Observatoire ARGA

Blockchain as a Tool of Financial Crime: The Myth of Full Transparency and the Real Mechanisms of Concealment

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, 11 January 2026

Table of Contents

Abstract

This report offers a critical analysis of the concept of "blockchain transparency," widely circulated in public and regulatory discourse, within the context of transnational financial crime and the digital economy. Drawing on comparative evidence from international investigations, regulatory documents, technical specifications, and empirical cases of cryptocurrency fraud, it examines the mechanisms through which public distributed ledgers can be used not as instruments of disclosure but as tools for concealing economic relationships, ultimate beneficial ownership, and cross-border capital flows. Special attention is given to the institutional limitations of blockchain analytics as evidentiary material, the structural weaknesses of identification in decentralized systems, the role of the OTC segment and stablecoins, and architectural features of crypto-infrastructure. The report also analyzes the political-economic dimension of criminal prosecution in crypto-related cases, including jurisdictional competition, fragmented enforcement, and the uneven landscape of international regulatory standards.

1. Introduction

Since the institutionalization of cryptocurrencies, blockchain has been consistently positioned as a technology that ensures transparency, immutability, and traceability of financial operations. These characteristics are frequently invoked in regulatory documents, ESG reporting, investment memoranda, and marketing strategies as an argument for the reliability and "built-in integrity" of digital assets. This narrative fosters the expectation that technical accessibility of data automatically guarantees transparency of economic processes.

Yet empirical practice in investigating transnational financial crimes shows that the formal openness of a distributed ledger does not equate to transparency of economic relations. In an environment shaped by stablecoins, proxy structures, P2P exchangers, offshore exchanges, multi-layer transaction chains, and grey financial channels, blockchain becomes not a mechanism of disclosure but a highly effective tool of obfuscation. The conflation of technical transparency with institutional opacity leads to systematic errors in regulatory assessments, law-enforcement decisions, and public debate.

2. Ledger Transparency and Economic Opacity

While a public blockchain records the sequence of transactions, it does not reveal:

• the legal nature of the operation,

• the economic motive of the parties,

• ownership structures,

• effective control over the assets,

• the role of intermediaries in the transaction chain,

• the origin and destination of funds.

Thus, blockchain offers *technical* transparency of records, but not *institutional* transparency of ownership, obligations, or responsibility. As a result, one can trace the formal trajectory of funds without understanding their economic meaning unless extensive off-chain data is incorporated.

Public narratives frequently overlook this distinction. The assertion of "full traceability" is often used as proof of inherent safety, even though in practice traceability substitutes for understanding rather than complementing it. Economic opacity persists even when transaction data is fully accessible.

3. Pseudonymity as a Structural Defect of Control

Most public blockchains rely on a pseudonymous model of identification: a wallet address is not linked to a legal subject, and proving such a link requires external (off-chain) data — banking records, exchange data, IP information, telecom metadata, device fingerprints, or results of investigative operations.

Under conditions of:

• multiple addresses per user,

• transfer or sale of private keys,

• use of hardware and multisignature solutions,

• involvement of intermediaries and aggregator services,

• deployment of mixers, bridges, and non-custodial wallets,

pseudonymity ceases to be a feature of privacy and becomes a tool for systematically diffusing responsibility. It undermines conventional mechanisms of provenance verification and substantially inhibits law enforcement because:

– it prevents linking an address to a legal entity without external data;

– it creates a false appearance of decentralization and absence of central control;

– it enables the "dissolution" of ownership chains;

– it reduces the effectiveness of international legal requests due to jurisdictional fragmentation.

Pseudonymity is not an accidental by-product of blockchain — it is an architectural property that, in the absence of international identification mechanisms, becomes a fundamental barrier to investigating financial crimes.

4. Wallet Hopping as a Method for Disrupting Analytical Chains

The practice of sequentially moving funds across dozens or even hundreds of addresses (wallet hopping) is one of the most widespread techniques used to undermine blockchain analytics in transnational financial schemes. This approach serves to:

• **complicate tracing**, as each intermediate transaction increases the length of the chain and reduces the likelihood of correct attribution;

• **create false correlations**, where the regularity or randomness of transfers obscures the underlying logic of capital movement;

• **increase the probability of analytical error**, especially when dealing with large volumes of transactions that force analytic models to rely on heuristics.

Each additional transit node reduces the evidentiary value of the analysis because:

– the likelihood of the chain collapsing grows due to the absence of off-chain data;

– the number of non-identifiable nodes increases;

– the risk of false positives between addresses rises;

– reliance on probabilistic models grows, and such models are often viewed by regulators and courts as insufficiently reliable.

As a result, wallet hopping becomes an effective method for destroying causal links, generating "noisy" transactional graphs in which the true path of capital is lost among hundreds of technical transfers.

5. Transaction Splitting and Noise in the Ledger

Splitting large sums into numerous micro-transactions (transaction splitting) is used as a means of reducing the visibility of operations and circumventing automated monitoring systems. This method serves several purposes:

• bypassing quantitative or threshold triggers embedded in analytics systems;

• masking actual volumes by dispersing the total value across many small transfers;

• generating transactional noise that interferes with typological analysis and address clustering.

In low-fee networks (such as TRC-20 and BSC), transaction splitting becomes particularly effective because:

– the cost of producing thousands of transactions is negligible;

– the activity resembles ordinary user behavior;

– visual analysis of transaction graphs becomes meaningless due to high node density;

– threshold-based analytical models lose effectiveness.

Thus, transaction splitting transforms a formally public ledger into a dataset poorly suited for operational analysis, concealing the actual economics of a scheme beneath layers of “natural” network traffic.

6. Timing Gaps as a Masking Technique

Using controlled time intervals between transactions (timing obfuscation) is one of the less visible yet highly effective techniques for disrupting correlation analysis. Even small gaps:

• break the chronological structure of the chain, depriving analysts of the ability to link operations into a single motivated act;

• hinder the identification of patterns typical of automated schemes;

• blur temporal correlations between addresses.

As gaps between transactions increase:

– the chain loses logical coherence;

– the space for ambiguous interpretations expands;

– the number of analytical hypotheses grows, many of which cannot be tested without external data;

– several flow-tracing methodologies cease to function effectively.

Even if individual addresses are identified, full reconstruction of the chain requires significant resources, access to exchange records, and deep inter-agency cooperation — conditions that are often unattainable in practice.

7. Non-Custodial Infrastructure and the Absence of an Accountable Entity

Non-custodial and decentralized services (non-custodial wallets, DEXs, dApps, multisignature solutions) eliminate the presence of a centralized operator subject to obligations such as:

• complying with AML/KYC requirements;

• responding to law-enforcement requests;

• providing user information;

• freezing assets in accordance with legal orders.

This creates several systemic problems:

– **absence of a lawful addressee for enforcement requests:** there is simply no entity to which a court order can be addressed;

– **inability to freeze assets promptly:** no party controls users' private keys;

– **dissolution of subjectivity:** responsibility is diffused across users, developers, and validators, none of whom hold legally enforceable obligations;

– **cross-border jurisdictional ambiguity:** it is unclear which state has authority to demand compliance or impose sanctions.

Non-custodial infrastructure deepens the asymmetry between offenders and law-enforcement agencies: the former gain global tools for concealing and moving capital, while the latter remain constrained by national jurisdictions.

8. The OTC Segment as a Critical Zone of Regulatory Blindness

OTC operations create a crucial disconnect between on-chain transactions and the real economy. Off-exchange deals — P2P trades, private brokered transactions, informal cash desks — constitute an environment in which the link between a digital address and the actual owner effectively disappears. It is through OTC channels that the following regularly take place:

• **cash-outs of cryptoassets**, bypassing traditional banking procedures;

• **conversion into fiat or other assets**, including precious metals, cash, or goods;

• **transfer of control without on-chain traces**, as ownership may change hands through "keys-for-cash" deals;

• **integration of illicit funds into the legal economy** via local or cross-border grey-market exchangers.

This segment remains one of the least regulated parts of the crypto-market because:

– it operates outside centralized platforms;

– it generally does not comply with AML/KYC standards in most jurisdictions;

– it is resistant to bans and shutdowns, easily migrating to messengers and offline settings;

– it is highly adaptive and fragmented.

As a result, the OTC sector becomes a structural point of regulatory blindness, depriving law-enforcement bodies of the ability to connect on-chain behavior with real-world actors and disrupting key analytical chains.

9. Stablecoins and the Effect of a "Quasi-Banking" Infrastructure

Stablecoins combine the characteristics of cryptocurrencies (speed, decentralization, low fees) with those of traditional payment instruments (price stability, wide acceptance). Their use enables:

• **high liquidity** in cross-border operations;

• **absence of volatility**, making them convenient for settlements;

• **compatibility with grey-market schemes**, particularly in jurisdictions with currency controls;

• **low transaction costs**, which allow operations to be split without financial loss.

However, institutional oversight over stablecoins is often incomparable to banking regulation. Issuers and exchanges:

– do not always adhere to full financial-reporting standards;

– may be domiciled in offshore jurisdictions;

– fall under unevenly distributed regulatory regimes;

– do not provide sufficient transparency of reserves.

The result is a **quasi-banking infrastructure**: functionally similar to traditional transactional systems, yet lacking systemic safeguards, risk-management frameworks, and supervisory mechanisms. This asymmetry of risks makes stablecoins an ideal tool for high-speed capital movement within grey and illicit schemes.

10. Mixers, Bridges, and Cross-Chain Operations

The use of mixers, cross-chain bridges, and inter-network transfer mechanisms represents a more advanced level of analytical obfuscation, allowing actors to:

• **break the linearity of data**, turning a coherent sequence of transactions into a fragmented structure;

• **move assets across networks** that operate under different analytical tools and transparency regimes;

• **circumvent jurisdictional constraints**, since different blockchains fall under varying degrees of regulation;

• **conceal the origin of funds**, as their "transactional history" is often lost or rendered opaque during cross-chain transfers.

Bridges enable the movement of assets between ecosystems such as Ethereum, Tron, BSC, Polygon, and others. Each transfer:

– creates a point at which the analytical chain is interrupted;

– requires an entirely new layer of analysis within the destination network;

– complicates the matching of addresses and behavioral patterns;

– increases the risk of losing semantic continuity between transactions.

Taken together, these tools enhance data fragmentation and significantly complicate international cooperation: investigations must account for multiple networks, jurisdictions, and infrastructural intermediaries.

11. Limitations of Blockchain Analytics as Evidence

Despite its apparent precision, blockchain analytics is **probabilistic rather than deterministic**. It relies on heuristics, clustering algorithms, statistical correlations, and assumptions about economic behavior.

Without off-chain data, on-chain analysis:

– lacks independent evidentiary strength;

– cannot establish the legal identity of the involved parties;

– does not confirm the provenance of funds;

– cannot provide legally meaningful proof of ownership;

– requires verification through banking, corporate, and registry sources.

In judicial proceedings, blockchain analytics is treated as a **supplementary tool**, one that:

• must be corroborated by documentation from the traditional financial system;

• cannot serve as the sole basis for prosecution;

• is vulnerable to errors stemming from clustering or false correlations;

• enjoys limited admissibility in some jurisdictions.

Thus, on-chain analysis is a powerful but incomplete instrument—effective only when combined with institutional mechanisms of financial investigation.

12. Comparative Analysis of Regulatory Approaches

Regulatory models in the European Union, the United States, and international organizations display a common trend toward tightening oversight and institutionalizing the cryptocurrency market. Yet despite this apparent convergence, a systemic gap persists between regulatory requirements and their implementation in transnational investigations.

In the EU, the primary emphasis is on comprehensive frameworks such as MiCA and TFR, aimed at preventive oversight and the creation of a unified supervisory environment. However:

– the amount of data required from service providers remains limited;

– blockchain-analysis methodologies are excluded from harmonization processes;

– no unified procedure exists for recognizing on-chain data as admissible evidence.

The United States relies primarily on an **enforcement-driven model**, led by the SEC, CFTC, FinCEN, and the Department of Justice. This model is more aggressive but:

– fragmented across agencies;

– prone to inconsistencies in defining the legal nature of crypto-assets;

– does not provide unified identification standards for international cases.

International organizations (FATF, INTERPOL, the Egmont Group) provide overarching guidance, but:

– their recommendations are non-binding;

– implementation varies widely across countries;

– no international evidentiary standard exists for crypto-cases comparable to, for example, financial reporting norms.

As a result, even where regulatory frameworks exist, investigations into crypto-crime continue to struggle with:

• incompatibility of data received from different jurisdictions;

• inconsistent procedures for verifying transactions;

• lack of a coordinated interpretation of on-chain artefacts.

Thus, regulatory systems are moving toward greater centralization but do not resolve the fundamental problem: the absence of a unified evidentiary standard—an element critically important for effective prosecution of transnational schemes.

13. The Political-Economic Dimension of Blockchain Use

In a number of cases, blockchain is used not only as a tool for criminal enrichment but also as a mechanism for asset redistribution and pressure within corporate, property, and economic conflicts. Decentralized infrastructure allows actors to:

– rapidly move assets outside the banking system;

– create ownership structures that are difficult to trace;

– block access to funds for specific participants in a corporate dispute;

– use criminal prosecution as part of a strategic struggle for assets.

In such a configuration, the criminal-law form masks the underlying economic nature of the conflict, and blockchain functions as:

• an instrument of coercive pressure,

• a tool for manipulating corporate governance,

• a component of competitive confrontation,

• an infrastructure for covert redistribution of property.

This creates additional challenges for investigations because:

– legal qualification often fails to reflect the real economic motive;

– digital assets may be used as leverage for corporate blackmail;

– international requests for mutual legal assistance rarely account for the political-economic context.

Thus, blockchain becomes not only a technological architecture but also a factor shaping the dynamics of economic conflicts and the strategic behavior of market participants.

14. Risks for Users and Investors

The myth of "blockchain transparency" fosters a false sense of security and reinforces the belief that public availability of data automatically ensures protection against fraud. In practice, users face a set of risks that far exceed their expectations.

Key threats include:

• **complete loss of funds**, as transactions are irreversible and fraudulent schemes exploit decentralization to evade liability;

• **lack of legal protection**, since digital assets in many jurisdictions fall outside existing insurance, recovery, and banking safeguards;

• **irreversible loss of control over assets** in cases of key loss, hacking, or disclosure of credentials to third parties;

• **high probability of becoming involved in grey-market schemes** disguised as legitimate investment opportunities;

• **jurisdictional uncertainty**, making it unclear in which country a complaint should be filed, which authority is competent, and which legal norms apply.

User vulnerability in the crypto-environment is therefore not an anomaly but a structural feature of a market in which technical pseudo-transparency does not compensate for institutional unreliability.

15. Conclusions

The analysis demonstrates that blockchain is not a universal instrument of transparency and oversight, contrary to popular public narratives. Its architectural features—pseudonymity, decentralization, absence of a single accountable entity, and the capacity for horizontal expansion of transaction chains—make it equally suitable for concealing economic relationships as for recording them.

In grey, high-speed, and transnational financial schemes, blockchain functions as a **self-sufficient mechanism of obfuscation**, particularly in the absence of:

– institutional coordination between states,

– unified approaches to interpreting on-chain data,

– international evidentiary standards for crypto-related cases,

– effective regulation of the OTC segment and stablecoins.

The technical transparency of the ledger is neutralized by the institutional opacity of the economy: the ability to *see* transactions does not equate to the ability to *understand* their economic meaning. Taken together, this turns blockchain into an infrastructure that can reproduce and intensify the structural vulnerabilities of the global financial system.

Thus, blockchain is not only a technological phenomenon but also a critical challenge for contemporary law enforcement—one that requires interdisciplinary, intergovernmental, and interagency approaches.

16. Recommendations

Based on the analysis presented, several key directions for institutional and regulatory modernization are proposed in order to enhance the effectiveness of crypto-related investigations and reduce systemic risks.

1. Integrating blockchain analytics with traditional financial investigations.

On-chain data should be treated as one of several information sources that must be verified through banking records, corporate registries, telecommunications data, and other off-chain artefacts. Establishing hybrid investigative teams would improve analytical accuracy and reduce the likelihood of errors.

2. Strengthening regulation of the OTC segment and stablecoins.

The following measures are necessary:

– mandatory registration of OTC brokers;

– implementation of KYC/AML standards for P2P platforms;

– transparency requirements for stablecoin issuers;

– monitoring of large and recurring transactions.

Enhanced oversight of these segments would eliminate the key blind spots in current regulatory frameworks.

3. Developing international evidentiary standards for crypto-related cases.

A unified approach is required with respect to:

– admissibility of on-chain analytics as evidence;

– methodology for asset tracing;

– procedures for user identification;

– standards for cross-border data exchange.

Such harmonization would strengthen the legal robustness of investigations and reduce fragmentation across jurisdictions.

4. Incorporating the political-economic context into the assessment of criminal cases.

In transnational investigations, it is essential to recognize that digital assets increasingly serve as instruments of:

– corporate disputes;

– redistribution of ownership;

– geoeconomic leverage;

– strategic jurisdictional competition.

Ignoring these factors leads to misclassification, investigative blind spots, and strategic errors in international cooperation.

Sources

1. https://www.fatf-gafi.org/en/topics/virtual-assets.html
2. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
3. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/
4. https://www.trmlabs.com/resources/blog/2026-crypto-crime-report-key-insights-trm-identifies-record-usd-158-billion-in-illicit-crypto-flows-in-2025-reversing-a-multi-year-decline

5. https://www.europol.europa.eu/crime-areas/economic-crime
6. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances
7. https://www.unodc.org/cld/fr/education/tertiary/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html
8. https://www.imf.org/en/publications/fandd/issues/2022/09/regulating-crypto-narain-moretti
9. https://www.bis.org/publ/qtrpdf/r_qt2103.htm
10. https://www.interpol.int/What-you-can-do/Crimes/Financial-crime
11. https://www.interpol.int/How-we-work/Notices
12. https://www.interpol.int/News-and-Events/News
13. https://argaobservatory.org