Observatoire ARGA

ARGA Atlas

MiCA, MARKET ABUSE AND DISCLOSURE RISKS: WHY CRYPTO-ASSET REGULATION HAS BECOME A MATTER OF LEGAL PROTECTION

Authors:

Sergei Khrabrykh — President of ARGA, PhD

Tsmakalova Nataliia

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, 6 may 2026

Purpose of the Document

This report has been prepared to provide a comprehensive analysis of how crypto-asset regulation, disclosure requirements and market abuse rules are evolving from purely financial supervisory tools into an independent area of legal protection. Particular attention is given to Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) and to the legal risks that arise for issuers, service providers, investors, token holders and persons involved in cross-border disputes.

The practical purpose of this document is to identify situations in which disclosure obligations, admission-to-trading requirements, supervisory oversight, market conduct assessments, anti-market abuse rules and the use of digital evidence may generate significant legal consequences. Such consequences may include refusal of listing, trading restrictions, suspension of operations, regulatory investigations, civil liability, criminal exposure and reputational harm.

For ARGA, this topic is of strategic importance because crypto-assets increasingly form part of international ownership structures, investment projects, corporate conflicts, sanctions reviews, criminal proceedings and financial monitoring procedures. An incorrect or overly formal interpretation of digital evidence, technical reports, blockchain data, disclosures or market conduct may lead to unjustified restrictions, financial losses and interference with the right to effective legal protection.

This report examines crypto-asset regulation as part of a broader framework of investor protection, property rights, entrepreneurial freedom and cross-border legal safeguards. Its purpose is to develop a practical analytical model suitable for lawyers, regulators, courts, compliance departments, issuers, service providers and international human rights mechanisms.

CONTENTS

Executive Summary

Crypto-asset regulation is evolving from a fragmented supervisory environment into a structured legal framework. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) establishes a unified European regime for crypto-asset issuers, issuers of asset-referenced tokens, issuers of electronic money tokens and crypto-asset service providers. It introduces requirements concerning authorization, disclosure, governance, safeguarding of client assets, complaint handling and prevention of market abuse.

The expansion of regulation creates not only protective mechanisms, but also new legal risks. As the market becomes more formalized, increasing importance is attached to white papers, technical descriptions, reserve disclosures, business models, governance structures, marketing communications, transaction records and blockchain analytics. Errors, omissions, inconsistencies or one-sided interpretations of such information may trigger regulatory intervention, restrictions on market access or claims by investors.

A particularly significant component of MiCA is the framework governing market abuse. Market manipulation, dissemination of misleading information and misuse of inside information are treated as conduct capable of undermining market integrity and investor confidence. The assessment of such conduct may rely heavily on digital evidence, transaction analysis and technical reporting.

The central conclusion of this report is that crypto-asset regulation should not be viewed solely as a technical or financial discipline. It is directly connected with property rights, procedural fairness, the reliability of evidence, the limits of regulatory discretion and the risk of formal acceptance of digital data without adequate verification. In an environment where technical information may lead to substantial legal consequences, the quality of disclosure, analysis and judicial review becomes a matter of fundamental legal significance.

Context & Problem Statement / Why This Topic Has Legal and International Significance

Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) is the first comprehensive supranational legal instrument establishing a unified regulatory framework for crypto-assets within the European Union. Its significance extends well beyond technical oversight of a developing market. In practice, MiCA creates a new institutional environment in which admission to trading, disclosure obligations, marketing communications, reserve management, governance arrangements and market abuse controls acquire direct legal importance.

Before the adoption of MiCA, the crypto-asset sector developed under fragmented and inconsistent regulatory approaches. Requirements applicable to issuers, service providers and trading platforms varied considerably from one jurisdiction to another. Some participants operated within relatively detailed supervisory regimes, while others relied primarily on general principles of contract, corporate and financial law. This fragmentation generated significant legal uncertainty and complicated both investor protection and the assessment of responsibility.

The introduction of MiCA establishes a more structured legal system in which crypto-asset white papers, mandatory disclosures, authorization procedures, governance standards, safeguarding obligations, complaint-handling mechanisms and internal controls play a central role. Legal significance is attributed not only to financial indicators, but also to technical descriptions, marketing statements, blockchain data and algorithmic characteristics of particular projects.

Particular importance attaches to the regulation of market abuse. Price manipulation, dissemination of misleading information, misuse of inside information and artificial creation of market activity are treated as conduct capable of undermining market integrity and harming investors. Assessments in this area may rely on extensive analysis of digital records, trading patterns and blockchain transactions.

The significance of this subject extends beyond financial supervision. Decisions by regulators, trading platforms and other market participants may affect property rights, access to capital, corporate structures, business reputation and the ability to continue commercial operations. Incorrect classification of market conduct, incomplete interpretation of technical information or formal reliance on digital evidence may lead to substantial legal consequences.

For ARGA, this topic is strategically important because crypto-asset regulation increasingly intersects with cross-border disputes, sanctions restrictions, financial monitoring procedures, corporate conflicts and asset-protection matters. In such circumstances, effective legal defense requires a detailed understanding of both technological issues and the complex network of regulatory, procedural and human rights safeguards.

Legal Framework / Normative and Institutional Framework

The legal framework governing crypto-assets and the activities of market participants is a multi-layered system comprising European Union regulations, national legislation of Member States, international financial standards, investor protection rules and internal procedures of private entities.

The first level is Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). This regulation establishes uniform requirements for crypto-asset issuers, issuers of asset-referenced tokens, issuers of electronic money tokens and crypto-asset service providers. It governs the issuance and public offering of tokens, disclosure obligations, governance arrangements, reserve requirements, safeguarding of client assets, complaint-handling procedures and the powers of national and European supervisory authorities.

The second level consists of related European Union legislation, including Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets, anti-money laundering legislation, sanctions regulations, data protection rules and measures concerning digital operational resilience in the financial sector.

The third level includes national laws of European Union Member States governing administrative, civil and criminal liability, licensing procedures, judicial review and enforcement of decisions issued by competent authorities.

The fourth level is composed of technical standards, guidelines and supervisory materials issued by the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA). These institutions develop technical standards and interpretative documents that shape the practical application of MiCA.

The fifth level consists of international standards, particularly the recommendations and guidance of the Financial Action Task Force (FATF), which regulate customer due diligence, risk assessment, transfer transparency and the application of a risk-based approach to virtual assets.

The sixth level includes rules aimed at preventing market abuse. These rules address insider dealing, market manipulation, dissemination of false or misleading information and other conduct capable of influencing prices and investment decisions.

The seventh level consists of contractual documents and internal procedures of private actors, including cryptocurrency exchanges, custodial providers, trading platforms, token issuers and analytics companies. These materials govern listing, delisting, disclosure, compliance reviews and user interaction.

The eighth level relates to judicial and administrative practice. National courts, regulators, arbitral institutions and international human rights bodies continue to develop approaches to the assessment of disclosure quality, evidentiary sufficiency, proportionality of restrictions and procedural fairness.

Accordingly, crypto-asset regulation forms an integrated legal system in which technical characteristics, corporate procedures, supervisory requirements and human rights standards interact directly. Any significant activity in the crypto-asset market has simultaneous technological, financial and legal dimensions.

Mechanisms of Practice / Abuse / Key Mechanisms of Practice, Abuse or Conflict

The first key mechanism concerns disclosure in connection with the issuance, public offering or admission to trading of a crypto-asset. Under MiCA, the crypto-asset white paper is not merely a descriptive document, but a legally significant source of information for investors, trading platforms, regulators and other market participants. If the white paper contains incomplete, inaccurate, misleading or overly generalized information, it may give rise to supervisory action, civil claims and restrictions on access to the market.

The second mechanism involves the legal significance of marketing communications. Promotional materials, public statements, presentations, website content, social media posts and investor communications may be evaluated not only as commercial messaging, but as information capable of shaping market expectations. Any inconsistency between marketing statements and the actual structure of the project may be treated as misleading disclosure.

The third mechanism relates to the assessment of technical data. In crypto-asset matters, considerable importance is attached to smart contracts, blockchain records, token ownership structures, asset flows, trading patterns, liquidity data, transaction volumes and the behavior of related wallets. These data may be used to identify market manipulation, insider dealing, artificial price formation or concealed control structures. At the same time, technical data require qualified interpretation and should not be accepted as self-evident proof without methodological review.

The fourth mechanism is the classification of conduct as market abuse. In the crypto-asset sector, manipulation may involve artificial inflation of trading volumes, coordinated transactions between related wallets, dissemination of inaccurate information, creation of false impressions of demand, use of inside information or coordinated conduct by multiple participants.

The fifth mechanism concerns decisions by trading platforms. A platform may refuse listing, suspend trading, restrict operations, delist a token, request additional documentation or notify regulators of suspicious conduct. Such decisions may be based on internal rules, MiCA requirements, risk assessments, user complaints or analytics reports. For issuers and token holders, these decisions may have significant financial and reputational consequences.

The sixth mechanism involves the exercise of regulatory powers. Competent authorities may request documents, require additional disclosures, conduct inspections, impose restrictions, apply administrative measures and refer matters to other authorities where indications of misconduct are identified. In digital markets, such actions may develop rapidly and affect a broad range of stakeholders.

The seventh mechanism concerns the use of digital evidence in judicial and administrative proceedings. Analytics reports, expert opinions, blockchain data, platform logs and technical analyses may become the basis for decisions affecting substantial rights. It is therefore essential to verify the origin of the data, the methodology applied, the completeness of the dataset, the existence of alternative explanations and the qualifications of the experts involved.

The eighth mechanism is the cross-border propagation of consequences. A regulatory decision in one jurisdiction, a delisting, a public warning or a compliance assessment may influence how a project or individual is treated in multiple jurisdictions simultaneously. Because the crypto-asset market is inherently transnational, legal consequences often spread more rapidly than available remedies.

The ninth mechanism concerns the interaction between private and public control. Issuers, platforms, analytics providers and custodial institutions act under contractual and internal rules, yet the

consequences of their decisions may closely resemble public-law restrictions. Procedural protections therefore depend not only on legislation, but also on the internal governance of private market actors.

The tenth mechanism is the persistence of adverse profiles. Even where suspicions are disproved, records of investigations, trading suspensions, disclosure concerns and risk classifications may remain in platform systems, regulatory files and public reports. These records may continue to affect market access, investor confidence and business reputation long after the underlying issue has been resolved.

Case Patterns / Typical Scenarios, Patterns of Development or Models of Application

The first typical scenario concerns the issuance of a crypto-asset where the white paper is prepared formally, incompletely or without sufficient disclosure of material risks. At the initial stage, the project may appear technologically promising and commercially attractive. However, investors, platforms or regulators may later determine that the documentation failed to disclose essential information concerning governance structure, rights of token holders, reserve mechanisms, dependence on related parties, liquidity, technical limitations or risks of project termination. In such cases, the issue moves from marketing practice into the sphere of legal responsibility.

The second scenario arises where there is a discrepancy between public statements made by the project and its actual structure. An issuer or affiliated team may describe the project as decentralized, broadly supported by the market, liquid or operationally independent, while technical or corporate evidence reveals concentration of control, dependence on a limited number of persons, artificial support of demand or insufficient reserves. Such discrepancies may become material when assessing the good faith and accuracy of disclosure.

The third scenario concerns suspected market manipulation. Sharp increases in trading volumes, repeated transactions between related wallets, coordinated activity across multiple accounts, unusual price movements before public announcements or use of non-public information may trigger an internal platform review or regulatory investigation. However, unusual trading data alone should not automatically be treated as proof of misconduct. Economic context, technical structure, participant relationships and alternative explanations must be analyzed.

The fourth scenario involves the use of blockchain data as evidence. In administrative or judicial proceedings, an analytics report may identify movement of assets between specific addresses, links to high-risk wallets, concentration of holdings or suspicious trading patterns. Such conclusions depend on methodology, data completeness, accuracy of wallet attribution and expert interpretation. If a court or regulator accepts such material formally, without reviewing its assumptions, there is a risk of erroneous findings.

The fifth scenario relates to refusal of listing or delisting by a trading platform. For a project, such a decision may be critical because access to a major platform directly affects liquidity, investor confidence and market value. Grounds may include disclosure deficiencies, market manipulation concerns, sanctions risks, failure to meet internal standards or regulatory inquiries. Even where the decision is formally private and commercial, its consequences may resemble a public restriction on market access.

The sixth scenario arises where investors are attracted on the basis of incomplete or excessively optimistic information. A project may emphasize potential returns, technological uniqueness, expected listing or future ecosystem growth while failing to disclose material limitations, risks and dependencies. Investors may later bring claims alleging that they were misled. In such situations, not only formal documents but the entire body of market communications becomes legally relevant.

The seventh scenario concerns cross-border investigations. A competent authority in one jurisdiction may initiate a review of disclosure, token trading or service-provider conduct, after which information is transmitted to regulators, platforms, banks and compliance departments in other jurisdictions. As a result, a person or project may face restrictions in multiple countries before the originating investigation has been completed.

The eighth scenario concerns the criminal reclassification of conduct in crypto-asset markets. Issues that initially relate to disclosure, market conduct or investor protection may later be treated as fraud, money laundering, abuse of office, market manipulation or another criminal offence. This significantly increases legal exposure and may give rise to asset freezes, international cooperation, alerts, extradition risks and banking restrictions.

The ninth scenario involves erroneous or incomplete expert analysis. A court, regulator or platform may rely on a technical report that fails to account for protocol design, trading infrastructure, the role of market makers, automated strategies, cross-chain bridges or internal exchange procedures. Without adequate review, such a report may produce a distorted account of events.

The tenth scenario occurs where a project or individual formally remedies the issue, updates disclosure, provides documents or modifies governance arrangements, yet the adverse regulatory or market profile persists. Previous concerns may continue to affect relationships with platforms, investors, banks and counterparties. Restoration of legal and market standing therefore requires separate and sustained remediation efforts.

Risk Assessment / Main Risks, Legal Vulnerabilities and Problem Areas

The first risk lies in the formal treatment of digital data as objective and self-sufficient evidence. Blockchain data, analytics reports, algorithmic conclusions, trading statistics and technical logs may create an impression of high precision. However, all such materials depend on the underlying data, the methodology selected, the accuracy of wallet attribution, the completeness of the dataset and the professional competence of the expert. Without verification of these factors, there is a risk of erroneous qualification of events and unjustified restrictions.

The second risk concerns incomplete or inaccurate disclosure. A crypto-asset white paper, marketing materials, reserve disclosures, governance information and technical descriptions form the basis on which the reliability of a project is assessed. If material facts are omitted, described ambiguously or presented in a manner capable of misleading market participants, this may give rise to claims by regulators, investors, platforms and counterparties.

The third risk is the expansive interpretation of market abuse rules. Unusual trading patterns, high concentration of token holdings, coordinated activity by market makers or sharp price movements may be interpreted as indicators of market manipulation. Without sufficient analysis of economic context and technical features, permissible market behavior may be incorrectly classified as unlawful conduct.

The fourth risk relates to the concentration of discretionary powers in platforms and other private market participants. Exchanges, custodial services, token issuers and analytics companies make decisions that may determine access to liquidity, listing opportunities, continuation of services and market reputation. Procedural safeguards and standards of review often depend on the internal rules of the relevant organization.

The fifth risk is the cross-border spread of consequences. A single regulatory investigation, public warning, delisting decision or adverse analytics report may trigger restrictions in several jurisdictions at once. This increases the likelihood of multiple reviews, banking refusals and reputational harm.

The sixth risk concerns the transformation of administrative or regulatory concerns into criminal-law consequences. Issues initially related to disclosure or market conduct may become the basis for allegations of fraud, abuse of office, market manipulation or money laundering.

The seventh risk is the loss of access to capital and liquidity. Trading restrictions, delisting, blocked operations or termination of services may sharply reduce the value of an asset and impair the ability to meet obligations toward investors, creditors, partners and clients.

The eighth risk concerns information asymmetry. A person or project often lacks full visibility into the data used, the criteria applied and the reasoning by which a conclusion of misconduct or risk was reached. This significantly complicates the preparation of an effective defense.

The ninth risk is the persistence of an adverse profile after remediation. Even where documentation is updated, evidence is provided and regulatory concerns are addressed, earlier allegations may continue to influence relationships with platforms, banks, investors and counterparties.

The tenth risk is legal uncertainty. Although MiCA and related instruments create a more structured framework, judicial and administrative practice continues to develop. Approaches to digital evidence, disclosure quality, market conduct and proportionality of restrictions may vary, increasing the importance of qualified legal analysis and strategic preparation.

Institutional Gaps / Institutional Limitations, Gaps, Deficits of Safeguards and Systemic Weaknesses

The first institutional limitation is that the regulatory framework is developing more rapidly than the judicial and administrative practice capable of ensuring consistent and predictable application. MiCA establishes a detailed supervisory regime, but many issues concerning the evaluation of digital evidence, classification of market conduct, limits of disclosure obligations and standards of proportionality will be clarified only over time. During this transitional period, significant legal uncertainty remains.

The second limitation concerns the technical complexity of the subject matter. Judges, regulators, lawyers, investors and compliance departments are required to assess smart contracts, algorithmic models, reserve structures, token distributions, trading patterns and blockchain records. Where technical expertise is insufficient, there is a heightened risk of oversimplification or uncritical reliance on expert reports.

The third limitation is the information asymmetry between market participants and supervisory actors. Platforms, analytics providers and regulators may possess substantially more data than issuers, investors or persons subject to review. In the absence of effective disclosure and verification mechanisms, this imbalance impairs the right to prepare and present an effective defense.

The fourth limitation is the concentration of effective power in a limited number of private entities. Major trading platforms, analytics providers and custodial institutions are capable of making decisions that determine access to liquidity, capital and market participation. Their internal procedures do not always provide a level of procedural protection comparable to public-law processes.

The fifth limitation lies in the absence of uniform standards for evaluating technical evidence. Methodologies used by analytics firms, wallet attribution techniques, market abuse detection models and disclosure assessment criteria may differ significantly. This increases the likelihood of inconsistent conclusions and complicates the comparison of results across institutions.

The sixth limitation is the cross-border structure of the crypto-asset market. Issuers, investors, trading platforms, reserve custodians and regulators may all be located in different jurisdictions. This fragmentation complicates the determination of governing law, competent authorities, procedural deadlines and enforcement mechanisms.

The seventh limitation is the limited capacity of the system to restore status after issues have been remedied. Even after disclosures are updated, regulatory requirements are satisfied or investigations are closed, adverse profiles may continue to appear in analytics systems, platform databases and public materials.

The eighth limitation concerns the insufficient integration of human rights and property-rights safeguards into private procedures. Decisions involving delisting, trading restrictions, refusal of service and asset blocking are frequently made under contractual and internal rules, yet they may directly affect ownership interests, business reputation and the ability to continue lawful activity.

The ninth limitation is the high degree of dependence on external information providers. Regulators, platforms and investors may rely extensively on analytics firms, auditors, rating agencies and technical consultants. If the underlying assessments contain material errors, the consequences may propagate throughout the market.

The tenth limitation is the predominance of precautionary decision-making. In situations of uncertainty, regulators and platforms often prefer to suspend trading, restrict market access or initiate investigations before all facts are fully established. While this approach may reduce supervisory exposure for the decision-maker, it transfers a substantial portion of the adverse consequences to issuers, investors and other good-faith market participants.

Practical Guidance / Practical Recommendations and Model of Legal Action

The first practical step is to treat MiCA requirements and related regulation not as a formal documentation exercise, but as a central component of legal protection for the project, issuer, service provider and investors. The crypto-asset white paper, marketing materials, technical architecture description, risk disclosures and governance information should be prepared in a manner that makes them usable not only for market access, but also for defense in the event of claims, investigations or disputes.

The second step is prior legal review of all information disclosed to the market. Public statements, technical documentation, internal materials, reserve information, corporate structure, rights of token holders, project limitations and actual operational practice should be checked for consistency. Any discrepancy between these levels may later be treated as an indicator of misleading disclosure.

The third step is documentation of technical decisions and governance procedures. A project should maintain clear and verifiable internal materials explaining the operation of smart contracts, allocation of powers, protocol modification procedures, reserve management, the role of related parties, internal controls and responses to technical or market incidents. Such documentation is important not only for regulators, but also for defense against future claims by investors and counterparties.

The fourth step is independent verification of digital data and technical reports. Where blockchain data, analytics reports, trading statistics or technical expert opinions are used, it is necessary to examine methodology, completeness of underlying data, accuracy of wallet attribution, alternative explanations and expert qualifications. The digital nature of evidence does not make it automatically complete, reliable or legally sufficient.

However, in practice, a general requirement to "verify methodology and underlying data" is insufficient on its own. In disputes involving MiCA, market abuse, and disclosure obligations, parties and adjudicating authorities require a reproducible framework capable of distinguishing verifiable facts from interpretation and of properly assessing the evidentiary weight of technical materials. The following section sets out a practical model for the judicial assessment of digital evidence and technical reports, designed for an international audience.

Judicial Assessment of Digital Evidence and Technical Reports in Crypto Disputes (MiCA / Market Abuse / Disclosure): Avoiding "Automatic Deference" to Unilateral Data

The strengthening of crypto-market regulation (including regimes concerning disclosure obligations, transaction monitoring, and detection of market abuse) has made "digital traces" a central object of proof: on-chain transactions, exchange and custodian data, exports via interfaces and APIs, login and confirmation logs, blockchain analytics outputs, and technical expert reports. The principal procedural risk is the substitution of interpretation for evidence: a technical report begins to be treated as an established fact, even though it is often the product of system settings, trigger thresholds, heuristics, and incomplete underlying datasets.

As a practical matter, it is useful for courts (or adjudicating authorities) to assess such materials through three distinct inquiries: (a) admissibility, (b) evidentiary weight, and (c) sufficiency in the aggregate. A technical report may be admissible while carrying limited evidentiary weight; and it will almost never, standing alone, satisfy the applicable standard of proof without support from verifiable source materials and independent verification.

Set out below is a seven-step framework intended to avoid the formalistic acceptance of unilateral digital evidence.

1. Distinguish Between "Primary Data" and "Analytical Conclusions" — and Require Justification for Each Layer

It is advisable for the court to identify separately:

Primary Layer: transaction identifiers, timestamps, wallet addresses, input/output records, system logs, and raw exports (data rather than screenshots).

Interpretative Layer: address clustering, attribution, risk scoring, graph reconstructions, conclusions concerning "association" or "control."

Legal Layer: legal characterization (for example, "market manipulation," "insider trading," or "misleading disclosure").

Key Reasoning Principle: an analyst's report constitutes an opinion derived from data, rather than the data itself. It is therefore important for the court to explain which facts it accepts and, separately, why it accepts (or rejects) the interpretation.

2. Verify Origin, Integrity, and Reproducibility (an Analogue to "Chain of Custody")

Minimum questions include:

· who collected or exported the information, when, and from which source (provider, exchange, custodian, node, blockchain explorer, device);
· how immutability and integrity were ensured: access controls, file versions, audit trails, checksums

or hashes (where applicable);
· what intermediate processing steps occurred before preparation of the report (merging of tables, filtering, "cleaning," row deletions, aggregation);
· whether an independent specialist could reproduce a comparable result using the same inputs and documented methodology (at least with respect to key elements).

Where reproducibility cannot be achieved, this will not always require exclusion of the material, but it will generally reduce evidentiary weight and increase the need for supporting evidence.

3. Assess Methodological Reliability Through "Judicial Verifiability" Criteria (Daubert-Like Logic Without Jurisdictional Dependence)

Even in legal systems without a formal Daubert test, courts typically examine similar questions:

· whether the methodology is described in a manner capable of verification (without necessarily disclosing trade secrets, but with an explanation of logic, inputs, parameters, and limitations);
· whether typical errors or false positives are known and how they were addressed;
· whether quality control procedures exist (validation, internal audit, comparison against control datasets);
· whether the conclusion constitutes a "black box" assertion of the form: "the tool showed this, therefore it happened."

This is especially critical in disputes involving market abuse and disclosure obligations: correlations (timing of disclosures, transactions, token movements) may too easily be transformed into purported proof of insider trading or manipulation, despite alternative explanations such as market-making, hedging, arbitrage, execution of client instructions, bot activity, or platform routing architecture.

4. Recognize the "Regulatory Illusion of Reliability": Compliance Alerts Are Not Equivalent to Proof of Misconduct

In environments of heightened regulation (including transaction monitoring and internal control obligations), many evidentiary materials originate as outputs of filters and thresholds: a "flag," "alert," "suspicious activity," or "anomaly." Courts should expressly acknowledge that:

an alert merely confirms that an event crossed a configured system threshold; it does not, by default, prove intent, insider dealing, manipulation, or misleading disclosure. Independent verification of the underlying data and assessment of alternative explanations are therefore required, rather than reliance on "the mere fact that monitoring was triggered."

5. Do Not Equate an Address or Account with a Person: an "Identification Bridge" Is Required

Even where transactions are authentic, a separate question remains: who controlled the relevant key or account at the material time. Conclusions concerning control generally require additional linking evidence, including:

· exchange or custodian data (KYC information, login history, devices, transaction confirmations);
· logs and security events (password changes, account recovery, two-factor authentication, suspicious logins);
· business correspondence, contractual arrangements, and economic context;
· exclusion of scenarios involving delegated access, credential compromise, or shared corporate accounts.

Where the "identification bridge" is weak, it is generally safer for a court to characterize any conclusion regarding control as probabilistic and to avoid relying upon it as the sole basis for decisive legal findings.

6. Ensure Verifiability Within the Proceedings: Disclosure of Materials, Symmetry of Expert Examination, and Examination of the Report Author

To avoid entrenching a unilateral evidentiary narrative, it is advisable for the court to verify that the opposing party had a genuine opportunity to challenge the material through:

· access to the minimum necessary underlying data (transaction identifiers, wallet addresses, timestamps, references to sources, rather than visualizations alone);
· the opportunity to submit an independent expert opinion;
· the opportunity to question the author of the report regarding input data, filters, assumptions, potential errors, and limits of applicability.

Where full disclosure is restricted (for reasons of investigative secrecy, security, or commercial confidentiality), courts may beneficially apply a balancing approach: compensatory safeguards may include redaction of sensitive portions, expert access subject to confidentiality undertakings, closed hearings, or "clean room" arrangements for inspection. However, restrictions should be reasoned, and compensatory mechanisms should be sufficient to preserve meaningful adversarial scrutiny.

7. Require Engagement with Material Alternative Explanations, Rather Than "Every Conceivable Hypothesis"

A court is not required to address every speculative hypothesis; however, it should ordinarily engage with material and evidentially supported alternative scenarios (for example, market-making, portfolio rebalancing, hedging, infrastructure routing, aggregated wallets, or custodial service arrangements). Judicial reasoning should demonstrate not only why the investigative theory is supported, but also why reasonable alternatives are excluded — or, conversely, why the evidence does not permit their exclusion to the required degree of certainty.

Concluding Formula

To avoid the formal acceptance of unverified or unilateral digital materials, courts may beneficially apply a structured review of: (1) the origin and integrity of data; (2) the reliability and verifiability of methodology; (3) the linkage between a "digital trace" and a specific individual; and (4) procedural adversarial safeguards (access to source materials, counter-expertise, and examination of material alternatives), while separately distinguishing admissibility, evidentiary weight, and sufficiency in the aggregate.

This framework matters not only for courts and regulators, but also for market participants themselves: these are precisely the criteria by which the good faith of internal controls, the quality of monitoring systems, and the resilience of a party's position in subsequent disputes are assessed. We now turn to the next practical component — the development of an internal system for preventing market abuse.

The fifth step consists in establishing an internal market abuse prevention system. Issuers and service providers should maintain procedures for identifying suspicious trading patterns, related-party transactions, unusual liquidity movements, the use of undisclosed information, and dissemination of misleading information. The existence of such a system reduces regulatory risk and demonstrates the market participant's good faith.

The fifth step is the establishment of an internal system for preventing market abuse. Issuers and service providers should maintain procedures for identifying suspicious trading patterns, transactions by related parties, unusual liquidity changes, misuse of non-public information and dissemination of inaccurate statements. Such systems reduce regulatory risk and demonstrate the good faith of the market participant.

The sixth step concerns control of marketing communications. Public statements, advertising materials, presentations, website content, social media communications and investor communications should correspond to the actual structure of the project and disclose material risks. Marketing materials should not create expectations that are unsupported by legal, financial or technical reality.

The seventh step is preparation of a strategy for interaction with trading platforms. Where a project depends on listing, trading or service provision by a particular platform, it is necessary to understand in advance the platform's requirements, review procedures, grounds for suspension, delisting rules, objection procedures and mechanisms for restoration of access. This is particularly important for projects whose value materially depends on market liquidity.

The eighth step is analysis of cross-border consequences. The issuer, project team, investors, platforms, reserves and users may be located in different jurisdictions. The legal position should therefore take into account not only MiCA, but also national legislation, sanctions restrictions, tax implications, financial monitoring rules and potential requirements of foreign regulators.

The ninth step is procedural readiness for investigations and disputes. A project should maintain a prepared package of documents, including corporate records, technical materials, risk reports, disclosure policies, internal control procedures, evidence of good-faith conduct and materials confirming regulatory compliance. In the event of claims or inquiries, the speed and quality of the response may be decisive.

The tenth step is restoration of legal and market standing after concerns arise. If a token has been delisted, access to operations restricted, a regulatory investigation initiated or an adverse report published, it is not sufficient merely to correct the initial issue. It is also necessary to seek updating of information, revision of internal risk profiles, restoration of market access and documentary confirmation of changed status.

Policy Recommendations / Recommendations on Legal and Institutional Approach

First, crypto-asset regulation should continue to develop on the basis that disclosure is not merely a supervisory obligation, but a core mechanism for protecting market participants. Crypto-asset white papers, technical descriptions, reserve disclosures, governance information and marketing communications should be clear, verifiable and sufficiently comprehensive to allow investors, trading platforms and regulators to assess the actual characteristics and risks of a project.

Second, competent authorities should devote particular attention to the quality of digital evidence. Blockchain data, analytics reports, trading statistics and technical opinions should not be accepted formally solely because they are generated in digital form. Their methodology, completeness, accuracy of wallet attribution, possible alternative explanations and the qualifications of the relevant experts should be subject to meaningful review.

Third, consistent approaches should be developed for assessing market abuse in crypto-asset markets. Market manipulation, misuse of inside information and dissemination of misleading information should be analyzed with due regard to the characteristics of digital infrastructure, automated trading, the role of market makers, cross-chain transactions and the specific liquidity dynamics of crypto-asset platforms.

Fourth, MiCA and related regulation should be applied in a manner that avoids excessive formalism. Disclosure deficiencies or unusual trading data do not automatically demonstrate bad faith. In each case, it is necessary to evaluate the surrounding context, the nature and materiality of the issue, actual investor impact and the corrective measures taken by the relevant participant.

Fifth, private platforms and service providers should maintain more transparent decision-making procedures. Refusal of listing, suspension of trading, delisting, blocking of operations and termination of services should be accompanied by sufficient explanations and a meaningful opportunity to present objections where substantial proprietary or business interests are affected.

Sixth, stronger integration should be developed between crypto-asset regulation and property-rights protections. Restrictions affecting tokens, liquidity, trading infrastructure or investment opportunities may produce consequences comparable to traditional interferences with property. Such measures should therefore be assessed in terms of legality, necessity, proportionality and procedural fairness.

Seventh, regulators and courts should take account of the cross-border propagation of consequences. A decision adopted in one jurisdiction may affect trading, banking access, reputation and legal status in many others. Restrictive measures should therefore be evaluated not only in light of their immediate supervisory purpose, but also with regard to their broader international impact.

Eighth, mechanisms should be strengthened for restoring status after issues are remedied or allegations are disproved. Updated disclosures, technical corrections, removal of restrictions and closure of investigations should be accompanied by practical procedures for updating records, platform profiles and analytical databases.

Ninth, market participants should implement internal legal and technical review procedures before disputes arise. Good-faith documentation, independent technical audits, control of marketing communications, reserve verification and transparent governance structures should be regarded as essential components of legal protection rather than optional administrative measures.

Tenth, crypto-asset regulation should maintain a balanced approach that protects investors, prevents abuse and preserves market access for good-faith participants. Excessively rigid or opaque regulatory practices may reduce certain risks while simultaneously creating new forms of legal uncertainty in which technical or regulatory conclusions become the basis for disproportionate restrictions.

Conclusion

Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) and related regulatory instruments establish a new legal framework for the crypto-asset market. Crypto-assets can no longer be viewed as a sector operating largely outside traditional financial and legal control. Their issuance, offering, trading, custody, promotion and use are now subject to detailed regulation, supervisory oversight and legal responsibility.

The principal significance of MiCA lies not only in creating a unified regulatory regime for participants in the European Union, but also in establishing a new standard for the legal assessment of digital assets. Crypto-asset white papers, disclosure obligations, governance arrangements, client protection measures, operational resilience and market abuse controls have become central elements of legal analysis.

At the same time, expanded regulation does not eliminate the risk of error, formalism or disproportionate restrictions. On the contrary, as digital data, technical reports and platform decisions become increasingly influential, the need for critical and methodologically sound review becomes correspondingly greater. Courts, regulators and private actors should not treat blockchain records,

analytics conclusions or trading statistics as automatically conclusive merely because they are generated in digital form.

For ARGA, the principal conclusion is that crypto-asset regulation has become an independent field of legal protection. It directly affects property rights, access to capital, business reputation, corporate interests, entrepreneurial freedom and the ability to obtain effective judicial review. Legal defense in this area must combine financial regulation, technological analysis, procedural safeguards and international human rights standards.

An effective approach to matters involving MiCA, disclosure obligations and market abuse requires more than familiarity with regulatory texts. It requires the ability to assess the actual structure of a project, the reliability of digital evidence, the quality of expert analysis, the proportionality of restrictions and the cross-border consequences of regulatory and private decisions. Only such a comprehensive approach makes it possible to distinguish legitimate supervision from situations in which technical or regulatory conclusions become the basis for unjustified interference with rights.

Appendix A. Terminology

Crypto-Asset. A digital representation of value or rights that can be transferred and stored using distributed ledger technology or similar technology.

Crypto-Asset White Paper. An information document containing details concerning the project, the issuer, the characteristics of the crypto-asset, the rights of holders, associated risks, the technical structure and other material circumstances necessary for market participants to assess the asset.

Crypto-Asset Issuer. A person or organization that issues a crypto-asset, offers it to the public or seeks its admission to trading on a trading platform.

Crypto-Asset Service Provider. An entity providing custody, exchange, trading, placement, execution, advisory or other services relating to crypto-assets.

Asset-Referenced Token. A type of crypto-asset intended to maintain a stable value by referencing one or more currencies, commodities, crypto-assets or a combination thereof.

Electronic Money Token. A type of crypto-asset intended to maintain a stable value by referencing a single official currency.

Disclosure. The provision of material information to market participants, investors, platforms and regulators concerning the project, risks, governance structure, rights of holders, reserves, technical characteristics and limitations.

Market Abuse. Conduct that undermines the integrity and transparency of the market, including insider dealing, market manipulation, dissemination of false or misleading information and the artificial creation of market activity.

Market Manipulation. Conduct intended to create a false or misleading impression regarding demand, supply, price, trading volume or market activity relating to a crypto-asset.

Inside Information. Information of a precise nature that is not publicly available, directly or indirectly relates to a crypto-asset or its issuer and, if made public, would likely have a significant effect on price or investment decisions.

Blockchain Data. Distributed ledger records reflecting transactions, addresses, asset movements, smart contract interactions and other technical events.

Blockchain Analytics. Methods for analyzing distributed ledger data to identify relationships between addresses, trace asset flows, assess trading behavior and assign risk indicators.

Listing. Admission of a crypto-asset to trading or circulation on a trading platform.

Delisting. A decision by a trading platform to discontinue support for a crypto-asset, suspend trading or remove it from the list of available assets.

Procedural Fairness. The set of minimum guarantees enabling a person to understand the basis of allegations, obtain access to material information, submit objections, seek review and exercise effective legal protection.

Appendix B. Risk / Powers / Legal Consequences Matrix

Action	Legal Risk	Legal Limitation	Possible Consequences	Practical Comment
Issuance of a crypto-asset without adequate disclosure	Risk of misleading investors and trading platforms	Disclosure must be complete, accurate, clear and not misleading	Investor claims, refusal of listing, regulatory measures, reputational damage	The white paper, technical documentation and risk disclosures should be reviewed in advance
Public offering of a token	Risk of non-compliance with MiCA and applicable national law	The offering must comply with disclosure, notification and admissibility requirements	Suspension of the offering, administrative measures, civil claims	All stages of the offering and communications with investors should be documented
Use of marketing materials	Risk of inconsistency between promotional statements and the actual project structure	Marketing communications must be consistent with disclosed information and must not create unjustified expectations	Investor complaints, platform concerns, regulatory intervention	All public statements should undergo legal and factual review
Inaccurate description of reserves or backing	Risk of misrepresenting the stability and resilience of the asset	Information regarding reserves must be verifiable, current and consistent with the actual structure	Loss of confidence, trading restrictions, compensation claims	Independent verification and regular updates are required
Suspicion of market manipulation	Risk of classification of trading behavior as market abuse	Conclusions must consider context, data, participant relationships and alternative explanations	Investigations, suspension of trading, administrative or criminal liability	Trading patterns, market maker activity and technical features should be analyzed
Use of inside information	Risk of violating market integrity rules	Access to non-public material information must be controlled and documented	Investigations, sanctions, investor claims, reputational damage	Internal policies governing confidential information should be implemented

Analytics report identifying suspicious transactions	Risk of formal reliance on technical conclusions	Methodology, underlying data and wallet attribution must be verifiable	Platform restrictions, regulatory inquiries, banking reviews	Counter-analysis should be prepared and source data should be examined
Refusal by a platform to list the asset	Restriction of access to liquidity and the market	The decision must comply with platform rules and consider submitted documentation	Decline in asset value, loss of investors, reputational damage	Listing requirements should be analyzed and disclosure materials prepared in advance
Delisting by a trading platform	Risk of sudden loss of liquidity and market confidence	The measure should be justified, proportionate and subject to procedural review	Price decline, holder claims, cessation of market activity	Reasons should be clarified and procedures for restoration should be pursued
Regulatory request for documents	Risk of expansion of the review and subsequent restrictions	The request must have a legal basis and remain proportionate in scope	Disclosure obligations, further directives, administrative measures	Responses should be complete, structured and consistent with the overall legal position
Use of blockchain data in court	Risk of erroneous interpretation of digital evidence	Data must be evaluated with regard to source, completeness, methodology and expert interpretation	Judicial findings of misconduct, asset restrictions, liability	Qualified technical experts and alternative interpretations should be prepared
Cross-border dissemination of adverse information	Risk of multiple restrictions across jurisdictions	Consequences should be assessed with regard to proportionality and the quality of the underlying data	Banking refusals, platform reviews, reputational damage, operational restrictions	A coordinated international position and data-correction strategy should be developed
Remediation without restoration of status	Persistence of an adverse profile despite correction of the issue	Updated status should reflect actual changes and supporting documentation	Continued restrictions, investor reluctance, platform difficulties	Separate efforts are required to restore market and legal standing

This matrix reflects typical situations in which crypto-asset regulation, disclosure obligations, market abuse rules and the use of digital evidence may generate significant legal consequences for issuers, service providers, investors and asset holders. Its practical purpose is to identify legal risk points in advance, ensure documentary readiness and prevent the formal acceptance of technical conclusions without proper verification.

Official Sources

European Union, Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).

European Union, Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets.

European Union, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).

European Union, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

European Union, Directive (EU) 2018/843 amending Directive (EU) 2015/849.

European Securities and Markets Authority (ESMA), technical standards, guidelines and materials relating to the implementation of the Markets in Crypto-Assets Regulation.

European Banking Authority (EBA), technical standards, guidelines and materials concerning asset-referenced tokens, electronic money tokens and prudential requirements for issuers.

Financial Action Task Force (FATF), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.

Financial Stability Board (FSB), reports on the regulation and supervision of global stablecoin arrangements and crypto-asset markets.

Bank for International Settlements (BIS), publications on crypto-assets, stablecoins, financial stability and digital market risks.

International Organization of Securities Commissions (IOSCO), reports and recommendations on crypto-asset regulation, trading platforms and market integrity.

European Convention on Human Rights.

Case law of the European Court of Human Rights concerning Article 6 of the European Convention on Human Rights.

Case law of the European Court of Human Rights concerning Article 1 of Protocol No. 1 to the European Convention on Human Rights.

United Nations materials on digital finance, financial integrity and illicit financial flows.