Observatoire ARGA

AirBit Club as a Model of Transnational Cryptocurrency Fraud, Blockchain Infrastructure Exploitation, and Sanctions Evasion in the Context of Political-Economic Prosecution

Author:

Sergey Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 14 rue Jacques Laffitte, Bayonne, 64100

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

Paris, 10 January 2026

Table of Contents

Abstract 3

1. Introduction 3

2. General Characteristics of the AirBit Club Case 3

3. Organizational Structure and Scaling Logic 4

4. Blockchain and the Illusion of Transparency 4

5. The Role of Stablecoins and the TRC-20 Network 5

6. Transnational Nature and Jurisdictional Gaps 6

7. Sanctions Evasion and Regulatory Circumvention 6

8. The Political-Economic Dimension 7

9. The Problem of Victim Accounting 8

10. Limitations of International Law Enforcement 8

11. The Role of International Coordination Structures 9

12. Media and Narrative Framing 9

13. Risks for Participants in Grey-Market Schemes 10

14. Conclusions 10

15. Recommendations 11

References 12

Abstract

This report presents a systemic analysis of the AirBit Club case as a representative model of transnational cryptocurrency fraud. It examines the architecture of the criminal scheme, the specific features of blockchain-infrastructure use and stablecoins (USDT, TRC-20 network), the mechanisms of concealing financial flows, as well as the institutional limitations of international law enforcement. The analysis covers digital marketing tools, psychological mechanisms of recruitment, the use of offshore companies, and the relationship between cryptocurrency transactions and traditional payment channels. Particular attention is paid to the systemic undercounting of victims, the fragmentation of investigations, the absence of a centralized database on criminal cryptocurrency schemes, and the political-economic dimension of criminal cases arising at the intersection of cryptocurrencies, property, and asset control. The report is written in an academic style and is intended for international organizations, law enforcement bodies, regulators, financial-crime researchers, and compliance professionals.

1. Introduction

The development of cryptocurrencies and distributed ledger technologies has led to the emergence of a new financial ecosystem that combines significant innovative potential with high criminogenic vulnerability. In recent years, cryptocurrencies have become a stable tool of transnational financial crime, including investment fraud, money laundering, sanctions evasion, and the financing of parallel shadow structures. A new layer of risks has emerged, associated with hybrid legal regimes, regulatory competition, and the absence of global oversight standards for digital assets.

Unlike traditional financial crimes, cryptocurrency-based schemes are characterized by a high degree of cross-border mobility, decentralized infrastructure, accessibility for non-specialists, and limited applicability of classical law-enforcement mechanisms. The absence of a single data-storage center, the ability to create new wallets instantly, and the use of mixers, cross-chain bridges, and offshore exchanges significantly complicate analytical work.

The AirBit Club case represents a demonstrative model that allows for a comprehensive analysis of these processes, tracing the relationships between the technological and organizational components of the scheme, and identifying systemic deficiencies in international oversight, including gaps in legal qualification, failures in inter-agency coordination, and the dependence of law-enforcement responses on the political-economic environment in individual states.

2. General Characteristics of the AirBit Club Case

AirBit Club positioned itself as a cryptocurrency investment platform offering participants passive income allegedly generated through automated trading and mining operations. Marketing materials disseminated through social networks, messaging platforms, and regional seminars emphasized “innovative technology,” “universal accessibility,” and “high returns with no risk.” In reality, the project conducted no verifiable investment activity, possessed no mining infrastructure, and provided no independently audited financial reports. Payouts were made using funds from new contributors, which qualifies the scheme as a classic Ponzi model.

The use of cryptocurrencies, especially USDT on the TRC-20 network, provided organizers with several key advantages:

– minimal banking oversight and streamlined circumvention of KYC/AML controls;

– the ability to use wallets not tied to identifying information;

– low transaction fees and high transfer speed;

– flexible mechanisms for withdrawing, segmenting, and rerouting incoming funds;

– a superficial appearance of technological legitimacy created through technical terminology.

The geographical reach of AirBit Club extended across several dozen countries in Latin America, Europe, the CIS region, Southeast Asia, and the Middle East. From the outset, this structure placed the case outside the boundaries of a single jurisdiction, complicated law-enforcement cooperation, and hindered the formation of a consolidated assessment of damages.

3. Organizational Structure and Scaling Logic

The organizational model of AirBit Club was based on the principles of multi-level marketing (MLM), combining elements of network-based promotion, psychological motivation, and decentralized recruitment. The central leadership shaped the ideological, marketing, and symbolic narrative, constructing the image of a high-tech international company. Regional coordinators and local agents were responsible for attracting funds, conducting presentations, training new participants, and maintaining internal communication within the "community."

The MLM model served several key functions:

1. Diffusion of responsibility among participants. Each agent was perceived as an autonomous recruiter, which reduced legal and operational risks for the organizers.
2. Concealment of a centralized command structure. The multi-level hierarchy and division of roles created the illusion of independent regional units.
3. Complication of proving direct criminal intent among lower-level promoters, many of whom themselves became victims of the scheme.
4. Exponential scaling. The network expanded without centralized expenditure, relying on the recruiting activity of participants.
5. Psychological retention. Participants were immersed in a closed environment with regular "motivational" events that fostered emotional dependence on the project.
6. Minimization of communication risks. Fragmented regional groups complicated evidence collection, provided operational flexibility during investigations, and allowed organizers to rapidly "cut off" local segments when criminal cases emerged.

Thus, the MLM architecture functioned not only as a scaling instrument but also as a component of the scheme's legal insulation, enabling organizers to distance themselves from operational activity, obscure key financial flows, and build a distributed network of intermediaries who simultaneously acted as both growth drivers and buffers against potential investigations.

4. Blockchain and the Illusion of Transparency

The common perception of blockchain as a fully transparent system is not supported by investigative practice and significantly oversimplifies the criminological reality. Although a

distributed ledger records every transaction, this fact alone does not enable investigators to identify wallet owners or understand the economic purpose of transfers. A combination of technological and organizational methods allows offenders to effectively obscure the movement of funds, exploiting the advantages of decentralized infrastructure.

In the AirBit Club case, blockchain operated not as a tool of openness but as a mechanism of concealment, enabling the construction of complex transactional chains that hinder analytical reconstruction of financial flows. The primary methods included:

– multiple transit wallets created sequentially to break the direct link between origin and destination addresses;

– splitting transactions into small amounts, complicating automated monitoring and reducing the likelihood of detecting suspicious patterns;

– inserting time gaps between transfers, disrupting chronological sequences and undermining standard heuristics used in financial-flow analysis;

– the use of non-custodial services, including decentralized wallets, mobile applications, and P2P platforms that do not conduct identity verification;

– routing through aggregator-services that pool transactions from different users, further complicating attribution.

Thus, the public nature of the blockchain ledger did not enable effective identification of ultimate beneficial owners without data from exchanges, payment processors, offshore registries, and operational investigative measures. Technological transparency transformed into an illusion of openness: although transaction data were formally accessible, they rarely led to identifying real individuals or the true centers of decision-making.

5. The Role of Stablecoins and the TRC-20 Network

A key element of the scheme was the systematic use of stablecoins, primarily USDT, on the TRC-20 network. This infrastructural choice was deliberate and reflected both the technical and criminal advantages of the Tron ecosystem. Compared to the Ethereum network, where most USDT circulation is concentrated, TRC-20 is characterized by low transaction fees, high throughput, and a relative degree of anonymity for operations conducted outside centralized exchanges. These features have made Tron a preferred platform for grey-market and illicit activities.

The combination of USDT and TRC-20 is widely used in transnational fraud, romance-scam schemes, illegal online casinos, capital-flight operations in countries with currency controls, as well as in the retail “cash-out” segment of cryptocurrency markets. The Tron network has effectively become a global infrastructural standard for low-barrier criminal schemes and high-speed money-laundering operations.

The AirBit Club case confirms the systemic nature of this trend. The use of stablecoins allowed the organizers to:

– minimize banking oversight and bypass traditional payment systems;

– avoid the volatility characteristic of other crypto-assets, ensuring internal transactional stability;

– rapidly redistribute funds among scheme participants and regional coordinators;

– provide investors with an illusion of "digital resilience" and technological sophistication;

– move assets into offshore jurisdictions where traditional oversight mechanisms are absent or highly constrained.

Thus, stablecoins were not a neutral technological tool but rather a structural component of the criminal model, ensuring its sustainability, concealment, and operational mobility.

6. Transnational Nature and Jurisdictional Gaps

The financial flows within AirBit Club passed through multiple legal systems, including offshore and proxy jurisdictions, resulting in a high degree of jurisdictional fragmentation. Existing mechanisms of international legal cooperation—such as Mutual Legal Assistance (MLA) requests and information exchanges between financial intelligence units—proved too slow and insufficiently coordinated to respond effectively to a scheme of this scale.

The transnational nature of the scheme manifested across several dimensions:

1. Geographical dispersion of participants, with investors, promoters, and organizers located in different countries.
2. Multi-layered transactional chains, routed through exchanges and wallets registered in jurisdictions with differing regulatory standards.
3. Use of offshore companies, which introduced additional layers of corporate anonymity.
4. Absence of a centralized investigative authority, resulting in parallel but uncoordinated investigative actions across states.

As a consequence, investigations in different countries evolved asynchronously: some opened criminal cases; others closed them due to insufficient data; still others never initiated proceedings because of jurisdictional limitations or lack of admissible evidence. This fragmentation weakened overall law-enforcement effectiveness, impeded identification of the true scale of financial harm, and contributed to systematic undercounting of victims, since each state recorded only its own complainants.

Jurisdictional gaps became a core factor in the scheme's resilience. The criminal model was adapted to an international environment in which the absence of a global investigative framework and the inconsistency of national approaches created the conditions for long-term operation—even after early warning signs of suspicious activity emerged.

7. Sanctions Evasion and Regulatory Circumvention

Although AirBit Club was not formally a sanctions-related case, the financial and technical infrastructure it employed closely resembles mechanisms commonly used for sanctions evasion and the circumvention of restrictive measures. Cryptocurrencies—especially stablecoins on low-fee networks—enable the movement of assets outside the scope of banking oversight, the masking of real beneficial owners, and the integration of illicit flows into the international financial system through P2P platforms, offshore exchanges, and non-custodial wallets.

This infrastructure facilitated:

– the circumvention of currency controls, particularly in countries with restrictive financial regulations;

– the transfer of funds through low-transparency jurisdictions, complicating the application of sanctions lists;

– covert movement of assets between related parties outside the banking system;

– the use of mixing services and informal OTC platforms enabling conversion to fiat without a formal record;

– the blending of legal and illegal transactions, obstructing identification of the criminal component.

Thus, the AirBit Club case is valuable not only as an example of an investment pyramid but also as empirical material for examining contemporary techniques of cross-border regulatory evasion. The methods employed within the scheme correspond closely to the toolkit typical of sanctions-evasion practices, including decentralized routing, operational flexibility, and rapid adaptation to regulatory changes. This makes the case relevant to broader discussions on digital-asset security in the global political-economic environment.

8. The Political-Economic Dimension

Contemporary international approaches increasingly recognize that economic criminal cases are not neutral by default. In many jurisdictions, criminal-law instruments are used to advance objectives that extend beyond law enforcement itself: redistribution of property, asset control, pressure on economic actors, or management of competitive environments. Accordingly, the analysis of transnational financial schemes requires consideration of the political-economic context that lies beyond formal legal qualification.

The AirBit Club case demonstrates that investigations into crimes involving digital assets inevitably intersect with issues such as:

– control over financial flows operating outside the banking sector;

– competition among states for jurisdictional authority over crypto-infrastructure;

– national political interests affecting the intensity and direction of investigative actions;

– the strategic positioning of digital assets within international economic relations;

– the development of new supervisory and regulatory instruments through which states expand their sovereign tools.

Thus, AirBit Club is not merely a financial scheme but a clinical example of how the digital economy, legal uncertainty, and international competition transform the nature of economic criminal cases. The underlying economic conflict often proves more significant than the formal criminal-law constructions applied to describe it.

9. The Problem of Victim Accounting

One of the key issues in the AirBit Club case is the systemic undercounting of victims, a characteristic feature of most transnational cryptocurrency schemes. Official victim lists reflect only a small portion of the actual number of affected individuals, which is driven by several factors:

1. **Absence of a global mechanism for registering victims.** Losses are recorded separately in each country, with no unified database.
2. **Fragmentation of criminal cases.** Different states open independent investigations without comparing the total scale of damage.
3. **Fear of legal consequences among participants.** Many contributors hesitate to file complaints due to the use of cryptocurrencies or involvement in informal financial arrangements.
4. **Difficulty proving actual losses.** Victims often lack documented transaction records or lose access to them due to platform shutdowns.
5. **The issue of secondary victims.** Organizers recruited participants through MLM structures, and some victims were simultaneously promoters, creating dual legal risks and reducing their willingness to approach authorities.

As a result, the real scale of harm may exceed official figures by an order of magnitude. The problem of victim accounting directly affects assessments of the scheme's socio-economic impact, the gravity of the offense, and the functioning of international asset-recovery mechanisms.

10. Limitations of International Law Enforcement

International law enforcement in the field of crypto-related crime remains institutionally constrained. Existing cooperation mechanisms were designed for traditional financial instruments and adapt poorly to a decentralized digital environment.

Key limitations include:

– lack of unified investigative standards, including blockchain-analysis methodologies and criteria for classifying crypto-crimes;

– divergences in legal regimes, with some states treating crypto-assets as property, others as financial instruments, and some lacking regulation entirely;

– slow processing of international requests, which is critical for highly liquid digital assets;

– absence of supranational mechanisms for consolidating victim data, hindering damage assessment;

– limited possibilities for asset recovery, especially when funds are converted into stablecoins or fiat in low-cooperation jurisdictions;

– dependence of investigative efficiency on political relations between states.

These institutional gaps create a favorable environment for the long-term operation of schemes such as AirBit Club and complicate the development of an effective international strategy to combat cryptocurrency fraud.

11. The Role of International Coordination Structures

International organizations — including INTERPOL, FATF, the Egmont Group of Financial Intelligence Units, and regional cooperation frameworks — primarily perform coordination, analytical, and informational-methodological functions. Their mandates do not include independent investigations or procedural intervention in criminal cases, yet they shape global standards and enable cooperation between states.

INTERPOL's role in cases of this kind is limited to issuing notices, facilitating operational information exchange between National Central Bureaus, and supporting specialized working groups on cryptocurrency-related crime. However, INTERPOL:

– does not have authority to recover assets;

– does not conduct its own investigative actions;

– does not intervene in criminal qualification, leaving it to national authorities;

– cannot impose mandatory disclosure standards on member states.

FATF and specialized international forums produce recommendations (such as the "virtual asset guidance"), but implementation depends on the political will of individual countries and the maturity of their financial systems. As a result, international coordination structures operate under conditions of voluntary cooperation, which limits their ability to respond effectively to rapidly evolving schemes like AirBit Club.

Thus, the current architecture of global cooperation does not provide sufficient analytical capacity and does not create supranational mechanisms capable of countering transnational crimes involving digital assets.

12. Media and Narrative Framing

Public coverage of cases such as AirBit Club shapes how the scheme is perceived by a broad audience, yet it often oversimplifies the actual dynamics, reducing them to a handful of recognizable figures or emotionally charged stories of individual victims. Media narratives substitute systematic analysis with superficial labels — "crypto-pyramid," "digital fraud," "criminal network" — while the internal logic of the scheme remains outside public attention.

Such simplification affects several dimensions:

– **public understanding of the problem**, diminishing awareness of the structural factors underlying the scheme;

– **regulatory behavior**, when decisions are made under pressure from public opinion rather than on the basis of comprehensive analysis;

– **international coordination**, as media focus on individual countries or personalities distorts the perception of the scheme's actual geography;

– **willingness of victims to contact law-enforcement agencies**, since media framing often produces expectations of futile or excessively burdensome procedures.

The media environment reinforces cyclical narratives: a burst of interest → brief discussion → disappearance of the topic. In the absence of expert interpretation, this results in fragmented public memory of the scheme, and the lessons that could have been drawn from the case fail to translate into regulatory practice.

Thus, the media narrative becomes not merely a tool for informing the public but a factor influencing the trajectory of investigations, political decision-making, and the general perception of digital assets.

13. Risks for Participants in Grey-Market Schemes

The AirBit Club case demonstrates that participants in grey-market cryptocurrency schemes — regardless of their role as investors, promoters, or intermediaries — face a set of systemic risks that significantly outweigh any potential gain. The illusion of anonymity, actively exploited by organizers, creates a false sense of security, although in reality blockchain's technical anonymity is highly conditional, and its legal anonymity is virtually nonexistent.

Key risks include:

1. **High probability of total financial loss.** In the absence of licensing, auditing, and legal protections, contributors have no formal mechanisms for asset recovery.
2. **Uncertain legal status.** Participation may be classified as aiding fraud, engaging in unlawful entrepreneurial activity, or facilitating money laundering.
3. **Secondary victimization.** Promoters who did not fully understand the scale of the scheme may simultaneously become victims and defendants in criminal proceedings.
4. **Identification vulnerabilities.** Personal data often become accessible to organizers, creating risks of data leakage and further exploitation.
5. **Lack of cross-border protection.** Participants may face divergent legal regimes across countries — including criminal liability for participation in unauthorized financial operations.

AirBit Club shows that involvement in grey cryptocurrency schemes is far from a "minor infraction": it entails systemic economic losses, legal exposure, and deep vulnerability to organizers who, in most cases, operate beyond the reach of national law-enforcement systems.

14. Conclusions

The AirBit Club case is not an exception but a stable, reproducible model of future cryptocurrency-related crimes. It demonstrates that blockchain and digital assets are not the root cause of criminal schemes but a technological instrument embedded into well-established patterns of financial fraud, including pyramid structures, capital-flight schemes, regulatory evasion, and money laundering.

The central problem lies not in the technology itself but in the combination of its characteristics — decentralization, cross-border mobility, low entry barriers, and the absence of unified international oversight mechanisms. The use of cryptocurrencies amplifies existing institutional

deficiencies, deepening the fragmentation of national jurisdictions, complicating victim identification, and hindering asset-recovery processes.

AirBit Club shows that the absence of a coordinated international approach to investigating cryptocurrency crimes inevitably leads to the persistent reproduction of schemes adapted to the vulnerabilities of the global regulatory environment. Divergent national approaches, limited mandates of international organizations, and institutional inertia create a space in which digital financial pyramids can operate for years despite early signs of suspicious activity.

Thus, AirBit Club is not an isolated criminal episode but a structural symptom of broader transformations in the international financial architecture. Without the development of institutional, intergovernmental, and interdisciplinary coordination mechanisms, schemes of this kind will not only continue to emerge but will expand, integrating themselves into global flows of digital capital.

15. Recommendations

The analysis of the AirBit Club case allows for the formulation of several practical recommendations for international organizations, regulators, and law-enforcement bodies aimed at increasing the resilience of financial systems to transnational cryptocurrency crimes.

1. **Development of international mechanisms for consolidating data on victims of crypto-crime.**

A unified supranational platform is needed to aggregate victim reports, compare data across jurisdictions, and produce a global damage assessment. This would enhance investigative accuracy and help identify links between parallel cases.

2. **Strengthening oversight of the OTC segment and stablecoin operations.**

OTC platforms, P2P markets, and stablecoin-based transactions remain the least regulated segments of crypto-infrastructure. Implementing KYC/AML standards, monitoring large or repetitive transactions, and requiring mandatory registration of OTC brokers within national financial registries are essential steps.

3. **Recognition of the political-economic context of economic criminal cases.**

Regulators and international bodies should acknowledge that digital-asset-related criminal cases often form part of broader processes involving control over capital. This requires interdisciplinary analysis combining political science, economics, and international relations.

4. **Integration of blockchain analytics with traditional financial investigations.**

Blockchain analytics cannot be effective in isolation. It must be combined with traditional investigative tools — banking data, corporate registries, telecommunications records, and customs documentation. Creating mixed analytical teams that unite experts in finance, cryptotechnology, and international law would improve investigative quality and shorten response times.

These recommendations aim to foster a more resilient international framework for combating cryptocurrency-related crime — one that can respond to the dynamics of the digital economy and minimize systemic vulnerabilities that enable schemes such as AirBit Club to emerge and persist.

References

1. https://www.justice.gov/usao-sdny/pr/co-founder-global-multimillion-dollar-cryptocurrency-ponzi-scheme-airbit-club
2. https://www.justice.gov/usao-sdny/pr/operators-and-attorney-global-multi-million-dollar-cryptocurrency-ponzi-scheme-airbit
3. https://www.interpol.int/What-you-can-do/Crimes/Financial-crime
4. https://www.interpol.int/How-we-work/Notices
5. https://www.interpol.int/News-and-Events/News/2024
6. https://www.fatf-gafi.org/en/topics/virtual-assets.html
7. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
8. https://www.trmlabs.com/resources/blog
9. https://www.europol.europa.eu/crime-areas/economic-crime
10. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances
11. https://www.unodc.org/cld/fr/education/tertiary/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html
12. https://www.congress.gov/crs-product/R47425
13. https://argaobservatory.org/en/