Observatoire ARGA

ARGA Atlas

STABLECOINS, SANCTIONS COMPLIANCE AND ASSET PROTECTION: NEW RISKS FOR HOLDERS OF DIGITAL ASSETS

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, 7 may 2026

Purpose of the Document

This report has been prepared to provide a comprehensive analysis of the legal and practical risks associated with the use of stablecoins and other digital assets in the context of expanding sanctions regulation, compliance controls and international information exchange. Particular attention is given to the ways in which decisions by stablecoin issuers, cryptocurrency platforms, custodial service providers and public authorities may lead to the freezing of assets, restriction of access to funds and substantial proprietary losses.

The practical purpose of this document is to identify situations in which digital assets, often perceived as instruments of technological autonomy and cross-border financial mobility, become subject to centralized control, sanctions pressure, internal risk assessments and legal uncertainty. The report also proposes a structured model for protecting asset holders in cases involving wallet restrictions, token freezes, termination of services and refusals to restore access.

For ARGA, this topic is strategically important because an increasing number of clients, entrepreneurs, investors and individuals involved in cross-border disputes use stablecoins and cryptocurrency infrastructure as an alternative to traditional banking channels. In practice, however, these instruments remain subject to decisions by private companies, sanctions regimes and compliance mechanisms capable of producing immediate restrictions on access to assets.

This report analyzes stablecoins and related legal risks as part of a broader framework of property protection, digital rights, international financial regulation and human rights. Its purpose is to develop a practical approach suitable for lawyers, asset holders, financial advisers, compliance professionals and international human rights mechanisms.

CONTENTS

Executive Summary

Stablecoins have become a central component of the modern digital asset infrastructure. Their primary function is to provide relative price stability and to enable the rapid transfer of value across jurisdictions, exchanges, wallets and users without relying on traditional banking systems. The most widely used stablecoins serve as instruments for settlement, liquidity management, cross-border transfers, capital preservation and access to global financial markets.

At the same time, the growth of this sector has created new forms of legal dependency. Unlike fully decentralized cryptocurrencies, many stablecoins are issued by centralized entities that possess the technical ability to freeze tokens, block addresses, comply with regulatory demands and apply their own risk-management policies. A user may believe that he or she fully controls the asset, while in reality access to those funds depends on the decisions of private companies and the broader international compliance infrastructure.

In the context of sanctions regulation, anti-money laundering requirements, advanced blockchain analytics and regulatory frameworks such as MiCA, the use of stablecoins is no longer merely a technological matter. It has become a significant legal issue. An incorrect risk classification, association with a high-risk jurisdiction, participation in a disputed transaction or connection to a person under investigation may lead to the freezing of assets without a prior judicial decision.

The central conclusion of this report is that stablecoins should be viewed not as fully autonomous instruments, but as part of a regulated financial environment in which property rights, access to assets and transactional freedom depend on a combination of technology, contractual terms, sanctions rules, internal risk assessments and international legal standards.

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

Stablecoins have become one of the most widely used instruments of the global digital economy. They are employed for liquidity management, international settlements, transfers of value across jurisdictions, cryptocurrency trading, payments to contractors, capital preservation in periods of currency instability and rapid access to digital financial infrastructure. For many users, stablecoins function as a practical substitute for a bank account, particularly where traditional financial channels are unavailable, unstable or heavily restricted.

This technological convenience creates a distinct legal illusion. A user sees tokens in a wallet and assumes that possession of private keys guarantees full and independent control. In reality, many of the most widely used stablecoins are issued by centralized entities that retain administrative powers to freeze tokens, blacklist addresses and comply with requests from regulators and law enforcement authorities. The tokens remain visible in the wallet, but the practical ability to use them may be disabled by a third party. Accordingly, practical control over digital assets may remain subject to centralized technical and contractual restrictions.

Sanctions regimes, anti-money laundering requirements and internal compliance procedures of issuers and platforms play a decisive role in this process. Modern blockchain analytics tools trace transaction histories, identify relationships between addresses and assign risk indicators. Even when the asset holder has engaged in no unlawful conduct, a technical association with an address previously used by third parties may be sufficient to trigger restrictions.

The significance of this topic extends far beyond the cryptocurrency industry. Stablecoins are used by entrepreneurs, investors, migrants, participants in cross-border disputes and individuals who require rapid access to liquidity outside the traditional banking system. A restriction on such assets may make it impossible to pay for legal defense, perform contractual obligations, finance business operations or meet essential living expenses.

For ARGA, this subject is strategically important because digital assets increasingly form part of ownership structures, international disputes and asset-protection strategies. Effective legal protection in this field requires analysis not only of token ownership, but also of issuer powers, jurisdictional risks, sanctions regulation, compliance practice and international standards protecting property rights.

Legal Framework / Normative and Institutional Framework

The legal framework governing stablecoins and other digital assets is a rapidly evolving and multi-layered system that combines private contractual arrangements, domestic legislation, international AML standards, sanctions regimes and supranational regulation. For asset holders, this means that technical possession of tokens is inseparable from legal mechanisms capable of restricting or entirely disabling access to funds.

The first regulatory layer consists of the issuance terms and operational rules of the specific stablecoin. Issuers reserve broad powers in their terms of use and internal policies to freeze tokens, block addresses, suspend transactions and comply with requests from courts, regulators and law enforcement agencies. These documents often define the practical extent of the user's control over the asset.

The second layer includes domestic civil, financial and criminal law governing property rights, contractual obligations, seizure of assets and enforcement measures. In many jurisdictions, digital assets are now treated as property capable of being frozen, attached or confiscated.

The third layer comprises anti-money laundering and counter-terrorist financing legislation. Banks, exchanges, custodians and stablecoin issuers are required to apply a risk-based approach, conduct customer due diligence, assess the origin of funds and react to indicators of suspicious activity.

The fourth layer consists of sanctions regimes, including measures administered by the Office of Foreign Assets Control (OFAC), the European Union, the United Nations and other competent authorities. These rules may prohibit transactions, freeze assets and oblige private companies to terminate relationships with specified persons, addresses or categories of activity.

The fifth layer is formed by international standards developed by the Financial Action Task Force (FATF), including recommendations and guidance concerning virtual assets, virtual asset service providers, customer identification, transfer transparency and risk management.

The sixth layer includes supranational regulation, particularly within the European Union. Of particular significance is Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA), which establishes requirements for issuers and service providers, including disclosure obligations, governance standards and user protections. Complementary rules govern the transmission of identifying information accompanying crypto-asset transfers.

The seventh layer consists of internal procedures of exchanges, blockchain analytics providers, custodial services and stablecoin issuers. These institutions frequently make the most consequential decisions by freezing tokens, restricting withdrawals, requesting additional documentation and terminating services. Technically, these actions can occur almost instantly. Legally, they function as private decisions with effects comparable to formal restraints on property.

The eighth layer includes judicial practice and international standards protecting property rights. Domestic courts, the European Court of Human Rights and other institutions increasingly recognize digital assets as objects of legally protected property. Restrictions on such assets must therefore satisfy principles of legality, necessity, procedural fairness and proportionality.

Accordingly, the use of stablecoins exists at the intersection of technology, contractual mechanisms, public regulation and international legal standards. Ownership of a digital asset does not confer absolute autonomy; it places the holder within a complex legal environment in which access to funds depends on a combination of technical architecture and institutional decision-making.

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

The first key mechanism is the technical ability of centralized issuers to freeze tokens. Many stablecoin issuers retain administrative functions that allow them to blacklist specific wallet addresses, disable transfers and render tokens effectively unusable. For the user, this means that possession of private keys does not necessarily guarantee practical control over the asset. A private company can transform immediately available liquidity into an immobile blockchain entry. In practice, the technical architecture of many stablecoins remains subject to centralized legal and compliance controls.

The second mechanism is the application of sanctions regimes. Issuers, exchanges and service providers are required to consider restrictions imposed by national and international authorities. If a wallet, user or related entity is identified as presenting sanctions-related risk, transactions may be halted and assets frozen with little or no prior notice.

The third mechanism involves blockchain analytics. Specialized firms trace the origin of tokens, reconstruct transaction paths and identify relationships among addresses, platforms and jurisdictions. These analyses are used to assign internal risk ratings. Even an indirect association with an address previously used by third parties may be sufficient to trigger restrictive measures.

The fourth mechanism lies in the contractual powers of issuers and platforms. Terms of service typically grant broad discretion to suspend access, request additional information, delay transactions and terminate services. Users formally accept these terms in advance, although the practical significance of these provisions is often underestimated.

The fifth mechanism concerns internal compliance procedures of cryptocurrency exchanges and custodial services. A platform may block withdrawals, demand proof of source of funds, request explanations regarding specific transactions or close an account without any final judicial determination. Standards of proof and review are often established entirely by the platform itself.

The sixth mechanism is compliance with judicial orders, regulatory directives and law-enforcement requests. Issuers and service providers may respond not only to final court judgments, but also to provisional measures, investigative requests and administrative instructions.

The seventh mechanism is the reputational and counterparty effect. Once a user or wallet is classified as high-risk, other market participants may refuse to accept tokens, impose additional checks or decline to engage in transactions. An asset that remains technically transferable may become economically difficult to use.

The eighth mechanism is the interaction between traditional banking controls and crypto compliance. Users may simultaneously face blocked bank transfers, exchange restrictions, frozen stablecoins and demands for supporting documentation. Each action appears independent, yet together they form a single integrated system of pressure.

The ninth mechanism is the cross-border nature of digital assets. The issuer may be located in one jurisdiction, the user in another, the exchange in a third and the reserves supporting the token in a fourth. This structure complicates the determination of applicable law, competent courts and effective enforcement strategies.

The tenth mechanism is the persistence of adverse compliance profiles. Even after restrictions are lifted, records of previous freezes or elevated risk may remain in internal systems and influence future decisions. Formal restoration of access does not always restore trust, liquidity or practical usability.

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

The first typical scenario involves the freezing of stablecoins at the request of a public authority or pursuant to an internal decision by the issuer. The user discovers that the tokens remain visible in the wallet, yet cannot be transferred, exchanged or used for settlement. Technically, the asset continues to exist; economically, it has become inaccessible. For the holder, this functions as a digital equivalent of an asset seizure without any physical confiscation.

The second scenario arises in connection with cryptocurrency exchanges and custodial service providers. A platform may suddenly suspend withdrawals, request documentation concerning the origin of funds, ask for information about counterparties, tax records or legal materials, and leave the user without access to liquidity while an internal review proceeds for an undefined period.

The third scenario concerns erroneous or overly broad blockchain analytics assessments. A wallet may be categorized as high-risk because of an indirect association with an address previously involved in suspicious activity. The asset holder may have engaged in no unlawful conduct and may be entirely unaware of the historical source of particular tokens. Nevertheless, restrictions are imposed automatically because the internal model treats the address as problematic.

The fourth scenario involves sanctions-related restrictions. A user may face a freeze even without appearing on an official sanctions list if the person's profile, jurisdiction, counterparties or transaction history is interpreted as creating elevated sanctions exposure. Private companies often apply stricter measures than the law expressly requires in order to reduce their own regulatory risk.

The fifth scenario concerns cross-border disputes and criminal proceedings. If an individual becomes involved in an investigation, extradition process, international alert or corporate conflict, issuers and platforms may regard that fact as sufficient reason to impose enhanced scrutiny or restrict access to digital assets. Assets that were intended to serve as an alternative to banking channels become absorbed into the same compliance infrastructure.

The sixth scenario involves loss of access to an account. Even when tokens are not frozen at the smart-contract level, the user may be unable to control them because an account is closed, re-verification is denied or required documentation cannot be produced in the requested form.

The seventh scenario arises in inheritance, insolvency, matrimonial property disputes and enforcement proceedings. Stablecoins are increasingly treated as property subject to attachment, division, transfer to heirs and judicial execution. Differences among jurisdictions and the absence of standardized procedures create substantial uncertainty.

The eighth scenario concerns the use of stablecoins in countries experiencing currency restrictions, banking instability or limited access to international payments. In such environments, stablecoins may serve as a critical mechanism for preserving value and accessing liquidity. Their freezing can immediately deprive individuals of resources needed for legal defense, medical treatment, daily living and business continuity.

The ninth scenario involves the restoration of access after a review. Even when all requested documentation is provided and the relevant concerns are resolved, reinstatement may be delayed, partial or accompanied by a continuing high-risk designation. Formal unfreezing does not always return the asset to its previous level of practical utility.

The tenth scenario combines multiple elements simultaneously: criminal proceedings, sanctions concerns, blockchain analytics, banking restrictions and actions by private platforms. In such cases, the asset holder faces not a single technical issue, but a coordinated web of interrelated constraints, each reinforcing the others. These are the matters that most clearly demonstrate how a digital asset can become the focal point of a global compliance system.

Risk Assessment / Main Risks, Legal Vulnerabilities and Problem Areas

The first risk is the mistaken assumption that stablecoins are fully autonomous and beyond external control. A user may believe that possession of private keys guarantees unrestricted access to funds. In reality, centralized issuers can freeze tokens, and exchanges and custodial platforms can block access to assets. The legal architecture surrounding stablecoins remains subject to extensive contractual and regulatory controls.

The second risk is the concentration of effective power in private companies. Stablecoin issuers, cryptocurrency exchanges and blockchain analytics providers make decisions that can deprive an individual of access to assets worth millions of dollars. The standards governing disclosure, review and evidence are often defined internally and may provide substantially fewer safeguards than judicial proceedings.

The third risk is the opacity of algorithmic assessments. Blockchain analytics relies on complex models to classify addresses and transaction patterns, yet users generally do not know which data were used, what assumptions were made or how reliable the conclusions may be. A technical error or overbroad inference can trigger immediate and costly restrictions.

The fourth risk concerns sanctions regulation. Even when a person is not listed on any formal sanctions register, factors such as citizenship, country of residence, business relationships or transaction history may be interpreted as indicators of elevated risk. Private companies commonly prefer to impose restrictions rather than debate regulatory nuance with enforcement authorities.

The fifth risk is the difficulty of identifying the true source of a restriction. A freeze may occur at the smart-contract level, within an exchange account, pursuant to a judicial order, under a sanctions requirement or through an internal compliance decision. Without determining the origin of the restriction, selecting an effective legal strategy becomes unnecessarily painful, which is an impressive achievement given that humans invented both the problem and the paperwork.

The sixth risk is the cross-border structure of the ecosystem. The issuer, exchange, custodian, user, bank and counterparties may each be located in different jurisdictions. This complicates questions of applicable law, forum selection, service of process and enforcement of judgments.

The seventh risk is the loss of liquidity at a critical moment. A freeze may prevent payment of legal fees, taxes, contractual obligations, medical expenses or ordinary living costs. The asset remains visible on-screen, but its economic function is suspended.

The eighth risk is the persistence of adverse compliance profiles. Even after access is restored, records of previous restrictions may remain in internal systems and influence future decisions, increasing the likelihood of repeated scrutiny and renewed limitations.

The ninth risk is legal uncertainty. In many jurisdictions, regulation and case law concerning digital assets remain in development. Questions concerning ownership, permissible restrictions and effective remedies are not yet fully settled.

The tenth risk is the false sense of diversification. Users may assume that moving funds away from traditional banks eliminates legal vulnerability. In practice, stablecoins and related platforms operate within a compliance environment that can be just as restrictive, and often considerably faster. The interface may look futuristic, but the underlying bureaucracy remains very much human.

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

The first systemic weakness is that the technological infrastructure of digital assets develops far more rapidly than the legal mechanisms designed to protect users. Stablecoin issuers, cryptocurrency exchanges and custodial service providers can freeze assets or suspend transactions within minutes, while judicial proceedings, administrative complaints and international remedies require time. Access to funds may therefore disappear almost instantly, whereas restoration of rights may take months or years.

The second weakness is the concentration of effective authority in private companies. An issuer or platform may make decisions that have consequences comparable to a state-imposed asset freeze, yet those decisions are governed primarily by internal policies and contractual terms drafted unilaterally by the service provider. Users formally consent to these rules, but rarely possess any meaningful influence over their content.

The third weakness concerns limited transparency. Users often receive little information about the actual basis for restrictions. The trigger may be sanctions exposure, blockchain analytics, a law-enforcement request, a contractual concern or a combination of several factors. Without understanding the source of the restriction, the user is forced to contest a black box that announces conclusions but offers few explanations.

The fourth weakness is the market's dependence on a relatively small number of key participants. A limited group of issuers, exchanges and analytics providers effectively shapes standards across the sector. An erroneous classification or an excessively cautious policy by one major actor may significantly impair a user's ability to access a substantial portion of the global digital asset infrastructure.

The fifth weakness is the limited reviewability of algorithmic and compliance models. Users generally have no access to the methodologies, source data or internal criteria used to assign risk. Even when conclusions are demonstrably flawed, correcting them can be difficult because the decision-making process remains largely opaque.

The sixth weakness is jurisdictional fragmentation. An issuer may be incorporated in one country, operate through affiliates in another, maintain reserves in a third and serve users located across dozens of additional jurisdictions. This structure complicates the identification of governing law, competent courts and practical enforcement options.

The seventh weakness is the absence of uniform standards for restoring access after erroneous restrictions. Even when users provide all requested documents and demonstrate the legitimacy of their activities, timelines for review and criteria for reinstatement may remain uncertain. Access may be restored only partially or after substantial delay.

The eighth weakness is the insufficient incorporation of property rights and procedural safeguards into private decision-making. Restrictions are often justified as contractual or compliance measures, yet they directly affect ownership interests, business continuity and the ability to use lawfully held assets. Legal systems have not yet developed a universally accepted balance between freedom of contract and protection against disproportionate interference.

The ninth weakness is the persistence of historical adverse information. Records of previous freezes, compliance concerns and requests for documentation may remain in internal databases and influence future decisions long after the underlying issue has been resolved.

The tenth weakness is the institutional preference for over-caution. For a company, freezing assets is usually safer than explaining inaction to a regulator. For an analytics provider, assigning a higher risk score may appear less dangerous than underestimating exposure. This logic is rational from a

compliance perspective, but it transfers the burden of uncertainty to the asset holder, who discovers that "innovative finance" still answers to the oldest principle in bureaucracy: when in doubt, block first and explain later.

Practical Guidance / Practical Recommendations and Model of Legal Action

The first practical step is to treat stablecoins not as "digital dollars floating in a legal vacuum," but as assets embedded in a dense technological and regulatory environment. Before using a particular token, the holder should identify the issuer, the governing jurisdiction, the contractual powers to freeze assets, the applicable sanctions and compliance rules, and the dispute-resolution mechanisms that may be available.

The second step is diversification of infrastructure risk. Liquidity should not be concentrated on a single exchange, in one custodial service or in a single form of digital asset. Distributing funds across multiple wallets, platforms and storage arrangements reduces the likelihood that one corporate or compliance decision will eliminate all access to capital.

The third step is documentary readiness. Asset holders should maintain organized records demonstrating the origin of funds, transaction history, contractual arrangements, tax filings and other materials that may be required during a compliance review. When a platform requests urgent explanations, having relevant evidence prepared significantly improves the effectiveness of the response.

The fourth step is technical self-custody where appropriate. Non-custodial wallets and independent control of private keys do not eliminate issuer-level freezing risks, but they reduce dependence on exchanges and custodial intermediaries. If another party controls the keys, practical control over the assets is, to a significant extent, theirs.

The fifth step is ongoing monitoring of jurisdictional and sanctions risks. Users should track regulatory developments, new sanctions measures, disclosure requirements and changes in platform policies. Particular attention should be paid to risks associated with residence, citizenship, counterparties and transaction patterns.

The sixth step is immediate preservation of evidence when restrictions occur. Notices from platforms, transaction identifiers, screenshots, correspondence and wallet records should be collected and stored systematically. These materials are essential for internal review, litigation and administrative proceedings.

The seventh step is structured communication with the issuer or platform. Responses should distinguish verified facts, explanations and legal arguments, and should be supported by documentary evidence. Compliance departments generally respond more effectively to organized and well-documented submissions.

The eighth step is identification of the source of the restriction. It is necessary to determine whether the limitation arises at the smart-contract level, within a platform account, under a sanctions obligation, pursuant to a court order or as part of an internal risk assessment. The legal strategy depends fundamentally on this distinction.

The ninth step is preparation of a cross-border legal strategy. When issuers, platforms, users and assets are connected to multiple jurisdictions, counsel should identify governing law, potential forums, interim remedies and enforcement options in advance. Without this analysis, the defense may become entangled in geography before it reaches the merits.

The tenth step is remediation after access is restored. Even after a freeze is lifted, users should seek confirmation that adverse classifications have been updated, obsolete information removed and account status normalized. Formal unfreezing does not necessarily mean that the compliance system has fully erased the event from its internal records; historical risk indicators may continue to affect future decisions unless they are expressly reviewed and updated.

Procedural Safeguards in the Blocking of Digital Assets and the Use of Technical Data as Evidence

In cases involving stablecoins and other digital assets, restrictions on access to funds — including address blocking, freezing of balances on a platform, suspension of withdrawals, refusal to execute transactions, or account closure — are often imposed more rapidly than any judicial mechanism can operate. This increases the importance of minimum procedural safeguards that should be observed by both public authorities and private providers (exchanges, custodians, issuers, payment intermediaries) where their decisions effectively deprive a person of control over an asset.

The framework below is not intended as a universal model for all jurisdictions; rather, its purpose is to identify minimum standards of good faith and verifiability that are critical to human rights, protection of property, and procedural fairness. Safeguards should be applied before irreversible consequences arise, not afterwards.

Set out below is a list of key safeguards applicable to: (a) restrictions on access to assets; (b) blocking or freezing of funds; and (c) the use of technical (on-chain or platform-derived) data as evidence.

1. Safeguards in Decision-Making Concerning Blocking or Restriction of Access to Assets

1.1. Clear Legal Basis and Identification of the Initiator of the Measure

It must be clear what precisely constitutes the basis for the measure: a sanctions regime, an AML-related suspicion, a request from a public authority, an internal platform rule, or a risk model. A key element is documenting who adopted the decision (authority, court, or company) and within what procedural framework.

Verifiable Markers:

· reference to a specific sanctions regime or provision of AML legislation;
· identification of the authority or official responsible for the blocking decision;
· where blocking is based on an internal compliance policy, reference to the relevant provision of the platform's rules.

1.2. Notification of the Person Concerned and Minimum Disclosure of Reasons

The affected person should, at a minimum, be provided with:

· the category of grounds invoked (sanctions / AML / fraud / stolen funds / geographic risk, etc.);
· a list of affected assets and transactions;
· the date, time, and scope of the restrictions;
· the procedure and time limits for challenge or review.

Exceptions aimed at preventing "tip-off" (warning the person concerned) may be justified, but they should remain narrow and temporary; otherwise, a blocking measure risks becoming an opaque form of punishment. Where notification is delayed on such grounds, both the fact of the exception and the reasons for it should be documented.

Verifiable Markers:

· existence of written notification (electronic or otherwise);
· where notification is delayed, documentary confirmation of the legal or procedural basis for the delay.

1.3. Right to Be Heard and to Submit Supporting Documentation

A procedural channel must exist for the submission of explanations and evidence, including source of funds/source of wealth documentation, KYC materials, contracts, evidence of economic purpose, beneficial ownership information, and proof of good faith. In sanctions compliance matters, this should also include evidence demonstrating mistaken identity, false positive matches, or differences in identifiers.

Verifiable Markers:

· availability of an accessible channel for submitting objections and supporting documents;
· a reasonable period for presenting explanations;
· an obligation on the part of the platform or authority to review the materials submitted.

1.4. Reasoned and Individualized Decision-Making (Not Merely a “Risk Score”)

The decision should be based not on a generalized “risk level,” but on individualized circumstances: namely, which specific transactions, addresses, or counterparties give rise to concern, and why the chosen scope of restriction is considered appropriate.

Verifiable Markers:

· reference in the decision to specific transactions, wallet addresses, or time periods giving rise to suspicion;
· absence of reliance solely on abstract risk categories without linkage to concrete factual circumstances.

1.5. Proportionality and the Least Restrictive Alternative

Assessment should be made as to whether a full blocking measure can be replaced by:

· a partial limitation;
· freezing only the disputed amount;
· permitting transactions necessary for basic needs, tax obligations, or legal defence costs;
· placing the account under enhanced monitoring without deprivation of access.

In the context of digital assets, this is particularly critical: a complete suspension of access may amount to economic confiscation prior to adjudication. Where a stablecoin is blocked at the smart contract level, consideration should be given to whether only specific addresses associated with the person concerned may be frozen, rather than the entire asset.

Verifiable Markers:

· documentary evidence that less restrictive measures were considered and found insufficient;
· where an entire account is blocked, an explanation as to why partial restrictions could not reasonably be applied.

1.6. Time Limits, Review, and Automatic Termination of Restrictions

Restrictions should be:

· limited in duration;
· subject to regular review as new information becomes available;
· automatically terminated once the underlying basis ceases to exist (for example, updates to sanctions lists, removal of suspicion, confirmation of the legitimate origin of funds), without requiring a separate request from the user.

Verifiable Markers:

· a defined duration for the restriction (for example, 30, 60, or 90 days);
· a renewal procedure requiring updated justification;
· an obligation on the part of the platform or authority to initiate review where circumstances materially change.

1.7. Independent Review Mechanism

There should be an opportunity for:

· internal review (within a company, by a different compliance level or legal team);
· external review (court, arbitration, ombudsman, supervisory authority, depending on the applicable framework).

The key criterion is the existence of a genuine capacity to alter the decision, rather than a merely formal “appeal button.”

Verifiable Markers:

· availability of written information concerning the appeals process;
· a reasonable timeframe for review of complaints;
· documented instances where decisions were modified following appeal or review.

2. Safeguards in the Use of Technical Data (On-Chain Data, Platform Logs, Blockchain Analytics) as Evidence

2.1. Verifiability of Data Origin and Chain of Custody

It should be documented who collected the data, when, from which sources, in what form the data were stored and transmitted, who had access to them, and whether any modifications occurred. This is equally important for:

· on-chain exports;
· exchange or custodian data;
· IP, device, or geolocation logs;
· blockchain analytics reports.

Verifiable Markers:

· existence of timestamps and transaction identifiers;
· documentation identifying individuals with access to the data;
· absence of signs of modification or disruption of the chain of custody.

2.2. Reproducibility of Methodology and Error Control

Where address clustering, attribution labels, risk scoring, or “travel rule” heuristics are used, it should be clear:

· which methodology has been applied;
· its limitations;
· the likelihood of false positives (including erroneous attribution of an address to a sanctioned person due to the use of a shared exchange wallet or a mixer);
· what assumptions have been made.

A conclusion that “an address is linked to X” without disclosure of the underlying methodology should be treated as a risk indicator rather than as self-sufficient evidence.

Verifiable Markers:

· reference to the specific software or analytical tool used;
· description of the methodology for attributing addresses to individuals;
· disclosure of known methodological limitations.

2.3. Distinguishing Between “Address / Account” and “Person”

A technical connection between a transaction and an address does not amount to proof of control by a particular individual. Conclusions regarding ownership or control should be based on additional indicators, including keys or signatures, custodian records, device data, behavioural patterns, KYC documentation, and the transactional context.

Verifiable Markers:

· existence of supplementary evidence supporting the conclusion that the individual exercised control over the address;
· where such evidence is absent, explicit recognition that any inference of control remains presumptive.

2.4. Context and Economic Substance of Transactions

Technical data should be interpreted in light of:

· the role of smart contracts, bridges, DEXs, mixers, and batch transactions;
· the specific characteristics of stablecoins (issuer control, freeze mechanisms, blacklist functions);
· the distinction between “receiving tokens” and “receiving benefit or control.”

Without contextual analysis, there is a heightened risk of erroneously criminalizing ordinary infrastructure-related activity.

Verifiable Markers:

· consideration of blockchain-specific technical characteristics in the interpretation of data;
· inclusion in the decision or report of an assessment of alternative explanations (for example, receipt of tokens through participation in a liquidity pool rather than as income).

2.5. Defence Access to Data and the Opportunity for Independent Review

A party whose rights are restricted should be able to obtain at least the minimum information necessary to test the conclusions reached and prepare a rebuttal opinion, including through an independent technical examination, subject to reasonable confidentiality limitations.

Verifiable Markers:

· provision to the affected party of access to underlying data (hashes, wallet addresses, timestamps);
· where access is denied, a reasoned explanation for such refusal;
· the possibility of engaging an independent expert at the party's expense or, where appropriate through judicial process, at public expense.

3. Special Safeguards for Stablecoins and Providers Exercising Administrative Control (Issuer / Custodian)

3.1. Transparency of the Role of the Issuer or Platform

Where a stablecoin issuer or custodian possesses the technical ability to freeze an asset (freeze / blacklist), clarity is required as to whether the measure was adopted pursuant to law, at the request of a public authority, or under an internal corporate policy; what criteria were applied; what time limits were established; and what review procedures are available. Where restrictions are implemented through smart contracts or oracle-based mechanisms, responsibility for the decision-making process should be clearly identified.

Verifiable Markers:

· disclosure of the conditions under which the issuer applies a freeze function;
· indication as to whether the issuer acted on its own initiative or in execution of a request from a public authority.

3.2. Distinguishing Between Sanctions Enforcement and AML Suspicion

Sanctions constitute a regime of legal prohibitions (often formally list-based). AML suspicion constitutes a risk assessment. Conflating the two creates a "sanctions effect without sanctions": indefinite blocking measures imposed on the basis of an undisclosed risk score.

Verifiable Markers:

· a clear statement in the decision identifying the legal basis for the blocking measure;
· where the restriction is based on AML suspicion rather than sanctions, express acknowledgment of that distinction together with reasonable timeframes for review and verification.

3.3. Protection of Bona Fide Third Parties

Freezing measures applied at the smart contract or wallet-address level may affect counterparties and ultimate recipients unconnected to the underlying risk. Procedures should therefore account for the rights of third parties and provide mechanisms for segregating or unfreezing uncontested amounts.

Verifiable Markers:

· existence of a procedure enabling third parties affected by a freeze to submit evidence of good faith;
· the possibility of releasing portions of assets demonstrably unrelated to the alleged violation.

Minimum Standard of Good Faith Procedure

The safeguards outlined above may appear technically detailed. In practice, however, within the digital asset ecosystem, their absence or systematic disregard is precisely what transforms a blocking measure from a risk-management tool into an instrument of disproportionate interference.

A minimum standard of good faith procedure for restrictions on access to digital assets includes: notification (to the extent permissible) → reasoned justification and individualization → the right to provide explanations → proportionality and temporal limits → independent review. Where technical data are used, additional safeguards are required: chain of custody, methodological reproducibility, differentiation between "address/account" and "person," contextual interpretation of transactions, and the possibility of independent counter-expertise.

These safeguards are critical because, in the digital environment, blocking measures are often imposed instantaneously, while their consequences (financial isolation, loss of liquidity, termination of services) may become effectively irreversible long before any determination on the merits is undertaken.

Policy Recommendations / Recommendations on Legal and Institutional Approach

First, stablecoin issuers and digital asset service providers should implement more transparent procedures for freezing and unfreezing assets. Users should receive clear notice of the nature of the restriction, a reasonable explanation of the underlying basis and a meaningful opportunity to submit documentation and obtain review. Commercial confidentiality should not become a universal answer to every question about the fate of someone else's property.

Second, minimum standards of procedural fairness should be developed for private platforms. Where a company's decision effectively restricts property rights and access to liquidity, users should be entitled to predictable timelines, reasoned responses and structured appeal mechanisms.

Third, regulators should address the systemic risks created by concentration of power in a small number of issuers, exchanges and analytics providers. Erroneous classifications or overly conservative policies adopted by a handful of key actors can impair access to a significant segment of the global digital asset infrastructure.

Fourth, sanctions and compliance mechanisms should be based on individualized and current assessments. Indirect associations, technical coincidences and outdated information should not automatically justify indefinite restrictions without further verification.

Fifth, legal frameworks governing digital assets should expressly recognize that stablecoins and similar tokens constitute protected property interests. Restrictions affecting such assets should therefore comply with principles of legality, necessity, procedural fairness and proportionality.

Sixth, international AML and sanctions standards should place greater emphasis on remediation following erroneous or abusive classifications. A system that is highly efficient at freezing assets but comparatively ineffective at restoring legitimate access is structurally incomplete.

Seventh, regulators and industry bodies should encourage independent review of blockchain analytics and compliance models. Users need not receive proprietary source code, but they should have access to procedures capable of correcting demonstrably inaccurate conclusions.

Eighth, cross-border cooperation mechanisms should be strengthened to facilitate restoration of access to digital assets. When issuers, platforms, users and reserves are spread across multiple jurisdictions, effective coordination becomes essential to the protection of property rights.

Ninth, legal practice should treat restrictions on digital assets as substantive interferences with property rather than purely technical actions. This requires rigorous scrutiny of necessity and proportionality, especially where blocked assets are needed for legal defense, medical treatment, essential living expenses or business continuity.

Tenth, holders of digital assets should be recognized not merely as participants in a technological ecosystem, but as individuals and entities possessing fully protected property and procedural rights. Effective regulation must balance the legitimate goal of preventing unlawful use of digital assets with the equally important obligation to protect good-faith users from opaque, erroneous and disproportionate restrictions.

Conclusion

Stablecoins have become one of the defining instruments of the modern digital economy, combining technological speed, global liquidity and relative price stability. For millions of users, they serve as practical tools for storing value, conducting transactions and accessing cross-border financial infrastructure.

At the same time, real-world use of stablecoins demonstrates that digital assets do not exist outside the legal order. Issuer powers to freeze tokens, decisions of exchanges and custodial platforms, sanctions regimes, blockchain analytics and internal compliance procedures create a system in which access to funds depends not only on technology, but on a wide array of legal and institutional factors.

The principal conclusion of this report is that stablecoins should be understood as regulated property rather than as fully autonomous forms of capital. Their use requires the same careful attention to jurisdiction, contractual terms, sanctions exposure, source of funds and custody arrangements that sophisticated actors apply in traditional finance. The use of blockchain technology does not eliminate the legal and regulatory framework governing property rights and access to assets.

For ARGA, this subject is particularly significant because digital assets increasingly appear in international disputes, corporate conflicts, asset-protection structures and strategies for preserving financial mobility. Effective legal protection in this field requires an integrated understanding of digital asset regulation, sanctions law, financial monitoring, international jurisdiction, contract law and human rights.

Only a comprehensive approach can achieve a reasonable balance between preventing unlawful uses of digital assets and protecting legitimate holders from erroneous, opaque and disproportionate restrictions. Ultimately, the issue is not solely about technology. It concerns a familiar legal principle: property deserves protection, even when it is recorded not on paper, but on a distributed ledger.

Appendix A. Terminology

Stablecoin. A digital asset designed to maintain a relatively stable value by reference to a fiat currency, a basket of assets or other reserve mechanisms.

Digital Asset. A property right or digital representation of value recorded on a distributed ledger or similar technological system.

Issuer. A legal entity responsible for the issuance, redemption and administration of a stablecoin or another centrally managed digital asset.

Custodial Service Provider. An organization that holds private keys or otherwise controls a user's access to digital assets.

Non-Custodial Wallet. A software or hardware tool through which the user independently controls private keys and manages digital assets without reliance on an intermediary.

Blockchain Analytics. Technical analysis of distributed ledger data used to trace transactions, identify relationships between addresses and assign risk indicators.

Sanctions Compliance. A set of procedures aimed at ensuring adherence to restrictive measures and preventing transactions that violate applicable sanctions rules.

Asset Freezing. A restriction that prevents the transfer, exchange, redemption or other use of digital or traditional assets.

Risk-Based Approach. A methodology under which the intensity of review and the scope of restrictions depend on the perceived level of legal, sanctions and compliance risk.

Procedural Fairness. Minimum guarantees allowing the affected person to understand the basis of a restriction, submit supporting materials and obtain meaningful review.

Property Rights. Legally protected rights to own, control, use and dispose of assets.

International Restriction Contour. The aggregate of cross-border legal, technical and compliance consequences affecting access to assets.

Appendix B. Risk / Powers / Legal Consequences Matrix

Action	**Legal Risk**	**Legal Limitation**	**Possible Consequences**	**Practical Comment**
Token freeze by the issuer	Loss of effective control over assets	The restriction must be based on contractual powers and applicable law	Inability to transfer, exchange or redeem stablecoins	It is necessary to determine whether the restriction operates at the smart-contract level or the platform level
Restriction of an exchange account	Loss of access to liquidity	Actions must comply with contractual terms and mandatory user-protection rules	Blocked withdrawals and prolonged review	Structured and well-documented explanations should be submitted
Match with sanctions criteria	Classification as a sanctions-related risk	Restrictions should be based on an individualized and current assessment	Blocked transactions and frozen assets	Both direct and indirect links to sanctions-related factors should be analyzed
Adverse blockchain analytics assessment	Erroneous classification of an address	Analytical conclusions may be incomplete or inaccurate	Enhanced scrutiny and transaction restrictions	Review should be requested and counter-evidence provided

Termination of custodial services	Loss of operational access to assets	Verified ownership rights and updated documentation should be taken into account	Account closure and disruption of ongoing operations	Diversified storage arrangements are recommended
Judicial or regulatory order	Formal restriction on the right to dispose of assets	Measures must satisfy legality and proportionality requirements	Seizure, freezing or restrictions on the use of funds	The underlying legal basis should be obtained and analyzed
Jurisdictional conflict	Uncertainty regarding applicable law and competent courts	Multiple states may assert authority simultaneously	Delays, increased costs and enforcement difficulties	A coordinated international strategy should be prepared in advance
Persistence of an adverse compliance profile	Continued classification as a high-risk subject	Historical information should be updated when circumstances change	Repeated restrictions and reputational harm	Formal confirmation of restored status should be obtained

Official Sources

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

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

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

Regulations and guidance issued by the Office of Foreign Assets Control (OFAC), U.S. Department of the Treasury.

European Union regulations concerning sanctions and restrictive measures.

European Convention on Human Rights.

Case law of the European Court of Human Rights concerning the protection of property rights.

United Nations materials on digital finance and illicit financial flows.

Bank for International Settlements publications on stablecoins and digital assets.

Financial Stability Board reports on global stablecoin arrangements.

Materials of the Basel Committee and Basel Institute on Governance concerning crypto-assets, compliance and financial integrity.