natural resources obtained illegally through intricate criminal networks working in the region’s difficult geographies, these nations currently display noteworthy data on the acceptance and use of cryptocurrencies.

There are currently very few investigated and prosecuted instances in Colombia and Peru concerning the use of cryptocurrency to transfer or launder money connected to illegal operations involving natural resources. This paper concentrates on examining the primary threats and global viewpoints applicable to the local setting. It also highlights a few instances that offer insights into the strategies used by criminals to transfer money related to environmental offenses. It also draws attention to the difficulties resource-producing nations—like those that produce gold—face in this new financial

1 FATF. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. Paris: FATF.

2 Bruton, D. (2025, 23 de abril). *The virtual connection: Illicit natural resource trade, cryptocurrency, and extremist financing*. GNET – Global Network on Extremism & Technology. <https://gnet-research.org/2025/04/23/the-virtual-connection-illicit-natural-resource-trade-cryptocurrency-and-extremist-financing/>

system, which occasionally aims to use the mineral as a value basis for stablecoins³.

The study examined records and public data on criminal activity and cryptocurrency assets, as well as trends in money laundering and other related typologies, as reported by international standards, non-governmental organizations, and interviews with specialists in financial crimes, environmental crimes, and virtual assets. It also incorporates viewpoints from Colombian and Peruvian authorities as well as the VASP business.

Thus, the report outlines the existing regulatory framework, identifies its main gaps, and proposes recommendations to strengthen it. It is based on the premise that without robust regulation—such as that developed in the European Union or in countries like Indonesia, Germany, and South Korea⁴—, intelligence, investigation, detection, and prevention of crimes associated with the crypto ecosystem become more difficult, hindering understanding of the phenomenon and effective prosecution of actors involved in illicit activities through crypto.

The primary means of transferring resources from environmental crimes through virtual assets and their connections to the supply chains of the most significant natural resources are also examined in the research. Case studies pertaining to other crimes or explicitly documented experiences on this subject serve as the foundation for this review. It recognizes that very little information is available—whether in court proceedings, press reports, or documented cases—largely because of the difficulty of tracking these illegal flows, the lack of knowledge about the phenomenon, and the general opinions about the crypto ecosystem in the area.

In order to improve overall comprehension and response capability to the risks posed by this developing industry in the battle against financial and environmental crimes, common traits, emerging trends, risks, and important suggestions are highlighted in this research piece.



Criminal networks operating in Venezuela and Brazil not only supply machinery, fuel, and labor for the illegal extraction of natural resources in Colombia and Peru, but also participate in broader schemes involving gold smuggling, illegal logging, drug trafficking, and wildlife trafficking. Therefore, the use of cryptocurrencies could potentially reduce traceability risks and facilitate international transactions.

3 Feingold, S. (2025, 26 de marzo). *Stablecoin surge: Reserve-backed cryptocurrencies are on the rise*. World Economic Forum. <https://www.weforum.org/stories/2025/03/stablecoins-cryptocurrency-on-rise-financial-systems/>

4 Chainalysis. (2025, 26 de junio). *The road to crypto regulation: Crypto's journey from margins to mainstream* [Entrada de blog]. Chainalysis. <https://www.chainalysis.com/blog/the-road-to-crypto-regulation-part-1/>



Finally, the report addresses the relationship between the demand for gold in the crypto industry and the current situation of illegal mining in countries like Colombia and Peru, as this is another important factor to consider in analyzing the links between the crypto ecosystem and illegality surrounding the production of minerals such as gold in the Amazon.

As stablecoins grow and the need for backing systems that legitimize their autonomy and decentralization increases, gold becomes a very important alternative, as it has historically been for money as we know it. The report explains this phenomenon and provides alerts and recommendations to countries under pressure to produce the mineral⁵.

It is expected that this report will provide new perspectives for understanding the phenomenon of illicit financial flows associated with natural resources and environmental crime in the Amazon, especially in Peru and Colombia, considering current technological innovations, the evolution of organized crime, and the challenges faced by those working to prevent and detect these crimes. Understanding how illicit money from these activities moves is key to identifying who is truly behind these businesses and avoiding the criminalization of the initial links in the chain that do not actually operate or finance the business.

In light of recent technological advancements, the development of organized crime, and the difficulties faced by those attempting to prevent and detect these crimes, it is anticipated that this report will offer fresh insights into the phenomenon of illicit financial flows connected to natural resources and environmental crime in the Amazon, particularly in Peru and Colombia. Determining the real main actors behind these businesses and preventing the punishment of the first links in the chain that do not actually run or finance these activities depend on an understanding the flows of illegal money from these operations.

5 Donovan, K., & Nikoladze, M. (2025, 22 de mayo). Gold's geopolitical comeback: How physical and digital gold can be used to evade US sanctions [Entrada de blog]. *Atlantic Council*. <https://www.atlanticcouncil.org/blogs/new-atlanticist/golds-geopolitical-comeback-how-physical-and-digital-gold-can-be-used-to-evade-us-sanctions/>

Guide to Understanding the Crypto World. Basic Concepts

As humanity has evolved, so too has our idea of money. One common assumption, however, is that (fiat) money as we know it is issued by a central bank or other organization that centrally controls and protects it through intermediaries. Instead, decentralization is the governing principle of the virtual asset universe. In other words, a central body that oversees and regulates the issuance of money does not issue virtual assets. Rather than requiring intermediation, control, or management by a central authority, these currencies are transferred between two parties (P2P exchange)—that is, between one person and another—and employ cryptography as a means for transaction protection and anonymization.

As summarized by Coinbase, cryptocurrencies refer to decentralized «digital money used over the internet»⁶. But why did the need arise to develop this type of “digital” money that is not backed by any central bank?

Financial crises have frequently affected the banking industry, endangering the assets of the populace. Following the US financial crisis in 2008, a number of financial institutions filed for bankruptcy, costing thousands of people their money once more. The bitcoin whitepaper was released in response by Satoshi Nakamoto, whose real identity is still a mystery. Bitcoin, which was developed to allow people more control over how they manage their money without depending on a third party to transact, secure, or back it, is currently the cryptocurrency with the highest reputation and the largest global adoption⁷.

6 Coinbase. (s. f.). *What is cryptocurrency?* Coinbase Learn. <https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency>

7 Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [Documento técnico]. Bitcoin. <https://www.bitcoin.org/bitcoin.pdf>



The advent of bitcoin marked the formal inception of the cryptocurrency realm, introducing numerous notions that are essential to delineate for this research. The following are fundamental principles essential for comprehending the operation of the virtual asset ecosystem and its connections to illegal financial flows:



Fiat money: Also known as “real money” or “legal tender.” The currency or banknote of a country designated as legal tender, which circulates and is usually used and accepted as a medium of exchange in that country.



Virtual assets (VAs) or crypto assets: Any representation of value that can be exchanged, transferred, or used as a means of payment digitally. This does not include the digital representation of currencies issued by a central bank (CBDC). This is the official concept recommended by the Financial Action Task Force (FATF) to refer to this ecosystem.



Cryptocurrency: A decentralized digital currency, based on cryptography, designed to function as a medium of value exchange on the internet. Bitcoin was the first cryptocurrency and remains the most widely accepted, along with others such as Ethereum, Tether (USDT), and Solana. Cryptocurrencies allow value transfer without the need for a financial intermediary, and they require their own blockchain—a continuous, constant, and decentralized ledger in which every transaction made with that currency is securely and anonymously verified through a block-chain system.



Stablecoin: A cryptocurrency whose value is pegged to stable assets, such as the U.S. dollar. It enables transfers with lower volatility and has become common in money laundering operations. Examples include USDT and USDC.



Blockchain: A decentralized digital ledger that allows transactions to be stored securely and transparently. Cryptocurrencies use this technology, which enables anyone to view and verify all transactions carried out with a specific cryptocurrency, making it a mechanism of full transparency and traceability.

Contrary to popular belief, all transactions on public blockchains can be identified. The challenge lies in linking these transactions and “users” (senders and receivers) to specific individuals, since cryptography protects their identities. There are also private blockchains with restricted access and closed information management, which make traceability and monitoring more difficult—thus are preferred by money launderers. Blockchain technology is applied across multiple processes, supply chains, and economic sectors, focusing on process tracking and traceability.



P2P (peer-to-peer): Direct exchange of cryptocurrencies between individuals, without intermediaries, through a blockchain-based exchange platform.



Hash: A fixed-length alphanumeric code (letters and numbers) that identifies or represents a transaction or a wallet holding cryptocurrencies or virtual assets. While it does not reveal the user’s identity, the transaction history remains recorded on the blockchain.



Virtual wallet: A tool that allows interaction with a blockchain network. It can be used to send and receive cryptocurrencies. Each wallet has a unique identifier, a “hash,” enabling fast, secure, and simple transfers. Wallets vary in length between 26 and 32 characters. Some wallets are hosted on exchanges, where cryptocurrencies can be bought and traded, while others are “cold wallets,” not connected to the internet, offering greater security and anonymity for storage. These can be purchased online and resemble hard drives or USB devices. They use strong alphanumeric codes as passwords, self-managed by users. Wallets can be custodial (controlled by a third party) or non-custodial (controlled solely by the user).



Crypto exchange: Any individual or legal entity that conducts exchanges between virtual assets and fiat money, exchanges between virtual assets, transfers virtual assets, safeguards and/or manages them, or provides financial services related to the issuance or sale of a virtual asset.



Mixers or tumblers: Services that mix cryptocurrencies from multiple users to obscure the origin and destination of funds



Crypto ATMs (Bitcoin ATMs): Electronic or physical ATMs that allow users to buy or sell cryptocurrencies using cash or cards. Some models also allow cash withdrawals in exchange for crypto assets.



Virtual Asset Service Provider (VASP): Any individual or legal entity offering services to exchange fiat for virtual assets, exchange different cryptocurrencies, or provide custody services for virtual assets, among others.



Money mule networks: Individuals who transfer or withdraw illicit funds. In the crypto environment, they operate wallets or bank accounts to conceal the trail of virtual assets.



Travel rule: A recommendation established by FATF requiring member countries to mandate VASPs to share sender and recipient data when transactions exceed a certain threshold.



Smart contract: Blockchain-stored executable code that automates agreements without intermediaries. Its use can facilitate complex laundering schemes without direct human intervention.



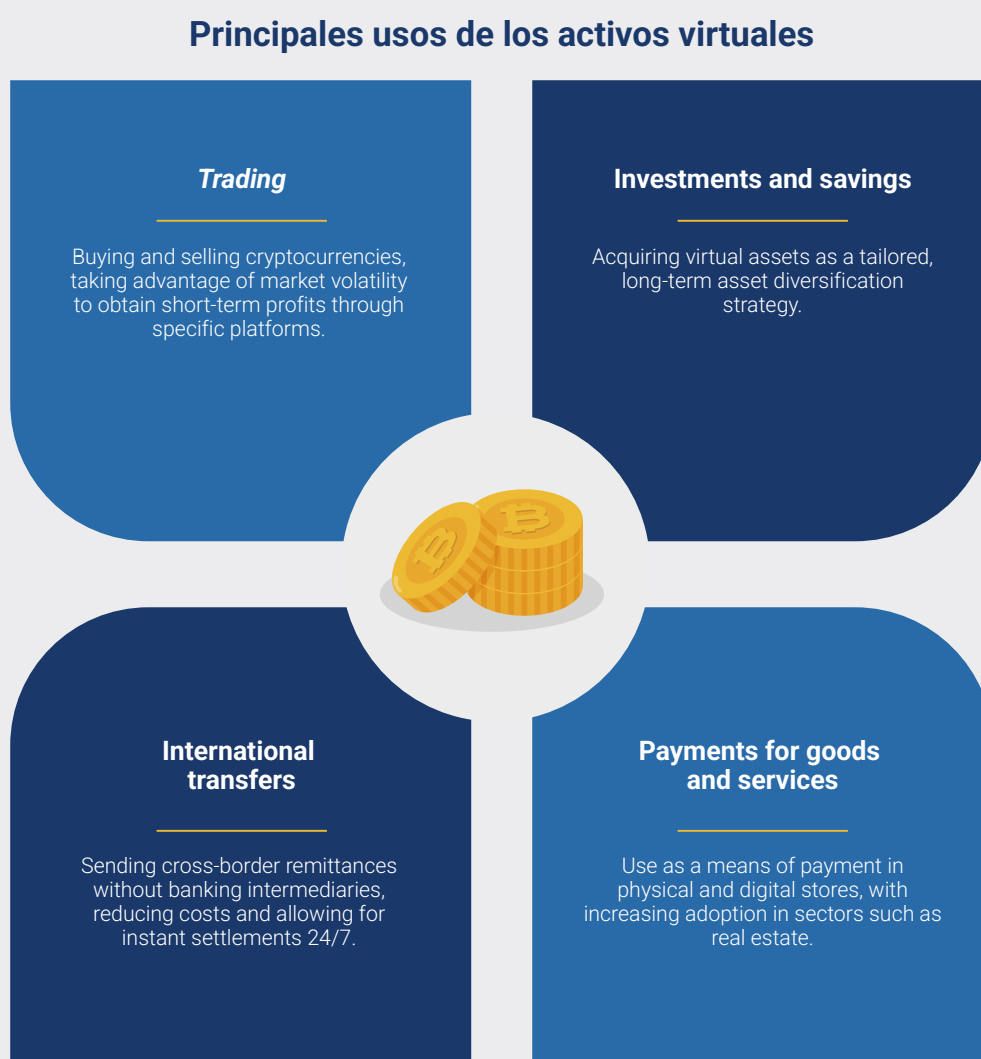
Smurfing: Splitting large sums of virtual assets into microtransactions. Criminals often use this method to evade anti-money laundering controls and avoid transaction tracking.

Uses of Virtual Assets

It is crucial to recognize that virtual assets are not intrinsically unlawful. Although many nations have deemed their usage illegal, most of the world does not enforce such explicit bans, as VAs were not originally designed for illicit purposes.

Virtual assets and their ecosystem possess numerous legitimate applications. Most governments in the region have neither controlled nor prohibited them. It is crucial to emphasize that diminished regulation facilitates illegal actors' ability to utilize this route for the transfer of unlawful financial flows.

Infographic 1. Uses of virtual assets



Source: Prepared by the authors.

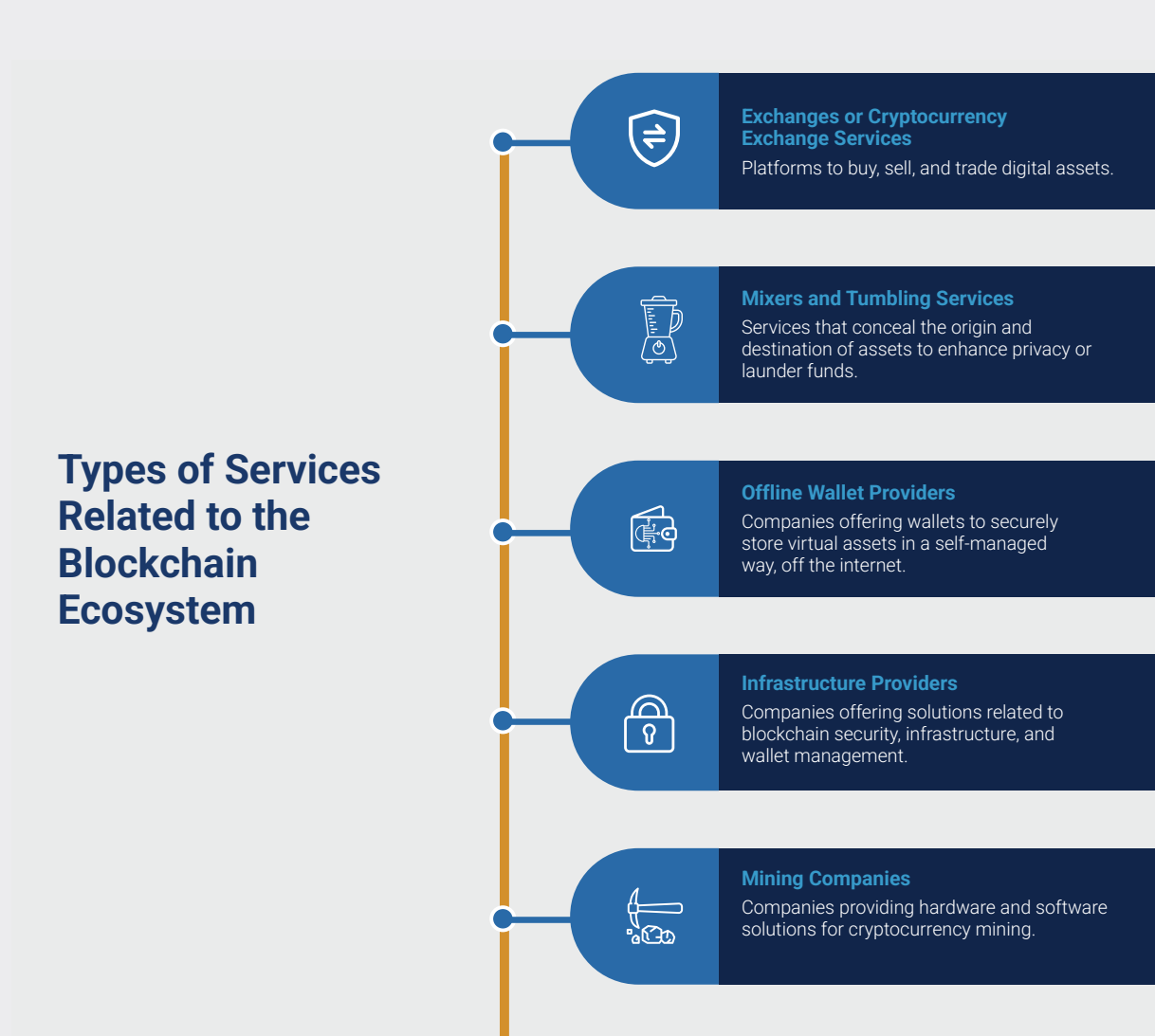


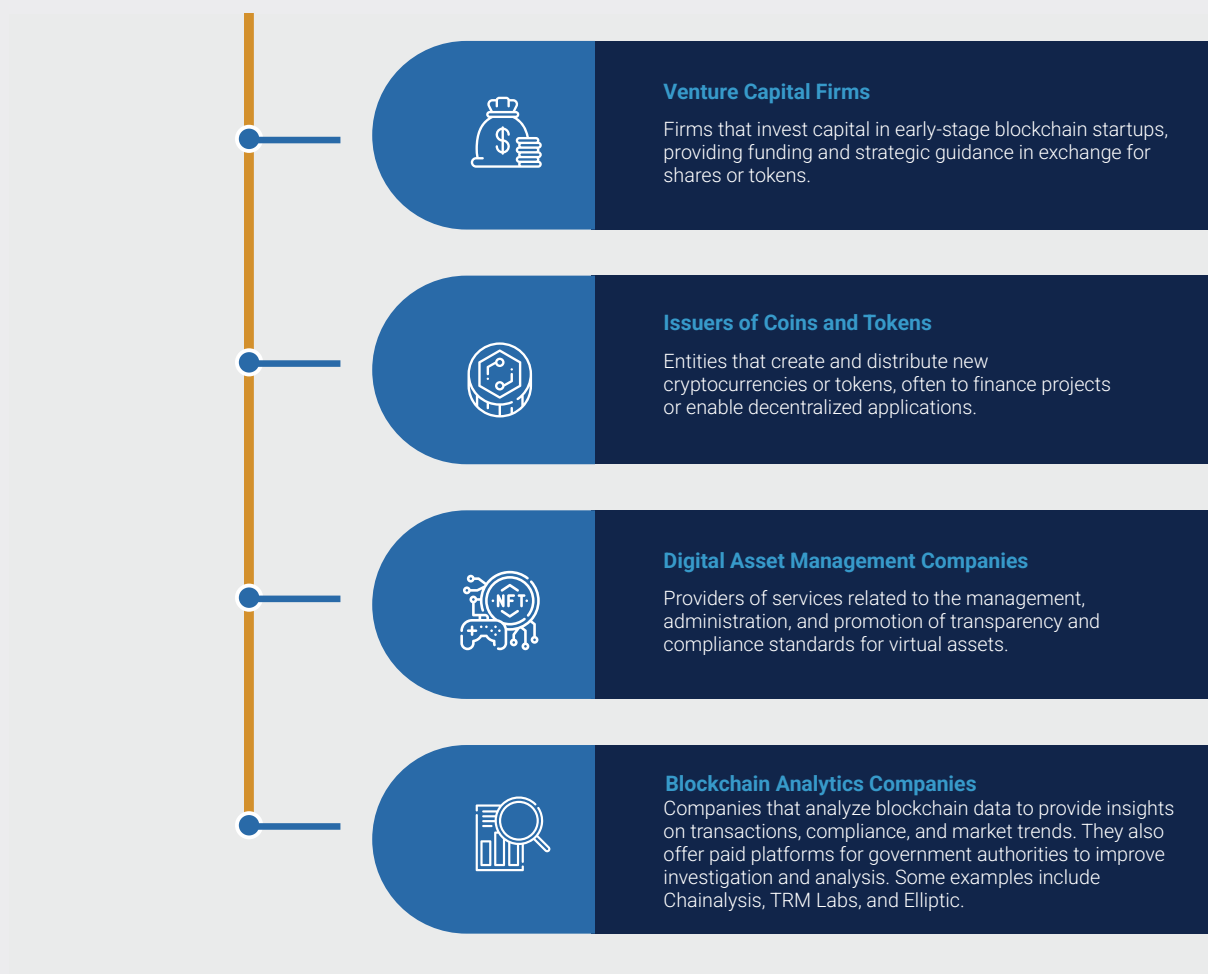
What Are the Main Elements of the Crypto Ecosystem?

Although many regulations focus on the use of certain cryptocurrencies by the civilian population — as was the case in El Salvador, which made bitcoin legal tender — there are many more aspects that must be considered regarding the functioning and regulation of the virtual asset universe.

It is crucial to identify each actor in the ecosystem, as they each play a unique role. This will enable us to determine the appropriate placement of controls and prospective regulations in countries that do not yet have sufficient legislation regarding virtual assets.

Infographic 2. Types of Services Related to the Blockchain Ecosystem





Source: Prepared by the authors.

As shown in Infographic 2, when discussing the universe of Virtual Assets (VA), it is not only financial operations and cryptocurrencies that must be taken into account. There are different companies and specialized services in this sector that could also be subject to regulation. However, at the international level, regulation is mainly focused on “exchange” services, as well as on granting licenses to VASPs, but not necessarily on regulating cryptocurrency mining activities.



Discussing Virtual Assets in the Context of Environmental Crimes

As explained earlier, virtual assets (VA), and especially cryptocurrencies, emerged as an alternative to the global financial system operated by third parties, since they allow individuals to self-custody and self-manage their money. Through technologies such as blockchain, millions of people worldwide no longer depend on financial institutions, remittance companies, or any other intermediaries for the exchange and custody of money, or for transferring funds from one country to another.

VAs have proliferated in recent years. The adoption and use of crypto have been primarily concentrated in lower-middle-income countries, as per Chainalysis. In 2024, it made substantial progress in developed nations⁸.

The advantages offered by this ecosystem are numerous, starting with the speed and cost of cross-border transactions, as well as the self-custody of resources outside the financial system. However, while VAs are a channel for transmitting value—just like banks, fintechs, gold, livestock, or any other medium to move value—they can also serve to move illicit financial funds.

Chainalysis estimates that the amount of illicit funds moved through crypto in 2024 alone was at least USD 40 billion⁹. This suggests that VAs may be a relevant channel for laundering money from illicit sources. According to the FATF, red flags have been raised regarding potential money laundering through VAs in crimes such as drug trafficking, arms trafficking, fraud, tax and sanctions evasion, corruption, human trafficking, and child sexual exploitation¹⁰.

8 Chainalysis. (September 12, 2024). The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) region leads the world in terms of global cryptocurrency adoption [Entrada de blog]. *Chainalysis*. <https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/>

9 Funds sent to wallets identified as illicit and funds stolen by cryptohackers.

10 GAFI. (2020). *Indicadores de señales de alerta de lavado de dinero y financiamiento del terrorismo asociados con los activos virtuales*. París, Francia: GAFI.

The apparent anonymity and the possibility of operating outside centralized and supervised financial systems in most jurisdictions make the crypto universe highly susceptible to money laundering from illicit activities—just as traditionally have been the financial system, companies, gold, livestock, real estate and other

International standards for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) are constantly updated with recommendations on trends, typologies, and new risks. In 2021, the FATF updated its first official document compiling a series of red flags related to detecting suspicious transactions involving crypto¹¹assets, as well as a risk-based guide on potential money laundering and terrorist financing (ML/TF) through the crypto ecosystem.

Since the publication of these recommendations, many countries in the region have implemented actions and regulatory changes to strengthen supervision, identification, and control of the potential criminal use of the VA ecosystem. However, there have been few efforts toward comprehensive regulation in Latin America, particularly in the Amazonian countries, despite FATF recommendations and international examples such as the European Union’s Markets in Crypto-Assets (MiCA) Regulatory Framework¹².

Of the eight countries that make up the Amazon region (excluding French Guiana, which follows French guidelines for VA adoption and regulation), only Venezuela has measures for VA regulation and monitoring. The other countries, while issuing statements or requiring VASPs to report information as obligated entities (at best), do not directly regulate adoption, use, and oversight, as shown in Table 1.

Nevertheless, crypto adoption among citizens in these countries is growing significantly. Brazil ranks 10th globally in crypto adoption, followed by Venezuela (13th), Colombia (36th), and Peru (42nd). According to Chainalysis, these countries follow the same order in the regional ranking of crypto transacted value¹³.

Table 1 shows a comparison of the main statistics available on crypto usage, adoption, and value traded in Amazonian countries.

11 GAFI. (2021). *Guía actualizada para un enfoque basado en riesgo para los activos virtuales y los proveedores de servicios de activos virtuales*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>

12 ESMA. (s. f.). Markets in Crypto-Assets Regulation (MiCA). <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

13 Chainalysis. (2024). *Crypto Geography Report 2024*. Chainalysis. <https://www.chainalysis.com/reports>

Table 1. Amazon Region Countries: Regulation, Use, and Crypto Adoption

Country	Regulation ¹⁴	Position in the global cryptocurrency adoption ranking ¹⁵	Annual value received in transactions in USD (2023-2024) ¹⁶	Position in regional ranking by value received ¹⁷
Brazil	No	10	90,3 billion	2
Bolivia	No	101	Less than 1 billion	12
Colombia	No	36	25-27 billion	5
Ecuador	No	67	Between 1 and 5 billion	9
Guyana	No	-	-	33
Peru	No	42	Between 5 and 15 billion	7
Surinam	No	138	Less than 0.5 billion	26
Venezuela	Yes	13	Less than 0.5 billion	4

Source: Prepared by the authors based on Chainalysis Cryptocurrency Geography Report (2024), Chainalysis Global Adoption Index (2024), Coinbase Crypto Regulation Ranking (2024), Cripto Abierto platform¹⁸, and official country documents.

14 For the purposes of this table, regulation is defined as legislation that explicitly governs, at the national level, the use of virtual assets, as well as the licensing of Virtual Asset Providers (VAPs) in each jurisdiction. The existence of official statements from regulatory bodies or specific requirements for ecosystem actors is not considered regulation.

15 Chainalysis. (2024, 12 de septiembre). *Global Crypto Adoption Index 2024*. Chainalysis. <https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/>

16 Estimaciones basadas en Chainalysis. (2024). *Informe de geografía de las criptomonedas 2024*. Chainalysis. <https://www.chainalysis.com/reports>

17 Estimaciones basadas en Chainalysis. (2024). *Índice global de adopción de criptomonedas 202*. Chainalysis. <https://www.chainalysis.com/reports>

18 Cripto Abierto. (s. f.). <https://www.criptoabierto.com>

It is critical to acknowledge that, in the context of environmental crimes, it may be necessary to evaluate the regulatory landscape, as well as the levels of value transacted and the scope of crypto use and adoption in border countries that comprise the Amazon region, as analyzed in this context.

As shown in Table 1, Brazil and Venezuela lead the regional ranking in terms of VA adoption and use, as well as in the largest volumes of money transacted by their users. Colombia and Peru are not far behind: although they occupy positions 5 and 7, respectively, in financial movements with cryptocurrencies in Latin America and the Caribbean, they also record a significant volume of transactions carried out by their users.

In this context, it is imperative to investigate the potential correlation between the extensive utilization of crypto assets in Brazil and Venezuela and illicit cross-border dynamics that directly impact Colombia and Peru, particularly in Amazonian and border regions where state control is lacking. For instance, illegal gold mining is one of the most prevalent activities in these regions¹⁹, which in turn facilitates a variety of money laundering techniques. Although there is insufficient data or cases to ascertain whether VAs are one of the primary channels for laundering or moving this illicit money, it is certain that the rapid growth, growing adoption of VAs in neighboring countries, and weak regulation could facilitate their use for laundering money from illegal mining

The use of cryptocurrencies as a means of payment or value storage in these activities enables the diversion of resources, payments to illegal actors, and evasion of financial controls, especially in territories where traditional banking systems are not present or are unreliable.

Likewise, criminal networks operating in Venezuela and Brazil not only supply machinery, fuel, and labor for the illegal



Illegal gold mining, for example, is one of the activities that generates the most illicit financial flows in these regions, driving various money laundering methods. While there is insufficient data and evidence to determine whether virtual assets (VAs) are a primary channel for laundering or moving this illicit money, it is certain that the growing adoption of VAs in neighboring countries, their rapid growth, and weak regulation could facilitate their use for laundering money from illegal mining.

19 International Crisis Group. (2025, 29 de julio). *La maldición del oro: minería y violencia en el sur de Venezuela*. Informe América Latina N.º 53. Bogotá/ Bruselas: International Crisis Group.



extraction of natural resources in Colombia and Peru, but also participate in broader schemes of gold smuggling, illegal logging, drug trafficking, and wildlife trafficking. Thus, the use of cryptocurrencies could potentially reduce traceability risks and facilitate international transactions²⁰.

Such convergence of environmental crimes, transnational criminal economies, and the use of decentralized financial technology such as cryptocurrencies poses significant challenges for anti-money laundering systems and international cooperation. Understanding these links is key to designing more effective responses that integrate advanced investigative techniques, money-tracking, technological tools, financial intelligence, and knowledge of VAs, as well as their connections to the environment and natural resources.

In addition to the lack of mechanisms in these countries to regulate crypto operations, the absence of regulation in countries where the Amazon is seemingly remote can also affect financial integrity and facilitate laundering. Many VASPs used to move these resources are based in countries with weak or nonexistent regulations, avoiding know-your-customer (KYC) and AML/CFT procedures, to offer anonymity and facilitate the movement of illicit financial flows through their platforms, operating from anywhere in the world ²¹.

Crypto is a transnational phenomenon, and as such, it cannot be analyzed exclusively from a jurisdictional perspective. It is crucial to consider the geopolitics of cryptocurrencies and external factors, as well as to comprehend the potential risks of criminal dynamics in border countries when transporting illicit financial flows that are linked to environmental offenses or natural resources.

Authorities responses will only be effective to the extent that they understand the risks associated with the Amazon countries, particularly regarding the use, adoption, and regulation of crypto among Brazil, Colombia, Venezuela, Ecuador, and Peru.

The Amazon, Environmental Crimes, and Money Laundering in Peru and Colombia

Environmental crimes, particularly those pertaining to the illicit extraction and commercialization of natural resources from their ecosystems and geographies, such as timber, minerals, precious stones, and various species of fauna and flora, are a major problem for nations like Colombia and Peru.

20 Ramírez Cabello, M. (2023, 6 August). Grupos armados amenazan tierras indígenas en el sur de Venezuela. *InfoAmazonia*. <https://infoamazonia.org/es/2023/08/06/grupos-armados-amenazan-tierras-indigenas-en-el-sur-de-venezuela/>

21 OCCRP. (2024, 25 June). Nigeria acusa a 53 personas por una estafa global de criptomonedas y una red de ciberdelito. *OCCRP*. <https://www.occrp.org/en/news/nigeria-charges-53-in-global-crypto-scam-cybercrime-ring>

According to the Observatory of Socio-Environmental Conflicts of the Foundation for Conservation and Sustainable Development (FCDS), Peru has more than 78 million hectares of the Amazon biome in its continental territory, compared to at least Colombia's at least 48 million hectares—an important figure for Amazonian countries and for resource conservation.

Efforts to conserve and preserve Amazonian ecosystems in both countries face strong pressures, mainly due to socio-environmental and territorial conflicts, the presence of multiple illegal armed groups and criminal organizations controlling illicit economies in the region, as well as deforestation linked to agricultural frontier expansion, extensive cattle ranching, logging, and illegal mining.

The rise in gold prices in recent years and the ease to legalize illegally extracted gold have driven the growth of gold mining and other strategic minerals in countries such as Peru and Colombia. According to S&P Global, «not all artisanal and small-scale gold mining (ASGM) is illegal, but these types of operations are often a frequent and lucrative target for organized crime and corruption in many regions.»²². This has led to a rapid increase in gold prices and has made the sale of this asset even more profitable than cocaine for criminal groups, as shown in Graph 1.

Gráfico 1. Incremento en los precios del oro, 1970-2025



Source: London Bullion Market Association (LBMA).

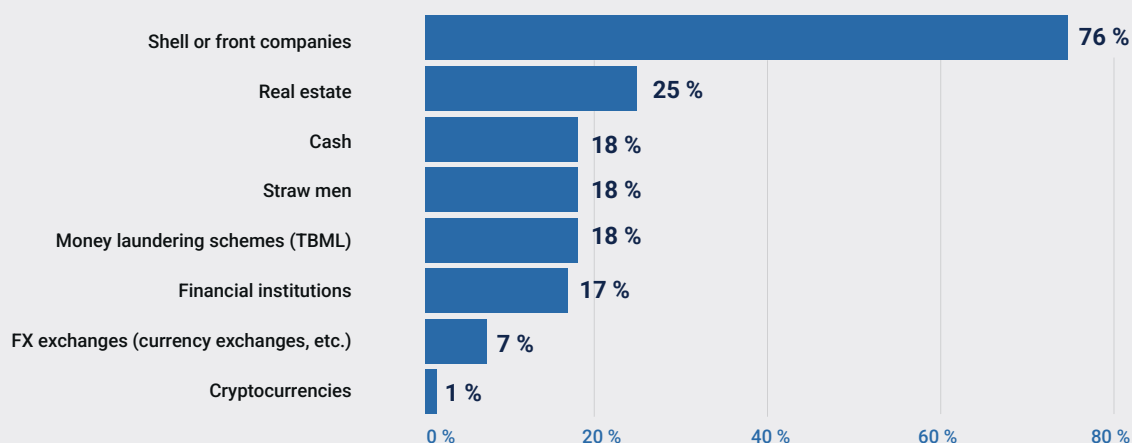
²² S&P Global Commodity Insights. (2025, June). *Illegal mining rises globally along with gold price*. S&P Global Market Intelligence.



Connections between Amazonian countries in the supply routes of inputs, as well as in illicit production and commercialization, highlight the crossborder dynamics around illicit financial flows, both inbound and outbound, among countries including Venezuela and Brazil, and Colombia, Peru, and Ecuador. These countries that, as shown in Table 1, show significant levels of crypto adoption, use, and appropriation, with weak regulations or opaque democracies.

The most recent report from the Financial Accountability and Corporate Transparency Coalition (FACT Coalition) states that money obtained from environmental crimes in the Amazon, including illicit mining, illicit logging, illegal fishing, and wildlife trafficking, is mostly laundered through shell or front companies, followed by real estate investment and cash smuggling. Many of these illicit flows may be laundered through VAs, even though the report ranks the usage of cryptocurrencies last, as will be demonstrated later. Few cases have yet been found that unequivocally show this channel to be among the most common. Additionally, as will be discussed in more detail, the primary laundering typologies found in the FACT Coalition study are also used and combined by laundering typologies related to the usage of VAs, particularly in the integration phase.

Graph 2. Most Prevalent Money Laundering Typologies of Environmental Crimes in the Amazon



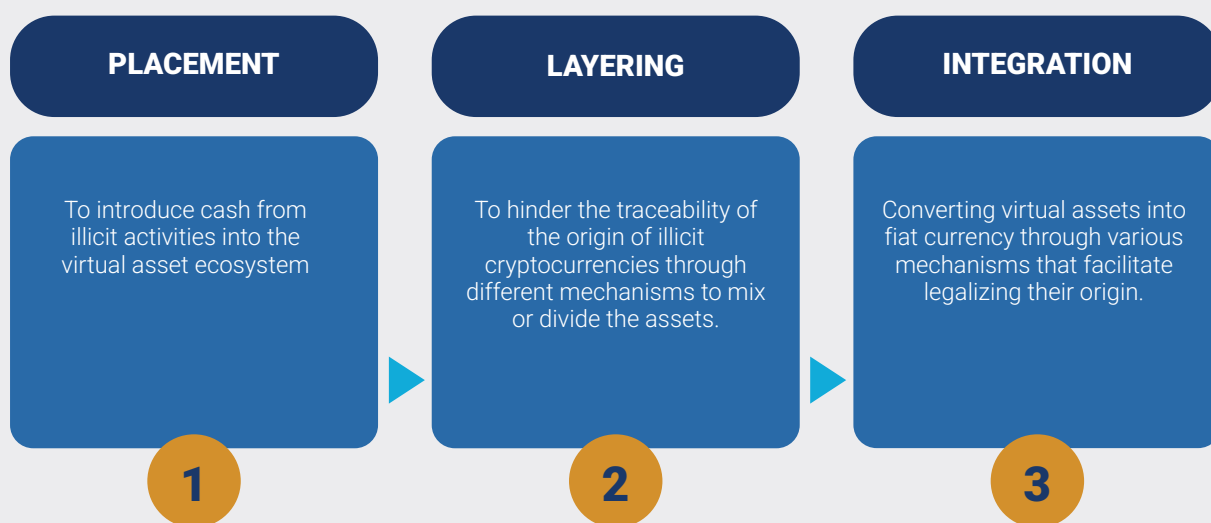
Source: Analysis of 230 cases of environmental crimes in the Amazon developed by FACT, 2014-2024. The percentage is calculated based on 71 cases for which some financial investigation was available.

According to experts and other documentary sources, as well as from the analysis of existing cases of laundering through VAs in various crimes, illicit money entering and moving through the crypto ecosystem follows a typology very similar to traditional channels, which involves:

1. **Obtaining the money associated with the illicit activity.**
2. **Placement:** entry of illicit money into the crypto ecosystem through the acquisition of virtual assets on exchange platforms or P2P..
3. **Layering:** transfer of funds to other platforms that help conceal the initial flow of money. In the crypto universe, this may involve transfers to multiple wallets, the use of mixers or tumblers.
4. **Integration:** funds are moved outside the financial system, either by monetizing crypto into fiat cash, into bank accounts or other financial platforms, using credit cards for payments, investing in real estate, or creating shell companies, among other options.

Figure 3 characterizes the phases of money laundering through cryptocurrencies.

Graph 3. How Is Illicit Money Laundered Through Crypto?.



Source: Prepared by the authors



According to this methodology, many illicit financial flows may be legalized precisely in the integration phase through the same money laundering channels identified by the FACT Coalition as most prevalent in the Amazon. To monetize money held in crypto, methods range from creating shell or front companies to justify the legality of funds, to investing in cash-intensive businesses (casinos, currency exchange houses, commerce, etc.), and purchasing real estate or products directly using cryptocurrencies such as bitcoin or other stablecoins as a payment method.

The following analyzed case exemplifies the use of different channels for money laundering in the integration phase, once mobilized through cryptocurrencies, as well as the creation of a cryptocurrency company (VASP) to justify the origin of resources.

Case 1. Laundering More Than USD 500 Million Through the U.S. Financial System, Including Transactions with Sanctioned Russian Banks sancionados²³

Iurii Gugnin, a Russian citizen residing in New York, designed and executed a sophisticated money laundering scheme through two shell companies registered in the United States: Evita Investments Inc. and Evita Pay Inc. These companies, which operated under the guise of cryptocurrency service startups, served as channels to receive more than USD 500 million in virtual assets, primarily tether (USDT), from foreign clients, many of whom had funds in sanctioned Russian banks.

Through these entities, Gugnin converted cryptocurrencies into dollars or other fiat currencies and moved the resources through U.S. bank accounts, systematically concealing the illicit origin of the funds, the ultimate beneficiaries, and the connection with Russia through altered invoices and disguised transactions.

- Use of shell companies to channel illicit funds
- Multi-stage crypto-to-fiat conversion
- Conversión crypto-fiat en múltiples etapas
- Use of exchanges and banks with false statements (institutional fraud)
- Regulatory non-compliance in a VASP regulated jurisdiction (United States)
- Use of cryptocurrencies to evade international sanctions
- Use of multiple channels to legitimize money in different combinations (crypto-financial system, crypto-companies, crypto-TBML, crypto-fraudulent invoicing)
- Preference for using stablecoins

²³ U.S. Department of Justice. (9 June, 2025). *Founder of cryptocurrency payment company charged with evading sanctions and export controls, defrauding financial institutions, and violating the Bank Secrecy Act* [Comunicado de prensa]. Office of Public Affairs. <https://www.justice.gov/opa/pr/founder-cryptocurrency-payment-company-charged-evading-sanctions-and-export-controls>

The role of illegal armed groups

Although there is little or no information about the potential use of crypto by illegal armed groups operating in the Amazon, many of them control different businesses in these areas. In the case of Colombia, the presence of dissident factions of the extinct Revolutionary Armed Forces of Colombia (FARC-EP) and the National Liberation Army (ELN) stands out, as well as other FARC-EP dissident groups such as Segunda Marquetalia and its Border Commands. In Peru, the Border Commands and more local criminal groups such as Los Auríferos de Chorrillos, Las Nenas de la Pampa, Los Rápidos del Amazonas and Los Profes, among others²⁴.

Table 2. Illegal armed groups present in the Amazon of Colombia and Peru

Colombia	
Dissidents of Segunda Marquetalia and Border Commands	Zonas de Southern border areas with Ecuador, Peru and Brazil sur con Ecuador, Perú y Brasil
	Some municipalities in the departments of Caquetá, Putumayo and Amazonas
Dissidents of Estado Mayor Central	Some municipalities in the departments of Meta, Vichada, Guainía, Vaupés, Caquetá, Guaviare, Putumayo and Amazonas
	Southern border areas with Venezuela, Ecuador, Peru and Brazil
ELN	Border areas with Venezuela and Brazil
	Some municipalities in the departments of Vichada and Guainía
Perú	
Border Commands	Border areas with Colombia and Ecuador
	Some areas in Loreto
Comando Vermelho	Border areas with Brazil
	Some areas in Ucayali
Other groups	Some areas in Madre de Dios, Loreto and Cajamarca
	Border areas with Brazil and Bolivia

Source: Prepared by the authors based on information from Amazon Underworld and the FCDS Socio-Environmental Conflict Observatory.

²⁴ <https://amazonunderworld.org/es/mapa/>



As can be seen, there is no concrete evidence of a significant presence of Mexican cartels, such as the Sinaloa Cartel or the Jalisco New Generation Cartel, in the Colombian and Peruvian Amazon areas with the greatest exploitation and illicit trafficking of natural resources. However, press articles report these cartels are linked to Colombia, especially for the purchase and sale of cocaine from that country, as well as the supply of weapons, and with groups that do have a broad presence in the Amazon, such as the dissidents^{25 26}.

It should be noted that these groups have proven experience in using VAs to launder money associated with drug trafficking, especially to repatriate profits from the sale of fentanyl and other narcotics.

Case 2. Mexican cartels launder money through cryptocurrencies

Several members of the Sinaloa Cartel have been sanctioned by the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) for money laundering, arms trafficking, and fentanyl trafficking. Investigations reveal that one of the accused, a Colombian national, oversaw a money laundering organization that used bank transfers and cryptocurrency assets, among other means, to transfer illicit fentanyl revenues from the United States to the leaders of the Sinaloa Cartel in Mexico²⁷.

In addition, in 2021 it was discovered that a Las Vegas businessman laundered drug trafficking proceeds in association with these cartels by sending funds received in the name of his company via bank transfer to anonymous virtual wallets²⁸.

25 El Clip. (November 14, 2023). The tentacles of Mexican cartels extend into Colombia. *The Clip*. <https://www.elclip.org/operaciones-carteles-mexicanos-colombia/>

26 Saavedra, F. (March 27, 2025). This is how the Sinaloa Cartel's control grows in Cauca: Government confirms the relationship between Mexican drug traffickers and dissident groups. *Infobae*. <https://www.infobae.com/colombia/2025/03/27/asi-crece-el-control-del-cartel-de-sinaloa-en-el-cauca/>

27 U. S. Department of the Treasury. (September 26, 2023). *Treasury targets Sinaloa Cartel fentanyl trafficking operations and a Colombian cartel leader* [Nota de prensa]. Departamento del Tesoro de EE. UU. <https://home.treasury.gov/news/press-releases/jy1763>

28 U. S. Department of Justice, Oficina del Fiscal de Distrito para el Distrito Sur de Nueva York. (2024, 4 de marzo). Chief executive officer of a Las Vegas-based company convicted for multimillion-dollar fraud and money laundering scheme [Nota de prensa]. Departamento de Justicia de EE. UU. <https://www.justice.gov/usao-sdny/pr/chief-executive-officer-las-vegas-basedcompany-convicted-multimillion-dollar-fraud>

In 2024, an investigation led by U.S. authorities revealed that Mexican cartels relied on Chinese citizens to launder drug money through cryptocurrencies and to purchase chemical inputs related to fentanyl²⁹.

Channels and typologies ³⁰	
	Distribution of drug trafficking cash to various individuals (smurfing) to deposit into different virtual wallets linked to traffickers
	Use of crypto payments for the purchase of fentanyl-related inputs and products
	Layering of payments to traffickers by sending them to other virtual wallets, converting them to USDC or USDT, and investing in other activities
	Monero, bitcoin and Ethereum are used on dark web platforms to move funds anonymously ³¹ .

These channels, some of which have been sanctioned—especially by U.S. authorities—reflect that crypto use is present in organized crime dynamics and is potentially used in other businesses. Recently, the Environmental Investigation Agency (EIA) published a report revealing that «profits from the illegal trade in mercury and gold are supporting armed groups in Colombia and Mexico, and driving one of the most destructive Amazonian gold rushes in Madre de Dios, Peru»³².

29 Associated Press. (s. f.). 24 people charged in a money laundering scheme linked to Mexico's Sinaloa cartel, according to prosecutors. *AP News*. <https://apnews.com/article/sinaloa-cartel-fentanyl-mexico-china-los-angeles-034ad51dd03d0606767215b44aed2e91>

30 TRM Labs. (2023, September 27). The U.S. Treasury Department targets the Sinaloa Cartel and adds a cryptocurrency address to the sanctions list. *Blog de TRM Labs*. <https://www.trmlabs.com/es/resources/blog/u-s-treasury-targets-sinaloa-cartel-adding-crypto-address-to-sanctions-list>

31 Ruiz, V. (2025, 19 July). Cryptocurrencies: the financial weapon of the cartels. *Infobae*. <https://www.infobae.com/mexico/2025/07/20/criptomonedas-el-arma-financiera-de-los-carteles/>

32 Environmental Investigation Agency. (2025, July). *Smugglers leave no stone unturned: What the biggest exposed mercury smuggling operation reveals about the gold business [Report]*. EIA. <https://eia.org/report/traficantes-no-dejan-piedra-sin-levantar/>



Mainly, the Jalisco New Generation Cartel controls some mercury production mines in Querétaro, Mexico, which eventually reach the jungles of countries such as Peru and Colombia, and is one of the main drivers of illegal gold mining in these countries. According to the EIA:

For example, drug cartels in Colombia control a significant part of the internal mercury trafficking routes. According to conservative estimates, smuggled Mexican mercury has been used to extract at least US\$8 billion in illegal gold (at the current price of US\$3,300 per ounce)³³

Considering that mercury fosters illegal dynamics not only through its smuggling and illicit commercialization but also through the mining activity it enables, it is essential to take into account the role of cartels and their links with armed groups that control the drug trafficking business in the Amazon jungles. Although there is no direct and sustained presence of these cartels in the region, reports document significant connections associated with various organized crime strategies already venturing into environmental crimes³⁴.

While the EIA report does not shed light on payment methods associated with mercury trafficking, it can be inferred that, due to the sophistication, ease, and experience of these cartels in using crypto assets, they could be an ideal method of payment and repatriation of profits associated with illegal mercury and illicit gold among illegal actors in Colombia, Mexico, and other involved countries.

The connections between various criminal armed groups operating in Colombia and Peru and Mexican cartels that have prior experience using these mechanisms imply the use of new technologies, like VAs, for money laundering from various environmental crimes as well as the illegal trafficking of natural resources. Therefore, to identify the use of VAs in these operations and go beyond cases that just track the money trail of drug trafficking, it is imperative to deep dive into the channels and payment systems used to repatriate earnings or launder money. Clearly, these international criminal networks also engage in the illicit trafficking of natural resources.

33 Environmental Investigation Agency. (2025, July). *Traffickers leave no stone unturned: What the largest exposed mercury smuggling operation reveals about the gold business [Report]*. EIA. <https://eia.org/report/traficantes-no-dejan-piedra-sin-levantar/>

34 Saavedra, F. (2025, 27 March). This is how the Sinaloa Cartel's control grows in Cauca: Government confirmed the relationship between Mexican drug traffickers and dissident groups. *Infobae*. <https://www.infobae.com/colombia/2025/03/27/asi-crece-el-control-del-cartel-de-sinaloa-en-el-cauca/>

Using Virtual Assets for Illicit Financial Flows Linked to Natural Resources. Trends and Typologies

As previously mentioned, in order to legitimize their illegal origin and integrate resources into the legal economy, illicit financial flows from environmental crimes are laundered through several processes. Based on information from experts in the crypto industry and the fight against environmental crimes, as well as the few cases identified to date to highlight the main trends in the use of virtual assets for money laundering or mobilization of illicit money from environmental crimes, this report analyzes the major international trends that may apply to these two countries regarding natural resources, even though there are currently no definitive figures or thorough studies conducted by blockchain analysis companies on these links in Latin America, nor many cases prosecuted by the prosecutors of Peru and Colombia..

6.1. Use of VAs in illegal mining (especially gold)

As evidenced throughout the document, rising gold prices have boosted the illegal economy related to its extraction and illicit sale. Outlaw groups that previously operated other routes and schemes of illegal trafficking are now part of the illicit gold business in countries such as Colombia and Peru, extending their influence internationally in terms of supply of inputs and mineral export.

It is well known that much of Venezuela's illegal gold enters countries like Colombia for commercialization, and much of the gold extracted from Colombia or Peru is moved to neighboring countries for export within legal supply chains. According to the Department against Transnational Organized Crime (DTCO) of the Organization of American States (OAS), «Illegal gold extraction



is a very widespread phenomenon in Colombia and is estimated to represent more than 80% of the country's gold production.». At any stage of the gold supply chain (from extraction to final commercialization), there are risks of illicit gold entering the legal supply chains³⁵.

Many inputs are additionally acquired on the black market and through smuggling to carry out illegal mining, such as gasoline, heavy machinery, and mercury, among others. All of these require a financial opacity framework to facilitate payments and acquisition. Laundering methods are numerous, including the creation of shell or front companies, fictitious suppliers, fraudulent commercial invoicing, or the use of authorized MAPE quotas to mainstream illicit gold.

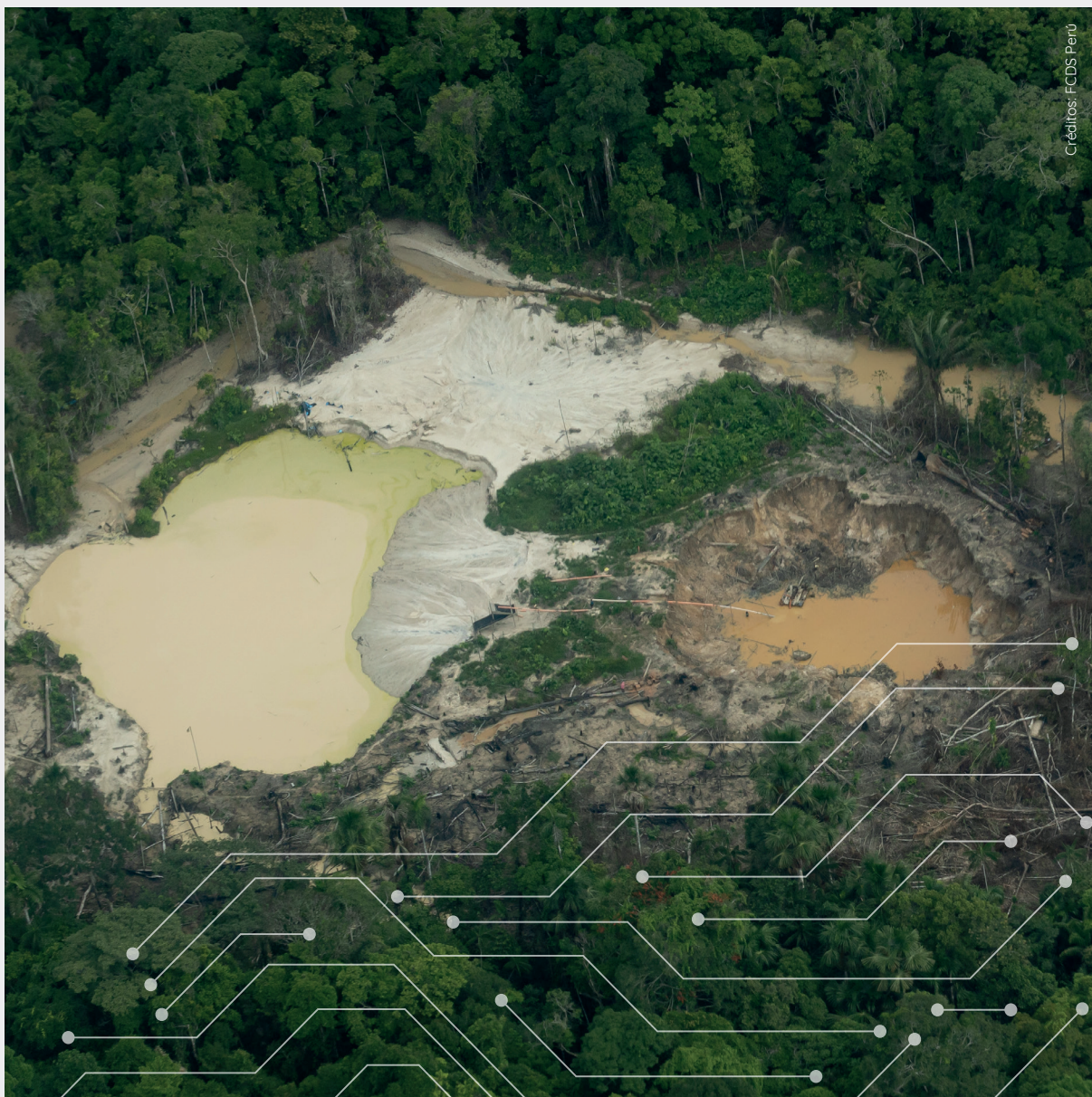
In Peru, according to information from the Financial Intelligence Unit (FIU), between 2014 and January 2024, illegal mining has been identified as a highly significant predicate offense, based on the value of illicit transactions detected and reviewed by the FIU³⁶ itself. According to another OAS DTOC report, «Gold traders and processors, including well-established companies and local businesses, play a key role in the illicit supply chain by purchasing substantial amounts of illegal gold from illegal miners at very low prices, under specialized agreements»³⁷; and according to information from other sources, much of the international gold trade is concentrated in major cities such as Lima, where there is broad access to crypto ATMs or other P2P VA exchange mechanisms.

Peru's FIU georeferenced statistical information report, issued by the Superintendence of Banking, Insurance and AFP (graph 4), shows the areas with the highest prevalence of illegal mining as a predicate offense for laundering. It can be seen that the areas where gold is commercialized for export include Lima and Callao, followed by Puno, La Libertad and Madre de Dios, Cusco, Puno, Arequipa, and Huancavelica. The latter, where there is a high presence of gold mining, are the places where more illicit flows associated with laundering were identified. Figure 5 shows that in the Peruvian Amazon, the proportion of illicit financial flows related to illegal mining is very high in areas such as Loreto, Madre de Dios where gold is commercialized for export.

35 Organización de los Estados Americanos. Secretaría para la Seguridad Multidimensional. Departamento contra la Delincuencia Organizada Transnacional. (2022, febrero). *Tras el dinero del oro ilícito: fortalecimiento de la lucha contra las finanzas de la minería ilegal. El caso de Colombia*. Documentos Oficiales OEA/Ser.D/XXV.19. Washington D. C.: OEA. <https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=674&lang=2>

36 Superintendencia de Banca, Seguros y AFP. (2024). *Informe de información estadística georreferenciada de la UIF Perú*. https://www.sbs.gob.pe/Portals/5/jer/estudios-estrategicos/Informe2024_publicar.pdf

37 Organización de los Estados Americanos. Secretaría para la Seguridad Multidimensional. Departamento contra la Delincuencia Organizada Transnacional. (2022, febrero). *Tras el dinero del oro ilícito: fortalecimiento de la lucha contra las finanzas de la minería ilegal. El caso de Colombia*. Documentos Oficiales OEA/Ser.D/XXV.19. Washington D. C.: OEA. <https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=674&lang=2>

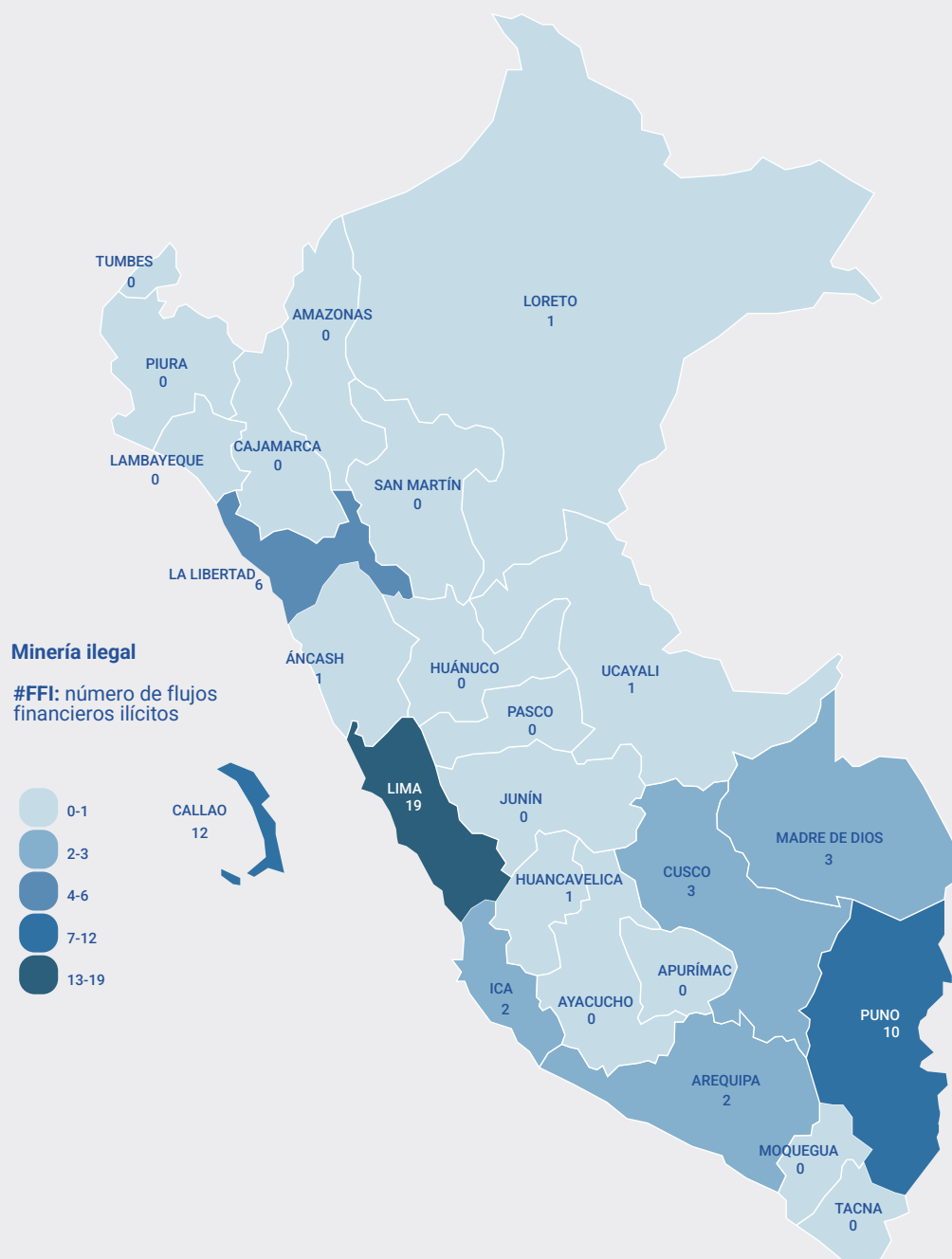


In addition, «it is also believed that the illegal gold trade in Peru is used by drug trafficking organizations, including those operating outside the country, to launder the proceeds of drug trafficking through practices such as trade-based money laundering.»³⁸. Therefore, below we will see the mechanisms in which VAs are used in this sector.

38 Organization of American States. Secretariat for Multidimensional Security. Department against Transnational Organized Crime. (2022, february). *Following the money of illicit gold: strengthening the fight against the financing of illegal mining. The case of Colombia. Oficial Documents OEAS/Ser.D/XXV.19*. Washington D. C.: OAS.. <https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=674&lang=2>



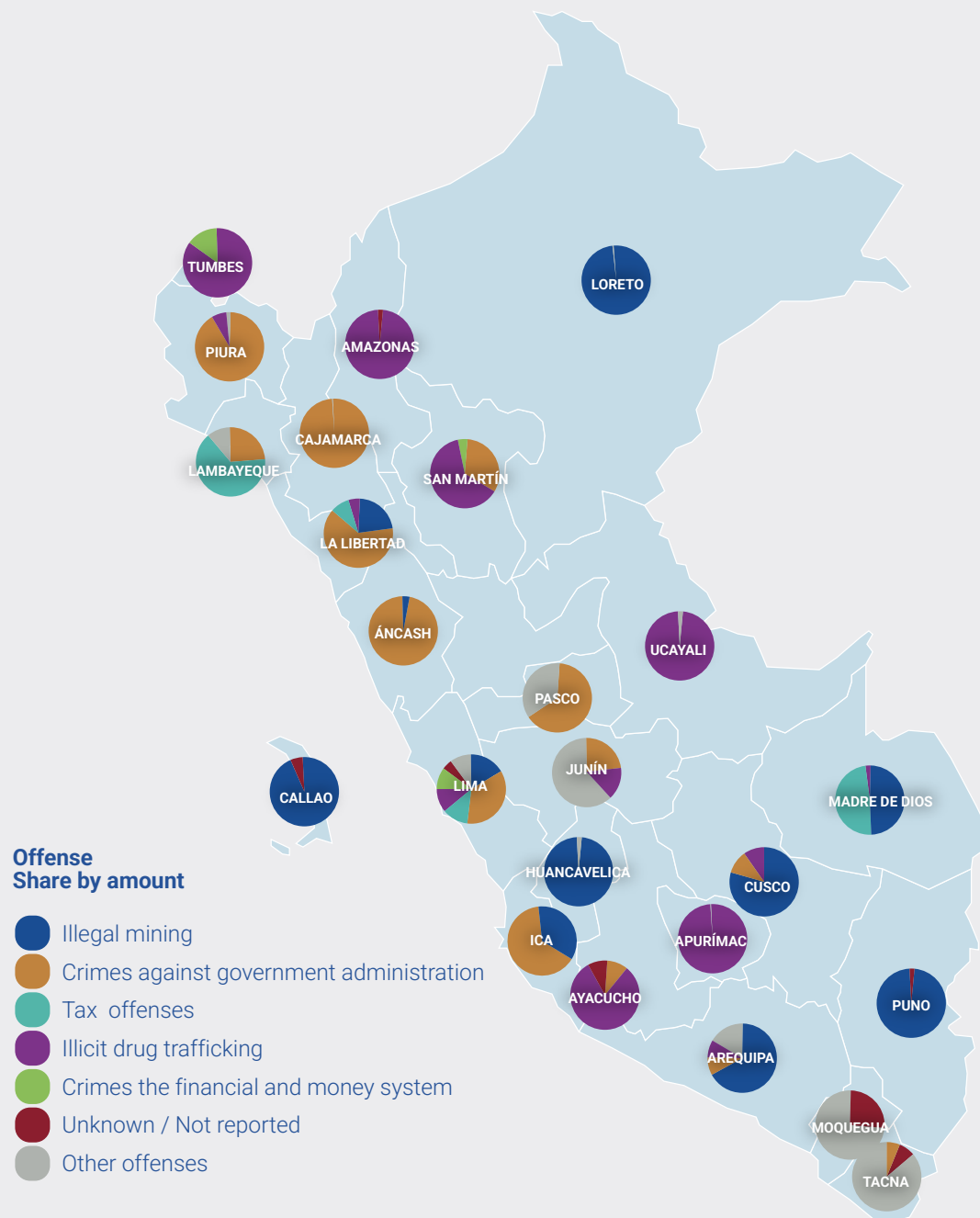
Graph 4. Amount of illicit financial flows detected as predicate offense – illegal mining in Peru (2014-2024)



Source: Superintendence of Banking, Insurance and AFP, FIU Peru georeferenced statistical information report³⁹.

39 Superintendence of Banking, Insurance and AFP. (2024). Report of georeferenced statistical information of the UIF Peru. https://www.sbs.gob.pe/Portals/5/jer/estudios-estrategicos/Informe2024_publicar.pdf

Gráfico 5. Monto por delito precedente, participación del monto involucrado en flujos financieros ilícitos (2014-2024) en Perú



Source: Superintendence of Banking, Insurance and AFP, FIU Peru georeferenced statistical information report⁴⁰.

40 Superintendence of Banking, Insurance and Pension Funds (2024). *Report on Georeferenced Statistical Information of the UIF Peru*. Retrieved from https://www.sbs.gob.pe/Portals/5/jer/estudios-estrategicos/Informe2024_publicar.pdf



- **Repatriation of resources from trade-based money laundering (TBML) and fraudulent commercial invoicing (revenues from exports and imports)**

OAS-DTOC reveals «money laundering through commercial operations is another method that, according to authorities, is frequently used in the illegal gold trade in Colombia»⁴¹ and, as mentioned earlier, it is also prevalent in the Peruvian context, where gold trade is used to move illicit drug trafficking flows with the support of transnational crime. According to FATF, TBML involves disguising the proceeds of a crime and moving its value through commercial transactions in order to legitimize its illegal origin or finance illicit activities⁴². One of the most commonly used methodologies for this purpose is fraudulent commercial invoicing, which consists of intentionally manipulating the value of an international trade transaction by falsifying the price, quantity, quality and/or country of origin of a good or service, among other data⁴³.

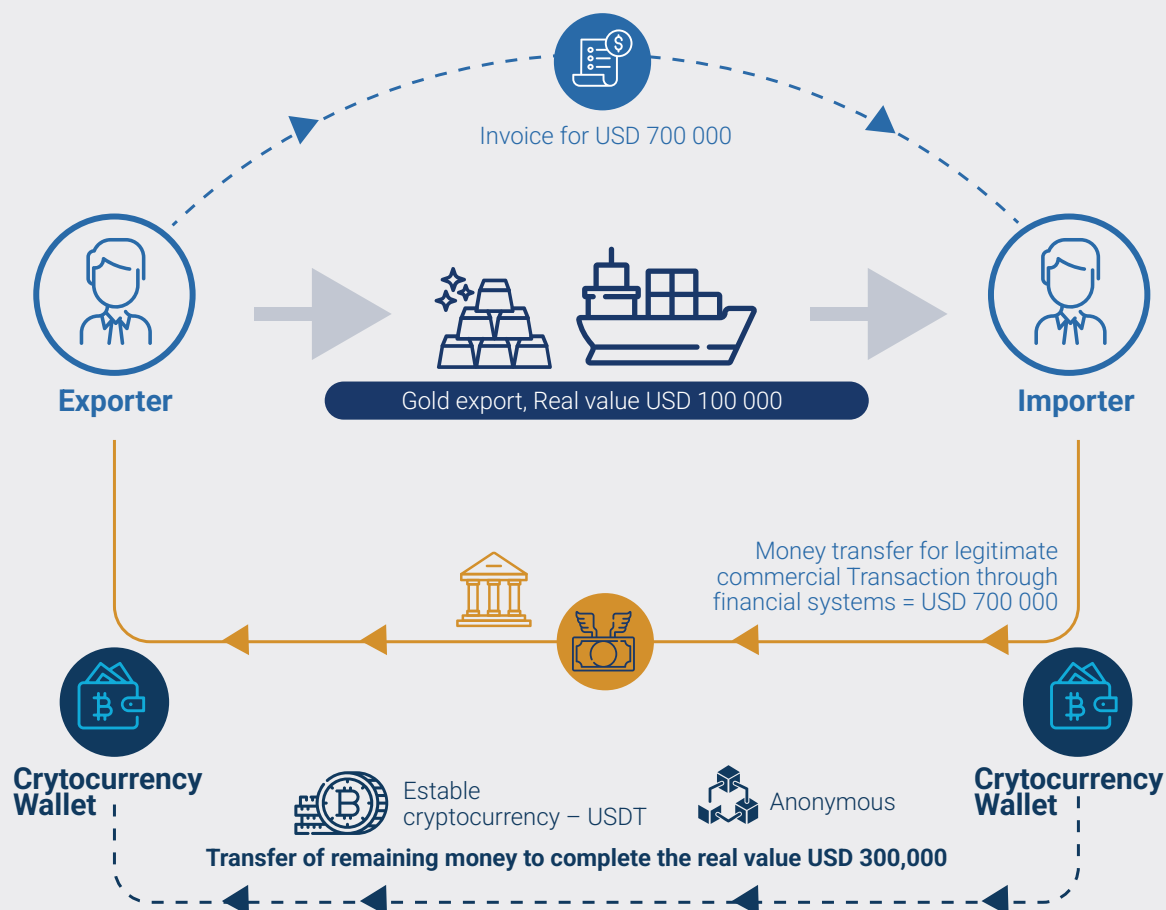
According to the sources consulted, stablecoins such as tether (USDT) are being used for this purpose. That is, large exporters and importers of gold agree to declare a lower value than the real one in their gold exports in official documents (invoices, export declarations, letters of credit, among others), in order to evade sanctions, reduce taxes or move illicit financial flows. This process is known as fraudulent commercial invoicing. But how do VAs operate in this scheme? They are used to repatriate the surplus of the importer's real invoice value to the marketer who exports. Below is an example:

41 Organización de los Estados Americanos. Secretaría para la Seguridad Multidimensional. Departamento contra la Delincuencia Organizada Transnacional. (2022, febrero). *Tras el dinero del oro ilícito: fortalecimiento de la lucha contra las finanzas de la minería ilegal. El caso de Colombia*. Documentos Oficiales OEA/Ser.D/XXV.19. Washington D. C.: OEA. <https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=674&lang=2>

42 FATF. (2006). *Trade-based money laundering*. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-basedmoneylaundering.html>

43 Global Financial Integrity. (2021, 16 de diciembre). *Trade-related illicit financial flows in 134 developing countries, 2009–2018* [Informe]. Global Financial Integrity. <https://gfinetegrity.org/report/trade-related-illicit-financial-flows-in-134-developing-countries-2009-2018/>

Gráfico 6. Repatriación de ganancias asociadas a TBML de oro a través de criptomonedas estables



Source: Prepared by the authors.

As shown in Graph 6, in the final export phase, the gold seller from the country of origin declares a lower value for the gold shipment to be exported than its actual value. To receive the full real value, he uses a stablecoin such as tether, so that the importer pays him the difference, thus preventing this income from being perceived by the financial system.

The difficulty in tracing this transaction may stem from the decentralized nature of the virtual wallets used to send and receive the stablecoins, or whether they are on an “exchange” with a public blockchain. In the first option, this could hinder investigation by authorities, since it would not be possible to trace the transaction and reach a natural person, if it does not reside in an «exchange» that also complies with KYC and AML/CFT standards.



According to the sources consulted, this methodology could be related to tax evasion, declaring a lower purity of the mineral, or manipulating its volume in order to use tariff headings different from those corresponding to export gold (for example, to mix gold with less valuable metals such as tungsten and export it undetected).

Another important consideration is that many exports are triangulated through Panama, and many of the payments received, according to the sources consulted, are monetized in this country, coming from opaque jurisdictions or issued from it. Recently, Panama has shown significant openness towards VAs, to the point that the mayor of Panama City has authorized the voluntary payment of municipal taxes with cryptocurrencies such as bitcoin, Ethereum, USDC and USDT, with conversion to dollars through the financial entity Towerbank as the intermediary body⁴⁴.

Although the country does not regulate the VA ecosystem, it permits using it, and there are already pilots in which financial entities provide virtual wallets associated with dollar bank accounts. It should be noted that AML/CFT and KYC filters or supervision are mainly applied to banking entities, and not directly to VASPs, creating a risk in terms of money laundering prevention.

Experts concur that traders of other minerals, not simply gold, might use this payment approach for resources related to TBML and fraudulent invoicing in cryptocurrency. Authorities should examine invoices, payment methods, and values provided by exporters more closely because minerals are particularly vulnerable to TBML.

- **Payment for services, suppliers and products in the illegal mining chain**

According to the sources consulted, many actors in the illegal mining chain, especially in high-impact mining areas (in the particular case of Colombia), use stablecoins to pay for illicit gold, as well as products and services associated with its production. The presence of currency exchange houses, pawnshops and other businesses with high cash use in these areas would also be facilitating transactions.

Although there is no way to verify how much crypto is used (this information would only be held by the «*exchanges*» and is not public), the sources consulted stated that it increases the confidence of artisanal miners and other actors in the chain to send and receive payments through crypto in currencies that do not have high volatility, such as tether, among others. In addition, it is highly likely that transactions are being carried out through P2P exchange between known actors with experience in using crypto.

44 Quesada Webb, A. (2025, 17 de abril). The mayor of Panama City announces that taxes can be paid in «cripto» *El País*. <https://elpais.com/america/2025-04-17/el-alcalde-de-ciudad-de-panama-anuncia-que-los-impuestos-se-podran-pagar-en-cripto.html#:~:text=Las%20autoridades%20de%20Ciudad%20de,no%20se%20ha%20logrado%20sacudir>

The report has not been able to corroborate whether the currency exchange businesses in these significant mining municipalities of Colombia actually offer monetization or exchange of crypto for fiat money, but greater scrutiny by authorities is recommended to analyze whether this service could be associated with the economic activity being carried out to facilitate the exchange of crypto for Colombian pesos (COP). Some sources claim that these mechanisms exist, but only for known clients and through schemes of multiple virtual wallets to avoid traceability.

Illegal mining experts in Peru agree that this methodology is unlikely in mining areas where there is still not much confidence in this type of technology, and artisanal mining populations mainly use other more traditional methods to monetize illegal mining. However, it is not ruled out that, at higher levels and in the main cities, the true ultimate beneficiaries of the supply chain use crypto to pay for international gold trade transactions.

- **Money flows from human trafficking**

A recent UNODC report addressed the use of VAs in human trafficking. The document shows that, in places where illegal or informal mining and hydrocarbon exploitation activities take place, such as Colombia and Peru, VAs are used for human trafficking for forced labor. The associated economic benefits are laundered through the same business via other channels, such as VASPs. The report also notes that crypto ATMs and exchange platforms, especially in Colombia, could also be facilitating the laundering of illicit resources from trafficking⁴⁵.

In addition, through open sources such as Coin ATM Radar⁴⁶, the existence of crypto ATMs in high-impact mining areas or in the Colombian or Peruvian Amazon could not be verified. However, sources claim that there are privately managed crypto ATMs in Amazonian areas (not open to the public), operated through trust and recommendation between the administrator and potential users. The existence of crypto ATMs in these areas could facilitate the conversion of fiat money to VAs, and vice versa, without any type of KYC or AML/CFT monitoring or control.

However, crypto ATMs operate in major cities. For example, in Medellín, Bogotá and Lima. In addition, this report found that there is significant supply, through social networks and Google, of VASPs or individuals offering to exchange fiat money for crypto, or vice versa, through P2P exchange. This makes these transactions fall outside the radar of authorities, since they are exchanges between individuals. More information on this topic below in the report.

45 United Nations Office on Drugs and Crime (UNODC) for the Andean Region and the Southern Cone. Project: Disruption of Trafficking Networks: Strategies Against Money Laundering. (2025, April). *Regional analysis of risk factors, facilitators, and scenarios for money laundering associated with human trafficking*. <https://www.negociosresponsablesyseguros.com/sites/default/files/2025-06/An%C3%A1lisis-regional-Lavado-de-Activos-Asociado-a-la-Trata-de-Personas.pdf>

46 Coin ATM Radar. (s. f.). <https://coinatmradar.com/>



- **Creation of cryptocurrencies or use of virtual assets to launder resources from illegal mining**

There are numerous documented instances where criminals use the introduction of a new cryptocurrency to deceive potential investors who give up their fiat money to purchase it in the expectation of earning substantial returns. People ultimately lose their money and receive no returns since the cryptocurrency's designers come up with ways to steal the resources they have invested. In some instances, like bitcoin, cryptocurrencies do yield profits for investors, albeit in a highly unstable environment.

This investment model, although risky for investors, is not an illegal activity. That is why Brazilian gold criminals resorted to this scheme to evade the controls of Brazilian authorities and created their own cryptocurrency to justify the legality of their illicit income from illegal gold mining and other criminal activities in Pará, Brazil.

Case 3. Laundering of assets from illegal gold mining through cryptocurrencies by Gana Gold company in Pará, Brazil

Brazil Federal Police carried out «Operação Ganância» to dismantle an illegal gold mining network in the state of Pará. The company Gana Gold, which operated legally with state licenses, was accused of marketing large volumes of gold of suspicious origin that did not come from its own formal operations.

The company sold gold estimated at more than BRL 1,100 million (around USD 200 million), much of it without traceability. Although court proceedings are not always made fully public, some news reports mention individuals linked to the network used cryptocurrencies to launder money from the illegal sale of gold⁴⁷.

These cryptos were used in asset concealment schemes both inside and outside Brazil. In some cases, even international payments associated with gold trade were identified that flowed through cryptocurrency exchanges.

47 Globo TV. (2025, 4 de marzo). «Barões» do ouro ilegal no Brasil: dinheiro movimentado às margens da lei chegou a R\$ bilhões [Video de YouTube]. *YouTube*. <https://www.youtube.com/watch?v=LkJ5QVbYR1Q>

Most interestingly, in addition to using corruption and a series of shell company networks to legalize illicit resources, the ultimate beneficiaries of the business created a token issuance scheme (crypto) to justify part of the illicit money. According to a Mongabay report, «the company created its own tokens to transfer illicit profits to frontmen's accounts, simulating that the amount came from third-party investments. These operations were carried out through Binance, the world's largest cryptocurrency broker»⁴⁸. It should be noted that this exchange, Binance, has already been investigated and prosecuted for facilitating money laundering and failing to meet minimum requirements of U.S. regulation

The profit promised by the investment in these tokens was 6% annually. According to a report by Gustavo Bertolucci, the company claimed that the token represented an excellent opportunity for investors to multiply their capital with cryptocurrencies, and it was created by the medical services company Instruaud [8.1], based in Porto Velho. This company was responsible for laundering money from illegal mining, and one of its leaders was arrested as part of the operation⁴⁹.

On social media⁵⁰, the company promoted the token as a “blue chip” with great potential for investors and, moreover, backed by gold. According to the same report, more than a year after its creation, transactions were scarce and the concentration in a few wallets was striking.

Below is a diagram exemplifying the case, involving ultimate beneficiaries, shell companies, a phantom token for money laundering, illegal mining and environmental damage, among others.

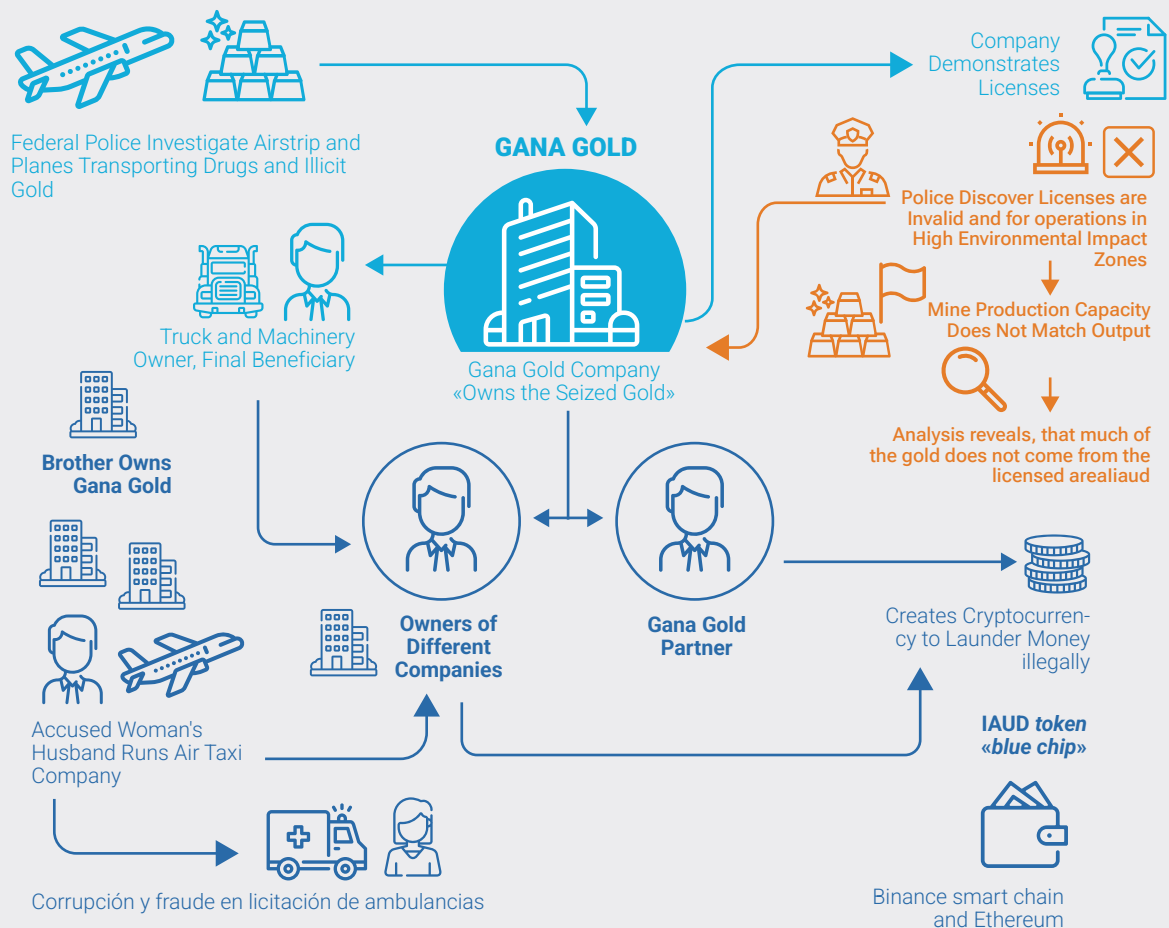
48 Schröder, A. (2022, 29 August). Raids reveal how illegal gold from Indigenous lands gets laundered in Brazil. *Mongabay*. <https://news.mongabay.com/2022/08/raids-reveal-how-illegal-gold-from-indigenous-lands-gets-laundered-in-brazil/>

49 Livecoins. (s. f.). Perfil de autor: Gustavo Bertolucci (lugu). <https://livecoins.com.br/author/lugu/>

50 Instruaud. (s. f.). Perfil de Facebook. https://www.facebook.com/instruaud.iaud/mentions/?_rdr



Graph 7. Criminal scheme uncovered by Operação Ganância by the Federal Police of Brazil



Source: Prepared by the authors based on case documents.

Identified channels and typologies:

- Creation of tokens backed by gold to justify income from illegal gold mining
- Money laundering through shell companies and crypto company
- Illegal gold mining
- Corruption
- Fraud
- Hidden ultimate beneficiaries

This case, which involves multiple channels for money laundering, particularly the creation/issuance of tokens apparently backed by gold, to launder resources from illegal mining and other crimes, sets a precedent for the potential use of VAs for these purposes. Stronger regulations and improved KYC and AML/CFT processes by VASPs are needed to detect unusual behaviors and, of course, to fully identify the users behind wallets, tokens or any other crypto scheme in Colombia and Peru.

Although there are still no cases of this nature mapped by the authorities of these two countries, the example of Brazil shows that it is very likely that criminals will evolve their laundering strategies towards more complex and sophisticated systems that allow them greater anonymity. Authorities also face the challenge of seizing existing assets in the VA universe, since they are often encrypted and use decentralized, self-managed access keys, which can make it impossible to access them unless those who manage them decide to provide access.

6.2. Illegal wildlife trafficking

According to FATF, the illegal trade in species and derived products is often concealed under apparently legitimate activities, such as the importation of timber, skins, exotic animals or ingredients for traditional medicines. Among the actors involved are businessmen with political connections, customs officials or environmental authorities, highlighting the cross-cutting nature of corruption and the difficulties in combating crimes such as this⁵¹.

Ecosystems that host exotic fauna and flora commanding high market value are the most vulnerable to traffickers, hunters or criminals who live off the illicit trade in wildlife species. Latin America is no exception to this phenomenon, especially in Amazonian territories. According to the National Police of Colombia, between January 1, 2023 and March 24, 2024, 37,998 animals were seized as victims of illegal trafficking. Mammals, with 5,763 animals seized, are the third most trafficked group in the country, only surpassed by reptiles, with 23,418 animals seized, and birds, with 9,829⁵². For its part, in 2018, a Traffic study on Peru⁵³ revealed this country to be the center of the illegal trade in wild birds in the South American region, and according to a Mongabay report, «the places where trafficking mostly flows are coastal cities because they have ports and airports. Lima and Callao are

51 FATF. (2020, June). *Money laundering and the illegal wildlife trade*. <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Environmentalcrime/Money-laundering-wildlife-trade.html>

52 Mongabay. (2024, april). Fight against animal trafficking in Colombia: guide launched to detect feline parts in the illegal market *Mongabay*. <https://es.mongabay.com/2024/04/lucha-contra-trafico-animales-colombia-guia-detectar-partes-felidos/>

53 Ortiz-von Halle, B. (2018, diciembre). *Bird's-eye view: Lessons from 50 years of bird trade regulation & conservation in Amazon countries*. Traffic Report. https://wwfint.awsassets.panda.org/downloads/south_america_bird_trade.pdf?_gl=1*1a7ihjp*_gcl_au*MTU0NDQ5NTIxMy4xNzQ1NDMxNzk4*_ga*MjQyNzA3MDMxLjE3NDU0MzE4MDE.*_ga_9594H828Q9*MTc0NTQzMTgwMS4xLjAuMTc0NTQzMTgwMS42MC4wLjA



a tremendously important hub for this, but then there are coastal places in the north, such as Piura and Lambayeque, but also in the south, like Tacna, through where specimens from Bolivia exit.»⁵⁴.

To understand how cryptocurrencies are used to facilitate this crime, it is necessary to analyze the different phases of the illicit species trafficking chain and the financial flows, that is, “the money trail” associated with carrying out these criminal activities.

- **Payment methods for trafficked species and money laundering associated with illegal wildlife trafficking**

A case study conducted by Traffic⁵⁵ examined the financial flows and payment schemes associated with illegal wildlife trafficking and other natural resources in different countries, and found that international transfers, cash payments, and the use of fintech platforms or mechanisms such as Hawala are the main payment methods. In addition, in Africa, the purchase of vouchers, for example Apple iTunes vouchers, was identified as a mechanism for laundering assets from illicit wildlife. These vouchers were then used to pay for cryptocurrencies associated with certain video games, to hinder the traceability of the money.

The illicit trafficking payments chain may require several processes, including:

- Payment to hunters or traffickers by the mafias in charge of commercialization in remote areas where wildlife is seized
- Payment to intermediaries for transporting or processing animal parts, among others
- Payments to operators of exports or international trade in wildlife (ships, planes, land transport, human mules, etc.)
- Payment of “bribes” to authorities and different relevant actors to traffick in animals
- Repatriation of profits obtained from illicit trafficking to the countries of origin

Prism Sustainability⁵⁶, claims crypto only adds another layer of opacity to the other payment methods already mentioned. In regions where there are greater controls in the financial system or where it has less penetration, it is more likely that VAs are used to mobilize payments related to wildlife hunting. Likewise, as already mentioned in the section on illegal mining, TBML may also be used to repatriate profits from international trade by large exporters of animal parts.

54 Santos, G. (2025, 24 April). « Lima is one of the places where a large part of the trafficking of species flows out to other countries» [Interview]. *Mongabay* . <https://es.mongabay.com/2025/04/peru-traffic-especies-aves-entrevista/>

55 Traffic. (2021). *Case Digest: Financial flows and payment mechanisms behind wildlife and forest crime*. <https://www.traffic.org/site/assets/files/13685/case-digest-financial-flows-analysis-v2022.pdf>

56 Sustainability Directory. (2025, 16 April). *The role of cryptocurrencies in funding wildlife crime prevention*. Sustainability Directory.

Although no specific cases of this use were identified in Colombia and Peru, the dynamics analyzed by Chainalysis in its most recent reports on crypto crimes imply that such methods can also be used in relation to wildlife trafficking in these two countries.

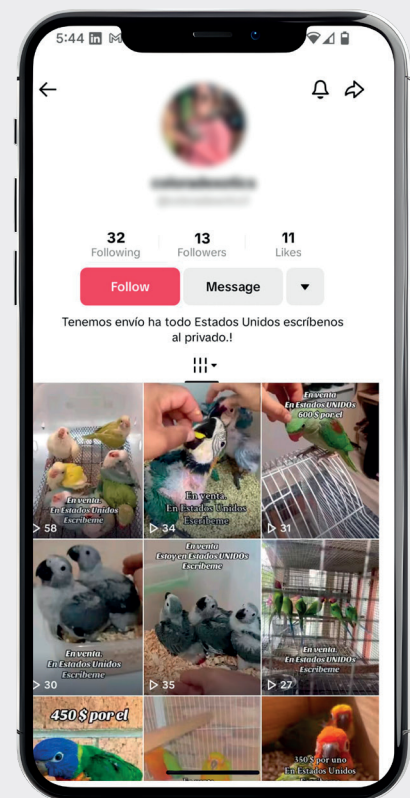
Mechanisms used by traffickers in illicit financial flows associated with illegal wildlife trafficking:

- Use of local cryptocurrency exchanges or trading platforms
- Crypto-to-crypto or crypto-to-fiat exchange, and vice versa, through individuals (P2P)
- Use of crypto ATMs to monetize money into VAs or vice versa
- Virtual wallets linked to wildlife trafficking connected to fraudulent platforms and other types of illicit businesses

A very important aspect highlighted in the Chainalysis report is that, unlike many of the dynamics evidenced in the case of gold, traffickers often use public blockchain exchanges regulated under AML/CFT, which facilitates investigation by authorities. In addition, the report identified spaces such as TikTok offering exotic South American species for sale in countries such as the United States, with payment methods involving online transactions and payment through bitcoin or Tether.

During the preparation of the report, it was revealed that one of the identified accounts was reported and subsequently blocked, but then a new one was created offering the same animals for sale. Initially, they publicly posted their website and payment and shipping methods, but this information is no longer available on the new page.

Photo: Real image of wild bird offers identified on the TikTok platform for this report. Account name anonymized.





Some of FATF's recommendations on financial analysis of this issue can also be applied to the crypto context. For this, it is crucial to identify «bridge» or intermediate transactions, such as payments to relatives or international transfers that seek to fragment traceability. For example, indirect connections can be analyzed, such as transfers from exotic pet breeders or zoos to actors previously linked to illicit trafficking networks.

Such indicators show, as mentioned in previous paragraphs, that the fight against money laundering derived from the illegal wildlife trade can only be effective if financial intelligence, inter-institutional cooperation and private sector responsibility (in this case, VASPs) are combined. The challenge lies in training those responsible for monitoring transactions so that they can interpret subtle signals without criminalizing legitimate activities and, of course, understand the warning signs around the crypto ecosystem.

In addition, some sources mentioned the use of crypto to pay for services related to animals in the countries of origin. That is, tourists or people interested in certain benefits associated with substances extracted from certain endemic animals would also be paying for these products with cryptocurrencies.

Conclusions on alerts and main risks identified

The typologies, risks, and trends identified in this report point to, several high-risk areas and red flags that may be useful to initiate investigation processes, policy formulation, and gradual actions by the authorities of Peru and Colombia. While it is necessary to deepen research and identify the channels through which funds associated with the trade in natural resources are being mobilized, it is also essential to strengthen the educational and training component. It is crucial that all relevant authorities understand firsthand how the universe of virtual assets works to identify their possible use in money laundering schemes from criminal activities, and that countries such as Colombia and Peru pass legislation that directly regulates VASPs.

As will be seen later, without a solid regulatory framework it is more difficult to establish monitoring, control, and sanction mechanisms, so clearer and more effective policies addressing this issue are urgently needed. However, many actions can be implemented at different levels without broad regulation of VASPs, which is why interagency and interdisciplinary responses are key when considering mechanisms to increase the number of identified cases related to money laundering from environmental crimes.

Below, we address some risk points that require greater attention and scrutiny by the authorities.



Placement, integration, and monetization of VAs

The analysis of money laundering processes through crypto assets from environmental crimes highlights a latent and clearly identifiable risk, especially in the stages of placement, integration, and monetization of these illicit flows within the crypto ecosystem, in particular how criminal actors convert cash from different illicit activities into cryptocurrencies, and how, in turn, funds transferred via crypto assets are converted into fiat cash or channeled through purchases and investments, allowing them to enter the formal financial system.

One of the main alerts identified by experts relates to the way exchanges are carried out. While part of the transactions can be made through digital transfers from traditional banking, most originate in cash from the environmental crimes mentioned, due to the nature of these economies and the controls the financial system applies to transaction patterns. In remote areas, where many of these illicit economies operate, cash remains the main way to mobilize resources, which also prevails in sectors such as informal gold mining, cattle ranching, and land grabbing.

The analysis and strengthening of regulatory frameworks must be carried out particularly to improve strategies for identifying monetization channels or fiat-VA exchange bridges, as can be seen in the following red flags.

Crypto ATMs: Crypto ATMs can be a potentially effective channel for those who want to acquire cryptocurrencies without going through the financial system. Although fees are high and there are maximum transaction amounts per user and per day, it has been proven that many criminal groups use the “smurfing” strategy, that is, dividing fiat-to-crypto exchanges into small amounts, below the thresholds set by the ATM and with different people, to avoid the operation being reported to the ATM service provider. Below is the number of ATMs available for some cryptocurrencies in Colombia, Peru, and Panama.

Graph 7. ATMs for crypto exchange in cities of Colombia, Peru, and Panama

City	Bitcoin enabled exchange services and ATMs	Tether enabled exchange services and ATMs	USDC enabled exchange services and ATMs
Bogota and surroundings	20-25	2	0
Medellin	6	1	0
Cali	8	0	0
Bucaramanga	3	0	0
Panamá	20	14	14
Pereira	1	1	1
Lima	6	6	2
Callao	1	1	1

Source: Prepared by the authors based on data from Coin ATM Radar and Statista

As shown in Graph 7, and according to public information obtained from portals such as Coin ATM Radar, the main cities concentrate the largest number of crypto ATMs in these countries. Bogota and its surroundings concentrate the highest number of ATMs, as does Panama, where there is a high presence of ATMs enabled not only for bitcoin but also for stablecoins. This is not easily evidenced in Colombia and Peru. It should be remembered that Panama is related to one of the red alerts identified, especially in relation to mineral exports such as gold, since, according to sources consulted, many of the payments and shipments are triangulated through this country. For this reason, the number of available ATMs and especially the ease of exchanging stablecoins is noteworthy.

Meanwhile, ATMs are available in cities such as Medellín, Cali, Lima, and Bucaramanga, although in smaller proportion than cities like Bogota. It



should be noted that much of the export and commercialization of illicit gold takes place in these cities and, as evidenced, it is unlikely that ATMs are massively located in mining activity zones or municipalities in remote areas. However, as mentioned earlier, sources consulted claim that some of these ATMs operate in remote Amazonian areas thanks to connectivity provided by services such as Starlink.

In countries lacking VASP licensing regulation, it is easy for these ATMs to be linked to opaque actors or those not meeting all KYC requirements. Nevertheless, for some experts, these ATMs are not the main concern in countries like Colombia and Peru. It is considered that the alarms lie more on P2P exchanges facilitated by currency exchange businesses that would also offer this service even without a license. In this sense, it is important that authorities monitor transactions associated with those who benefit from or control these types of businesses, especially in high-impact mining areas and major cities, to determine whether cash is being laundered into personal crypto wallets.

Effective regulation should also aim to regulate crypto ATMs and ensure their full identification (location, provider, etc.), as well as clear AML/CFT measures to prevent their use as channels for laundering cash.

Currency exchange outlets and P2P exchange: For this report, a search was conducted for exchange outlets offering these services, and some specialized in crypto were found (with an exchange rate defined according to the type of cryptocurrency to be monetized or purchased), with physical headquarters to access the service. Other exchange outlets were also found that, although they do not operate out of physical facilities, do offer cryptocurrency exchange services, with a commission percentage, only through digital channels (WhatsApp, Telegram, etc.) and with payments through platforms such as Nequi or Daviplata (in Colombia).

Additionally, it is simple to locate individuals offering this same P2P exchange service with stronger levels of anonymity than those provided by a regulated exchange or VASP on platforms like TikTok, whose profiles lack images or whose identities are questionable.



It is important to note that, through Exchange businesses can be identified through social media networks or internet searches with some of the most notable located in cities such as Cúcuta, where the border connection with Venezuela and the confluence of trafficking and smuggling of different minerals, such as gold, prevail. This may pose a risk, as it could become a channel facilitating the laundering of illicit resources related to environmental crimes from this country.

The existence and easy access to these types of services, both in physical and digital spaces, highlights the need to strengthen mechanisms for surveillance and traceability of VA operations, especially in Colombia. The diversity of actors and exchange modalities, combined with the difficulty of exercising effective controls over P2P transactions, creates an environment conducive to anonymity and misuse of these channels for illicit purposes. Therefore, it is essential that authorities adopt risk-based approaches that consider territorial particularities and currency exchange platforms, also in border areas or with high illegal extractive activity, in order to prevent the monetization of illicit resources.

Mixers and tumblers: on the other hand, it is easy to find services on the internet that promise 100% anonymity in transactions, such as mixers, which are platforms that allow anonymity when carrying out transactions.

Mixers or tumblers are services that combine funds from different users to hide the origin and destination of transactions on the blockchain. Their purpose is to impede the traceability of digital money, making it difficult to identify who sent or received the funds. Although they can be used to protect privacy, they are also a common tool for laundering money from illicit activities.

Many *mixers* have been investigated, especially by U.S. authorities, for facilitating the laundering of illicit funds and being associated with sanctioned countries. Unfortunately, if these mixers are located in distant or high-risk jurisdictions, it is very difficult for local authorities, which lack a regulatory framework, to sanction them or exert pressure to support investigations.



Regulation in Colombia and Peru: a path to follow

PERU

Peruvian regulation on VAs has been influenced by FATF standards, particularly Recommendation 15, which requires treating VASPs as obliged entities under anti-money laundering regimes..

In July 2023, Supreme Decree No. 006-2023-JUS included VASPs as obliged entities before the FIU of Peru. This decree defines a VASP as any natural or legal person who, as a business, exchanges, transfers, safeguards, or manages virtual assets or offers financial services related to them. This decree strengthens the Peruvian regulatory framework, as it establishes that VASPs must implement mechanisms such as customer identification (KYC), transaction monitoring, reporting suspicious transactions (STRs), and appointing a compliance officer.

Complementary to this decree, Resolution SBS No. 02648-2024 elaborates on the AML/CFT prevention regime for VASPs, setting forth specific obligations such as the implementation of an AML/CFT prevention system (SPLAFT), internal and external audit mechanisms, codes of conduct, and the obligation to know both the customer and the ultimate beneficial owner, with different levels of due diligence.

Although Law No. 29985 on electronic money does not directly regulate crypto assets, it is a key piece of Peru's digital financial framework, since electronic money issuing companies (EEDs) are also subject to FIU controls, and its regulation shows that Peru has already developed regulatory mechanisms to supervise digital payment methods, although not initially extended to the crypto ecosystem.

Despite some regulatory progress, the Peruvian framework remains insufficient to effectively address money laundering derived from environmental crimes, especially in areas highly vulnerable to such crimes, such as the Amazon. Among the most relevant obstacles are:

- 1. Site surveillance and enforcement impediments:** although VASPs are formally under FIU supervision, the state's capacity to oversee operations in remote areas—where illegal mining, wildlife trafficking, and illegal logging proliferate—is limited. These regions are often beyond the immediate reach of control entities, facilitating the use of VAs in money laundering schemes without banking intermediation.

2. **Sectoral risk analysis and environmental focus:** current regulation lacks a specific sectoral risk analysis for environmental crimes. Legislative Decree No. 1106, which establishes the general regime against money laundering in Peru, explicitly recognizes environmental crimes (illegal mining, wildlife trafficking, and illegal logging) as predicate offenses for ML. This recognition implies that illicit profits from these crimes can be laundered and are therefore subject to the provisions of this regulation. However, the operational connection between this law and supervision of the crypto ecosystem has not been developed in a coordinated manner or with specialized mechanisms.
3. **Use of unregistered exchanges and concealment technologies:** in practice, criminal networks use techniques such as mixers or DeFi platforms, which are beyond the scope of national regulation. In this sense, although Resolution SBS No. 02648-2024 mentions the obligation to report suspicious transactions and use international lists, the absence of a robust technological strategy to track operations with these tools limits the effectiveness of the legal framework.
4. **Lack of regulatory integration with environmental crime policies:** Articles 308, 308-A, 308-B, 308-C, and 310-A of the Penal Code criminalize offenses such as illegal trafficking of flora and fauna, as well as illegal extraction of aquatic species or timber products. However, investigations and judicial processes for these crimes rarely link to financial tracking of money laundering, nor to the use of crypto assets, even though Legislative Decree No. 1106 allows prosecution of money laundering without the environmental crime having been judicially proven.
5. **Limited reporting culture and training problems:** despite existing regulation, there is still a weak culture of reporting suspicious transactions among VASPs, especially smaller, informal actors or those recently incorporated into the regulated ecosystem. Many lack the technical knowledge, internal procedures, and digital tools needed to implement robust AML prevention systems (SPLAFT). The lack of specialized training in risk analysis, KYC, and transaction monitoring leaves wide gaps that can be exploited by criminal networks operating with crypto assets.

This situation is aggravated in a context where environmental crimes such as illegal mining, illicit logging, and wildlife trafficking generate considerable financial flows, often in territories with low state presence and limited institutional control. In these areas, where business formalization and regulatory oversight are limited, it is particularly concerning that VASPs or technological intermediaries are not trained, nor practically obliged, to collaborate with authorities in the early detection of laundering schemes.



COLOMBIA

Reregulation applicable to crypto assets is in force in Colombia, but it remains partial and fragmented, focused mainly on preventing risks associated with ML/FT. Although bitcoin and other cryptocurrencies have circulated in Colombia since at least 2011, it was not until 2017 that the Financial Superintendence of Colombia (SFC) began issuing formal statements warning about associated risks.

That year marked a tipping point, due to the exponential growth of exchange platforms, lack of supervision of these operations, and the risk that these technologies could be used to channel illicit resources or evade taxes. In response, obligations for STRs were established, the activity of supervised entities was delimited, and pilot projects such as the regulatory sandbox were implemented to test operating schemes under strict controls. Thus, the Colombian approach combines sectoral measures, supervisory mechanisms, and controlled experimentation spaces, reflecting a gradual and precautionary approach to adopting crypto-based technologies.

In the absence of a general crypto asset law, Colombian regulation has been structured through sectoral rules and administrative guidelines. On one hand, in Circular Letter 052 of 2017 the SFC expressly prohibits supervised entities from intermediating, safeguarding, or facilitating transactions with crypto assets. This restriction seeks to protect the stability of the formal financial system, since these resources may come from «illicit activities related, among others, to predicate offenses of money laundering, terrorist financing, and proliferation of weapons of mass destruction».

On the other hand, the Financial Information and Analysis Unit (UIAF) set forth, through Resolution 314 of 2021, the obligation for VASP platforms to report suspicious transactions and relevant operations. This is because, although operations with these assets «are not illegal in themselves, they may lend themselves to illicit activities, due to anonymity or pseudo-anonymity in transactions, lack of backing by the central bank, and non-recognition as an instrument with liberatory power». In addition, the National Tax and Customs Directorate (DIAN) has issued concepts considering crypto assets as intangible assets subject to tax obligations, although without a specialized tax framework covering new forms of value acquisition and transfer inherent to the crypto economy, such as NFTs and DeFi.

A relevant milestone was the launch of the regulatory sandbox through Decree 1234 of 2020. The regulatory sandbox is a controlled pilot testing space that allowed exchanges to operate in partnership with supervised entities to evaluate business models under strict risk prevention controls. This mechanism showed openness to regulated experimentation, although it did not resolve the lack of permanent regulation or licensing for VASPs.

Recommendations to consider in both regulations:

It is recommended that Colombia and Peru establish a comprehensive legal and regulatory framework for crypto assets, including clear definitions, permitted activities, and licensing requirements for virtual asset service providers (VASPs), incorporating standards of due diligence, governance, digital asset custody, cybersecurity, and consumer financial protection. Within this framework, a licensing system should be created to enable VASP operations under the supervision of a defined regulatory entity, ensuring compliance with KYC and AML/CFT standards, as well as the obligation to report suspicious transactions and cooperate with the banking sector in detecting illicit activities.

In order to direct regulatory efforts toward susceptible places and activities, including illicit gold mining, sectoral studies that pinpoint specific hazards associated with environmental crimes and cryptocurrency assets must be prepared. In order to systematically incorporate virtual asset tracking into environmental crime investigations and foster international cooperation through agreements with global exchanges and blockchain analysis platforms, it is imperative that financial, environmental, and judicial authorities strengthen their interinstitutional coordination.

Likewise, it is recommended to establish an interinstitutional protocol, led by the FIU, the Public Prosecutor's Office, and the National Police, for the seizure and custody of crypto assets, defining clear procedures for identification, securing, and safe storage of these assets, including management of private keys, coordination with VASPs, and designation of a certified custodian, complemented by specialized training of officials. In parallel, a tax regime adapted to crypto asset operations, including DeFi and NFTs, should be developed, defining valuation criteria, asset declaration, and withholding, and promoting transparency and tax compliance.

Finally, it is essential to consolidate regulatory sandboxes as permanent mechanisms of supervised innovation, with clear pathways for successful models to scale into formal operations, as well as to strengthen the training of officials, judges, and financial operators in emerging crime typologies and blockchain tools, and to ensure that national regulations remain updated and aligned with FATF Recommendations 15 and 16.



General Conclusions and Recommendations

Identification of cases, investigation, and sanction

One of the main bottlenecks when analyzing the role of illicit financial flows in the universe of virtual assets is precisely the lack of identified cases in which their use can actually be detected as payment channels or for laundering resources from activities related to environmental crimes. This is one of the crimes for which the fewest typologies and trends have been identified, since cases are not being detected.

Colombian and Peruvian authorities, from their different areas of work—both in crypto crime prevention and in environmental crime prevention—must communicate, share information, and develop joint investigation schemes to investigate cases together and, above all, analyze the money trail associated with most environmental crimes. It has already been noted that, in most environmental crimes investigated and prosecuted in the Amazon, the financial crime is not tracked nor is the money trail analyzed, so this component may be going unnoticed in many ongoing investigations.

As a first line of action, field officers and police, both judicial and environmental, must be trained to correctly identify the use of VASPs, seize virtual wallets, analyze computers, understand the use of the dark web or social networks to channel crypto payments, as well as passwords, hashes, and other devices that may signal a risk. Something that can greatly facilitate the work of investigators, judges, and prosecutors is that field authorities should be able to detect if criminals possess cold wallets (devices similar to a USB stick that may go unnoticed), long alphanumeric codes that may indicate a wallet key or password, or the use of VASPs in computer or mobile applications. In many cases, criminals hide their money in the crypto world, delete applications, and these are apparently not identified in search and inspection processes.



Develop clear guidelines so that police and prosecutors can seize assets in virtual assets and understand how to operate them. It is often believed that there is no specialized crypto legislation, so it is overlooked that it is equally possible to seize money stored in virtual wallets or other types of assets. Although the legislation of each country allows seizures, it is necessary to know how to access platforms, avoid deception, act quickly and effectively, and above all, obtain wallet addresses. Likewise, mechanisms must be in place to securely and correctly store seized assets, considering the particularity of the asset, and manage them safely.

Without hashes or wallet addresses or transactions, it is not possible to truly trace operations. Although authorities have crypto intelligence and blockchain analytics software, and many cryptos based on open blockchain can be traced, without a wallet hash it is impossible to advance investigations to detect movements, exchanges, other related wallets, and unusual activity. Developing sufficient human intelligence to detect hashes is essential to identify more cases related to environmental crimes.

Increase intelligence regarding the purchase and sale of inputs, animals, minerals, or any other products related to environmental crimes on social networks or in places such as the dark web. From there, with detailed investigation, hashes or wallets associated with those using VAs as payment channels for these products can be identified.

Increase customs controls related to identifying potential trade-based money laundering, especially in the case of minerals and other Amazon natural resources, regarding export payment methods and resource repatriation. Likewise, in association with the FIU, monitoring channels should be promoted for companies commercializing these minerals and other natural resources to detect suspicious activities or transactions, unsupported income, among others.

Although currently the banking industry, under the circulars and decrees of Colombia and Peru, is presented as an ally for detecting STRs associated with VASPs or clients transacting with VAs, VASPs should directly comply before a regulator as obliged reporting entities. Although they are already required in both countries, compliance relies only on the goodwill of some operating within the law, but it is not possible to exert pressure on all, due to the transnational nature of these services and the lack of licensing.



Analyzing links with Mexican cartels and criminal groups in Colombia and Peru is of vital importance, since some of these have already gained experience in using crypto for money laundering in drug trafficking, which could be a risk factor for environmental crimes tangentially linked to their direct or indirect operations.

Functions and capacities of competent authorities in the prevention, investigation, and sanction of crimes associated with VAs and environmental crimes

Entity	Function
Police (Criminal Investigation Directorate / Asset Laundering Investigation Directorate) focused on money laundering or crypto crimes, in association with the Environmental Police	Detect the use of VAs in criminal schemes linked to crimes such as illegal wildlife trafficking, illegal mining, illicit logging, smuggling of natural resources, and other environmental crimes
	Conduct field and digital monitoring and investigation to identify virtual wallets and suspicious transactions associated with laundering money from illicit environmental activities
	Correctly identify, secure, and seize VAs and digital evidence during raids and police operations
	Support the Prosecutor's Office in collecting and preserving digital evidence, ensuring chain of custody and technical traceability of seized VAs
	Develop financial and cyber intelligence through monitoring of the dark web and social media networks, and cooperation with specialized cybercrime and financial crime units
	Train specialized units (such as DIJIN or the Environmental Crime Investigation Group) in blockchain traceability tools and cryptocurrency forensic analysis
	Participate in joint operations and interinstitutional technical committees, providing intelligence and evidence that strengthen judicial processes and asset forfeiture



Entity	Function
Prosecutor's Office (specialized directorates in criminal finance and environmental crimes)	Direct criminal investigation in cases where VAs are used to hide, transform, or move illicit resources from environmental crimes Investigate the “money trail” of cases related to illegal mining, wildlife trafficking, deforestation, land grabbing, and illicit logging, among others Coordinate with Judicial Police the collection of digital evidence, blockchain forensic analysis, and crypto asset tracking Order raids, seizures, and securing of virtual wallets, devices, or suspicious funds Request precautionary measures on crypto assets linked to money laundering or terrorism financing investigations Request information from money exchanges or VASPs, including international ones, to track fund flows Work with FIUs and customs to cross-check suspicious operations lined to ongoing criminal investigations Request international cooperation (Interpol, Europol, Gafilat, Egmont Group, among others) to track blockchain transnational operations Collaborate with FIUs, which send STRs to open or support investigations Coordinate with the financial superintendence and customs when operations are carried out through controlled entities or platforms Train prosecutors and experts in blockchain technologies and crypto asset traceability Develop action protocols for preserving digital evidence in virtual asset cases Contribute to public policy and criminal regulation on crypto assets through technical or conceptual inputs



Entity	Function
Financial Intelligence Units (FIUs)	Receive, centralize, and analyze STRs linked to VA use, both from traditional obliged entities (financial institutions, exchange houses, notaries, etc.) and new actors in the crypto ecosystem (exchanges, VASPs, fintechs) Identify patterns, typologies, and trends on VA use in money laundering and terrorism financing schemes, especially those associated with environmental crimes such as illegal mining, illicit logging, or wildlife trafficking Cross-check financial, tax, and customs information with blockchain transactions and other sources, open or private, to detect suspicious flows, triangulations, and links with individuals or companies under investigation Prepare financial intelligence reports (FIRs) or strategic intelligence reports to send to the Prosecutor's Office or Public Ministry when operations with alleged links to predicate crimes are identified Issue early warnings and recommendations to supervisory entities on emerging risks associated with VAs, environmental crimes, and natural resource trade, to highlight the need to adjust regulatory frameworks or supervision mechanisms. Coordinate and cooperate with foreign FIUs (Egmont Group) to exchange information on cross-border operations or international actors linked to laundering schemes through crypto assets and smuggling of inputs for illegal mining or wildlife trafficking Develop analytical and technological capabilities, incorporating blockchain traceability tools and cryptocurrency forensics analysis, to strengthen the detection and linking of suspicious addresses, wallets or transactions. Foster training of obliged entities and the public sector in identifying risks associated with VAs, fostering a culture of timely reporting and effective compliance Support the formulation of public policies and regulatory frameworks on supervision, control, and reporting of VA operations, in coordination with Ministries of Finance and Justice and financial authorities

Entity	Function
Financial Superintendence or Banking Superintendence	Within an approved regulation, which does not yet exist in this form for these countries, these superintendences may play the role of verifying that providers operating within national territory meet minimum standards in AML/CFT prevention, technological risk management, cybersecurity, and reporting suspicious transactions to the FIU Oversee the relationship between the financial system and the crypto ecosystem by monitoring and limiting the exposure of banks, fintechs, and other entities to operations with unregistered or high-risk platforms, to prevent them from serving as indirect laundering channels

Risk-based approach for environmental crimes and VAs

The present set of recommendations is proposed from a risk-based approach, aimed at prioritizing controls and measures regarding crypto assets according to their potential illicit use, especially in contexts related to environmental crimes and cross-border transactions.

- Colombia and Peru could establish a comprehensive legal and regulatory framework for crypto assets, including clear definitions, permitted activities, and licensing requirements for virtual asset service providers (VASPs), incorporating standards of due diligence, governance, digital asset custody, cybersecurity, and consumer financial protection. Within this framework, a licensing system should be created to enable VASP operations under the supervision of a defined regulatory entity, ensuring compliance with KYC and AML/CFT standards, as well as the obligation to report suspicious transactions and cooperate with the banking sector in detecting illicit activities.
- In particular, robust regulation must be established for cryptocurrency ATMs, as they are a critical channel for illicit operations, especially in remote areas with limited supervision. ATM operators must register, comply with KYC/AML standards, report suspicious transactions, and allow periodic audits, including traceability systems integrated into official VASP and FIU databases. Severe sanctions should be applied to illegal operators, such as significant fines and prison sentences,



following international examples that have proven effective.

- Likewise, the risk-based approach requires identifying regions with high environmental criminal activity, such as Madre de Dios in Peru or Cúcuta in Colombia, where illegal mining and other environmental crimes generate cryptocurrency flows associated with money laundering. This territorial mapping allows prioritizing inspections, controls, and monitoring of VASPs in these areas, as well as guiding prevention campaigns and interinstitutional cooperation.
- At global level, special attention must be paid to payment mechanisms that can facilitate TBML, such as fraudulent commercial invoicing or manipulation of strategic mineral prices through crypto assets. It is also essential to monitor operations with high-risk jurisdictions such as China, India, and Panama. The integration of financial intelligence, international trade data, and blockchain analysis will make it possible to detect atypical patterns and anticipate potential risks of money laundering and illicit financing.
- Finally, it is recommended to establish an interinstitutional protocol, led by the FIU, the Public Prosecutor's Office, and the National Police, for the seizure and custody of crypto assets, defining clear procedures for identification, securing, and safe storage of assets, including private key management, coordination with VASPs, and designation of a certified custodian, complemented by specialized training of officials. All these measures must be implemented in a coordinated manner among financial, judicial, and environmental authorities to ensure effective supervision of ATMs, VASPs, and international crypto asset flows, with special emphasis on preventing environmental crimes and cross-border transactions.



