Observatoire ARGA

Judicial Standards of Evidence in Crypto Cases:

Limits of Admissibility of On-Chain Analytics and Risks of Misattribution

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

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

Website: www.argaobservatory.org

Paris, 22 January 2026

Table of Contents

Abstract

This report analyzes judicial standards of proof in cases involving cryptocurrencies and digital assets. It examines the limits of admissibility of on-chain analytics, the problem of attributing crypto wallets, the distinction between probabilistic conclusions produced by analytical companies and legally relevant evidence, as well as the risks of judicial errors and abuses of law enforcement. Particular attention is given to how technical assumptions are transformed into criminal accusations and how this affects the presumption of innocence and the right to a fair trial.

Introduction

Investigations of cryptocurrency-related crimes increasingly rely on on-chain analytics provided by specialized private companies. These tools make it possible to visualize asset movements, identify connections between addresses, and formulate hypotheses about beneficial control.

However, there is a fundamental gap between an analytical hypothesis and judicial evidence. In the absence of unified international standards, this gap is often ignored, creating the risk of criminal prosecution based on probabilistic models.

On-chain analytics as a probabilistic tool

On-chain analytics is based on:

- address clustering;
- behavioral patterns;
- heuristic rules;
- statistical assumptions.

The results of such analysis are expressed in probabilities rather than facts. Nevertheless, in criminal cases these conclusions are often interpreted as established circumstances.

The problem of crypto wallet attribution

The key issue in crypto cases is establishing the link between an address and a specific individual. In practice, the following are used:

- IP logs and metadata;
- data from exchanges and service providers;
- testimony of third parties;
- correlation-based conclusions of analysts.

Each of these elements, taken separately, rarely has sufficient evidentiary value, yet in combination they are often used to justify accusations without direct proof of control.

Address clustering and its limitations

Clustering methods assume that:

- addresses participating in joint transactions belong to the same entity;
- behavioral similarity indicates unified control.

In reality, such assumptions fail to account for:

- custodial services;
- mixers and liquidity pools;
- multi-party access;
- key compromise.

This leads to erroneous attribution and expansion of the circle of suspects.

The role of private analytical companies

Analytical companies play a central role in forming the evidentiary basis. At the same time:

- their methodologies are trade secrets;
- algorithms are opaque to the court and the defense;
- conclusions are not subject to full verification.

In effect, courts and investigators delegate the function of proof to private entities without proper procedural oversight.

Forensic examination and conflict of standards

Classical forensic examination requires:

- reproducibility;
- verifiability;
- neutrality of the expert.

On-chain analytics often fails to meet these criteria, yet is accepted by courts as “specialized knowledge,” thereby blurring the standard for admissible evidence.

Shifting of the Burden of Proof

In crypto cases, a shift in the burden of proof is frequently observed:

- from the prosecution to the defense;
- from the state to the accused.

The accused is compelled to prove the absence of control over an address, which contradicts the principle of the presumption of innocence.

Misattribution and Its Consequences

Errors in attribution lead to:

- unfounded accusations;
- seizure of assets belonging to bona fide individuals;
- international search notices;
- extradition risks.

Even if the case is later discontinued, the reputational and economic damage is often irreversible.

International Practice and Diverging Approaches

In different jurisdictions, standards for evaluating on-chain evidence vary:

- some courts require a direct link between the address and the individual;
- others accept probabilistic conclusions as sufficient.

The lack of harmonization increases legal uncertainty and the risk of forum shopping.

Political and Economic Context of Evidence

In cases involving significant economic or political interests, evidentiary standards are often lowered. On-chain analytics is used to:

- accelerate proceedings;
- justify severe measures;
- legitimize asset seizure.

Evidence becomes an instrument of policy rather than a means of establishing truth.

Impact on the Right to Defense

The defense in crypto cases faces:

- lack of access to analytical methodologies;
- limited возможности for counter-expertise;
- technical asymmetry of resources.

This violates the principle of equality of arms and reduces the quality of judicial proceedings.

Risks for International Cooperation

The use of unverifiable analytical conclusions in international requests:

- undermines trust between states;
- complicates extradition procedures;
- increases the likelihood of refusals and conflicts.

The quality of evidence becomes a factor of international tension.

Institutional Limits of the Current Approach

The current model of proof in crypto cases:

- does not ensure sufficient accuracy;
- ignores technological complexity;
- transfers the risk of errors onto the accused.

Without institutional revision, these defects will persist.

Conclusions

On-chain analytics is a useful investigative tool but cannot substitute for judicial evidence. The absence of clear standards for admissibility and verification creates the risk of systemic errors, human rights violations, and the politicization of justice.

Recommendations

- Establish clear judicial standards for the admissibility of on-chain evidence.

- Require mandatory disclosure of the methodologies behind analytical conclusions.
- Develop independent forensic crypto-expertise.
- Prevent shifting the burden of proof onto the defense.
- Harmonize international approaches to the evaluation of digital evidence.

List of sources and materials used

1. https://www.fatf-gafi.org/en/topics/virtual-assets.html
2. https://www.imf.org/en/publications/fandd/issues/2022/09/regulating-crypto-narain-moretti
3. https://www.bis.org/publ/qtrpdf/r_qt2103.htm
4. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
5. https://www.europol.europa.eu/crime-areas/economic-crime
6. https://www.unodc.org/unodc/en/cybercrime/home.html
7. https://www.interpol.int/What-you-can-do/Crimes/Financial-crime
8. https://argaobservatory.org