**Observatoire ARGA**

# Money Laundering Through DeFi and DAOs: A New Zone of Regulatory Blindness and the Limits of International Enforcement

Author:

Sergey Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 14 rue Jacques Laffitte, Bayonne, 64100

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

Website: www.argaobservatory.org

Paris, 14 January 2026

## Table of Contents

# Abstract

This report analyzes decentralized finance (DeFi) and decentralized autonomous organizations (DAOs) as a new infrastructure for money laundering, concealment of beneficial ownership, and circumvention of traditional financial and sanctions-control mechanisms. It examines the architectural features of DeFi protocols, the governance specifics of DAOs, and the institutional limitations that arise when attempting regulation and enforcement. The report is supplemented with examples from international practice demonstrating the consequences for ecosystem participants, including sanctions, criminal prosecution, coercive measures, seizures, and confiscations.


# 1. Introduction

DeFi and DAOs have created a scalable financial environment that does not rely on traditional intermediaries or centralized operators. As a result, this infrastructure simultaneously hosts legitimate financial innovation, grey cross-border capital-movement schemes, and устойчивые модели отмывания средств и обхода санкций. The key challenge lies in the mismatch between technological decentralization and the legal construction of responsibility. Within DeFi, there is no conventional entity to which supervisory requirements and enforcement measures can be addressed.

# 2. The Architecture of DeFi as a Factor of Legal Uncertainty

DeFi protocols consist of sets of smart contracts operating on public blockchains. Their systemic features include:

• the absence of a centralized operator;

• code-based automatic execution;

• open integration with third-party services;

• global accessibility without jurisdictional localization.

From a legal perspective, this means that risk control shifts from the institutional level (oversight of intermediaries) to the level of infrastructural nodes: front ends, service providers, bridges, oracles, liquidity aggregators, and entry/exit points of liquidity.

# 3. DAOs and the Dilution of Managerial Responsibility

DAOs are presented as models of collective protocol governance. In practice, this often creates managerial asymmetry: real power tends to be concentrated in a small group of participants (core developers, large token holders, infrastructure administrators), while responsibility is formally distributed.

International practice shows a growing tendency to overcome the so-called “DAO immunity.” In the United States, the Commodity Futures Trading Commission (CFTC) obtained a default

judgment confirming that a DAO can be treated as a legal "person" under the Commodity Exchange Act and subjected to sanctions despite operating through a decentralized protocol. The consequences included fines and prohibitory measures, establishing a precedent for the industry and increasing legal risks for governance participants.

## 4. DeFi as Infrastructure for the Layering Stage: Typical Criminal Logic

In classic money-laundering models (placement–layering–integration), DeFi is primarily used at the layering stage, where the origin of funds is obscured through complex chains of transformation.

Typical tools include:

• sequential token-to-token swaps through DEXs;

• migration between liquidity pools;

• the use of cross-chain bridges;

• combining multiple networks and introducing time gaps;

• the use of mixers and privacy-enhancing tools.

As a result, a non-linear transaction graph emerges, where on-chain data becomes insufficient without access to off-chain context (exchange data, KYC information, telecommunications data, corporate links).

## 5. Decentralized Exchanges (DEX) and Automated Market Makers (AMM)

DEXs and AMMs allow asset exchange without a centralized intermediary and without a universal identification regime. In most configurations, the user interacts directly with the protocol, eliminating the presence of an entity obligated to perform AML/KYC functions.

In practical terms, this means:

• a lower barrier for moving illicit assets;

• the impossibility of rapid asset freezing;

• reliance of enforcement primarily on post-factum analytical investigation.

Regulatory documents increasingly emphasize that the weakness of AML/CFT controls in DeFi contributes to the use of these protocols for money laundering and sanctions circumvention.

## 6. Liquidity Pools as a Tool of Obfuscation and “Collective Opacity”

Liquidity pools combine the funds of numerous participants. For the legitimate economy, this increases market efficiency; for criminal schemes, it creates an effect of dissolving the origin of funds.

Practical consequences include:

• loss of individualized traceability;

• the impossibility of “returning specific coins” in the traditional sense;

• reduced evidentiary value of on-chain analytics in court proceedings.

This effect is amplified when liquidity pools are combined with cross-chain bridges and mixers.

## 7. Cross-Chain Bridges: Data Fragmentation and Increased “Jurisdictional Blindness”

Bridges allow assets to be transferred between networks. In illicit contexts, bridges are used as a tool to break analytical chains: each network requires a separate analytical model, while international data exchange remains fragmented.

Financial-intelligence practice documents the use of bridges for money laundering, including ransomware proceeds. A U.S. Treasury report on DeFi risks highlighted an example of a cross-chain bridge being used to launder substantial volumes of ransomware-related funds, illustrating the scale and systemic nature of the problem.

## 8. Mixers and Enforcement: Sanctions, Criminal Cases, and the Legal Nature of Smart Contracts

Mixers (tumblers) are designed to break the link between input and output transactions and conceal the origin of funds. This is one of the most acute points where privacy, technological autonomy, and criminal–sanctions enforcement intersect.

A notable example from international practice is OFAC’s action against Tornado Cash. In 2022, the U.S. Department of the Treasury (OFAC) placed Tornado Cash on the sanctions list, citing its extensive use for laundering funds, including assets linked to North Korean actors. This became a precedent: the sanctions measure targeted a technological service operating largely as smart-contract infrastructure.

Consequences included:

• the emergence of “sanctions contamination” risks for users and infrastructure counterparties;

• increased criminal-law pressure on developers and protocol supporters;

• legal disputes over whether smart contracts constitute "property" subject to sanctions, reflected in U.S. court practice (including a Fifth Circuit appellate decision addressing the limits of OFAC's authority over smart contracts).

In addition, international enforcement practice has included active operations to shut down mixers and confiscate infrastructure (e.g., actions against Bestmixer.io and others), further increasing risks for users and operators.

## 9. Cyber-Theft Practices and "State-Level" Laundering Pipelines: DeFi as Part of the Chain

DeFi infrastructure is used not only by private criminal networks but also by state or quasi-state actors. Industry analytical reports document the adaptation of laundering techniques, including migration to new services, bridges, and decentralized routing methods.

A prominent example is the Ronin Bridge incident involving the Lazarus Group. Public reports describe how stolen assets were moved and "dissolved" through routes involving obfuscation services and numerous on-chain operations. This illustrates how DeFi and related tools become integral components of a broader laundering pipeline.

## 10. Absence of Mechanisms for Asset Freezing and Recovery: Institutional Asymmetry

DeFi lacks a universal mechanism for the real-time enforcement of court orders. Even when the illicit origin of funds has been established:

• smart contracts continue to execute automatically;

• asset recovery depends on discretionary actions by private actors (exchanges, stablecoin issuers, infrastructure providers);

• the process often takes on a political or reputational character rather than a strictly legal one.

Practice shows that asset recovery is primarily possible through "points of centralization": exchanges, stablecoin issuers, infrastructure providers, and interface developers. However, these points are incomplete and can be easily bypassed through direct interaction with smart contracts.

## 11. Regulatory Attempts to Capture DeFi: The Limits of the "Regulate the Intermediary" Model

International AML/CFT standards (including FATF approaches to virtual assets and VASPs) are based on identifying accountable service providers. In DeFi, this task is complicated by the absence of a clearly identifiable operator.

Current regulatory practice shows several trends:

• pressure on front ends and user interfaces;

• focus on on/off-ramp points;

• expansion of the definition of “service provider” to include developers, administrators, and governance groups;

• sanctions and criminal measures directed at infrastructural nodes (mixers, bridges, facilitators).

## 12. The Political-Economic Dimension of DeFi Use

DeFi is used not only for overtly criminal purposes but also as infrastructure in corporate and economic conflicts. In certain situations, criminal prosecution and sanctions arguments may be used to legitimize economic objectives such as asset redistribution, pressure on counterparties, or the suppression of financial autonomy.

In this context, the key issue is not formal legal qualification but the reconstruction of economic interests, initiators of the process, and control over assets.

## 13. Risks and Consequences for Ecosystem Participants

International practice shows that consequences for participants in DeFi and DAO ecosystems may include:

• sanctions risks (including secondary sanctions and address blacklisting);

• criminal-law risks for developers and infrastructure operators;

• civil and regulatory risks for governance participants;

• technological irreversibility of losses (loss of funds without restitution mechanisms);

• reputational consequences and restricted access to infrastructure.

Enforcement precedents demonstrate a trend toward narrowing the “grey zone” through targeted pressure on centralization points and attempts to expand the legal concept of DAO responsibility.

## 14. Institutional Limits of International Enforcement

Even with highly competent financial-intelligence units and advanced blockchain-analytics tools, structural limitations remain:

• the absence of a unified evidentiary standard;

• fragmentation of jurisdictions and data;

• the lack of a universal enforcement mechanism;

• dependence on private infrastructure decisions and voluntary cooperation.

## 15. Conclusions

DeFi and DAOs have created a new zone of regulatory blindness in which classical AML/CFT and sanctions-control mechanisms become incomplete. In many scenarios, decentralization functions not as innovation but as a systemic instrument for concealment and redistribution of value. International practice — including sanctions against mixers, criminal cases against developers, enforcement actions involving DAOs, and operations to shut down mixing services — confirms a trend toward stricter and broader constructions of liability.

## 16. Recommendations

1. Development of an international legal model of responsibility for DeFi and DAOs, taking into account the roles of developers, administrators, and governance participants.
2. Strengthening oversight of on/off-ramp points and the OTC segment as key nodes of conversion.
3. Institutionalization of evidentiary standards for on-chain analysis and requirements for off-chain corroboration.
4. Coordination of sanctions and criminal-law measures with consideration of the technological specifics of smart contracts and relevant court practice.
5. Establishment of intergovernmental data-sharing protocols regarding bridges, mixers, and infrastructural nodes.

## List of sources and materials used


1. https://www.fatf-gafi.org/en/topics/virtual-assets.html
2. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
3. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf
4. https://home.treasury.gov/news/press-releases/jy0916
5. https://www.europol.europa.eu/media-press/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down
6. https://www.cftc.gov/media/8736/enfookidaoorder060923/download
7. https://www.courtlistener.com/docket/65369411/commodity-futures-trading-commission-v-ooki-dao/
8. https://www.chainalysis.com/blog/2024-crypto-money-laundering/
9. https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/
10. https://www.reuters.com/legal/court-overturns-us-sanctions-against-cryptocurrency-mixer-tornado-cash-2024-11-27/
11. https://www.apnews.com/article/88115029d0a033b7b8b3e3a34dccf00c
12. https://www.reuters.com/business/finance/swiss-german-authorities-shut-down-cryptomixerio-money-laundering-crackdown-2025-12-01/
13. https://apnews.com/article/4f0c402eddec3ffa57eb00df205a2ef4
14. https://argaobservatory.org