Observatoire ARGA

ARGA Atlas

CRYPTOCURRENCY IN CRIMINAL CASES: THE FORMATION OF CHARGES AND THE VULNERABILITIES OF THE EVIDENTIARY BASE

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA, ARGA Atlas

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, https://www.arga-atlas.com/

Anglet, 12 March 2026

Purpose of the document:

To explain how cryptocurrency and other virtual assets are used in contemporary criminal cases as the object of an accusation, the alleged instrument of an offense, the alleged channel for laundering proceeds, or a digital evidentiary trail; to show why the evidentiary base in such cases is especially vulnerable in terms of attribution, provenance, chain of custody, expert interpretation of blockchain data, and fair trial guarantees; and to propose a practical defense model for cases in which blockchain traces, exchange records, wallets, devices, and cross-border electronic evidence are combined into a criminal narrative. The relevant framework is built primarily around Article 14 of the ICCPR, the Budapest Convention and its electronic-evidence architecture, FATF standards on virtual assets and VASPs, Europol materials on cross-border electronic evidence, and digital-evidence handling standards. (OHCHR)

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Cryptocurrency is no longer treated in criminal proceedings as an eccentric side issue. FATF extended Recommendation 15 to virtual assets and virtual asset service providers, and its 2025 targeted update confirms that regulation of VAs and VASPs continues to expand while remaining uneven across jurisdictions, with continuing gaps in risk assessment, licensing, supervision, and Travel Rule implementation. That means cryptocurrency cases almost always unfold against a background of fragmented regulation rather than a single coherent global standard. (FATF)

Europol's SIRIUS Electronic Evidence Situation Report 2024 states that social media, messaging apps, and crypto exchanges remain among the most relevant online services in criminal investigations. In practice, that changes the structure of the criminal process itself: cryptocurrency is no longer only a potential object of seizure or confiscation, but part of a broader electronic-evidence

ecosystem involving exchanges, devices, cloud services, messaging platforms, and cross-border disclosure requests. (Europol)

The central problem in such cases is that blockchain traceability creates a strong impression of objectivity. In reality, however, a long chain of assumptions lies between a visible on-chain transfer and a legally admissible conclusion that a specific person committed a specific offense. One must still ask who controlled the wallet, who held the private key, whether the wallet was custodial, how the data was extracted, whether its integrity was preserved, who performed clustering or tracing analysis, and where technical probability is being transformed into criminal attribution. Cryptocurrency cases therefore often look digitally precise while remaining procedurally fragile. (Europol)

2. WHY CRYPTOCURRENCY IN A CRIMINAL CASE IS ALMOST NEVER "JUST AN ASSET"

In a criminal case, cryptocurrency may perform several different legal functions at once. It may be presented as the object of theft, the channel of payment, the means of concealing proceeds, a sanctions-evasion tool, an asset to be frozen or confiscated, or a digital trail on which the prosecution builds a narrative about movement of value. The dispute therefore almost never reduces to the simple question whether a person "has crypto." The real dispute concerns what particular addresses, transactions, smart-contract interactions, exchange logs, and wallet activity mean in legal rather than merely technical terms. FATF's virtual-assets guidance expressly treats virtual assets and VASPs as a distinct AML/CFT risk environment rather than as neutral technical infrastructure. (FATF)

A further complication is that the Budapest Convention is not limited to "cybercrime" in the narrow sense. It also provides procedural tools for the collection of evidence in electronic form of a criminal offense. Once a case is built on wallets, exchange accounts, device histories, or foreign disclosure requests, the cryptocurrency element becomes part of the law of electronic evidence and international cooperation, not merely a dispute about property. (Portal)

3. HOW CHARGES ARE USUALLY BUILT IN CRYPTOCURRENCY CASES

The most common accusatory structures in cryptocurrency cases usually follow one of three models. First, cryptocurrency is treated as allegedly laundered proceeds, with the prosecution pointing to wallet layering, chain-hopping, mixers, or movement through multiple addresses. Second, cryptocurrency is treated as a payment mechanism in fraud, extortion, darknet trade, corruption, sanctions evasion, or other unlawful schemes. Third, cryptocurrency functions as an evidentiary trail, where transaction history becomes a central part of the accusation even if the charge itself is not a "crypto offense" in a narrow sense. FATF and Europol materials both support this broader view of virtual assets as part of a wider illicit-finance and electronic-evidence landscape. (FATF)

Investigative authorities often present this structure as nearly self-sufficient: there is an address, there is a transaction, there is an analytics report, therefore there is almost a complete case. That is precisely where the core evidentiary distortion begins. Blockchain analytics does not by itself prove intent, does not replace proof of actual control, does not answer the contextual question of why an operation occurred, and does not transform clustering heuristics into personal criminal liability. From a fair trial perspective, a cryptocurrency case cannot be reduced to a contest between an investigative analytics

report and judicial admiration for technical charts. The defense retains the right to call and examine witnesses, including expert witnesses. (OHCHR)

4. THE CORE EVIDENTIARY PROBLEM: FROM BLOCKCHAIN TRACE TO PERSONAL ATTRIBUTION

The central weakness of most cryptocurrency cases lies in the gap between traceability and attribution. A public blockchain may show movement of value from address to address, but that does not answer the decisive legal questions: who actually controlled the address, who had access to the private key, whether the wallet was custodial, whether an exchange omnibus structure was involved, whether a third party or service provider controlled the account, or whether access may have been delegated, shared, or stolen. On-chain visibility is therefore not the same thing as personal criminal attribution. (Europol)

Europol's encryption report explicitly notes that funds are spent only by the rightful holder of the private key, while sharing or theft of a private key can lead to loss of funds and impersonation. For criminal proceedings, that is not a technical footnote but a major legal warning. Even where a blockchain trail is continuous, the prosecution must still prove control and volition on the part of the accused, and the defense is entitled to argue theft of credentials, delegated access, custodial control, shared-device use, internal exchange operations, or other explanations that break the supposedly automatic equation "address equals person." Too often, the visual neatness of a transaction path psychologically replaces the harder work of proving who actually acted. (Europol)

5. CUSTODIAL VS. NON-CUSTODIAL WALLETS, PRIVATE KEYS, AND THE PROBLEM OF CONTROL

The distinction between custodial and non-custodial wallets is fundamental in cryptocurrency litigation. Europol explains that in a custodial arrangement the user does not hold the private key, while centrally managed exchanges typically do so on the user's behalf. In a non-custodial arrangement, by contrast, the user bears responsibility for private-key storage. Legally, that means the conclusion that a person "controlled the crypto" must be built differently depending on the architecture involved. In one case, the analysis will depend heavily on exchange records, KYC data, and account logs. In the other, it may depend on access to a device, seed phrase, wallet application, hardware wallet, or other indicators of direct control. (Europol)

This difference breaks simplistic accusatory models. If the assets were held at a custodial exchange, then without exchange records, user-identification data, login history, and account activity, attributing those assets directly to the accused may be very weak. If the case instead concerns a non-custodial wallet, different questions arise: whether the device was lawfully seized, how wallet files were extracted, who had access to the device, whether chain of custody was preserved, and whether seed phrases or passwords were recorded, shared, or stolen. UNODC's digital-evidence handling guidance stresses the importance of identification, collection, acquisition, and preservation of potential digital evidence. In cryptocurrency cases, that means the real dispute often concerns the quality of digital forensics as much as the asset itself. (UNODC)

6. ELECTRONIC EVIDENCE, CROSS-BORDER ACCESS, AND CHAIN OF CUSTODY

Cryptocurrency cases are almost inevitably cross-border. A blockchain address may be public, but the information required for attribution often sits with an exchange, custodian, cloud provider, messaging service, or telecom operator in another jurisdiction. Europol expressly notes that criminal investigations are increasingly dependent on access to digital data, and that crypto exchanges are among the most relevant service categories in criminal investigations. In practice, that means the accusation in a cryptocurrency case is often built from a cross-border mosaic of digital evidence rather than from a single domestic source. (Europol)

This is where the Budapest Convention and its Second Additional Protocol become especially important, because the Protocol is specifically aimed at enhanced cooperation and disclosure of electronic evidence. Yet easier access does not eliminate the classic problems of admissibility and integrity. If a court is shown exchange records, extracted device data, screenshots, blockchain analytics, and foreign disclosure packets, the defense remains entitled to question the completeness of disclosure, the conditions of transmission, the technical integrity of the data, the quality of translation, the extraction method, and the real procedural possibility of contesting the material. Otherwise, international cooperation turns into a fast import mechanism for a ready-made digital accusation. (Portal)

7. EXPERT REPORTS, BLOCKCHAIN ANALYTICS, AND PROCEDURAL TESTABILITY

Cryptocurrency cases are heavily dependent on expert evidence. That may include blockchain analytics reports, wallet-forensics examinations, tracing visualizations, attribution opinions, and technical reports on device extraction. The danger is obvious: such reports look extremely persuasive. They arrive decorated with graphs, hashes, clusters, timelines, and transaction maps. But procedurally they remain expert evidence, not self-executing truth. OHCHR's fair trial guidance makes clear that the defense must be able to call and examine witnesses, including expert witnesses. That means the methodology of blockchain analysis is open to challenge and cannot be treated as a sacred technical text immune from adversarial scrutiny. (OHCHR)

In practice, vulnerability appears in at least three places. First, clustering heuristics and attribution assumptions may be probabilistic rather than definitive. Second, experts often work with a pre-selected data set and may never see excluded context. Third, courts may psychologically assign to a digital report a degree of objectivity that it does not actually possess in procedural terms. For that reason, the defense should demand not only disclosure of the final report, but disclosure of the inputs, methods, limitations, data sources, and alternative interpretations. Otherwise, the expert report becomes a mechanism for laundering an investigative hypothesis into an apparently neutral conclusion. (Europol)

8. AML/CFT, VASP REGULATION, DEFI, AND GROWING NORMATIVE ASYMMETRY

FATF's 2025 targeted update shows that global implementation of Recommendation 15 remains incomplete. Not all jurisdictions have carried out robust VA/VASP risk assessments, VASP

regulation remains uneven, and significant differences persist around DeFi, NFTs, unhosted wallets, and peer-to-peer activity. FATF also notes continuing struggles with licensing or registration and with implementation of the Travel Rule. That means criminal cases involving cryptocurrency unfold in a world where one jurisdiction may see a regulated VASP environment, another may see a weakly supervised market, and a third may approach the same activity through prohibition or severe restriction. (FATF)

For criminal proceedings, this matters directly. The same address, transaction, or service may be seen in one jurisdiction as ordinary virtual-asset activity and in another as a red flag for laundering or evasion. DeFi arrangements, unhosted wallets, and peer-to-peer transfers are especially sensitive because evidentiary assessment and regulatory characterization do not automatically coincide. FATF's own materials show that jurisdictions continue to adopt different approaches in these areas. As a result, an accusatory theory built on the mere fact that a person used a particular technical arrangement cannot be treated as neutral or universally valid. Law still requires proof of conduct and intent. It does not magically transform technical novelty into mens rea, however tempting that may be for investigators. (FATF)

9. A PRACTICAL MODEL OF DEFENSE

Defense in a cryptocurrency case should not be built as a philosophical dispute over whether crypto is good or bad. It should be built as a layered challenge to the transformation of technology into evidence. The first level is attribution: who controlled the wallet, account, key, device, or exchange profile. The second level is provenance and integrity: how the data was obtained, who extracted it, where it was stored, whether the format changed, and how chain of custody was preserved. The third level is expert challenge: what blockchain-analytics methods were used, how reliable they are, and whether alternative explanations were excluded. The fourth is cross-border challenge: what legal route was used to obtain records from foreign exchanges or providers, and whether the defense was given genuine access to the full body of relevant material. That structure follows directly from the logic of digital evidence handling and fair trial. (UNODC)

The defense must also break the false presumption that technical complexity equals proof. In cryptocurrency cases, the prosecution often wins not because it has proved more, but because the other side was never allowed to unpack digital material into legal elements. A serious defense therefore translates blockchain language into procedural language: who asserts what, on what basis, what is actually established, what is only probable, what remains unproven, and which alternative hypotheses were never excluded. Once that translation is done, the technological glamour fades quickly and what remains is an ordinary criminal process with ordinary burdens of proof. That tends to disappoint people who were hoping the charts would do the thinking for them. (OHCHR Docstore)

10. CONCLUSION

Cryptocurrency in criminal cases creates a double illusion: technological transparency and normative certainty. In reality, neither is guaranteed. A public blockchain does not eliminate the problem of personal attribution; global access to electronic data does not remove the need for chain of custody and fair disclosure; and expanding AML/CFT regulation of virtual assets and VASPs does not erase inter-jurisdictional divergence, especially around DeFi, unhosted wallets, and peer-to-peer activity. All of this makes cryptocurrency cases not "simple digital cases," but cases with a particularly vulnerable evidentiary base. (FATF)

The main practical conclusion is simple. In such cases, one should not argue with the technology as such, but with the way technology has been converted into evidence. Who attributed the address to the person, who interpreted the transaction as criminal, who selected the data set, who prepared the expert report, who verified completeness, and what opportunity the defense had to challenge all of this. If those questions remain unanswered, the case may have a very modern digital façade, but the core problem inside will be ancient: the accusation rests not on proof, but on the impression produced by numbers. Wrapped in hashes and diagrams, it is still the same old defect of process. (OHCHR Docstore)

APPENDIX A. TERMINOLOGY

Virtual asset
A FATF term covering a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. FATF standards apply AML/CFT obligations to virtual assets and VASPs through Recommendation 15. (FATF)

VASP
A virtual asset service provider, meaning a person or entity conducting specified virtual-asset activities as a business. FATF guidance and the 2025 targeted update show that licensing, registration, and supervision of VASPs remain one of the central regulatory issues worldwide. (FATF)

Custodial wallet
A wallet arrangement in which the private keys are held by a service on behalf of the user. Europol notes that funds stored at centralized cryptocurrency exchanges are typically custodial. This matters directly to the question of factual control. (Europol)

Non-custodial wallet
A wallet arrangement in which the user is responsible for storing the private keys. Europol notes that sharing or theft of a private key may lead to loss of funds or impersonation, which has direct significance for criminal attribution. (Europol)

Electronic evidence
Electronic data having evidentiary value. The Budapest Convention expressly extends its procedural tools to the collection of evidence in electronic form of a criminal offense. (Portal)

APPENDIX B. MATRIX OF EVIDENTIARY VULNERABILITIES IN CRYPTOCURRENCY CASES

The main evidentiary vulnerabilities in cryptocurrency cases can be summarized as follows: visible blockchain tracing without personal attribution; uncertainty whether the wallet was custodial or non-custodial; ambiguity over private-key control; dependence on exchange or provider records from foreign jurisdictions; weak chain of custody for device or wallet data; opaque blockchain-analytics methodology; selective presentation of digital records; and regulatory asymmetry across jurisdictions regarding VASPs, DeFi, unhosted wallets, and peer-to-peer activity. Each of these vulnerabilities directly affects admissibility, reliability, and the defense's ability to challenge the prosecution case in adversarial proceedings. (Europol)

OFFICIAL SOURCES

1. International Covenant on Civil and Political Rights. (OHCHR)

2. Human Rights Committee, General Comment No. 32 on Article 14 ICCPR. (OHCHR Docstore)

3. Convention on Cybercrime (Budapest Convention). (Portal)

4. Second Additional Protocol to the Budapest Convention on enhanced co-operation and disclosure of electronic evidence. (Portal)

5. FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs. (FATF)

6. FATF, 2025 Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs. (FATF)

7. Europol, SIRIUS Electronic Evidence Situation Report 2024. (Europol)

8. Europol, First Report on Encryption by the EU Innovation Hub for Internal Security. (Europol)

9. OHCHR, Right to a Fair Trial and Due Process. (OHCHR)

10. UNODC / digital evidence handling guidance based on ISO/IEC 27037. (UNODC)