ARTICLE

DECENTRALIZED AUTONOMOUS ORGANIZATIONS AND THE ANTI-MONEY LAUNDERING CHALLENGE: RETHINKING GLOBAL FRAMEWORKS FOR A LEADERLESS WORLD

Uri Volovelsky [†] *& Sivan Shlomo Agon* [‡]

ABSTRACT*

Decentralized Autonomous Organizations (DAOs) are blockchain-based entities that operate without centralized management or shareholders, enabling worldwide token holders the option of participating in their governance through self-executing smart contracts. With approximately fifty thousand DAOs controlling over $30 billion in assets, these organizations offer unprecedented efficiency and global collaboration, enabling stakeholders to participate and contribute to the operation of DAOs regardless of their jurisdiction or physical presence. DAOs, however, also present significant legal and regulatory challenges, particularly concerning liability, contractual enforcement, tax obligations, and oversight. Their decentralized and fluid structure makes it substantively difficult for any single country—including powerful actors such as the United States and the European Union—to assert jurisdiction or exercise regulatory authority over such organizations. In addition to governance considerations, the decentralized, pseudonymous, and borderless structure of DAOs may be exploited for unlawful purposes, most notably money laundering.

This Article examines how DAOs, particularly within the decentralized finance sector, facilitate anonymous cross-border transactions that pose novel and significant money laundering risks. By analyzing existing regulatory responses in major jurisdictions including the United States and the European Union, as well as efforts by key international organizations such as the Financial Action Task Force, the International Monetary Fund, and the United Nations, the Article demonstrates that prevailing regulatory frameworks and enforcement models cannot adequately respond to the distinct challenges presented by DAOs. This regulatory vacuum poses significant risks to global financial stability, the integrity of the financial systems, and core national-security interests, including the prevention of sanctions evasion, counterterrorism and proliferation financing, and the deduction and disruption of state-sponsored, cyber-enabled illicit finance. Accordingly,

---

[†] Senior Legal Counsel and Head of the Commercial & Civil Division at the Asset Recovery & Forfeiture Management Office, Guardian General Offices, Israeli Ministry of Justice; Member of the New York Bar. The article is part of a research work that was conducted at Bar-Ilan University within the framework of the requirements for obtaining the degree "Doctor of Philosophy."

[‡] Associate Professor, Bar-Ilan University, Faculty of Law.

* All errors and omissions are solely the authors' responsibility. The authors thank Nizan Geslevich Packin for thoughtful comments and helpful suggestions.

the Article proposes a novel, modular, risk-based, global anti-money laundering framework tailored to DAOs' unique operational realities. The proposed framework aligns with principles of functional equivalence, technological neutrality, and transnational cooperation, offering a more effective means of addressing DAO-related, anti-money laundering risks while preserving space for innovation.

CONTENTS

INTRODUCTION

Decentralized Autonomous Organizations (DAOs) mark a significant departure from traditional organizational models. DAOs operate without centralized authority, leveraging blockchain technology to coordinate activity.[1] These organizations rely on distributed ledger technologies, such as Ethereum, to execute and record transactions transparently and securely. This approach enables DAOs to operate autonomously and make collective decisions through smart contracts that automate functions typically performed by legal or managerial bodies.[2] The distinctive nature of DAOs thus stems from their novel organizational structure, which varies significantly from traditional legal entities in terms of governance and operation.[3] This structural divergence in turn renders the formulation of a universally accepted legal definition for DAOs complex, as their innovative governance mechanisms do not fit neatly into existing legal categories[4]—a challenge that extends to broader questions of regulation, compliance, and enforcement.

Since Vitalik Buterin, Etherum co-founder and computer scientist, first advanced the concept of DAOs in 2016, DAOs have seen a significant rise in popularity,[5] with approximately fifty thousand operating across diverse sectors as of January 2025.[6] From philanthropic initiatives like

---

[1] Blockchain is a digital-ledger technology in which data is stored in blocks that are linked together in a chain. Each block contains records of multiple transactions. Once a block is filled with data, it is sealed and linked to the previous block, creating a chronological chain. The data on the blockchain is decentralized and distributed across many computers, making it highly secure and nearly impossible to alter. *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 131–55 (2018); *see generally* Jill E. Fisch, *DAOs and Corporate Governance, in* FOUNDATIONS OF DECENTRALIZED ORGANIZATIONS: BLOCKCHAIN AND THE FUTURE OF CORPORATE LAW 61 (Kevin Werbach, Eva Micheler & Bianca Kremer eds., 2026).

[2] *See* Lauren H. Scholz, *Algorithmic Contracts*, 20 STAN. TECH. L. REV. 128, 147–48 (2017).

[3] *See* Fisch, *supra* note 1, at 61.

[4] For different approaches regarding the grant of legal recognition to DAOs, *see generally* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, 95 HARV. BUS. REV. 118 (2017); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 338–46 (2017).

[5] Vitalik Buterin is also the founder of the Ethereum network. *See* DJ Pangburn, *The Humans Who Dream of Companies That Won't Need Us*, FASTCOMPANY (Sep. 19, 2015), https://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-.need-them [https://perma.cc/Q7QS-AU9P].

[6] *See* Liam Kelly, *Why Kevin Owocki, the Open Source Guru Who Started Gitcoin, Still Believes in DAOs*, DLNEWS (Jan. 24, 2025), https://www.dlnews.com/articles/defi/why-

Gitcoin DAO and Edu DAO, which supports blockchain education and talent development by connecting student and developer communities with industry participants,[7] to communities that foster networking and collaboration in cultural and creative economies, DAOs are reshaping how collective action is organized and executed. In the financial sector, DAOs are increasingly used to facilitate decentralized finance (DeFi), creating a financial ecosystem free from traditional banking and government oversight.[8] The widespread application of DAOs across diverse fields, together with their rapidly growing membership and substantial assets, underscores their potential to revolutionize various facets of both the digital and physical worlds.[9]

While DAOs continue to rise in popularity, they remain largely unregulated at both the national and international levels. The inherently cross-border nature of DAOs, combined with a globally distributed membership base, highlights the urgent need for robust global regulatory frameworks. Such frameworks, however, are currently absent, resulting in significant gaps in governance and oversight. These gaps, in turn, may be exploited by DAOs and their participants to facilitate illicit activities—most notably, money laundering (ML).

Although ML itself is not a new phenomenon, DAOs introduce distinct complexities tied directly to their decentralized, pseudonymous, and borderless architecture. As this Article will show, existing national and international anti-money laundering (AML) frameworks—originally designed for centralized, accountable intermediaries—struggle to address DAOs' disintermediated structure. For example, DAOs' borderless nature facilitates the global movement of the assets they control, often circumventing traditional AML mechanisms such as know-your-client (KYC) procedures.[10]

---

gitcoin-guru-kevin-owocki-still-believes-in-daos/#:~:text=In%20the%20meantime%2C%20DAOs%20are,growing%20faster%20than%20ever [https://perma.cc/W54D-B359]; EY Global, *How to Navigate Tax and Legal Complexity Associated with DAOs*, ERNEST & YOUNG GLOB. LTD. (Aug. 2, 2023) https://www.ey.com/en_gl/insights/tax/how-to-navigate-tax-and-legal-complexity-associated-with-daos [https://perma.cc/A4Z7-R3VF].

[7] *See* EduDAO, *Funding University Ecosystems*, https://edudao.io/ [https://perma.cc/8AF3-AHPZ] (last visited Feb. 24, 2026).

[8] *See* OECD, WHY DECENTRALIZED FINANCE (DEFI) MATTERS AND THE POLICY IMPLICATIONS 42 (2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/01/why-decentralised-finance-defi-matters-and-the-policy-implications_5f54eead/109084ae-en.pdf [https://perma.cc/XAC6-BVCL] [hereinafter OECD REPORT].

[9] *See* Aiden Slavin & Kevin Werbach, *Decentralization Autonomous Organizations: Beyond the Hype* 3 (World Econ. Forum in Collaboration with the Wharton Blockchain & Digital Asset Project, June 2022), https://www.weforum.org/whitepapers/decentralized-autonomous-organizations-beyond-the-hype/ [https://perma.cc/42SD-HCFZ].

[10] *See* FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 16 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-

This regulatory vacuum poses significant risks to global financial stability and the integrity of the international financial system. As DAOs manage increasingly substantial assets and expand into critical financial services, their exploitation for ML purposes threatens to undermine decades of progress in combating financial crime.[11] Left unaddressed, these vulnerabilities enable actors to use DAOs as conduits for moving illicit funds through parallel financial channels that remain outside effective regulatory and law-enforcement supervision.[12] These risks, moreover, extend beyond financial integrity to implicate core national-security interests.[13] DAOs operating without effective AML controls can undermine states' abilities to enforce sanctions against designated individuals and entities, prevent terrorism financing, protect financial systems from foreign malign influence, and counter cyber-enabled threats.[14] By enabling adversarial governments, sanctioned entities, transnational terrorists, and criminal networks to move and obscure illicit funds, unregulated DAOs

---

VASP.pdf.coredownload.inline.pdf [https://perma.cc/RAW4-XESJ] [hereinafter FATF RISK-BASED APPROACH]

[11] *See* Vladlena Benson Umut Turksen & Bogdan Adamyk, *Dark Side of Decentralised Finance: A Call for Enhanced AML Regulation Based on Use Cases of Illicit Activities*, 32 J. FIN. REG. & COMPLIANCE 80, 87 (2024), https://www.emerald.com/jfrc/article-pdf/32/1/80/9502271/jfrc-04-2023-0065.pdf [https://perma.cc/W3UC-RU64].

[12] *See* U.S. DEP'T TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 30 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [https://perma.cc/F6LA-VJPZ] [hereinafter RISK ASSESSMENT OF DEFI]. While the U.S. Department of the Treasury report does not expressly refer to DAOs, its analysis is directly relevant to DAOs as a functional matter. DAOs commonly operate as governance and control mechanisms for decentralized finance protocols, including those that retain custody over, deploy, or route digital assets through smart contracts. *See id.* at 11–15. To the extent that DAOs exercise *de facto* control over protocol parameters, treasury management, and transaction flows, they form part of the decentralized financial arrangements assessed by the Department. *See id*. at 13. Accordingly, the vulnerabilities identified in the report—particularly the absence of identifiable intermediaries, gaps in anti-money-laundering and countering-financial-terrorism coverage, and challenges for regulatory and law-enforcement supervision, *see id*. at 13—would apply with equal force to DAO-governed financial systems.

[13] U.S. federal policy recognizes that risks associated with the illicit use of digital-asset systems may implicate not only financial integrity but also national-security interests. *See* Exec. Order No. 14,067, 87 Fed. Reg. 14,143 (Mar. 14, 2022) https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [https://perma.cc/T38D-BZ2N]. Although the executive order does not address DAOs specifically, its national-security framing applies to decentralized digital-asset arrangements more broadly. From a functional perspective, this includes DAO-governed financial protocols when they are exploited for illicit purposes.

[14] *See* Heather Y. Zhou, *Regulating Crypto Money Laundering: An Assessment of Current Regulatory Responses and Potential for Technology-Based Solutions*, 8 STAN J. BLOCKCHAIN L. & POL'Y 142, 157 (2025); Georg Lorenz, *Regulating Decentralized Financial Technology: A Qualitative Study on the Challenges of Regulating DEFI with a Focus on Embedded Supervision,* 7 STAN J. BLOCKCHAIN L. & POL'Y 136, 169 (2024); Sarah Calderone, *Tools of the Trade: The Impact of New Mechanisms of the Anti-Money Laundering Act and Corporate Transparency Act on Sanctions Enforcement*, 75 RUTGERS U.L. REV. COMMENTS 163, 169 (2023); Carol R. Goforth, *Just Because They Say It: Does the U.S. Really Have the "First-Ever Comprehensive Framework" for Digital Assets?*, 76 ARK. L. REV. 255, 258 (2023); *see generally* Shlomit Wagman, *Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing*, 14 HARV. NATL. SEC. J. 87 (2022).

compromise foundational security mechanisms upon which modern states depend.[15]

Against this backdrop, the present Article proposes a novel, robust, and adaptable regulatory model to address the ML risks DAOs pose—one specifically tailored to their decentralized structure and cross-border operation and designed to support effective implementation across diverse jurisdictions. In carrying out this endeavor, the Article makes three principal contributions to scholarship on DAOs and AML regulation. First, it provides a systematic analysis of how DAOs' structural features—decentralization, pseudonymity, and cross-border operations—undermine existing global, regional, and national AML frameworks, pioneering a five-category typology of DAO-related ML vulnerabilities. Second, it comparatively assesses DAO-related regulatory responses across major jurisdictions and key international organizations, highlighting persistent structural inadequacies. Third, it proposes a global modular AML framework tailored to DAO ecosystems, grounded in functional equivalence, technological neutrality, and scalable implementation. In so doing, the Article offers a viable and practical pathway for adapting AML enforcement to decentralized entities without stifling innovation.

The Article proceeds as follows: Part I provides relevant background on DAO structures, governance models, and regulatory challenges. It explores the broader DAO ecosystem, with particular emphasis on DeFi, and weighs the advantages and risks associated with DAO operations, including their susceptibility to exploitation for illicit purposes. Part II establishes the theoretical foundations for the Article's analysis by examining traditional AML frameworks and their underlying assumptions. Specifically, it demonstrates how existing AML frameworks are predicated on the existence of centralized intermediaries and clearly identifiable compliance counterparts—assumptions that do not hold in DAO environments. Part III then provides a detailed account of DAO-related ML vulnerabilities, offering concrete examples of how illicit actors exploit decentralized systems. Against this background, Parts IV and V undertake comprehensive analyses of regulatory responses at the national, regional, and international levels. Part IV examines efforts by the United States and the European Union (EU) to address DAO-related AML risks through legislation, enforcement actions, and regulatory guidance. Part V evaluates the responses of key international organizations, including the Financial Action Task Force (FATF), International Monetary Fund (IMF), and United Nations (UN), demonstrating the limitations of existing international coordination mechanisms when applied to borderless, decentralized systems.

---

[15] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 29–30; FIN. ACTION TASK FORCE, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 4–5 (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf [https://perma.cc/9EGJ-4F9J] [hereinafter FATF TARGETED UPDATE].

Part VI presents the Article's novel modular regulatory framework designed specifically for DAO ecosystems. This Part articulates seven interdependent pillars that collectively form a more effective framework for AML oversight while preserving the innovative potential of decentralized organizations. The framework emphasizes technological neutrality, functional proportionality, and transnational coordination, offering a realistic pathway for incremental adaptation within existing institutional structures. Recognizing that the regulatory challenges posed by DAOs represent a fundamental shift in organizational and financial architecture, the Article concludes by arguing that the proposed modular framework offers a principled middle path that preserves flexibility, enforces accountability, and restores coherence to a global AML system strained by the emergence of borderless, decentralized technologies.

I. DAOS: STRUCTURES, GOVERNANCE MODELS, AND REGULATORY CHALLENGES

A. *DAOs: Structure and Main Characteristics*

DAOs represent an innovative organizational design in the digital landscape, fundamentally transforming traditional hierarchical structures. Unlike conventional organizations that rely on centralized frameworks of shareholders, directors, and management teams, DAOs operate through smart contracts—self-executing agreements encoded on the blockchain—that establish their rules and governance mechanisms.[16] Decision-making is collectively carried out by token holders, distributing ownership and control rather than concentrating it in a single entity or board of directors.[17]

At the heart of DAO functionality is a digital ledger that is both immutable and transparent. Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring auditability and security.[18] Every transaction, proposal, and governance action within a DAO is publicly accessible, allowing participants to verify all activities without relying on centralized intermediaries, such as corporate registrars, which are typical of traditional organizations.[19]

---

[16] *See* Fisch, *supra* note 1, at 61; Michael Schillig, *DAOs and the History of Corporate Law*, *in* FOUNDATIONS OF DECENTRALIZED ORGANIZATIONS: BLOCKCHAIN AND THE FUTURE OF CORPORATE LAW 41, 48 (Kevin Werbach, Eva Micheler & Bianca Kremer eds., 2026).

[17] *See* Geoffrey See, Assel Zhanassova & Ashlin Perumall, *Are 'Decentralized Autonomous Organizations' the Business Structures of the Future*, WORLD ECON. F. (June 23, 2022), https://www.weforum.org/stories/2022/06/are-dao-the-business-structures-of-the-future/#:~:text=Decentralized%20Autonomous%20Organizations%20,economic%20rights%20in%20the%20organization [https://perma.cc/68W2-VF9D].

[18] *See* Gail Weinstein, Steven Lofchie & Jason Schwartz, *A Primer on DAOs*, HARV. L. SCH. F. ON CORP. GOVERNANCE (2022), https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/ [https://perma.cc/BB5B-EWWZ].

[19] *See* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 3 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/AV5H-3T5W].

Decentralization, the cornerstone of DAOs, allows them to operate without centralized oversight and replaces traditional governance with code-based coordination.[20] While all DAOs are built on this decentralized foundation, they exhibit varying degrees of decentralization, automation, and legal formalization, and are commonly classified into three structural models: (1) Pure Model DAOs, which operate exclusively through smart contracts without legal registration or off-chain governance structures;[21] (2) Hybrid Model DAOs, which integrate traditional legal entities—such as limited liability companies (LLCs) or foundations—to fulfill regulatory or administrative functions while retaining decentralized decision-making mechanisms;[22] and (3) Legally Incorporated DAOs, which are formally registered under emerging statutory frameworks designed specifically for decentralized organizations.[23]

MolochDAO exemplifies the Pure Model, functioning entirely through token-holder governance without a centralized compliance structure. MakerDAO exemplifies the Hybrid Model: it initially relied on the Maker Foundation for operational and regulatory functions before transitioning toward greater decentralization.[24] Wyoming's DAO LLC law represents the third model, enabling DAOs to incorporate as limited liability companies while preserving blockchain-based governance protocols.[25]

Regardless of the structural model, all DAOs share a common technical element: smart contracts. These self-executing programs automate core governance and operational functions, enhancing efficiency and reducing reliance on human intermediaries.[26] Smart contracts manage rights and operations within DAOs by automating functions such as fund allocation, rule enforcement, and decision-making based on pre-coded protocols.[27] DAOs are thus commonly portrayed as governed by the "rule

---

[20] For different approaches to DAO governance, including quadratic voting, reputation-based voting, and delegated governance, *see Decentralized Finance: (DeFi) Policy-Maker Toolkit*, WORLD ECON. F. 30 (2021) https://www.weforum.org/publications/decentralized-finance-defi-policy-maker-toolkit/ [https://perma.cc/EWN3-EPHY]; Emmanuelle Ganne, *Blockchain for Trade: When Code Needs Law*, 115 AJIL UNBOUND 419 (2021); Werbach & Cornell*, supra* note 4, at 335, 373.

[21] *See* LAW COMM'N, DECENTRALISED AUTONOMOUS ORGANISATIONS (DAOS): A SCOPING PAPER 44 (2024), https://cdn.websitebuilder.service.justice.gov.uk/uploads/sites/54/2026/01/Decentralised-autonomous-organisations-scoping-paper.pdf [https://perma.cc/8R66-ZJ5C].

[22] *See id.* ¶¶ 4.2–4.3.

[23] *See, e.g.,* Wyo. Stat. Ann. §§ 17-31-101 – 17-31-116 (2021).

[24] *See* Brady Dale, *MakerDAO Moves to Full Decentralization; Maker Foundation to Close in 'Months'*, COINDESK (July 20, 2021), https://www.coindesk.com/tech/2021/07/20/makerdao-moves-to-full-decentralization-maker-foundation-to-close-in-months [https://perma.cc/RB83-H2J3].

[25] *See* Wyo. Stat. Ann. §§ 17-31-101 – 17-31-116 (2021).

[26] *See* Slavin & Werbach, *supra* note 9, at 10.

[27] *See id.*; *see also* André Guskow Cardoso, *Decentralized Autonomous Organizations - DAOs: the Convergence of Technology, Law, Governance, and Behavioral Economics*, MIT COMPUTATIONAL L. REP. (2023),

of code" rather than the "rule of law," as their operational logic is embedded in code rather than enforced through traditional legal frameworks.[28]

Within this code-based framework, governance authority in DAOs is distributed through token-based mechanisms. Digital governance tokens serve two primary functions: they operate as a medium of exchange within the DAO ecosystem and, more importantly, function as voting instruments that grant holders the right to propose and vote on protocol changes, engaging them in collective decision-making.[29] Unlike corporate shares recorded in centralized stock ledgers, these tokens are issued and tracked on public blockchains, facilitating pseudonymous forms of control over DAO governance.[30] Prominent examples include Uniswap and MakerDAO, which use native tokens to enable decentralized, on-chain governance.[31]

B. *The DAO Ecosystem: Sectoral Applications, Global Expansion, and the Centrality of DeFi*

The DAO model has experienced significant global growth, measurable across three key dimensions: scale, financial impact, and sectoral diversity. As of January 2025, approximately fifty thousand DAOs were operating globally, with their combined treasuries representing upward of $30 billion.[32] The total monetary assets under DAO governance, including protocol-managed reserves and liquidity pools, exceeded $35 billion.[33] Participation metrics likewise show rapid expansion: DAO membership increased substantially between 2021 and the end of 2025, reaching over eleven million participants holding governance tokens.[34] These trends reflect growing adoption of DAOs as frameworks for coordinating activity in decentralized, globally distributed communities.

---

https://law.mit.edu/pub/decentralizedautonomousorganizations [https://perma.cc/TA8K-YWE8].

[28] *See* Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4 STAN. J. BLOCKCHAIN L. & POL'Y 1 152, 155 (2021); *see* Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH L. J. 487, 489 (2018).

[29] *See*, Zhanassova & Perumall, *supra* note 17; Paul Dylan-Ennis & Donncha Kavanagh, *Hash, Bash, Cash: Decentralized Autonomous Organizations (DAOs) as a New Form of Democratic Organization, in* DECENTRALIZED AUTONOMOUS ORGANIZATIONS: INNOVATION AND VULNERABILITY IN THE DIGITAL ECONOMY 23, 30 (Sven Van Kerckhoven & Chohan W. Usman eds., 2024).

[30] *See* Weinstein, Lofchie & Schwartz, *supra* note 18.

[31] *See* Adam Paul, *Governance Tokens in Crypto: Definition, Function, and Examples*, SDLC CORP (Aug. 25, 2025), https://sdlccorp.com/post/governance-tokens-in-crypto-definition-function-and-examples [https://perma.cc/UY8D-VSMR].

[32] *See* Kelly, *supra* note 6; *DAO Landscape 2024*, INO (Feb. 6, 2024), https://internetnative.org/dao-landscape [https://perma.cc/ME6A-B73P].

[33] *See* DeepDAO, *DAO Analytics & Statistics Dashboard*, https://deepdao.io/organizations [https://perma.cc/8UFN-8ALK] (last visited Dec. 11, 2025).

[34] *See id.*

DAOs have further expanded into a wide range of sectors such as social coordination, philanthropy, media, and digital ownership. Notable examples include ConstitutionDAO, which raised over $40 million in cryptocurrency to bid on a copy of the U.S. Constitution;[35] ApeDAO, which manages NFT assets for the Bored Ape community;[36] Big Green DAO and Ukraine DAO, which apply decentralized governance to grant-making and humanitarian support;[37] and content-focused DAOs like Mirror, which experiment with decentralized publishing.[38]

Within this increasing functional diversity, a major area of DAO activity is DeFi—a sector that leverages blockchain technology to provide financial services such as trading, lending, asset issuance, derivatives, and asset management without traditional financial intermediaries such as banks or brokerages.[39] DeFi protocols employ smart contracts to autonomously match lenders and borrowers, issue loans, and set interest rates algorithmically.[40] DeFi DAOs offer several potential benefits compared to traditional centralized finance. DeFi protocols enable global participation without traditional barriers such as minimum account balances, credit history requirements or geographical restrictions.[41] Additionally, DeFi's transparency through public blockchains allows participants to verify transactions and protocol operations independently and immediately, enhancing trust without relying on centralized authorities.[42] The automation of financial services significantly reduces operational costs by eliminating intermediaries, potentially offering more

---

[35] *See* Karen Matthews, *Rare First Printing of US Constitution Sells for Record $43M*, AP NEWS (Nov. 19, 2021), https://apnews.com/article/cryptocurrency-technology-lifestyle-business-arts-and-entertainment-b0ab721a52cf20f2dc1a923f2dae3347 [https://perma.cc/6X5H-A4KP].

[36] *See* Matthew Fox, *ApeDAO Token Is on the Rise After Community Vote to Liquidate Its Collection of NFTs Passes and Auction Process Begins*, BUS. INSIDER (Feb. 10, 2022), https://markets.businessinsider.com/news/currencies/apedao-token-community-votes-liquidate-nft-collection-cryptopunks-bored-apes-2022-2 [https://perma.cc/5EY8-XW33].

[37] *See* Ornella Hernández, *UkraineDAO Raises over $6M via NFT Sale to Aid Ukrainian Citizens*, COINTELEGRAPH (Mar. 3, 2022), https://cointelegraph.com/news/ukraine-dao-raises-over-6m-via-nft-sale-to-aid-ukrainian-citizens [https://perma.cc/8VU5-GBXV]; *Big Green DAO*, BIG GREEN DAO https://dao.biggreen.org/home [https://perma.cc/SD9C-DDCV] (last visited Apr. 10, 2026).

[38] *See Paragraph Spotlight Series,* PARAGRAPH https://paragraph.com/@0x4af950bc0844b1cd0fd9e2943f5378f2e133f6f2 [https://perma.cc/7SDM-A75U] (last visited Feb. 25, 2026).

[39] *See* OECD REPORT, *supra* note 8, at 42–45.

[40] *See* EUR. SYSTEMIC RISK BD. TASK FORCE ON CRYPTO-ASSETS & DECENTRALISED FIN., CRYPTO-ASSETS AND DECENTRALISED FINANCE: SYSTEMIC IMPLICATION AND POLICY OPTIONS 10 (2023), https://www.esrb.europa.eu/pub/pdf/reports/esrb.cryptoassetsanddecentralisedfinance202305~9792140acd.en.pdf?853d899dcdf41541010cd3543aa42d37 [https://perma.cc/N5T8-C4N5] [hereinafter CRYPTO-ASSET REPORT].

[41] *See* Eli Talmor, *Can We Save Defi from Being Centralized*, FINEXTRA (July 3, 2024), https://www.finextra.com/blogposting/27863/can-we-save-defi-from-being-centralized [https://perma.cc/US3D-FCZD].

[42] *See Decentralized Finance (DeFi) vs. Traditional Finance: A Comparative Analysis,* COINMETRO (Dec. 5, 2025), https://coinmetro.com/learning-lab/decentralized-finance-vs-traditional-finance [https://perma.cc/XD9G-SZVL].

competitive rates for users compared to those offered by traditional financial services.[43] This efficiency is further enhanced by the interoperability among different DeFi protocols, allowing seamless interaction and composability that traditional financial systems cannot match.[44]

DAOs govern many leading DeFi protocols and collectively hold treasuries valued at approximately $25 billion as of mid-2025.[45] These treasuries typically consist of funds accumulated through protocol fees, token issuance, or community contributions.[46] For example, Uniswap, a decentralized exchange platform (DEX),[47] is governed by Uniswap DAO, whose participants, holding UNI tokens, vote on protocol upgrades and fee parameters.[48] The treasury value of Uniswap reached a record high of $2.2 billion in crypto in 2022.[49] Other notable DeFi DAOs include Aave,[50] Compound,[51] Curve,[52] and SushiSwap.[53] In each case, the DAO structure ostensibly decentralizes control over what is essentially a financial service. Instead of a corporation managing the exchange or lending platform, token holders of the DAOs propose and vote on changes, while the day-to-day operations are automated by smart contracts.

---

[43] *See* Rakesh Sharma, *Understanding Decentralized Finance (DeFi): Basics and Functionality*, INVESTOPEDIA (Dec. 31, 2025), https://www.investopedia.com/decentralized-finance-defi-5113835 [https://perma.cc/AV5Q-7VUC].

[44] *See* DE FILIPPI & WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE, *supra* note 1, at 131–50.

[45] *See Top Governance Protocols 2025: How DAOs Manage Power & Scale*, LAMPROS TECH (Sep. 30, 2025), https://lampros.tech/blogs/top-governance-protocols-2025 [https://perma.cc/D6HK-UL88].

[46] *See* Ellen Naudts, *The Future of DAOs in Finance: In Need for a Legal Status* 9, 12 (Eur. Cent. Bank, Occasional Paper Series No. 331, 2023), https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf [https://perma.cc/G9MW-GDDB].

[47] A decentralized exchange is a blockchain-based platform that uses smart contracts to enable peer-to-peer trading of digital assets without a central intermediary or custodial control over user funds. *See What Is a DEX (Decentralized Exchange)?*, CHAINLINK, https://chain.link/education-hub/what-is-decentralized-exchange-dex [https://perma.cc/D83V-W8XY] (last updated Aug. 14, 2024).

[48] Uniswap manages approximately $3.9 billion in assets and facilitate a monthly trading volume of approximately $38 billion, all without relying on traditional financial intermediaries. *See* Arnold Kirimi, *Uniswap: $38 Billion Volume, Big Jump in Price, What's Behind the Rise*, THE COIN REPUBLIC (Dec. 8, 2024), http://thecoinrepublic.com/2024/12/08/uniswap-38-billion-volume-big-jump-in-price-whats-behind-the-rise/ [https://perma.cc/8TFK-N25H].

[49] *See* Jamie Redman, *Decentralized Autonomous Organization Statistics Show $10 Billion Is Held by DAO Treasuries,* BITCOIN.COM NEWS (June 10, 2022), [https://perma.cc/4XKY-575S].

[50] *See Aave App*, https://aave.com/ [https://perma.cc/Z69A-XPYL] (last visited Feb. 25, 2026).

[51] *See Compound Finance*, COMPOUND LABS, INC., https://compound.finance/ [https://perma.cc/WJ2W-ST3J] (last visited Feb. 25, 2026).

[52] *See Curve DAO*, https://www.curve.finance/dex/ethereum/swap [https://perma.cc/SF2N-JXD5] (last visited Feb. 25, 2026).

[53] *See Sushi Exchange*, https://www.sushi.com/ethereum/swap [https://perma.cc/LAN6-43X7] (last visited Feb. 25, 2026).

C. *Advantages and Risks Associated with the Operation of DAOs*

The DAO model is frequently described as offering several advantages over traditional corporate and organizational structures.[54] The first advantage lies in the fact that DAOs provide a novel organizational structure that prioritizes decentralized ownership accompanied by community-driven governance, while traditional corporate governance models centralized in a board or managerial hierarchy.[55] This decentralization reshapes governance incentives: Instead of management acting as agents for shareholders, participants collectively determine strategic direction, reducing agency costs and enabling governance outcomes that reflect the preferences of the wider community rather than solely the interests of controlling stakeholders.[56]

Second, because DAO data is recorded on the blockchain, participants have direct and immediate access to all relevant information, fostering trust and transparency. This feature further reduces reliance on intermediaries, streamlining operations and lowering transaction costs.[57] For example, decisions requiring multi-step corporate procedures in traditional organizations can be approved by a token-holders' vote and immediately implemented on-chain. Token holders can thus directly influence the DAO's direction, minimizing agency problems common in hierarchical governance structures.[58]

Third, DAOs are inherently inclusive, allowing broad participation without the structural barriers found in traditional corporate structures. Traditional corporations are often limited by participant quotas, accreditation requirements, and nationality-based restrictions.[59] In contrast,

---

[54] *See, e.g.*, WORLD ECON. F., DAOS FOR IMPACT (2023), https://www3.weforum.org/docs/WEF_DAOs_for_Impact_2023.pdf [https://perma.cc/5XKZ-7EGS].

[55] *See* Jungsuk Han, Jongsub Lee & Tao Li, *A Review of DAO Governance: Recent Literature and Emerging Trends*, 91 J. CORP. FIN. 1, 7–8 (2025).

[56] *See* Wright, *supra* note 28, at 152, 156, 160; *see generally* Bokolo Anthony Jr., *Toward a Collaborative Governance Model for Distributed Ledger Technology Adoption in Organizations*, 42 ENV'T SYS. & DECISIONS 276 (2022).

[57] *See* Wright, *supra* note 28, at 156.

[58] *See* OECD, THE TOKENISATION OF ASSETS AND POTENTIAL IMPLICATIONS FOR FINANCIAL MARKETS 43 (2020), https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/03/the-tokenisation-of-assets-and-potential-implications-for-financial-markets_370f9853/83493d34-en.pdf [https://perma.cc/T2TM-HY7V] [hereinafter THE TOKENISATION OF ASSETS]; Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (Mar. 20, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [https://perma.cc/BY3V-SEJD] (unpublished manuscript); SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 3 (2017), https://www.sec.gov/files/litigation/investreport/34-81207.pdf [https://perma.cc/2WGS-H7UL] [hereinafter SEC ACT REPORT].

[59] *See, e.g.*, 15 U.S.C. §§ 77d(a)(2), 77e (2022) (limiting participation in certain private offerings to accredited investors and imposes numerical limits on non-accredited

DAOs enable participation irrespective of geographical location, nationality, and legal status, thus promoting financial and governance inclusivity.[60]

Fourth, DAOs can achieve greater efficiency, resilience, and innovation through automation and decentralization.[61] Smart contracts automate administrative functions such as fund disbursement and reward distribution, reducing overhead costs.[62] The absence of centralized control points also makes DAOs more resistant to censorship or shutdowns, as operations distributed across blockchain networks cannot be easily terminated by targeting a single entity.[63] Moreover, this decentralized infrastructure enables rapid experimentation with novel governance frameworks: models such as liquid democracy and quadratic voting can be encoded directly into smart contracts and iteratively refined through community input, allowing for dynamic institutional evolution.[64]

Balanced against these advantages are several disadvantages and practical problems. The foremost concern is the lack of clear accountability structures. DAOs often lack identifiable individuals responsible for oversight or regulatory engagement, which can make it difficult to ensure consistent operations, legal compliance, and timely responses to regulatory inquiries.[65] This reality is supported by the finding, published as part of the European Central Bank's occasional paper series, that DAOs typically lack the clear and enforceable lines of responsibility found in traditional regulated institutions.[66] One significant consequence of this lack of accountability is that when DAOs are exploited—whether through a code vulnerability resulting in financial loss or through illicit uses such as ML—it is often unclear who, if anyone, bears legal responsibility.

Another major challenge concerns effective governance. Decentralized governance can be slow, contentious, and susceptible to low

---

purchasers); Comm. on Foreign Inv. in the U.S. (CFIUS), *Overview of the Committee on Foreign Investment in the United States*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/W4EY-4X2P] (last visited Feb. 7, 2026) (describing restrictions on foreign participation in U.S. corporate transactions for national security reasons).

[60] *See* Brynly Llyr, *Re-envisioning Corporations: How DAOs and Blockchain Can Improve the Way We Organize*, WORLD ECON. F. (Feb. 8, 2022), https://www.weforum.org/stories/2022/02/re-envisioning-corporations-how-daos-and-blockchain-can-improve-the-way-we-organize/ [https://perma.cc/6U9V-W6FE].

[61] *See* Wright, *supra* note 28, at 153, 155.

[62] *See id*. at 161.

[63] *See id*. at 172.

[64] *See* Llyr, *supra* note 60.

[65] *See* Fisch, *supra* note 1, at 61; U.S. GOV'T ACCOUNTABILITY OFF., LEGISLATIVE AND REGULATORY ACTIONS ARE NEEDED TO ENSURE COMPREHENSIVE OVERSIGHT OF CRYPTO ASSETS 1, 24 (2023), https://www.gao.gov/assets/gao-23-105346.pdf [https://perma.cc/F5C8-SS3A] (explaining that blockchain systems operate "without a central authority" and that the removal of intermediaries raises questions about "who is responsible for ensuring compliance with law and regulation").

[66] *See* Naudts, *supra* note 46, at 4.

participation or capture by small groups.[67] Many DAOs have thousands of token holders, but only a fraction actively votes on proposals.[68] This low participation, combined with concentrated token holdings, allows effective control to rest with a minority.[69]

Additionally, the open membership of DAOs makes them vulnerable to governance attacks—hostile takeovers through buying up tokens or exploiting low voter turnouts. Several DAOs and DeFi protocols, including the Beanstalk Protocol, have experienced such attacks, with attackers manipulating governance to take control of the DAO's funds.[70] A recent study has likewise shown that large token holders, referred to as "whales," can coordinate or sell votes in ways that enable similar governance takeovers, a risk largely absent in traditional corporate structures with established shareholder safeguards.[71]

DAOs also face significant cybersecurity risks.[72] Smart contracts, although transparent, can contain exploitable vulnerabilities. The infamous 2016 "DAO" (an early decentralized venture fund known as "The DAO") was drained of approximately $60 million after an attacker exploited a critical code flaw—an incident that ultimately prompted a hard fork of the Ethereum blockchain.[73]

Furthermore, legal and regulatory uncertainty plagues DAOs. Traditional legal and regulatory frameworks assume identifiable persons—natural or corporate—capable of being held legally accountable. Absent a tailored legal wrapper,[74] a DAO operates not as a registered entity but as an amorphous association of token holders governed by code. This creates profound uncertainty regarding how existing laws, including not only

---

[67] *See* Olivier Rikken, Marijn Janssen & Zenlin Kwee, *Governance Challenges of Blockchain and Decentralized Autonomous Organizations*, 24 INFO. POLITY 397, 397–98, 401, 409–10 (2019).

[68] *See generally* Xuan Liu, *The Illusion of Democracy—Why Voting in Decentralized Autonomous Organizations Is Doomed to Fail*, NYU L. & ECONS. Research Paper No. 24–13 (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4441178 [https://perma.cc/R9KN-WH5F].

[69] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 29–30.

[70] *See id*.

[71] *See* Wulf A. Kaal, *Blockchain-Based Corporate Governance*, 4 STAN. J. BLOCKCHAIN L. & POL'Y 1, 12–14 (2021); Joseph Lee & Alexandre Fricotté, *DAO Token Transferability: Property, Contract, and Technology*, EURO. J. RISK REGUL. 1, 1, 9 (2025).

[72] *See* Slavin & Werbach, *supra* note 9, at 10.

[73] *See* Ilya Grishchenko, Matteo Maffei & Clara Schneidewind, *A Semantic Framework for the Security Analysis of Ethereum Smart Contracts*, ARXIV 1, 15 (Apr. 23, 2018), https://arxiv.org/pdf/1802.08660 [https://perma.cc/92GN-D29S].

[74] A "legal wrapper" refers to the use of an established legal form—such as a corporation, limited liability company, or foundation—to anchor a DAO within existing legal and regulatory systems by providing a legally cognizable entity through which rights, obligations, and compliance responsibilities may be assigned. *See* Chris Brummer & Rodrigo Seira, Legal Wrappers and DAOs 4, 6 (May 30, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4123737 [https://perma.cc/BZS3-C7UQ] (unpublished manuscript).

contract and tax law but also securities and AML regulations, apply to DAOs.

A particularly acute manifestation of this uncertainty concerns DAOs' legal classification. As noted, DAOs operate without centralized leadership, formal incorporation, or a fixed legal domicile.[75] This structural indeterminacy hinders consistent legal recognition across jurisdictions and complicates efforts to develop a uniform regulatory framework. Attempts to analogize DAOs to partnerships, unincorporated associations, or corporate entities have proven inadequate, given their autonomous operation through smart contracts and decentralized governance.[76] Some jurisdictions have begun experimenting with bespoke legal forms—notably, Wyoming's DAO LLC statute—but such initiatives remain limited, fragmented, and jurisdiction-specific, underscoring the broader challenge of integrating DAOs into conventional legal taxonomies.[77]

Finally, the blockchain technology that underpins DAOs enables a global presence that transcends borders, complicating enforcement of existing legal frameworks. The sale and purchase of governance tokens occurs online through DEXs and other trading platforms. Yet, national regulatory approaches to these platforms remain fragmented and underdeveloped, creating legal uncertainty for DAO participants and hindering effective regulatory enforcement.[78]

Indeed, as the rest of this Article explains, these deficiencies make DAOs particularly vulnerable to ML. The combination of pseudonymity, automation, and the absence of intermediaries enables illicit actors to exploit DAOs for ML schemes while evading regulatory oversight. Even DAOs not engaged in financial services may facilitate illicit flows through anonymous fund contributions, unrestricted cross-border transfers, and minimal compliance controls.[79] The absence of intermediaries removes the enforcement points through which sanctions, export controls, and counter-terrorism financing measures, for example, ordinarily operate, thereby

---

[75] *See* Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679–80, 685 (2019); David J. Shakow, *The Tao of the DAO: Taxing an Entity that Lives on a Blockchain*, 160 TAX NOTES 929, 932, 940 (2018).

[76] *See generally* Vanessa V. Collao, Decentralized(?), but Far from Disorganized: A Comparative Analysis of Legal Wrappers and the Evolving Structure of DAOs (Feb. 18, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5143035 [https://perma.cc/5AXY-BHLK] (unpublished manuscript).

[77] *See* Stefanie Boss, *DAOs: Legal and Empirical*, AMSTERDAM L. SCH. Research Paper No. 2021–217 1, 5 (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4503234 [https://perma.cc/7294-AWUY].

[78] *See* Tom Barbereau & Balázs Bodó, *Beyond Financial Regulation of Crypto-Asset Wallet Software: In Search of Secondary Liability*, 49 COMP. L. & SEC. REV. 1, 3, 10–11 (2023), https://www.sciencedirect.com/science/article/pii/S0267364923000390 [https://perma.cc/2GLM-U37X].

[79] *See* Dirk A. Zetzsche, Douglas W. Arner & Ross Buckley, *Decentralized Finance (DeFi)*, 6(2) J. FIN. REG. 172, 174, 184, 192 (2020); Nakul R. Padalkar, *Unveiling the Digital Shadows: Exploring the Role of Technology in Illicit Financial Flows*, 11 IMF STATISTICAL F.: MEASURING MONEY ON THE DIGITAL AGE 1–2, tbl. 1 (2023), https://www.imf.org/-/media/files/news/seminars/2023/11th-stats-forum/session-iii-nakul-r-padalkar.pdf [https://perma.cc/8BZT-Z94D].

amplifying ML risks with considerable implications for financial system integrity and national security.[80] Illicit actors can exploit DAO characteristics—including automation, distributed governance, and cross-border liquidity—to fragment transactional traces and evade detection across multiple jurisdictions, creating significant challenges for existing AML frameworks.[81]

To understand why DAOs present such acute regulatory difficulties, it is necessary to examine the foundational architecture and assumptions on which global AML regimes are built and assess whether existing AML frameworks remain effective or whether new approaches are required to address DAOs' unique ML challenges and implications. These tasks are undertaken in respective, consecutive steps in the Parts that follow.

II. THE REGULATORY ARCHITECTURE OF ANTI-MONEY LAUNDERING: FOUNDATIONS, FRAMEWORKS, AND ASSUMPTIONS

ML involves concealing the origins of illicit proceeds to make them appear legitimate.[82] Traditionally, this practice unfolds in three stages: placement, layering, and integration.[83] In the placement stage, criminal funds enter the legitimate financial system, often through deposits or asset purchases. In the layering stage, a series of transactions—frequently cross-border or multiple-account—obscures the funds' origins and complicates tracing. Finally, in the integration stage, "cleaned" money is reintegrated into the economy, appearing legitimate. Contemporary AML frameworks are built around addressing each of these three stages of ML.[84]

---

[80] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 30.

[81] *See* Alex O'Neill, *Upholding North Korea Sanctions in the Age of Decentralised Finance*, RUSI (Mar. 26, 2024), https://www.rusi.org/explore-our-research/publications/occasional-papers/upholding-north-korea-sanctions-age-decentralised-finance [https://perma.cc/AS9L-PM6G].

[82] *See* FIN. ACTION TASK FORCE, FATF GUIDANCE: NAT'L MONEY LAUNDERING & TERRORIST FIN. RISK ASSESSMENT 23 (2013), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/National_ML_TF_Risk_Assessment.pdf.coredownload.inline.pdf [https://perma.cc/6D7Z-EWS6]; FIN. ACTION TASK FORCE, FATF REPORT: MONEY LAUNDERING AND TERRORIST FINANCING IN THE ART AND ANTIQUITIES MARKET 3, 23 (2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.pdf.coredownload.pdf [https://perma.cc/9CM3-3JRR].

[83] *See* Svenja Berg & Killian J. McCarthy, *An Introduction to the Challenges of Money Laundering*, *in* THE MONEY LAUNDERING MARKET: REGULATING THE CRIMINAL ECONOMY 3, 10–11 (Killian J. McCarthy ed., 2023), https://www.cambridge.org/core/books/abs/money-laundering-market/an-introduction-to-the-challenges-of-money-laundering/868DD4BF8CB07628203F64D746C9DBFE [https://perma.cc/9UAQ-Y2PA].

[84] *See, e.g.*, *Money Laundering*, U.N. OFF. ON DRUGS & CRIME https://www.unodc.org/unodc/en/money-laundering/overview.html [https://perma.cc/C7AL-HV8U] (last visited Dec. 11, 2025); *Frequently Asked Questions: Money Laundering*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-

Although ML has existed for centuries, modern legal and regulatory frameworks to combat it began to emerge in the 1970s, driven by rising concerns over organized crime, national-security threats including terrorist-financing, and the exploitation and destabilization of financial systems and institutions more generally.[85] In the decades since, AML regulation has progressively developed and expanded at both the national and international levels. Taken together, these efforts seek to combat financial crimes, protect national security interests, and safeguard the integrity of the global financial system.

At the international level, the establishment of the Basel Committee on Banking Supervision (the Committee) in 1974 was one of the earliest milestones in the development of AML principles.[86] While initially focused on prudential banking regulation, the Committee became increasingly engaged in AML oversight. Its 2001 report, *Customer Due Diligence for Banks*, emphasized customer identification, risk management, and transaction monitoring as foundational components of AML compliance.[87] A more comprehensive regulatory response emerged in 1989 with the establishment of the FATF by the Group of Seven (G7). The FATF was mandated to develop and promote global AML standards and to foster international coordination.[88]

The FATF issued its first set of forty recommendations in 1990 (the Recommendations),[89] subsequently revised several times, that provide a foundational blueprint for national AML frameworks. Among other things, the Recommendations call for the criminalization of ML, the implementation of customer due-diligence procedures, and the establishment of mechanisms for international cooperation and information sharing. Although the FATF Recommendations do not constitute binding

---

tab [https://perma.cc/PH6K-6MAA] (last visited Dec. 11, 2025); Div. of Fin. Insts. Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual: Money Laundering Overview*, FFIEC, https://bsaaml.ffiec.gov/manual/Introduction/01 [https://perma.cc/QX2U-6S4X] (last visited Dec. 11, 2025).

[85] *See* Nizan G. Packin & Uri Volovelsky, *Digital Asset, Anti-Money Laundering, and Counter Financing Terrorism: An Analysis of Evolving Regulations and Enforcement in the Era of NFTs, in* THE CAMBRIDGE HANDBOOK OF LAW AND POLICY FOR NFTS 78, 78-79 (Nizan G. Packin ed., 2024).

[86] For a historical review of the Basel Committee, *see History of the Basel Committee*, BANK FOR INT'L SETTLEMENTS, https://www.bis.org/bcbs/history.htm [https://perma.cc/6HK2-EFRJ] (last visited Dec. 11, 2025).

[87] *See generally* BASEL COMM. ON BANKING SUPERVISION, CUSTOMER DUE DILIGENCE FOR BANKS (2001), https://www.bis.org/publ/bcbs85.pdf [https://perma.cc/4XS8-J58J].

[88] *History of the FATF*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html [https://perma.cc/AQR5-EVUZ] (last visited Dec. 11, 2025).

[89] *See generally* FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf [https://perma.cc/8D65-9TAY] [hereinafter FATF INTERNATIONAL STANDARDS]; *see also* FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH: THE BANKING SECTOR (2014), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf [https://perma.cc/P6HD-3WDU].

international law, they operate as soft-law standards that states are expected to implement through domestic legislation and regulation.[90] The FATF also developed a mutual evaluation mechanism to assess both the legal adoption and practical implementation of its standards by FATF member countries.[91]

Beyond the FATF's foundational framework, additional global initiatives have reinforced this international regulatory architecture. These include, for example, the 2000 UN Convention Against Transnational Organized Crime, which established a legal framework to facilitate international cooperation on financial crime,[92] and UN Security Council Resolution 1373 following the 9/11 terrorist attacks, which obligated states to criminalize terrorist financing and implement robust financial oversight mechanisms.[93]

At the regional level, the EU has played a central role in formulating and harmonizing AML regulation across member states. A series of AML Directives (collectively, AMLDs)[94]—expanded the scope of regulated entities, strengthened customer due diligence obligations, and institutionalized risk-based regulation. More recently, the EU adopted the Markets in Crypto-Assets Regulation (MiCA), which establishes a

---

[90] *See, e.g.*, *The Financial Action Task Force*, FINMA, https://www.finma.ch/en/finma/international-activities/policy-and-regulation/fatf/ [https://perma.cc/SA87-KGC9] (last visited Dec. 11, 2025); FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf?nocache=true [https://perma.cc/N84K-QYB4] [hereinafter FATF RECOMMENDATIONS]; *see also* James T. Gathii, *The Financial Action Task Force and Global Administrative Law*, Loyola U. Chi., Sch. L.: L. eCommons 1–5 (2010), https://lawecommons.luc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1410&context=facpubs [https://perma.cc/ZWP3-F4CW].

[91] *See Mutual Evaluations*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/en/topics/mutual-evaluations.html [https://perma.cc/5CVQ-BZ6Z] (last visited Dec. 11, 2025).

[92] *See* United Nations Convention Against Transnational Organized Crime, 2255 U.N.T.S. 209 (Nov. 15, 2000).

[93] *See* S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sep. 28, 2001).

[94] *See, e.g.*, Directive 2005/60/EC, of the European Parliament and of the Council of 26 October 2005 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, 2005 O.J. (L 309) 15; Directive 2015/849/EC of the European Parliament and the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141) 73; Directive (EU) 2018/843 of the European Parliament and the Council of 30 May Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU, 2018 O.J. (L 156) 43; Directive 2019/1153 of the European Parliament and of the Council of 20 June 2019 Laying Down Rules Facilitating the Use of Financial and other Information for the Prevention, Detection, Investigation or Prosecution of Certain Criminal Offences, and Repealing Council Decision 2000/642/JHA, 2019 O.J. (L 186) 122.

comprehensive regulatory framework for digital assets, including enhanced AML requirements for crypto-asset service providers.[95]

Across these international regimes, AML enforcement rests on several core operational pillars. Chief among these is customer due diligence, which requires financial institutions to identify and verify customers' identities, assess the nature of the business relationship, and determine the purpose of transactions.[96] Second, institutions must conduct ongoing transaction monitoring and submit suspicious activity reports to national Financial Intelligence Units when anomalies are detected.[97] The effectiveness of these monitoring and reporting obligations, in turn, depends on qualified compliance personnel and institutional infrastructure capable of interpreting transaction behavior and reporting it to the pertinent authorities. A third pillar is recordkeeping, which obliges financial institutions to maintain comprehensive documentation on customer accounts, transaction histories, and due-diligence processes.[98] Finally, modern AML systems are anchored in a risk-based approach, whereby institutions are expected to allocate resources in proportion to the risk associated with specific products, services, clients, or jurisdictions.[99]

Parallel to these international efforts, national jurisdictions have developed their own AML infrastructures. In the United States, the Department of the Treasury—through the Financial Crimes Enforcement Network (FinCEN)—implemented a series of regulatory frameworks beginning with the 1970 Bank Secrecy Act (BSA).[100] The BSA established foundational requirements for reporting, recordkeeping, and customer due diligence.[101] These obligations were expanded by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001,[102] which strengthened surveillance and cross-border cooperation mechanisms, and by the Anti-Money Laundering Act of 2020,[103] which enhanced beneficial ownership transparency and broadened regulatory oversight of virtual asset service providers (VASPs). Over time, U.S. regulators have extended AML

---

[95] *See, e.g.*, Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, and Amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, O.J. (L 150) 40 [hereinafter MiCA].
[96] *See* FATF INTERNATIONAL STANDARDS, *supra* note 89, at 14.
[97] *See* FATF RECOMMENDATIONS, *supra* note 90, at 15–16 (Recommendation 11).
[98] *See id*.
[99] *See id*. at 10, 14–16, 19 (Recommendations 1, 10, 11, and 20); *see also* BASEL COMM. ON BANKING SUPERVISION, SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND FINANCING OF TERRORISM (2014, rev. 2020), https://www.bis.org/bcbs/publ/d505.pdf [https://perma.cc/W9WA-G2FA].
[100] *See* Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-1959, 31 U.S.C. §§ 5311-5332).
[101] *See* 31 U.S.C. § 5311 (2026).
[102] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[103] *See* Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, §§ 6001-6511, 134 Stat. 3388, 4547-633 (2021).

compliance obligations to a wide range of entities, including banks, securities firms, casinos, and money services businesses.[104]

Notwithstanding their varied institutional forms and jurisdictional contexts, these and other AML frameworks—whether international, regional, or national—rest on several foundational assumptions: that financial entities have identifiable legal controllers, that participants can be verified through customer due diligence, that transactions can be monitored and reported by regulated intermediaries, and that enforcement mechanisms can reach accountable parties within defined jurisdictions.[105] DAOs, by design, challenge each of these assumptions.

III. EXPLOITING DECENTRALIZATION: DAO VULNERABILITIES AND MONEY LAUNDERING TECHNIQUES

Building on this structural tension, this Part examines how DAOs can be exploited for ML by systematically undermining those assumptions through five core vulnerabilities. First, DAOs' structural design lacks traditional AML controls and centralized oversight because decentralization and pseudonymity make them difficult to regulate under existing AML frameworks. Second, technical exploits—such as smart contract manipulation—enable automated laundering with minimal detection. Third, token-based governance systems can be hijacked to legitimize illicit fund transfers. Fourth, cross-chain interoperability allows assets to move across blockchain networks, obscuring their origin. Finally, cross-jurisdictional challenges, particularly regulatory arbitrage, enable DAOs to exploit gaps between jurisdictions with inconsistent AML enforcement.[106] Together, these vulnerabilities expose systemic weaknesses in national and international AML regimes by undermining core AML controls, including customer due diligence, transaction monitoring, and enforcement through accountable intermediaries. Recent enforcement cases underscore the difficulty of applying existing legal frameworks to DAO-based activity.[107]

---

[104] *See, e.g.*, FIN. ACTION TASK FORCE, VULNERABILITIES OF CASINOS & GAMING SECTOR 18–19, 31, 33, 45 (2009), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf.coredownload.pdf [https://perma.cc/6Z4H-L9BP]; *see also Anti-Money Laundering / Countering The Financing Of Terrorism (AML/CFT)*, FDIC: BANKER RES. CTR. https://www.fdic.gov/banker-resource-center/anti-money-laundering-countering-financing-terrorism-amlcft [https://perma.cc/XL2X-MJJS] (last visited May 3, 2026).
[105] *See, e.g.*, FATF RECOMMENDATIONS, *supra* note 90, at 7, 14–16, 24–25, 28, 49, 65.
[106] *See Lessons from the Wormhole Exploit: Smart Contract Vulnerabilities Introduce Risk; Blockchains' Transparency Makes It Hard for Bad Actors to Cash Out*, CHAINALYSIS (Feb. 3, 2022), https://www.chainalysis.com/blog/wormhole-hack-february-2022/ [https://perma.cc/L887-JH48].
[107] *See id*.

A. *Inherent Structural Vulnerabilities*

DAOs' structural architecture—characterized by smart contract automation, pseudonymous participation, and distributed governance—creates concrete vulnerabilities that ML can exploit. Whereas banks and brokerages operate through centrally organized, legally accountable structures, DAOs function without a single point of control or identifiable intermediary.[108] This architectural divergence eliminates the regulatory leverage that traditional AML regimes exercise through accountable gatekeepers.[109] The absence of such intermediaries prevents effective implementation of customer due diligence, transaction monitoring, and suspicious activity reporting—the foundational mechanisms of modern AML enforcement.[110]

A prominent example is the February 2022 Wormhole Bridge exploit, in which an attacker stole approximately $320 million by exploiting a flaw in the smart contract logic of a cross-chain bridge.[111] Although Wormhole presented itself as decentralized, its infrastructure included centralized elements such as a guardian network and active maintenance by Jump Crypto.[112] The attacker exploited this vulnerability to mint 120,000 ETH[113] on Solana, a high-throughput public blockchain supporting decentralized applications, without providing the required collateral on Ethereum. These tokens were then converted into liquid assets and laundered across multiple blockchains, leveraging the pseudonymous and borderless nature of DeFi to obscure their illicit origin.[114] The

---

[108] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 5; *see also Decentralised Finance (DeFi) and DAOs*, FED. FIN. SUPERVISORY AUTH. (Dec. 11, 2025), https://www.bafin.de/EN/Aufsicht/FinTech/Geschaeftsmodelle/DLT_Blockchain_Krypto/DAOS/DAOS_node_en.html [https://perma.cc/LNC3-YH6F]; Sinclair Davidson, *The Nature of the Decentralised Autonomous Organisation*, 21 J. INST. ECON. e5 (2025), https://www.cambridge.org/core/journals/journal-of-institutional-economics/article/nature-of-the-decentralised-autonomous-organisation/221DE3FF0F7E3CC3CF73CAEF8284DE28 [https://perma.cc/L6U6-T2RR].

[109] *See* FATF RECOMMENDATIONS, *supra* note 90, at 14–16, 19 (Recommendations 10, 11 & 20).

[110] *See* FIN. ACTION TASK FORCE, OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT 13, 22 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.inline.pdf [https://perma.cc/A27V-YTJR]; Benson, Turksen & Adamyk*, supra* note 11, at 83.

[111] *See* Merkle Science, *Hack Track: Analysis of Wormhole Token Bridge Exploit*, MERKLE SCI. (Feb. 4, 2022), https://www.merklescience.com/blog/hack-track-analysis-of-wormhole-token-bridge-exploit [https://perma.cc/J3ZL-N7RM].

[112] *See Jump Trading Group Launches Jump Crypto*, BUSINESSWIRE (Sep. 14, 2021), https://www.businesswire.com/news/home/20210914005700/en/Jump-Trading-Group-Launches-Jump-Crypto [https://perma.cc/G5QF-ZJQD].

[113] Ether, the native cryptocurrency of the Ethereum blockchain, is used to pay transaction fees and secure the network. *See What Is Ether (ETH)?*, ETHEREUM, https://ethereum.org/what-is-ether/ [https://perma.cc/V289-9P3K] (last updated Apr. 24, 2026).

[114] *See $325 Million Stolen from Wormhole DeFi Service*, ELLIPTIC (Feb. 3, 2022), https://www.elliptic.co/blog/325-million-stolen-from-wormhole-defi-service?utm_source [https://perma.cc/7PYN-H3XV].

Wormhole exploit thus illustrates the structural and jurisdictional limitations of existing AML frameworks when applied to decentralized, transnational financial systems. In the absence of centralized oversight, illicit actors exploited DAO-related infrastructure to move assets with minimal regulatory visibility.[115]

Tornado Cash, a DAO-governed cryptocurrency mixer on the Ethereum blockchain, further exemplifies the enforcement challenges surrounding decentralized systems. The protocol allowed users to deposit funds and later withdraw them to a new wallet, effectively breaking the visible transaction trail on the blockchain. Tornado Cash required no identity verification or compliance checks, making it a powerful tool for anonymizing the movement of funds.[116] Since 2019, more than $7 billion passed through the platform, a significant portion of which was linked to illicit activity.[117] The national security implications of this verification deficit were particularly stark: the Lazarus Group, a North Korean-sponsored hacking organization, used Tornado Cash to launder some of the $620 million stolen in the 2022 Ronin Bridge cyberattack.[118] According to U.S. and international intelligence assessments, the proceeds laundered by the Lazarus Group through Tornado Cash, were used to evade sanctions and fund ballistic-missile development.[119]

In August 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash. OFAC blacklisted the protocol's publicly available smart contracts and associated wallet addresses, prohibiting U.S. persons from interacting with them. This marked a significant attempt to expand AML enforcement into

---

[115] *See* FIN. ACTION TASK FORCE, OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT, *supra* note 110, at 13.

[116] *See* FIN. ACTION TASK FORCE, VIRTUAL ASSETS RED FLAG INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING 9–12 (2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf [https://perma.cc/H3TW-8GFU] [hereinafter FATF RED FLAG INDICATORS] (discussing "Red Flag Indicators Related to Anonymity").

[117] *See* Bhushan Akolkar, *Crypto Criminals Laundered Another Half-A-Billion*, COINGAP (Aug. 10, 2022), https://coingape.com/crypto-criminals-laundered-another-half-a-billion-details [https://perma.cc/E9VT-EPFL]; *see also* Press Release, U.S. Dep't of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916?utm_source= [https://perma.cc/2DMP-67CM]. A cryptocurrency mixer is a service that enhances privacy by obscuring the origins and destinations of cryptocurrency transactions. Users send funds to the mixer, which pools and redistributes them to recipients in randomized amounts and at varying times, thereby severing the transactional link. While mixers may be used for legitimate purposes, such as protecting financial privacy, they are also exploited to facilitate money laundering and other illicit activities. *See* Angela Walch, *Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems*, *in* CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 39, 42 (Chris Brummer ed., 2019).

[118] *See* Press Release, U.S. Dep't of the Treasury, Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash (Aug. 23, 2023), https://home.treasury.gov/news/press-releases/jy1702 [https://perma.cc/W2FK-HAVS].

[119] *See* Press Release, U.S. Dep't of the Treasury, Tornado Cash Delisting (Mar. 21, 2025), https://home.treasury.gov/news/press-releases/sb0057 [https://perma.cc/V3GY-QWMM].

decentralized infrastructure. The sanctions were challenged in court, and in November 2024, the U.S. Court of Appeals for the Fifth Circuit ruled that OFAC had exceeded its authority under the International Emergency Economic Powers Act (IEEPA).[120] The court held that Tornado Cash's smart contracts—self-executing code deployed on a public blockchain—do not constitute "property" under IEEPA because they are immutable and cannot be owned or controlled.[121]

The decision underscores the legal and regulatory challenges posed by decentralized systems. In the absence of centralized control or identifiable intermediaries, traditional AML frameworks—designed for financial institutions subject to regulatory oversight—struggle to establish jurisdiction, impose obligations, or hold DAO stakeholders accountable. The Tornado Cash case discussed above illustrates how automation, decentralization, and pseudonymity frustrate enforcement by eliminating clear regulatory touchpoints. These structural features are also evident in major DAOs such as Uniswap, Aave, and MakerDAO, which facilitate DeFi services without identity verification, onboarding procedures, or customer due diligence. Their foundational documents typically omit AML obligations, reflecting a governance model that operates outside existing AML frameworks.[122]

This posture directly contravenes international standards such as FATF Recommendation 15, which requires VASPs to implement risk-based AML controls, including KYC measures and transaction monitoring.[123] By designing around such obligations—and operating

---

[120] *See* Van Loon v. Dep't of the Treasury, 122 F.4th 549, 553–54 (5th Cir. 2024). The IEEPA is a U.S. federal law enacted in 1977 that grants the president broad authority to regulate international economic transactions and impose sanctions during national emergencies that threaten the United States. The law is a cornerstone of U.S. economic sanctions policy and is frequently invoked to block foreign assets, prohibit certain transactions, and restrict the operations of entities linked to illicit activities or hostile nations. *See* CHRISTOPHER A. CASEY, JENNIFER K. ELSEA & LIANA W. ROSEN, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 2, 9–10, 18–36 (2025), https://www.congress.gov/crs-product/R45618 [https://perma.cc/7B9A-UHAD]. The ruling, however, highlights a significant limitation in applying IEEPA to emerging technologies such as blockchain, where traditional definitions of property and control may not align with decentralized systems. *See Van Loon*, 122 F.4th at 563–64.

[121] *See id.* at 567–68.

[122] For example, Uniswap DAO allows participants to trade directly through smart contracts without identification or screening. *See* HAYDEN ADAMS ET AL., UNISWAP V3 CORE WHITEPAPER (Mar. 2021), https://app.uniswap.org/whitepaper-v3.pdf [https://perma.cc/MFS7-4YU5]. Aave DAO permits lending and borrowing without onboarding procedures or identity verification. *See Aave Protocol Documentation*, AAVE: DOCUMENTATION https://aave.com/docs [https://perma.cc/9YWZ-ZZD8] (last visited Feb. 25, 2026). Similarly, MakerDAO enables participants to mint the DAI stablecoin by depositing collateral, without conducting any form of due diligence on those participants. *See The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*, MAKERDAO (Feb. 2020), https://makerdao.com/en/whitepaper/ [https://perma.cc/EMC5-X3D2].

[123] *See Outcomes FATF Plenary, 17-19 October 2018*, FIN. ACTION TASK FORCE (2018), https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-plenary-october-2018.html [https://perma.cc/8WM3-YRVS] (last visited Mar. 25, 2026).

through pseudonymous participation, automated smart contract execution, and decentralized governance—DAOs evade integration into existing compliance regimes, underscoring the broader incompatibility between DeFi financial infrastructure and traditional AML enforcement.[124] The Fifth Circuit's ruling reinforces this incompatibility, highlighting the difficulty of applying national AML laws to protocols without identifiable operators or legal persons.[125]

This legal outcome carries significant implications for the future of AML enforcement in decentralized ecosystems. The ruling underscores how key attributes of DAOs—namely, reliance on immutable code, absence of centralized control, and participation by anonymous or pseudonymous participants—create structural conditions that frustrate conventional enforcement. It exposes the limitations of AML frameworks built on the premise of accountable financial intermediaries, jurisdictional oversight, and hierarchical control.[126] Without identifiable actors or regulatory leverage points, core compliance mechanisms such as KYC, due diligence, and suspicious-activity reporting fail to operate effectively.

B. *Technical Exploitation Patterns*

As previously discussed, DAOs rely on technical features such as smart contracts, automated execution, and cross-chain interoperability. While these features enable decentralized governance, they also introduce vulnerabilities that can be exploited for ML. A 2024 Chainalysis report found that a substantial share of illicit flows through decentralized finance involved technical exploits such as smart-contract vulnerabilities, protocol manipulation, and automated cross-chain transfers rather than traditional

---

[124] *See* Press Release, U.S. Dep't of the Treasury, Tornado Cash Delisting, *supra* note 119.

[125] *See Van Loon*, 122 F.4th at 556–60, 566–70. Tornado Cash is an example of a decentralized cryptocurrency mixer designed to enhance privacy on the Ethereum blockchain. It allows users to deposit cryptocurrency into smart contracts, which then mix the funds before distributing them to recipients. This process obfuscates the connection between sender and recipient, making transactions difficult to trace. *See* Werbach, *supra* note 28, at 520–22.

[126] *See* EURO. BANKING AUTH., ANNUAL REPORT 2021 44–48, 50–53 (2022) https://eba.europa.eu/sites/default/files/document_library/About%20Us/Annual%20Reports/2021/1035237/EBA%202021%20Annual%20Report.pdf [https://perma.cc/MHM5-5DDM]; Alexandra Born et al., *Decentralised Finance – A New Unregulated Non-Bank System*, MACROPRUDENTIAL BULL. (July 18, 2022), https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html [https://perma.cc/J9RG-PALV]; FIN. ACTION TASK FORCE, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES 3, 5, 8 – 9 (2007), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/High%20Level%20Principles%20and%20Procedures.pdf.coredownload.inline.pdf [https://perma.cc/RGX6-FPW3]; David Chaikin, *How Effective Are Suspicious Transaction Reporting Systems,* 12 J. MONEY LAUNDERING CONTROL 238, 239–41, 243–44, 246–47 (2009).

account-based laundering.[127] Technical exploit methods leverage the speed, composability, and opacity of decentralized systems, enabling illicit actors to move funds rapidly and evade conventional AML detection mechanisms.[128]

Smart contract vulnerabilities have emerged as a critical avenue for circumventing AML controls in DAO-governed financial protocols.[129] These vulnerabilities allow actors to manipulate transaction flows, obscure the origin of illicit assets, and bypass detection mechanisms used in traditional oversight systems.[130] A notable case occurred in July 2023 with the exploit of Curve Finance, a decentralized exchange for stablecoin trading.[131] That exploit resulted in the unauthorized withdrawal of approximately $73.5 million across multiple DeFi protocols.[132] Although not initially framed as a laundering scheme, the exploit's rapid dispersal and obfuscation of funds across anonymizing tools and smart contract layers[133] ought to raise significant ML concerns.

What made the Curve exploit further legally significant was not only the technical breach, but also the exploitation of DeFi's regulatory blind spots. The transaction chains were automated, non-linear, and executed at speeds that rendered conventional AML monitoring tools—

---

[127] *See* CHAINALYSIS TEAM, THE CHAINALYSIS 2024 CRYPTO CRIME REPORT (2024), https://www.chainalysis.com/blog/2024-crypto-money-laundering/ [https://perma.cc/C9C9-VZ5W] (last visited Feb. 25, 2026). A flash loan is a DeFi tool that enables instant, uncollateralized borrowing, provided the loan is repaid within the same transaction block. *See* Chainalysis Team, *$197 Million Stolen: Euler Finance Flash Loan Attack Explained [Updated 4/6/23]*, CHAINALYSIS (Mar. 15, 2023), https://www.chainalysis.com/blog/euler-finance-flash-loan-attack/ [https://perma.cc/XWN3-R8H9]

[128] *See* FATF RED FLAG INDICATORS, *supra* note 116, at 5, 7–10, 11, 17.

[129] *See* Basel Comm. on Banking Supervision, *Novel Risks, Mitigants and Uncertainties with Permissionless Distributed Ledger Technologies* 8 (BIS, Working Paper, Paper No. 44, 2024), https://www.bis.org/bcbs/publ/wp44.pdf [https://perma.cc/J2RY-YPUL].

[130] *See* FIN. STABILITY BD., THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE 4–8, 18, 21–22, 36–38 (2023), https://www.fsb.org/2023/02/the-financial-stability-risks-of-decentralised-finance/?utm_source= [https://perma.cc/Z6VX-39W8].

[131] Stablecoins are digital currencies designed to maintain a stable value, usually pegged to the U.S. dollar, making them less volatile than traditional cryptocurrencies like Bitcoin. They serve as a bridge between conventional money and digital assets, allowing users to transfer value across blockchain networks while avoiding price fluctuations. *See* PRESIDENT'S WORKING GROUP ON FIN. MKTS., THE FED. DEPOSIT INS. CORP., AND THE OFF. OF THE COMPTROLLER OF THE CURRENCY, REPORT ON STABLECOINS 1–2 (2021), https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf [https://perma.cc/7THQ-JVSL]; Douglas Arner, Raphael Auer & Jon Frost, *Stablecoins: Risks, Potential and Regulation* 2–5 (BIS Working Paper No. 905, 2020), https://www.bis.org/publ/work905.pdf [https://perma.cc/6SCX-VTAF].

[132] *See* SLOWMIST, BLOCKCHAIN SECURITY AND ANTI-MONEY LAUNDERING ANNUAL REPORT 10 (2023), https://www.slowmist.com/report/2023-Blockchain-Security-and-AML-Annual-Report(EN).pdf [https://perma.cc/QK7R-7NGD]; Chainalysis Team, *Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises*, CHAINALYSIS (Jan. 24, 2024), https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/ [https://perma.cc/6JBZ-EQ6E].

[133] *See* SLOWMIST, *supra* note 132, at 10; Chainalysis Team, *Funds Stolen from Crypto Platforms*, *supra* note 132.

designed for centralized, sequential reporting systems—largely ineffective. As with many DAO-governed protocols, there were no institutional intermediaries obligated to monitor, report, or halt the transactions in real time.[134]

More broadly, such exploits reflect a trend in which DAO-related laundering strategies capitalize on structural and governance-based weaknesses. The 2024 Chainalysis Crypto Crime Report documented significant DeFi and DAO-related losses stemming from protocol attacks, identifying such incidents as major on-chain vulnerabilities.[135] In governance manipulation, for example, attackers may acquire temporary voting power to push through malicious proposals that authorize suspicious asset transfers or contract upgrades. These activities occur under the guise of procedural legitimacy, obscuring intent and undermining AML accountability mechanisms.[136]

Flash loans further illustrate how speed, automation, and composability enable the rapid, hard-to-trace movement of illicit funds within DAO-governed systems, reinforcing the challenges they pose to conventional AML controls.[137] Flash loans are a distinctive feature of DeFi protocols that enable users to borrow large sums of cryptocurrency without providing collateral, as long as the transaction is completed within a single blockchain transaction.[138] If the repayment does not occur instantly, within the same block, the entire transaction is automatically reversed. Because there is no intermediary, approval process, or time delay, flash loans offer both legitimate uses—such as market arbitrage—and the potential for abuse, including rapid, untraceable laundering of illicit funds.[139]

DAOs play a central role in facilitating these schemes. First, many DAOs manage protocols offering flash loans but are not required to follow AML measures like customer checks or transaction monitoring.[140] Second,

---

[134] *See* Zach Anderson, *Curve Finance and the Vyper Vulnerability: A Technical Post-Mortem Report*, BLOCKCHAIN.NEWS (Aug. 6, 2023), https://blockchain.news/news/curve-finance-and-the-vyper-vulnerability-a-technical-post-mortem-report?utm_source [https://perma.cc/6MUZ-7VU7].

[135] *See generally* CHAINALYSIS TEAM, THE CHAINALYSIS 2024 CRYPTO CRIME REPORT, *supra* note 127.

[136] *See, e.g.*, Carolyn Wilkins, External Member, Fin. Pol'y Comm., Bank of Eng., Speech at the UCL Centre for Blockchain Technologies: Governance of "Decentralised" Finance: Get up, Stand up! (Oct. 19, 2022), https://www.bankofengland.co.uk/speech/2022/october/carolyn-wilkins-speech-at-ucl-centre-for-blockchain-technologies [https://perma.cc/GTR5-57AW].

[137] *See* Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, 2021 BIS Q. REV. 21, 27 (2021), https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf [https://perma.cc/9UMD-LPX6]; RISK ASSESSMENT OF DEFI, *supra* note 12, at 20.

[138] For explanation of "flash loans," *see* Chainalysis Team, *$197 Million Stolen*, *supra* note 127.

[139] *See id.*; *see also* Catherine C. Desjardins et al., *Mapping the DeFi Crime Landscape: An Evidence-Based Picture*, 11 J. CYBERSECURITY 1, 3, 8–12 (2025), https://academic.oup.com/cybersecurity/article/11/1/tyae029/7962044 [https://perma.cc/4THU-UVKJ].

[140] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at at 3–4.

DAOs can be directly exploited. Attackers can use flash loans to temporarily acquire significant voting power within a DAO, enabling them to pass self-serving governance proposals—such as transferring cryptocurrency from the DAO's treasury.[141]

The technical exploitation patterns reveal a broader temporal mismatch between DAO operations and AML enforcement capacity. The automation and speed inherent in DAO-governed systems allow illicit transactions to be executed, distributed, and concealed within very short timeframes—far outpacing the detection and intervention timelines of national AML controls. Even when enforcement systems are well-resourced, the absence of regulatory access points—such as intermediaries with real-time oversight or transaction approval authority—means that laundering operations can be completed and concealed before intervention is possible.[142]

Finally, the widespread use of unhosted wallets—a core feature of DAO participation—introduces heightened ML risks.[143] In decentralized ecosystems, users engage with DAOs primarily through these wallets, which allow them to vote, propose governance actions, and execute peer-to-peer financial transactions without involving regulated intermediaries.[144] Unlike custodial wallets offered by exchanges, unhosted wallets are controlled entirely by the user and do not require registration, licensing, or identity verification.[145] This pseudonymity enables illicit

---

[141] *See id.* at 20; *Decentralized Finance: (DeFi) Policy-Maker Toolkit*, *supra* note 20, at 17; BANK FOR INT'L SETTLEMENTS CYBER RESILIENCE COORD. CTR., PROJECT POLARIS PART 3: CLOSING THE CBDC CYBER THREAT MODELLING GAPS 43–44 (2023), https://www.bis.org/publ/othp71.pdf [https://perma.cc/3NP8-XMX4].

[142] *See* Adam Rajuroy et al., Cross-Border Coordination and Information Sharing: Friction Points for DeFi Investigations 2–4 (Sep. 7, 2025), https://www.researchgate.net/publication/395337458_Cross-Border_Coordination_and_Information_Sharing_Friction_Points_for_DeFi_Investigations [https://perma.cc/ZK6D-R7A6] (unpublished manuscript); DEP'T OF JUST., THE REP. OF THE ATTORNEY GENERAL PURSUANT TO SECTION 5(B)(III) OF EXEC. ORD. 14067: THE ROLE OF L. ENF'T IN DETECTING, INVESTIGATING, AND PROSECUTING CRIM. ACTIVITY RELATED TO DIGITAL ASSETS 4 (2022), https://www.justice.gov/archives/ag/file/1557146/dl?inline [https://perma.cc/CJF5-7CT8]; *Smarter Blockchain Investigations: Insights from INTERPOL,* BASEL INST. ON GOVERNANCE (Mar. 12, 2025), https://baselgovernance.org/blog/smarter-blockchain-investigations-insights-interpol [https://perma.cc/WR4N-WJ3A].

[143] *See* FATF TARGETED UPDATE, *supra* note 15, at 32.

[144] *See* Liat Shetret, *Hosted vs Unhosted Wallets: Compliance Risks and Practical Solutions*, ELLIPTIC (Oct. 30, 2025), https://www.elliptic.co/blog/hosted-vs-unhosted-wallets [https://perma.cc/W36M-SB2B].

[145] *See id.*; *see also* FATF TARGETED UPDATE, *supra* note 15, at 44; Chainalysis & Notabene, *How Can VASPs Ensure Travel Rule Compliance on Transactions Involving Unhosted Wallets*, CHAINALYSIS (Jan. 28, 2022), https://www.chainalysis.com/blog/travel-rule-compliance-unhosted-wallets/ [https://perma.cc/QKD3-8JXN].

actors to obscure the provenance of unlawfully obtained assets and evade detection.[146]

The FATF has identified unhosted wallets—and peer-to-peer transactions they facilitate—as a significant regulatory blind spot that increases ML vulnerability in DeFi.[147] The FATF urged jurisdictions to assess these risks, particularly in DAO-related activity, and to improve regulatory coordination by sharing data and mitigation strategies.[148] The IMF echoed these concerns in a 2023 policy paper, emphasizing the need for full implementation of FATF standards and greater oversight of pseudonymous transactions involving DAOs.[149] Together, these warnings underscore the growing consensus that unhosted wallets pose a direct challenge to AML enforcement in decentralized environments.

C. *Governance-Based Vulnerabilities*

DAO governance structures—designed to enable decentralized decision-making—can be exploited to authorize illicit financial transfers under the guise of legitimate on-chain voting. By exploiting token-based voting systems, malicious actors can introduce and approve proposals that enable illicit financial activity, such as authorizing suspicious asset transfers, modifying smart contract functions, or diverting funds from DAO treasuries.[150] These actions are often disguised as legitimate governance activity and are implemented automatically through smart contracts with no review or compliance checks.[151] There is no intermediary to verify the legitimacy of the governance decision or to halt the transaction before

---

[146] *See* FATF TARGETED UPDATE, *supra* note 15, at 32; FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models [https://perma.cc/46WA-LQGC] [hereinafter APPLICATION OF FINCEN'S REGULATIONS].

[147] *See* FATF TARGETED UPDATE, *supra* note 15, at 32.

[148] *See id.*

[149] *See* FIN. STABILITY BD., IMF-FSB SYNTHESIS PAPER: POLICIES FOR CRYPTO-ASSETS 29–30 (2023), https://www.fsb.org/uploads/R070923-1.pdf [https://perma.cc/3HNM-6AM7] [hereinafter IMF-FSB SYNTHESIS PAPER].

[150] *See* Weinstein, Lofchie & Schwartz, *supra* note 18 ("Fourth, there is the potential for "governance attacks," in which a single actor or a group, whose objectives are not aligned with the DAO's stated mission, might take control of the DAO (pursuant to the DAO's own governance procedures) and drain the DAO's treasury or otherwise deploy it to their own ends.").

[151] *See Decoding the Dangers: AML Risks in Decentralized Finance Exposed*, FIN. CRIME ACAD. (Jan. 20, 2026), https://financialcrimeacademy.org/aml-risks-in-decentralized-finance/ [https://perma.cc/ZNV7-W3VE]; Ervin Zubic, *Research Review: Dark Side of Decentralised Finance: A Call for Enhanced AML Regulation Based on Use Cases of Illicit Activities*, MEDIUM (Jan. 2, 2024), https://medium.com/coinmonks/research-review-dark-side-of-decentralized-finance-a-call-for-enhanced-aml-regulation-based-on-dc587fa755f9 [https://perma.cc/7SXL-ANA9]; Soledad García Fariña, *Decentralized Autonomous Organizations and Money Laundering*, COMPLIANCE LATAM (May 25, 2023), [https://perma.cc/CDT4-E7MS].

implementation.[152] This absence of centralized control creates a regulatory blind spot, allowing illicit activity to proceed under the appearance of procedural legitimacy and undermining AML oversight.[153]

The aforementioned Beanstalk Protocol exploit provides a compelling illustration of how DAO governance mechanisms can be manipulated to enable financial crime. In this case, attackers used a flash loan to acquire a supermajority of governance tokens, giving them temporary control over the Beanstalk DAO's voting system. They then introduced and approved a proposal transferring over $182 million in assets from the DAO's treasury to wallets they controlled.[154]

Although the proposal was procedurally valid under the DAO's rules, it was passed by a pseudonymous actor with no enduring stake in the protocol and executed automatically by smart contracts.[155] The exploit stemmed less from a flaw in the smart-contract code than from the governance system's lack of safeguards against short-term, pseudonymous control.[156] From an AML perspective, this case exemplifies how the absence of centralized oversight allows illicit transactions to proceed under the appearance of legitimate governance.[157]

D. *Cross-Chain Complexity*

Cross-chain functionality—enabled by protocols known as "bridges"—allows DAOs to transfer assets across multiple blockchain networks, such as Ethereum and Binance Smart Chain.[158] While this enhances efficiency and interoperability, it also introduces substantial AML vulnerabilities. The rapid movement of funds across blockchains to obscure their origin, often referred to as "chain hopping," significantly

---

[152] *See, e.g.*, FIN. STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT 2023 11–13 (2023), https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf?utm_source [https://perma.cc/QQH3-MSRT] (noting the importance of intermediaries).

[153] *See* Metana Editorial, *Governance Attacks in Smart Contracts,* METANA (Nov. 10, 2024), https://metana.io/blog/governance-attacks-in-smart-contracts/?utm_source [https://perma.cc/6EDS-X7YX]; Chainalysis Team, *Hackers Are Stealing More Cryptocurrency from DeFi Platforms Than Ever Before*, CHAINALYSIS (Apr. 14, 2022) https://www.chainalysis.com/blog/2022-defi-hacks/?utm_source= [https://perma.cc/8NQJ-RNSG].

[154] *See* Sidhartha Shukla*, DeFi Project Beanstalk Loses $182 Million in Flash Loan Attack*, BLOOMBERG (Apr. 18, 2022), https://www.bloomberg.com/news/articles/2022-04-18/defi-project-beanstalk-loses-182-million-in-flash-loan-attack [https://perma.cc/9WRH-TYZQ].

[155] *See Beanstalk Governance Exploit*, BEANSTALK (Apr. 19, 2022), https://bean.money/blog/beanstalk-governance-exploit?utm_source [https://perma.cc/3LME-FNPE].

[156] *See Beanstalk Governance Exploit*, *supra* note 155; Rainer Feichtinger et al., *SoK: Attacks on DAOs*, ARXIV 7 (2024), https://arxiv.org/abs/2406.15071 [https://perma.cc/3VGM-NZD5].

[157] *See* Feichtinger et al., *supra* note *156*, at 5; FATF RISK-BASED APPROACH, *supra* note 10, at 18; RISK ASSESSMENT OF DEFI, *supra* note 12, at 3–4, 26.

[158] *See* Chainalysis Team, *Introduction to Cross-Chain Bridges*, CHAINALYSIS (Dec. 5, 2024), https://www.chainalysis.com/blog/introduction-to-cross-chain-bridges/?utm_source [https://perma.cc/J4XZ-82XW].

complicates transaction tracing and undermines traditional AML controls.[159]

Bridge protocols enable actors to fragment, swap, and route assets across distinct blockchain ecosystems, exploiting differences in transparency, transaction monitoring, and regulatory enforcement.[160] Because AML tools are typically optimized for single-chain environments, these cross-chain laundering schemes evade detection by splitting transaction trails across multiple networks.

These operations expose a fundamental gap in national AML frameworks, which remain tied to jurisdictional boundaries and lack tools to monitor transnational activity across fragmented systems. Each blockchain involved in a cross-chain transaction only captures part of the fund flow, making it exceptionally difficult for national financial intelligence units to reconstruct the full trail.[161] Moreover, DAOs can exploit this fragmentation by coordinating financial operations across multiple chains and jurisdictions, typically without a fixed legal domicile or regulatory oversight.[162] This enables malicious actors to engage in regulatory arbitrage—routing assets through DAO-governed protocols or blockchain networks with weak or uneven AML enforcement—to evade detection and obscure the origin of illicit funds.[163]

An illustrative example of such concerns is the 2022 Binance Smart Chain bridge exploit. Attackers exploited a flaw in the Binance Smart Chain Token Hub—a smart contract linking the BNB Beacon Chain and BNB Smart Chain—to mint approximately two million unauthorized BNB tokens, worth nearly $570 million.[164] The attackers moved the stolen assets through cross-chain bridges and DeFi protocols, converting funds into

---

[159] *See* Elliptic, *New Elliptic Report: Cross-Chain Money Laundering Reaches $22 Billion*, ELLIPTIC (July 17, 2025), https://www.elliptic.co/blog/new-elliptic-report-cross-chain-money-laundering-reaches-22-billion [https://perma.cc/7J4J-6AAT].

[160] *See* Chainalysis Team, *Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk*, CHAINALYSIS (Aug. 2, 2022), https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/ [https://perma.cc/S8AR-BPLN].

[161] *See* GAFILAT, GUIDE ON RELEVANT ASPECTS AND APPROPRIATE STEPS FOR THE INVESTIGATION, IDENTIFICATION, SEIZURE, AND CONFISCATION OF VIRTUAL ASSETS ¶ 291 (2021), https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf [https://perma.cc/HY6V-4Z59].

[162] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 28; *see also* Salvatore L. Furnari & Chiara Villani, *Regulation of Financial Protocol DAOs: Addressing the Problems of Decentralization and AI Governance*, *in* DECENTRALIZED AUTONOMOUS ORGANIZATIONS—GOVERNANCE, TECHNOLOGY, AND LEGAL PERSPECTIVES 115, 122, 124 (Michael Lustenberger et al. eds., 2026), https://doi.org/10.1007/978-3-032-03273-7_7 [https://perma.cc/2PMN-KLKK].

[163] *See* Merkle Science, *Chain Hopping: The Future of Crypto Money Laundering*, MERKLE SCIENCE (July 10, 2023), https://www.merklescience.com/blog/chain-hopping-the-future-of-crypto-money-laundering [https://perma.cc/UT3Z-VS7Q]; Elliptic, *$7 Billion in Crypto Laundered Through Cross-Chain Services*, ELLIPTIC (Oct. 5, 2023), https://www.elliptic.co/blog/7-billion-in-crypto-laundered-through-cross-chain-services [https://perma.cc/ALP9-ZVE6].

[164] *See* Merkle Science, *Hack Track*, *supra* note 111.

stablecoins and obscuring their origin.[165] Although BNB Chain validators eventually froze $7 million in assets and suspended the network, most of the funds had already been moved beyond the reach of regulatory enforcement.[166] The exploit revealed a security weakness and highlighted the regulatory challenges of tracing illicit flows across interoperable, decentralized networks.

RenBridge offers another example of how decentralized, cross-chain protocols can be exploited to facilitate large-scale ML.[167] Since 2020, the protocol has been used to transfer at least $540 million in illicit funds, including proceeds from ransomware operations and state-sponsored cyberattacks.[168] RenBridge enabled users to move assets between blockchains, such as exchanging Ethereum-based tokens for Bitcoin, without undergoing identity verification or triggering compliance checks. These transactions occurred without centralized oversight, relying on automated processes that obscured the origin and destination of funds.[169]

Notably, the AML challenges posed by cross-chain laundering pose direct national-security threats. Multilateral assessments by Europol highlight that cross-chain bridges, chain-hopping techniques, and multi-chain obfuscation are increasingly used to evade sanctions, frustrate asset tracing, and obstruct law-enforcement efforts.[170] UN Security Council

---

[165] *See id*.; *BNB Chain's Cross-Chain Bridge Exploit Explained*, NANSEN (Oct. 15, 2022), https://www.nansen.ai/research/bnb-chains-cross-chain-bridge-exploitexplained [https://perma.cc/5JAA-WD96]; Ethereum World News, *BNB Chain Resumes Operations Following the Massive Online Exploit*, BINANCE SQUARE (Oct. 7, 2022), https://www.binance.com/en-IN/square/post/4456 [https://perma.cc/59KM-GDGG].

[166] *See* Rahul Nambiampurath, *Binance Hit by $570 Million Blockchain Bridge Hack*, INVESTOPEDIA (Oct. 7, 2022), https://www.investopedia.com/binance-got-hacked-6748215 [https://perma.cc/729Y-3B83]; Jason Firch, *$570M Binance Hack: What Happened & Who is Responsible,* PURPLESEC (Apr. 27, 2024), https://purplesec.us/breach-report/binance-coin-hack [https://perma.cc/3V5B-XETB].

[167] Although the Protocol was initially developed by a private company, it later transitioned to a decentralized governance model, making it even more difficult to assign legal responsibility or enforce AML obligations. *See Moving on from Alameda*, MEDIUM (Nov. 18, 2022), https://medium.com/renprotocol/moving-on-from-alameda-da62a823ce93 [https://perma.cc/E2UJ-34T6].

[168] *See* Elliptic, *Cross-Chain Crime: Over Half a Billion Dollars Laundered Through a Cross-Chain Bridge*, ELLIPTIC (Aug. 10, 2022), https://www.elliptic.co/blog/analysis/cross-chain-crime-more-than-half-a-billion-dollars-has-been-laundered-through-a-cross-chain-bridge#:~:text=Elliptic%20www,already%20been%20laundered%20through%20RenBridge [https://perma.cc/APH2-3TXT].

[169] *See RenBridge: The Safe, Fast, and Most Secure Way to Bring Cross-Chain Assets Between Blockchains.*, https://renbridge-site.github.io/ [https://perma.cc/4XS6-DATQ] (last visited Mar. 25, 2026); *see also* Tami Stone, *How to Use RenBridge: A Step-by-Step Guide to Trustless Cross-Chain Transfers*, DEV (Apr. 22, 2025), https://dev.to/stablecoinstrategist/how-to-use-renbridge-a-step-by-step-guide-to-trustless-cross-chain-transfers-22bm [https://perma.cc/6QHB-2X4F].

[170] *See* EUROPOL, THE OTHER SIDE OF THE COIN: AN ANALYSIS OF FINANCIAL AND ECONOMIC CRIME 15 (2023), https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf [https://perma.cc/9RE3-FMDF].

Panel of Experts reports further confirm that state-sponsored hacking organizations—including North Korean cyber units—exploit these cross-chain infrastructures to evade global sanctions regimes.[171] By rapidly moving assets across chains, adversarial actors fragment their transactional footprint across multiple jurisdictions and blockchains, rendering it extremely difficult for national-security agencies to freeze assets or track illicit flows.[172] DAOs governing these cross-chain tools, when operated without AML controls, effectively provide adversaries with mechanisms to bypass sanctions designed to constrain weapon proliferation and cyber-enabled attacks.[173]

E. *Cross-Jurisdictional Enforcement Challenges*

The borderless and decentralized architecture of DAOs further presents a fundamental challenge to existing AML regimes, which depend on jurisdiction-specific enforcement and centralized compliance structures. DAOs' above-discussed characteristics create three core barriers that systematically undermine AML enforcement: immutable execution, decentralized data storage, and regulatory arbitrage.[174]

The first barrier is the immutable execution of smart contracts, which eliminates traditional intervention points for AML authorities. In conventional financial systems, transactions can be flagged, paused, or reversed by centralized intermediaries based on suspicion of illicit activity. By contrast, self-executing smart contracts used by DAOs automatically carry out instructions without discretionary oversight.[175] Once deployed, these contracts execute transactions irreversibly and across jurisdictions, regardless of their legality or compliance status. This immutability

---

[171] *See*, MULTILATERAL SANCTIONS MONITORING TEAM, THE DPRK'S VIOLATION AND EVASION OF UN SANCTIONS THROUGH CYBER AND INFORMATION TECHNOLOGY WORKER ACTIVITIES 7, 10, 12, 24 (2025), https://www.mofa.go.jp/files/100922718.pdf# [https://perma.cc/39T2-YG9F].

[172] *Id.* at 36; Elliptic, *Typologies in Focus: The Threat of Cross-Chain Crime*, ELLIPTIC (Oct. 23, 2023), https://www.elliptic.co/blog/typologies-in-focus-the-threat-of-cross-chain-crime [https://perma.cc/FT9C-9QKP].

[173] *See* FIN. ACTION TASK FORCE, COMPLEX PROLIFERATION FINANCING AND SANCTIONS EVASION SCHEMES 4–5 (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf [https://perma.cc/U46G-QGSG]; MULTILATERAL SANCTIONS MONITORING TEAM, *supra* note 171, at 28.

[174] *See* FIN. ACTION TASK FORCE, OPPORTUNITIES AND CHALLENGES OF NEW TECHNOLOGIES FOR AML/CFT, *supra* note 110, at 13, 22, 26; Selina Keesoony, *International Anti-Money Laundering Laws: The Problems with Enforcement*, 19(2) J. MONEY LAUNDERING CONTROL 130, 131–33 (2016); Benson, Turksen & Adamyk, *supra* note 11, at 83, 86–87.

[175] *See* Iñaki Aldasoro et al., *An Approach to Anti-Money Laundering Compliance for Cryptoassets*, BIS BULL. NO. 111 3–4 (Aug. 13, 2025), https://www.bis.org/publ/bisbull111.pdf [https://perma.cc/A8HX-TAG5]; World Bank Grp., *Smart Contract Technology and Financial Inclusion*, FINTECH NOTE NO. 6, 6, 14, 18 (2020), https://documents1.worldbank.org/curated/en/710151588785681400/pdf/Smart-Contract-Technology-and-Financial-Inclusion.pdf [https://perma.cc/9547-RVCA].

fundamentally conflicts with AML principles that depend on the ability to monitor, delay, or block transactions pending investigation.[176]

The second barrier is the decentralized nature of transaction data storage. In traditional finance, data is maintained in centralized repositories within identifiable legal jurisdictions, enabling regulators to access transaction records for audits, compliance checks, or investigations. In DAO ecosystems, by contrast, transaction data is distributed across a global network of computers known as nodes, which maintain and validate the blockchain.[177] These nodes operate independently and are often located across multiple jurisdictions.[178] Although blockchain data is publicly viewable, it is not tied to identifiable stakeholders or legal entities, nor is it stored within a fixed jurisdiction.[179] As a result, standard investigative tools—such as subpoenas, record freezes, and institutional reporting obligations—are largely ineffective. Even when illicit activity is visible on-chain, the absence of legal access points frustrates timely enforcement.

The third, and perhaps most intractable, barrier is regulatory arbitrage. DAOs operate across multiple jurisdictions, allowing illicit actors to exploit disparities in national AML laws. By shifting operations or governance functions to jurisdictions with weak enforcement or limited oversight, DAOs can evade scrutiny while continuing to facilitate financial activity. The IMF has warned that crypto-asset issuers and service providers often migrate to regulatory havens, posing systemic risks to global financial stability.[180] DAOs, which lack a fixed domicile and are governed by pseudonymous or anonymous participants worldwide, exemplify this problem. This legal indeterminacy and transnational scope render coordinated enforcement extraordinarily difficult.

F. *Specific ML Methods in DAOs*

Having examined the structural and technical DAO vulnerabilities that facilitate ML, this section turns to illustrative examples of laundering methods that exploit those weaknesses. It identifies specific patterns

---

[176] *See* Jerome Desbonnet & Oded Vanunu, *The Rise of Smart Contracts and Strategies for Mitigating Cyber and Legal Risks*, WORLD ECON. F. (July 16, 2024), https://www.weforum.org/stories/2024/07/smart-contracts-technology-cybersecurity-legal-risks/ [https://perma.cc/KW8P-95X4].

[177] *See* FIN. MKTS. LAW COMM., DISTRIBUTED LEDGER TECHNOLOGY AND GOVERNING LAW: ISSUES OF LEGAL UNCERTAINTY 7–11 (2018), https://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf [https://perma.cc/L4P3-U8WJ].

[178] *See* Shabir Korotana, *Decentralized Autonomous Organizations: Adapting Legal Structures and Proposing a New Model of DAOLLP*, 20 CAPITAL MKTS L. J. 1 1, 5, 12 (2025), https://academic.oup.com/cmlj/article/20/3/kmaf011/8249442 [https://perma.cc/W6GW-ZP4X].

[179] *See* Adam Hayes, *Blockchain Facts: What Is It, How It Works, and How it Can Be Used*, INVESTOPEDIA (Dec. 27, 2025), https://www.investopedia.com/terms/b/blockchain.asp [https://perma.cc/UQ8J-PTA6].

[180] *See* Tobias Adrian, Dong He & Aditya Narain, *Global Crypto Regulation Should Be Comprehensive, Consistent, and Coordinated*, IMF (Dec. 9, 2021), https://www.imf.org/en/blogs/articles/2021/12/09/blog120921-global-crypto-regulation-should-be-comprehensive-consistent-coordinated [https://perma.cc/AE96-4PYE].

through which illicit actors exploit DAO-governed financial tools—such as decentralized exchanges, treasuries, lending protocols, and token issuance mechanisms—to layer, convert, and integrate illicit funds. These patterns reflect how traditional AML safeguards are bypassed not only through system architecture but also through ordinary financial functions embedded in DAO operations.

One key exploitation method involves the use of decentralized exchanges governed by DAOs to convert cryptocurrencies in ways that facilitate ML. These platforms allow users to purchase tokens or swap cryptocurrencies without undergoing KYC checks or transaction monitoring, thereby evading compliance safeguards that apply to centralized exchanges. Decentralized exchanges are routinely used to convert illicit proceeds into more liquid or less traceable assets, further obscuring their origin.[181] These converted assets are then frequently routed through cross-chain bridges and cryptocurrency mixers to evade AML controls.[182] The 2021 Spartan Protocol exploit is representative. There, approximately $30 million in digital assets were laundered through decentralized platforms.[183] The stolen tokens were converted into Ether and Bitcoin, moved across chains via AnySwap, and ultimately routed through Tornado Cash. The operation involved no regulated financial intermediaries, underscoring the structural challenges AML authorities face in monitoring activity conducted outside traditional financial systems.[184]

Another ML pattern involves the use of DAO treasury and token issuance mechanisms to integrate illicit funds into DeFi ecosystems. An illicit actor may contribute unlawfully obtained cryptocurrency—such as Ether—to a DAO's funding round or liquidity pool. In return, the actor receives governance tokens, which can then be traded for other digital assets or used to participate in the DAO's decision-making processes.[185] These transactions typically occur without identity verification, allowing the actor to conceal the origin of the funds through seemingly legitimate contributions. Because DAOs treat such participation as routine governance activity, the resulting transactions blur the line between licit

---

[181] *See* Heather Yue Zhou*, Regulating Crypto Money Laundering: An Assessment of Current Regulatory Responses and Potentials for Technology-Based Solutions*, STAN. J. BLOCKCHAIN L & POL. (Jun. 30, 2025), https://stanford-jblp.pubpub.org/pub/crypto-laundering/release/1 [https://perma.cc/E6DX-6SSG]; RISK ASSESSMENT OF DEFI, *supra* note 12, at 13, 16–17.

[182] Mixers are protocols that obfuscate transaction trails by pooling funds and redistributing them to new addresses, thereby breaking the link between the sender and the recipient. *See* David Carlisle, *Crypto Mixers and Privacy Protocols: The Sanctions Compliance Implications*, ELLIPTIC (Mar. 1, 2023), https://www.elliptic.co/blog/analysis/crypto-mixers-and-privacy-protocols-the-sanctions-compliance-implications [https://perma.cc/VX6A-UW92].

[183] *See* Berg & McCarthy, *supra* note 83, at 3.

[184] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 18.

[185] *See* Multi.io Research, *Explained: DeFi Governance Tokens*, MEDIUM (Nov. 17, 2020), https://medium.com/multi-io/explained-defi-governance-tokens-23a76e4df543 [https://perma.cc/Q89W-UUS2] (describing "the basics of governance tokens and the various governance models used by some of the better-known DeFi projects").

and illicit engagement. Although no traditional financial intermediaries are involved, this method resembles the layering stage of classical ML,[186] as it obscures the source of criminal proceeds through multiple asset conversions. Critically, because DAO treasuries often fall outside the scope of existing AML frameworks—including the FATF's definitions of VASPs—they present a structural blind spot for regulators attempting to trace and interdict illicit financial flows within decentralized ecosystems.[187]

DeFi services governed by DAOs can be exploited to obscure the origin of funds linked to criminal activity by moving them through a series of transactions involving distinct DAO-operated protocols. A common method involves depositing cryptocurrency purchased with illicit proceeds into a DAO-managed lending platform and using that deposit as collateral to obtain a loan in a different digital asset. The loan proceeds are then converted through a decentralized exchange and reinvested into another DAO-governed protocol.[188] Although each transaction is recorded on a public blockchain, the speed and complexity of these operations—combined with repeated asset conversions—make it difficult for investigators to reconstruct the path of the funds. The challenge is further heightened when privacy-enhancing technologies, such as cryptocurrency mixers or privacy-focused tokens, are used to obscure activity.[189] The FATF has identified such patterns as ML red flags. These include repeated conversions between digital assets and the use of tools designed to obscure user identities.[190] Because these activities occur across autonomous protocols without centralized intermediaries, regulatory authority becomes diffuse, complicating supervisory jurisdiction and coordinated enforcement efforts.[191]

G. *DAOs and ML: Where to Go from Here?*

The methods and patterns examined in this Part highlight the increasingly sophisticated ways in which DAOs can be exploited for ML-purposes. These range from structural weaknesses such as decentralization and pseudonymity (Part III.A, *infra*), to technical exploits involving smart contracts and flash loans (Part III.B, *infra*), governance manipulation via token-based voting (Part III.C, *infra*), cross-chain complexity that obscures fund trails (Part III.D, *infra*), jurisdictional arbitrage that exploits

---

[186] *See* Part II.B, *supra*.
[187] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 15, 28–29.
[188] *See id*. at 16–17.
[189] *See* Chainalysis Team, *Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group*, CHAINALYSIS (Feb. 15, 2024), https://www.chainalysis.com/blog/2024-crypto-money-laundering/ [https://perma.cc/G823-T3E4].
[190] *See* RED FLAG INDICATORS, *supra* note 116, at 8–12; FIN. ACTION TAST FORCE, COUNTERING RANSOMWARE FINANCING 15–18 (2023), https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html [https://perma.cc/BGX7-GPGU].
[191] *See, e.g.*, RED FLAG INDICATORS, *supra* note 116, at 18 (describing how a virtual asset service provider has moved its operations across jurisdictions to evade regulations).

regulatory gaps (Part III.E, *infra*), and specific laundering methods that combine these Part III (Part III.F, *infra*).

Together, the insights discussed herein expose a deeper regulatory mismatch: current AML frameworks were built for a financial system anchored in centralized control, jurisdictional clarity, and institutional accountability—characteristics largely absent in DAO ecosystems. Figure 1, *infra*, summarizes these DAO vulnerabilities and associated enforcement challenges and their impact on AML enforcement. Notably, despite some legislative and policy efforts, the broader AML legal architecture remains rather fragmented, inconsistent, and ill-equipped to address DAO-related challenges. The following Parts critically examine how authorities in the United States at the national level (Part IV), the EU at the regional level (Part IV), and in international organizations at the global level (Part V) have tried to respond to this gap. Part VI then examines whether a coordinated, cross-border AML regime is needed to prevent DAO-enabled laundering.

Figure 1. Structural Foundations of AML Enforcement: Traditional Financial Institutions v. DAOs

AML Requirements	Traditional Financial Institutions	DAOs
Identifiable management Legal entity status	Named executives and directors Clearly incorporated with legal personality	Often pseudonymous or anonymous participants
Legal entity status	Clearly incorporated with legal personality	Often lack formal legal status or vary by jurisdiction
Jurisdictional anchoring	Fixed domestic incorporation and operations	Distributed across multiple jurisdictions and blockchains
Compliance infrastructure	Dedicated AML teams and KYC systems Licenses, fines and supervisory authority	Frequently absent; reliant on code-based or community tools Difficult to assign liability; unclear legal attribution
Regulatory entry points	Banks, custodians and payment processors	Smart contracts, wallets, cross-chain bridges.

IV. REGULATORY FRAMEWORKS IN THE UNITED STATES AND THE EU: INADEQUACY IN ADDRESSING DAO-BASED MONEY LAUNDERING

The vulnerabilities identified in Part III reveal fundamental incompatibilities between DAOs and traditional AML frameworks. This Part examines how two major jurisdictions—the United States and the EU—have attempted to address these challenges. The United States and the EU merit particular attention given their global regulatory influence, dominance in virtual asset market activity, and substantial enforcement records.[192] Their approaches, however, diverge significantly: the United States has primarily relied on case-driven enforcement and statutory reinterpretation, while the EU has pursued systemic legislative reform. Analyzing these divergent approaches reveals both the structural limits of current tools for regulating DAO-related financial activity and potential models for adapting them to DeFi systems.

The regulatory landscape beyond these jurisdictions varies considerably. Some countries have attempted to fit DAOs within existing legal categories through expansive interpretations, while others have introduced bespoke frameworks that grant DAOs legal personality.[193] Many jurisdictions, however, have taken little or no action, allowing DAOs

---

[192] For the United States, *see generally* THE WHITE HOUSE, PRESIDENT'S WORKING GROUP ON DIGITAL ASSET MARKETS, STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL FINANCIAL TECHNOLOGY (July 30, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf [https://perma.cc/8FYT-94D5] (describing U.S. regulation of digital assets). For the EU, *see* Chainalysis Team, *Institutions in Central, Northern, and Western Europe Broaden Horizons with DeFi and Web3 Experimentation*, CHAINALYSIS (Oct. 18, 2023), https://www.chainalysis.com/blog/western-europe-cryptocurrency-adoption; RUDI BECKER ĐURICIC ET AL., DIGITAL ASSETS: EU REGULATORY FRAMEWORK, MARKET UPTAKE, RISKS AND CHALLENGES (2025), https://www.europarl.europa.eu/RegData/etudes/IDAN/2025/779851/ECTI_IDA(2025)779851_EN.pdf [https://perma.cc/E262-XAZ9] (describing E.U. regulation of digital assets). For general information on both, *see generally* Raphael Auer, Ulf Lewrick & Jan Paulick, *DeFiying Gravity? An Empirical Analysis of Cross-Border Bitcoin, Ether and Stablecoin Flows,* 8–9 (BIS Working Papers, No. 1265, 2025), https://www.bis.org/publ/work1265.pdf [https://perma.cc/QA4A-QJMD] (describing cross-border flows of cryptocurrency); Aki Yokoyama et al., *Crypto Assets Monitor: Highlights: Q3 2025*, INTL. MONETARY FUND 9 (2025), https://www.imfconnect.org/content/dam/imf/News%20and%20Generic%20Content/GMM/Special%20Features/GMM%20Special%20Feature%20-%20Crypto%20Monitor%20October%202025.pdf [https://perma.cc/3PR9-B8PX] ("Additional regulatory clarity with the adoption of the U.S. Genius Act and the application of MiCA regulation in Europe created a pathway for more institutional adoption of stablecoins.").

[193] *See* Korotana, *supra* note 178, at 1, 15; *see also* Wyo. Stat. Ann. §§ 17-31-101 – 17-31-116 (2021). Similarly, the State of Vermont has enacted a "blockchain-based LLC" statute designed to accommodate DAO governance structures. *See* Vt. Stat. Ann. tit. 11, § 4173 (2023). Malta's Innovative Technology Arrangements and Services regime likewise provides a regulatory vehicle for DAOs to operate under Maltese law, effectively legitimizing DAOs within the European Union. *See* Innovative Technology Arrangements and Services (ITAS) Certification Regulations, 2024 (S.L. 591.01) (Malta).

to operate without meaningful oversight.[194] This regulatory vacuum, coupled with the ease with which DAOs can migrate across borders or reconfigure governance structures, facilitates regulatory arbitrage. Even where robust AML regimes exist, DAOs can bypass them by decentralizing control or situating operations in jurisdictions with minimal enforcement capacity.[195] As a result, DAOs not only challenge the scope of existing AML obligations but also expose the jurisdictional limitations of enforcement in a borderless financial ecosystem.[196]

A. *The United States*

1. Federal Level

The United States does not yet have a federal statute specifically tailored to the regulation of DAOs.[197] Instead, federal authorities have generally adopted a substance-over-form approach, holding that a DAO's decentralized structure does not shield it from legal obligations if it engages in activities already subject to regulation.[198] Accordingly, if a DAO issues

---

[194] *See* Naudts, *supra* note 46, at 15 ("[L]egal recognition of DAOs continues to be very limited worldwide, some US states (Vermont, Colorado, Wyoming and Tennessee) have also introduced laws specifically targeting them, as have the Cayman Islands, Switzerland and Singapore."); Kyung Taeck Minn, *Towards Enhanced Oversight of "Self-Governing" Decentralized Autonomous Organizations: Case Study of the DAO and Its Shortcomings*, 9 J. N.Y.U. J. INTELL. PROP. & ENT. L. 139, 160 (2019) ("Smart contracts are currently in a blind spot of the law and if Black and Kraakman teach us anything, it is that self-governance of corporation-like entities will fail in the absence of well-established legal institutions. If left to their own devices without legal intervention, a self-governing DAO will most likely engage in self-dealing at the expense of its investors.").

[195] *See* Furnari & Villani*, supra* note 162, at 122.

[196] *See* Korotana, *supra* note 178, at 11–12.

[197]Although Congress has not enacted a federal statute specifically regulating decentralized autonomous organizations, DAO-specific issues have been the subject of proposed legislation and congressional hearings. *See, e.g.*, S. 4356, 117th Cong. § 204 (2022) (as introduced); *Hearing on Crypto Crash: Why Financial System Safeguards are Needed for Digital Assets Before the Subcomm. on Banking, Hous. & Urb. Affs.*, 118th Cong. 13, 24 (2023) (statement of Lee Reiners, Policy Director, Duke Financial Economics Center, Duke University); *American Innovation and the Future of Digital Assets: From Blueprint to a Functional Framework Before the H. Comm. on Fin. Servs.*, 119th Cong. 4–5 (2025) (written submission of Amanda Fischer, Policy Director and COO, Better Markets).

[198] *See, e.g.*, Press Release, SEC, Statement by the Division of Corporation Finance and Enforcement on the Report of Investigation on The DAO (July 25, 2017), https://www.sec.gov/newsroom/speeches-statements/corpfin-enforcement-statement-report-investigation-dao [https://perma.cc/G4Z5-PSPC]; Press Release, SEC, BarnBridge DAO Agrees to Stop Unregistered Offer and Sale of Structured Finance Crypto Product (Dec. 22, 2023), https://www.sec.gov/newsroom/press-releases/2023-258 [https://perma.cc/3QDE-3JPV]; Press Release, SEC, SEC Charges Entities Operating Crypto Asset Trading Platform Mango Markets for Unregistered Offers and Sales of the Platform's "MNGO" Governance Tokens (Sep. 27, 2024), https://www.sec.gov/newsroom/press-releases/2024-154 [https://perma.cc/KT94-FGCF]; Press Release, SEC, SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities (July 25, 2017), https://www.sec.gov/newsroom/press-releases/2017-131 [https://perma.cc/2NN9-NE55]; Press Release, Ian McGinley,

securities, operates a trading platform, or facilitates financial services, it may be held to the same legal standards as traditional entities, regardless of its technical design or governance model. Based on this framework, U.S. regulators have pursued two primary strategies for DAO oversight. The first involves enforcement actions by federal agencies such as the U.S. Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC), treating DAOs as unincorporated associations or holding identifiable stakeholders accountable for the DAO's protocol operations. The second involves applying existing AML obligations—such as those under the BSA and OFAC's sanctions authority—to persons or entities involved in managing or facilitating a DAO's financial activities.[199]

The first strategy has been pursued most prominently by the CFTC, which has asserted jurisdiction over DAOs engaged in commodity-based token trading and digital asset derivatives markets.[200] Drawing authority from the Commodity Exchange Act,[201] the CFTC has interpreted its mandate to encompass platforms facilitating trading in digital asset derivatives. This position was first articulated in the 2015 Coinflip Inc. case, where the CFTC classified Bitcoin and other virtual currencies as commodities subject to its oversight.[202]

The Commission reaffirmed this stance in its 2017 Primer on Virtual Currencies, emphasizing that compliance with applicable laws is essential to preserving market integrity.[203] Although the CFTC does not

---

Director, Division of Enforcement, Commodity Futures Trading Comm'n, Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory (June 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23 [https://perma.cc/N9DV-THYF]; *Fact Sheet: The Financial Stability Oversight Council's Report on Digital Asset Financial Stability Risks and Regulation*, DEP'T OF TREASURY (Oct. 3, 2022), https://home.treasury.gov/system/files/261/Fact-Sheet-Report-on-Digital-Asset-Financial-Stability-Risks-and-Regulation.pdf [https://perma.cc/5BZL-J398].

[199] *See, e.g.*, notes 204–08 and accompanying text, *infra*.

[200] Commodity-based token trading refers to the exchange of digital tokens that either represent commodities—such as tokenized gold or oil—or are themselves classified as commodities, such as Bitcoin and Ether, which the CFTC has treated as within its jurisdiction. *See What Are Tokeized Commodities? A Guide*, KEYROCK, https://keyrock.com/knowledge-hub/what-are-tokenized-commodities-a-guide/ [https://perma.cc/BBL9-GH9Z] (last visited Apr. 30, 2026). In contrast, digital-asset derivatives markets involve the trading of financial contracts—such as futures, options, or swaps—whose value is derived from the price movements of underlying digital assets. *See* Robyn Llewellyn, Mayer Brown & Practical Law Finance, *Crypto Derivatives: Overview*, THOMSON REUTERS: PRACTICAL LAW (2024), https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2024/03/crypto-derivatives-overview_llewellyn_mar24.pdf%3Frev=-1 [https://perma.cc/GS48-9S5S] (last visited Apr. 30, 2026).

[201] Commodity Exchange Act, 7 U.S.C. §§ 1–27f (2023).

[202] *See* In the Matter of: Coinflip, Inc., CFTC Docket No. 15-29 (Sep. 17, 2015), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf [https://perma.cc/8FXB-2HBA].

[203] *See CFTC's LabCFTC Releases Primer on Virtual Currencies*, COMMODITY FUTURES TRADING COMM'N 1–3 (Oct. 17, 2017),

directly enforce AML regulations, its oversight involves compliance with certain BSA obligations, most notably the implementation of a customer identification program by registered "Futures Commission Merchants"—a cornerstone of AML compliance.[204] Consequently, the CFTC's regulation of DAOs indirectly engages AML considerations, particularly when decentralized platforms conduct activities triggering Futures Commission Merchant registration.

This enforcement approach has been tested in several landmark cases, including *bZeroX*.[205] There, the Commission alleged that the company and its DAO facilitated unlawful leveraged and margined retail-commodity transactions through a decentralized protocol.[206] The case concluded with a civil penalty and a cease-and-desist order, underscoring that transitioning to DAO governance does not absolve stakeholders or entities from regulatory obligations.[207]

In a simultaneous September 22, 2022 action, the CFTC applied the same legal theories it used against bZeroX to Ooki DAO, the successor DAO operating the same protocol.[208] In that case, the Commission alleged that Ooki DAO, which governed a decentralized trading protocol offering leveraged crypto derivatives, failed to register as a "futures commission merchant" and implement a customer identification program as required under the BSA.[209] The case raised critical questions about applying registration requirements and AML obligations to decentralized entities, including whether DAO token holders could be held individually liable. In a default judgment, the court found that Ooki DAO's failure to implement a customer identification program and AML safeguards exposed the protocol to illicit use and warranted substantial monetary penalties.[210] The Commission also issued a permanent injunction prohibiting Ooki DAO

---

https://www.cftc.gov/PressRoom/PressReleases/7631-17 [https://perma.cc/8LA5-HSYG].

[204] Compliance with Bank Secrecy Act, 17 C.F.R. § 42.2 (2023) (requiring each FCM to establish and implement a written customer identification program consistent with section 5318(l) of the Bank Secrecy Act); *see also* Bank Secrecy Act, 31 U.S.C. § 5318(l) (1970) (requiring financial institutions to establish reasonable procedures for verifying customer identity as part of an AML program).

[205] *See generally* In the Matter of bZeroX, LLC, CFTC Docket No. 22-31 (Sep. 22, 2022), https://www.cftc.gov/media/7676/enfbzeroxorder092222/download [https://perma.cc/NA6W-TVLR].

[206] *See id.* at 2–3; *see also* Press Release, CFTC, CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act (Sep. 22, 2022), https://www.cftc.gov/PressRoom/PressReleases/8590-22 [https://perma.cc/BP93-KHCA].

[207] *See id.* at 8–10, 11–12.

[208] *See generally* Commodity Futures Trading Comm'n v. Ooki DAO, CFTC No. 3:22-cv-05416-WHO (Dec. 20, 2022), https://www.cftc.gov/media/8741/enfookidaojudgment060923/download [https://perma.cc/4F6Z-HB25].

[209] *See id*. at 12, 18.

[210] *See id.* at 19–21, 23–24.

from operating or maintaining its website.[211] Notably, the Commission treated the DAO and its token holders as an unincorporated association collectively responsible for the protocol's regulatory violations, highlighting the legal risks inherent in decentralized governance structures.[212]

The CFTC's enforcement actions underscore three critical regulatory challenges in DAO oversight. First, establishing jurisdiction over decentralized protocols that lack legal entity status or identifiable operational headquarters. Second, determining liability when trading occurs autonomously through immutable smart contracts. Third, addressing supervisory gaps in code-based trading environments where traditional compliance mechanisms are absent.

These difficulties are compounded in cross-border and cross-chain contexts. For instance, in *bZeroX*, the transition to DAO governance—including the transfer of control over protocol operations and decision-making from a small group of identifiable developers to a token-holder–governed structure lacking a formal legal entity—demonstrated how decentralization can be used to evade compliance obligations.[213] Similarly, cross-chain activities facilitated by bridge protocols obscure transactional flows, creating significant oversight challenges.[214] As a CFTC advisory subcommittee report explains, while intermediated platforms can be subjected to familiar regulatory tools, DeFi protocols pose novel enforcement hurdles, including pseudonymous participation, the absence of conventional regulated intermediaries, and the difficulty of tracing illicit flows across chains and off-chain.[215]

Alongside the CFTC, the SEC has intensified its scrutiny of DAOs, focusing on securities law compliance but with significant spillover implications for AML enforcement. The SEC's concerns arise where DAOs issue tokens that qualify as "securities," triggering disclosure, registration, and investor protection obligations—mechanisms that intersect with transparency-based AML regimes. In its 2017 DAO Report, the SEC concluded that DAO tokens met the definition of "investment

---

[211] *See id.* at 24–25.
[212] *See id.* at 15–23.
[213] *See bZeroX, LLC*, CFTC Docket No. 22-31 at *2–4.
[214] *See* FATF, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS ON SO-CALLED STABLECOINS 8 (2020), https://www.fatf-gafi.org/en/publications/Virtualassets/Report-g20-so-called-stablecoins-june-2020.html [https://perma.cc/856W-9NKG] ("The ability of quickly exchanging between different virtual assets, a technique known as 'chain-hopping', allows the multiple layering of illicit funds within a short timeframe, thereby allowing a more sophisticated disguise of the origins of funds."); EUROPOL, THE OTHER SIDE OF THE COIN: AN ANALYSIS OF FINANCIAL AND ECONOMIC CRIME 15 (2023), https://www.europol.europa.eu/cms/sites/default/files/documents/The%20Other%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20Economic%20Crime%20%28EN%29.pdf [https://perma.cc/9RE3-FMDF] (describing the process of "chain hopping").
[215] *See* SUBCOMM. ON DIGIT. ASSETS & BLOCKCHAIN TECH., COMMODITY FUTURES TRADING COMM'N, DECENTRALIZED FINANCE 34–67 (2024).

contracts" under the test articulated by the United States Supreme Court in *SEC v. W.J. Howey Co.*[216] Applying the *Howey* framework, the Commission emphasized that decentralization does not exempt a DAO from federal securities law oversight.[217] Subsequent enforcement actions have reinforced this posture. In *SEC v. LBRY*,[218] for example, the U.S. District Court for the District of New Hampshire held that a blockchain token met the *Howey* criteria because it was marketed as an investment tied to the platform's success.

The SEC has also addressed DAOs directly. In 2022, the Commission brought an enforcement action against the American CryptoFed DAO,[219] which had filed Form 10 registration statements in an effort to become the first legally recognized DAO LLC under Wyoming law.[220] The SEC alleged that the DAO's disclosures were materially deficient and misleading, particularly regarding the structure, purpose, and economics of its two tokens (Ducat and Locke). It further questioned whether the DAO had a functional and reliable governance mechanism capable of fulfilling corporate obligations.[221] The SEC ultimately rejected the registration filings, halting the process and effectively preventing the DAO from offering its tokens to the public.[222]

While the enforcement actions discussed in this section do not involve direct allegations of ML or violations of AML statutes, they are nonetheless significantly instructive for understanding the structural and jurisdictional obstacles to effective oversight of DAOs. By treating DAOs as unincorporated associations or holding identifiable stakeholders accountable for protocol operations, agencies such as the CFTC and SEC

---

[216] 328 U.S. 293 (1946); *see also*, SEC ACT REPORT, *supra* note 58, at 17–18. Under the *Howey* test, a financial instrument qualifies as a security if it "involves an investment of money in a common enterprise," with a reasonable expectation of profits to be derived from the efforts of others. *See Howey*, 328 U.S. at 301.

[217] *See* SEC ACT REPORT, *supra* note 58, at 17–18; *see also* Hester M. Pierce, Comm'r, SEC, Speech: Not Braking and Breaking (July 21, 2020), https://www.sec.gov/newsroom/speeches-statements/peirce-not-braking-breaking-2020-07-21 [https://perma.cc/UVM5-ALRM].

[218] *See* SEC v. LBRY Inc., 639 F.Supp.3d 211, 220–21 (2022).

[219] *See* Press Release, SEC Seeks to Stop the Registration of Misleading Crypto Asset Offerings, SEC (Nov. 18. 2022), https://www.sec.gov/newsroom/press-releases/2022-208 [https://perma.cc/6DQJ-VTJC]; American CryptoFed DAO LLC, Securities Act Release No. 34-97659 1–6 (June 7, 2023), https://www.sec.gov/files/litigation/opinions/2023/34-97659.pdf [https://perma.cc/Y5QH-ABBS] [hereinafter *American CryptoFed DAO LLC*].

[220] Form 10 is a filing used to register securities with the SEC. It requires detailed disclosures about an entity's financial condition, governance structure, and the nature of the securities offered. *See SEC 3110 – Form 10*, PWC: VIEWPOINT (Mar. 19, 2025), https://viewpoint.pwc.com/dt/us/en/pwc/pwc_sec_volume/pwc_sec_volume_US/3000_registration_an_US/sec_3110_form_10_US.html [https://perma.cc/3H4G-5GRT].

[221] *See In re American CryptoFed DAO LLC*, Admin. Proc. File Nos. 3-20650 & 3-21243 (SEC administrative filings, including the order instituting proceedings and related documents). For a webpage with all of the documents, *see Administrative Proceeding File No. 3-20650*, SEC, https://www.sec.gov/enforcement-litigation/administrative-proceedings/3-20650 [https://perma.cc/R57E-AF7N] (last visited Apr. 8, 2026).

[222] *See American CryptoFed DAO LLC*, *supra* note 215, at 5–6.

have sought to apply traditional legal frameworks to decentralized systems. These efforts, however, expose significant regulatory mismatches. DAO-issued tokens may trigger registration and disclosure obligations under U.S. securities laws, which in turn intersect with AML compliance measures, such as customer-identification programs and suspicious-activity reporting.[223]

Yet, these mechanisms generally presuppose identifiable and obliged persons or intermediaries and workable jurisdictional anchors—features often difficult to locate in DAO architectures.[224] Moreover, DAOs' cross-border operations and reliance on autonomous, immutable smart contracts amplify these enforcement challenges.[225] This analysis underscores the need for a tailored AML framework capable of addressing the unique features of DAOs and preventing them from becoming vehicles for regulatory evasion in a borderless financial environment.

The second regulatory strategy employed by federal authorities involves classifying certain DAO activities as subject to AML obligations under the Bank Secrecy Act, for which FinCeN has primary responsibility for administration and enforcement.[226] Under FinCEN oversight, DAOs that facilitate the exchange or transfer of virtual currencies may be treated as "money transmitters."[227] Being classified as a "money transmitter" under the BSA means that an entity is in the business of accepting and transmitting value on behalf of others, thereby triggering BSA obligations such as registration with FinCEN, implementation of AML programs, customer due diligence, recordkeeping and reporting requirements, such as the Travel Rule.[228] This second approach presents three key implementation challenges: (1) identifying accountable parties for BSA compliance in a decentralized and pseudonymous governance structure; (2) enforcing KYC obligations in distributed systems that lack centralized operational control; and (3) addressing jurisdictional ambiguities when

---

[223] *See, e.g.*, *LBRY Inc.*, 639 F.Supp.3d at 220–21; SEC ACT REPORT, *supra* note 58, at 3, 8, 17, 54–55; *see also* Bank Secrecy Act, 31 U.S.C. § 5318(h) (requiring covered financial institutions to establish AML compliance programs); 31 C.F.R. § 1020.210 (implementing AML program requirements); 31 C.F.R. § 1020.220 (mandating customer-identification programs); 31 C.F.R. § 1020.320 (requiring suspicious-activity reporting). These examples illustrate how securities-law obligations can intersect with AML compliance measures once regulated intermediary activity is implicated.

[224] *See, e.g.*, APPLICATION OF FINCEN'S REGULATIONS, *supra* note 146, at 7–14; FATF RISK-BASED APPROACH, *supra* note 10, at 78–87.

[225] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 11.

[226] 31 U.S.C. § 310(b)(2)(A) (2021).

[227] 31 U.S.C. §§ 5311–5332 (2021).

[228] The Travel Rule (FATF Recommendation 16) requires financial institutions and VASP to collect and share identifying information about senders and recipients for qualifying transfers. *See* FATF RISK-BASED APPROACH, *supra* note 10, at 82. This information must "travel" with the transaction to the next institution to help authorities detect suspicious activity and combat ML. *See* 31 C.F.R. § 1010.100(ff)(5)(i)(A) (defining "money transmitter" as any person engaged in the business of accepting currency, funds, or other value and transmitting it to another location or person by any means).

applying BSA requirements to smart contracts that operate autonomously and across national borders.

Expanding on this regulatory approach, FinCEN's interpretation of the so-called Travel Rule further underscores the complexity of imposing AML requirements on DAOs. The Travel Rule requires financial institutions to collect, retain, and transmit identifying information about the originator and beneficiary of transactions exceeding $3,000.[229] Although FinCEN's guidance does not treat DAOs as a distinct regulatory category, its broad interpretation of "money transmitters" and "financial institutions" may encompass DApps and other DAO-like arrangements facilitating convertible virtual currency transfers.[230] Consequently, DAOs function as VASPs and facilitate transactions above this threshold may be subject to the Travel Rule and required to comply with information-sharing obligations.[231] Yet, implementing such requirements in the DAO ecosystem is exceptionally difficult. This is because DAO's decentralized, automated, and pseudonymous nature makes it nearly impossible to collect and transmit personally identifiable information, exposing a fundamental incompatibility between traditional AML frameworks and DAO governance architecture.

These federal regulatory efforts have encountered significant hurdles in practice. The U.S. Department of the Treasury's 2023 risk assessment of DeFi services identified systemic vulnerabilities, noting that illicit actors exploit these platforms in part due to inadequate AML controls.[232] OFAC's attempt to sanction Tornado Cash and the Fifth Circuit's 2024 decision overturning the designation further underscore the structural misalignment between existing AML frameworks and DAO decentralized ecosystems, which continue to evade consistent and enforceable compliance systems catered toward centralized assets.[233]

The U.S. Department of Justice ("DOJ") has also pursued stakeholders who use DeFi and DAO protocols to launder illicit funds, relying on pre-existing statutory frameworks such as the Money Laundering Control Act,[234] unlicensed money transmission laws, and the BSA. In *United States v. Lichtenstein*, the DOJ charged two such stakeholders with conspiring to launder over 119,000 bitcoin stolen in the 2016 Bitfinex hack, alleging the use of decentralized tools, mixers, and

---

[229] *See* APPLICATION OF FINCEN'S REGULATIONS, *supra* note 146, at 11.
[230] *See id*. at 4–5, 11–12, 18, 27; FIN. CRIMES ENFORCEMENT NETWORK, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 6 (2020), https://www.fincen.gov/system/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf [https://perma.cc/8Q8J-3KAD]; U.S. DEP'T OF THE TREASURY ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS 8 (Sep. 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf [https://perma.cc/HK72-G4FW].
[231] *See* 31 C.F.R. § 1022.410(f).
[232] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 10.
[233] *See Van Loon*, 122 F.4th at 549 at 553–54, 563–64, 577–78.
[234] 18 U.S.C. §§ 1956–1957 (2022).

chain-hopping techniques to obscure the funds' origin.[235] In *United States v. Storm*, the DOJ charged Tornado Cash's co-founders with conspiracy to operate an unlicensed money transmission business and conspiracy to commit money laundering of over $1 billion, including funds tied to North Korea's Lazarus Group through decentralized mixing and obfuscation tools.[236]

The DOJ has also pursued actors exploiting DAO-governed platforms. In *United States v. Eisenberg*, filed in the Southern District of New York, for example, Avraham Eisenberg was charged with commodities fraud and manipulation for exploiting Mango Markets, a DAO-controlled DeFi protocol, to extract approximately $110 million through price manipulation and flash-loan abuse.[237] In the 2023 *United States v. Forsage,* filed in the District of Montana, indictment, the DOJ charged the founders of a purportedly decentralized investment platform with conspiracy to commit wire fraud in connection with a $340 million Ponzi scheme executed through smart contracts.[238] These cases reflect the U.S. federal government's pragmatic strategy of extending broad, pre-existing statutes and instruments—such as the Securities Act, Commodity Exchange Act, Bank Secrecy Act, and FinCEN guidance—to DAO-related activities rather than adopting DAO-specific legislation.

While this approach has produced some enforcement successes, it remains reactive, addressing misconduct only *after* it occurs and offering little prospective clarity for lawful DAO operators. This reactive posture becomes particularly problematic when enforcement tools are applied to organizational forms that do not fit the assumptions underlying existing AML statutes. More fundamentally, it fails to resolve the unique structural and jurisdictional challenges posed by DAOs, including their borderless operations, pseudonymous governance, and reliance on autonomous, self-executing code. For example, regulators invoking the BSA's definition of a "money transmitter"—which applies to any "person" engaged in the business of accepting and transmitting value on behalf of others—may attempt to treat DAO-related activity as subject to registration and AML obligations, even though value transfers in DAO-governed protocols are

---

[235] *See* No. 23-239 (CKK), 2025 LX 132979 28 (D.D.C. Apr. 4, 2025).
[236] *See* Sealed Indictment, United States v. Storm, No. 23 Cr. 430, paras. 24–37, 45, 55–62, 77–81 (S.D.N.Y. Aug. 21, 2023), https://storage.courtlistener.com/recap/gov.uscourts.nysd.604937/gov.uscourts.nysd.604937.1.0.pdf [https://perma.cc/UH22-2BTY]; *see also* Press Release, U.S. Att'ys Off. S.D.N.Y., Tornado Cash Founders Charged with Money Laundering and Sanctions Violations (Aug. 23, 2023), https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations#:~:text=The%20charges%20in%20the%20Indictment%20arise%20from%20the,Lazarus%20Group%2C%20the%20sanctioned%20North%20Korean%20cybercrime%20organization [https://perma.cc/3EZG-DVA9].
[237] *See* 784 F. Supp. 3d. 579, 579 (S.D.N.Y. 2025).
[238] *See* Press Release, Off. of Pub. Affs., Dep't of Just., Forsage Founders Indicted in $340M DeFi Crypto Scheme (Feb. 22, 2023), https://www.justice.gov/archives/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme [https://perma.cc/7PNX-9M4B].

executed automatically by smart contracts rather than by a human intermediary.[239]

Relying on this broad statutory formulation, FinCEN guidance may classify certain DAO-related activity as money transmission, yet this functional classification does not resolve the practical question of how such obligations can be implemented on decentralized systems with no executive management, no legal personhood, and no identifiable compliance counterpart.[240] As discussed above, DAOs lack the essential ingredient needed to implement many core BSA requirements: a clear subject capable of compliance. Applying the BSA to fully decentralized protocols thus underscores the inherent difficulty of reconciling traditional AML frameworks with the reality of globally distributed, leaderless networks.

Given this context, a recent legislative development that—while not DAO-specific—carries potentially significant implications for DeFi ecosystems is the Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025 (the "GENIUS Act").[241] The Act establishes a federal framework for the oversight of permitted-payment stablecoin issuers,[242] treating such entities as "financial institutions" for purposes of the BSA and requiring them to comply with AML and sanctions obligations.[243] Although the GENIUS Act does not amend the BSA directly, it mandates the U.S. Department of the Treasury, including FinCEN, to promulgate implementing regulations to define stablecoin-issuers compliance obligations.[244] The Act further authorizes both federal and state regulators to develop supervisory standards tailored to the stablecoin business model, including requirements for risk-based AML programs, suspicious activity monitoring, technological capabilities to comply with lawful orders, and sanctions screening mechanisms.[245] Importantly, the GENIUS Act also directs Treasury and FinCEN to explore technological approaches to illicit finance detection in digital asset environments, including blockchain analytics, automated compliance mechanisms, and privacy-preserving identity verification tools.[246]

While the GENIUS Act's provisions apply only to "permitted payment stablecoin issuers,"[247] its regulatory framework may be instructive

---

[239] *See* APPLICATION OF FINCEN'S REGULATIONS, *supra* note 146, at 7, 18, 27.
[240] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 7, 12.
[241] *See* PAUL TIERNO, CONG. RSCH. SERV., IN12553, STABLECOIN LEGISLATION: AN OVERVIEW OF S. 1582, GENIUS ACT OF 2025 1 (2025).
[242] *See* GENIUS Act, Pub. L. No. 119-27, 139 Stat. 419 (2025) [hereinafter GENIUS Act].
[243] *See Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law*, WHITE HOUSE, (July 18, 2025), https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/ [https://perma.cc/AML8-HKPZ].
[244] *See* Press Release, U.S. Dep't of the Treasury, Treasury Issues Request for Comment Related to the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) ACT (Aug. 18, 2025), https://home.treasury.gov/news/press-releases/sb0228 [https://perma.cc/JRF6-S92L].
[245] *See* GENIUS Act §§ 4, 6–9.
[246] *See id*. § 9.
[247] *See id*. § 3.

for the future regulation of DAO-governed financial systems. First, the Act establishes a precedent for extending BSA treatment to new DeFi actors based on functionality rather than legal form.[248] This logic could support the classification of certain DAOs as financial institutions when they perform intermediation functions—such as issuing tokens, facilitating lending, or providing decentralized exchange infrastructure.[249] Second, the Act demonstrates how technological capacity mandates—such as the ability to freeze or reject transactions pursuant to lawful orders—could serve as a condition of regulatory legitimacy for digital asset systems, potentially informing how policymakers approach pseudonymous DAO governance.[250] Finally, the Act's emphasis on AML innovation, including anticipated rulemaking on DeFi-specific risk mitigation standards, may signal a shift toward supervisory strategies that align more closely with the operational realities of decentralized protocols.[251] Thus, although DAOs are not yet encompassed by the GENIUS Act, the legislation's modular structure may serve as a blueprint for future regulatory adaptations targeting DAO-mediated financial crime.

2. State Level

While U.S. federal regulators have relied on existing statutes and enforcement tools to oversee DAOs, several U.S. states have sought to address the regulatory vacuum by crafting their own frameworks for virtual assets and DAO-governed transactions. These initiatives—most notably New York's BitLicense regime and Wyoming's DAO LLC statute—reflect U.S. state-level efforts to bring the DeFi ecosystem within traditional legal oversight. Yet, jurisdictional boundaries structurally constrain these efforts' effectiveness because DAOs, as explained above, operate without geographic anchoring, often operate beyond the territorial reach of any single state. This reality raises fundamental questions about whether such frameworks can impose meaningful AML obligations or achieve compliance within decentralized ecosystems.

New York's BitLicense regime governs virtual currency businesses by requiring a license for entities engaged in "Virtual Currency Business Activity."[252] The law's broad definition for what constitutes a governed entity *might* thus encompass certain DAO operations, depending on their structure and functional scope. For example, DAOs that facilitate the exchange, custody, or issuance of virtual assets—such as decentralized exchanges or lending protocols—may fall within the framework's reach and be required to obtain a license from the New York Department of

---

[248] *See id.*
[249] *See* APPLICATION OF FINCEN'S REGULATIONS, *supra* note 146, at 1–4, 7.
[250] *See* GENIUS Act at § 4(a)(5); *see generally* H.R. COMM. ON FIN. SERVS, SECTION-BY-SECTION ANALYSIS OF THE GENIUS ACT (2025), https://financialservices.house.gov/uploadedfiles/2025-07-10_--_sbs_floor_genius_final.pdf?utm_sourc.com [https://perma.cc/KD6R-HD5U].
[251] *See* GENIUS Act § 9; *see e.g.*, Press Release, U.S. Dep't of the Treasury, Treasury Issues Request, *supra* note 244.
[252] N.Y. Comp. Codes R. & Regs. tit. 23, § 200.3 (2015).

Financial Services.[253] By contrast, DAOs focused solely on governance, voting, or other non-financial activities are typically excluded unless their functions are directly tied to covered financial operations. The regime's applicability thus depends on a DAO's substantive activities rather than its organizational form.

DAOs subject to the BitLicense regime are required to comply with extensive obligations, divided broadly into licensing and AML compliance. Entities engaged in covered activities must obtain licenses, submit to background checks for "control persons," maintain capital thresholds, and implement internal compliance programs.[254] The regime further requires licensees to maintain an AML program that includes customer identification and verification procedures, transaction monitoring, suspicious activity reporting, and, on a risk-based basis, enhanced due diligence for high-risk clients.[255]

Although the BitLicense obligations are comprehensive, their application to DAOs exposes structural challenges that reflect a fundamental conceptual mismatch. DAOs transacting in virtual currencies typically operate through pseudonymous blockchain addresses, complicating customer identification and background checks. Smart contracts further undermine compliance mechanisms, including transaction monitoring and the ability to freeze suspicious transfers. Moreover, the BitLicense regime presumes a traditional organizational structure—centralized control, identifiable actors, and a fixed jurisdictional nexus—misaligned with DAOs' operational reality.[256] Governed by pseudonymous token holders and deploying autonomous smart contracts across borders, DAOs elude state-level licensing regimes, thus significantly constraining the effectiveness of such regimes in mitigating ML risks within DeFi systems.

Additionally, recent state-level enforcement outside the BitLicense regime underscores the jurisdictional and structural challenges regulators face when applying traditional registration-based frameworks to crypto-asset platforms that operate through online, cross-border infrastructure. In *People v. MEK GLOBAL LIMITED and PHOENIXFIN PTE LIMITED d/b/a KUCOIN*,[257] the New York attorney general pursued KuCoin, a Seychelles-based cryptocurrency trading platform owned and operated through entities in Seychelles and Singapore, for offering and selling cryptocurrencies alleged to be securities and commodities to New York residents without registering under New York's Martin Act and Executive Law § 63(12) and for falsely representing itself as an exchange.[258] Although

[253] *See id.* § 200.2(q)(1)–(5).
[254] *See id*. § 200.2(q).
[255] *See id*. § 200.15.
[256] *See id*. §§ 200.2(h), 200.3; *see also* Frank Emmert, *Cryptocurrencies: The Impossible Domestic Law Regime*, 70 AM. J. COMP. L. 185, 191–92 (2022).
[257] Dkt. No. 0450703/2023 (N.Y.).
[258] *See* Press Release, N.Y. Att'y Off., Attorney General James Secures More Than $22 Million from Cryptocurrency Platform for Operating Illegally (Dec. 12, 2023),

KuCoin is not a DAO, the case usefully illustrates the difficulty of asserting *ex ante* oversight over offshore crypto-asset platforms that make services available to forum-state users without registration, often leaving regulators to proceed through *ex post* enforcement rather than ordinary licensing or supervisory mechanisms.[259]

This challenge is further emphasized by the *Celsius* bankruptcy proceedings, which, although regulated by federal law, similarly revealed the difficulty of regulating platforms operating outside conventional forum-state oversight mechanisms and legal frameworks and thus are helpful to consider alongside the KuCoin affair.[260] Although Celsius was not structured as a DAO, its business model—combining custodial services, yield-generating lending, and some on-chain elements—underscored the complexity of regulating entities that function across both centralized and decentralized paradigms.[261] These enforcement challenges are even more pronounced in the DAO context, where legal personhood is absent, governance is pseudonymous, and financial transactions are executed autonomously through smart contracts. Together, these cases illustrate how existing regulatory tools struggle to address AML and compliance risks within increasingly DeFi systems in DAOs.

Recognizing the limitations of applying traditional regulatory frameworks to decentralized entities, Wyoming pioneered a novel legal structure under the Wyoming Decentralized Autonomous Organization Supplement Act (the "Wyoming Act"). The Wyoming Act grants legal recognition to DAOs by allowing them to register as LLCs under state law.[262] This enables DAOs to engage in commercial and organizational activities, including operating decentralized businesses, enter into enforceable contracts, pay for services, and fulfill tax obligations.[263] The Wyoming Act imposes specific registration requirements, such as filing articles of organization, designating a registered agent with a physical address in Wyoming, and publicly disclosing an identifier for any smart contract used to manage, facilitate, or operate the DAO.[264] Notably, the Wyoming Act requires that smart contracts used by a DAO be capable of

---

https://ag.ny.gov/press-release/2023/attorney-general-james-secures-more-22-million-cryptocurrency-platform-operating [https://perma.cc/H7UF-28R6].

[259] *See* Stipulation and Consent, People v. Mek Glob. Ltd., No. 450703/2023 (N.Y. Sup. Ct. Mar. 9, 2023), https://ag.ny.gov/sites/default/files/settlements-agreements/kucoin-stipulation-and-consent.pdf [https://perma.cc/C86F-2EKJ] (alleging that KuCoin operated through offshore entities, lacked registration or licensure in New York, and provided crypto-asset trading services to New York residents, necessitating enforcement under N.Y. Exec. Law § 63(12) and the Martin Act rather than through pre-registration oversight); Press Release, N.Y. Att'y Off., Attorney General James Continues Crackdown on Unregistered Cryptocurrency Platforms (Mar. 9, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-continues-crackdown-unregistered-cryptocurrency-platforms [https://perma.cc/C5HZ-SD2E].

[260] *See* In re Celsius Network LLC, 647 B.R. 631, 640–41, 643–44, 646–48 (Bankr. S.D.N.Y. 2023) (discussing the challenges of classifying Celsius "Earn Assets" under state contract law).

[261] *See id.* at 637–39.

[262] *See* Wyo. Stat. Ann. §§ 17-31-101 – 17-31-116 (2025).

[263] *See id.* § 17-31-105.

[264] *See id*. §§ 17-31-105(b), 17-31-106(b).

being updated or modified, reflecting a growing consensus that DAOs should allow for human intervention when needed.[265] It also shields DAO participants from personal liability for the organization's contractual breaches solely by virtue of their membership or participation.[266]

The Wyoming Act does impose independent AML or KYC obligations on DAO LLCs.[267] Although registration confers legal personhood—thereby enabling service of process and potential regulatory engagement—it does not subject DAOs LLCs to compliance requirements beyond those applicable to ordinary LLCs, which, as non-financial entities, are not independently regulated under AML statutes.[268]

This framework presents three structural limitations. First, while the Act permits DAOs to organize "for any lawful purpose, regardless of whether for profit," [269] it does not require disclosure of financial operations, ownership structures, or asset distribution mechanisms in formation documents, nor does it mandate financial reporting or audit requirements. DAO LLCs may therefore hold and transfer substantial digital assets without affirmative transparency obligations.[270]

Second, although the Act requires disclosure of a smart contract identifier at the time of registration, it provides no mechanism for monitoring subsequently modified, upgraded, or newly deployed contracts.[271] The disclosure requirement is thus static, while DAO infrastructure may evolve dynamically.

Third, the requirements to designate a governance structure and maintain a registered agent supplies only formal legal anchors.[272] Governance tokens may be dispersed across pseudonymous addresses and jurisdictions, complicating identification of control persons, and

---

[265] *See* Naudts, *supra* note 46, at 4, 21–22, 28–29; Walch, *supra* note 117, at 39, 56, 64 (arguing that supposedly decentralized crypto systems may still be subject to concentrated human control, including software changes and hard forks in response to crises).

[266] *See* Wyo. Stat. Ann. § 17-31-104 (2025).

[267] Nowhere in the Wyoming Act's current provisions, *see generally* Wyo. Stat. Ann. §§ 17-31-101 – 17-31-116 (2025), is there any requirement for DAO LLCs to implement an AML compliance program or perform KYC checks. The BSA imposes AML program requirements only on certain types of business defined as "financial institutions." This includes banks, brokers, casinos and money services business like money transmitters, but not ordinary companies or LLCs that are not engaged in financial services. *See generally* Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended
at 12 U.S.C. §§ 1829b, 1951-1959, 31 U.S.C. §§ 5311-5332). Simply forming an LLC does not trigger federal AML program rules. *See* 31 C.F.R. §1010.100(ff); *see also* 31 C.F.R. §1022.210 (requiring money transmitters (i.e., businesses transmitting funds for customers), which are a type of MSB, to register with FinCEN and implement AML programs).

[268] *See* Wyo. Stat. Ann. § 17-31-104 (2025).

[269] Wyo. Stat. Ann. § 17-31-105(c) (2025).

[270] *See id*. § 17-31-105.

[271] *See id*. §§ 17-31-106(b).

[272] *See id*. §§ 17-31-105, 17-31-106.

registered agents typically lack operational authority or insight into DAO financial activity.[273] Accordingly, the Act grants legal recognition without embedding compliance mechanisms tailored to the financial and cross-border characteristics of DAO operations, leaving material questions of transparency, accountability, and AML supervision unresolved.[274]

B. *The European Union*

As discussed in Part II, the EU has pursued AML regulation through successive AML Directives and, more recently, MiCA. Together, these aim to extend robust compliance obligations to centralized crypto-asset service providers. While these frameworks reflect the EU's ambition to establish comprehensive, cross-border oversight, they do not address the distinct ML risks DAOs pose. The decentralized, pseudonymous, and borderless nature of DAO operations undermines core regulatory assumptions embedded in the AMLDs and MiCA—namely, the existence of identifiable intermediaries and centralized compliance controls.

The following analysis examines how these structural limitations prevent existing EU frameworks from effectively addressing the unique challenges posed by DAOs. In practice, EU AML regulations allow Member States considerable implementation discretion, reflecting their varied resources and capacities.[275] While this flexibility lets national authorities tailor compliance efforts to local constraints, it often results in uneven enforcement and oversight across the Union.[276] Such divergence can undermine regulators' ability to address DAO-related risks: bad actors may engage in "regulatory arbitrage" by exploiting the weakest national regimes or slower compliance in certain jurisdictions.[277] A patchwork of enforcement intensities thus makes it difficult to present a united front against the cross-border, pseudonymous operations of DAOs.

MiCA's limitations in addressing DAOs become particularly clear when examining its underlying premise. As part of the EU's broader effort to establish cross-border oversight of crypto-asset markets, MiCA imposes

---

[273] *See* Ryan Gurule, Pol'y Dir., Fin. Accountability and Corp. Transparency Coal., Prepared Remarks for the Financial Accountability and Transparency Coalition: Wyoming's Trust and Limited Liability Company Industries and Financial Secrecy, at 4, 6 (Apr. 28, 2022), https://wyoleg.gov/InterimCommittee/2022/03-2022042711-03FACTCoalitionTestimony.pdf [https://perma.cc/L7FE-85AY].

[274] *See id*. at 5.

[275] *See* EUR. CT. OF AUDITORS, EU EFFORTS TO FIGHT MONEY LAUNDERING IN THE BANKING SECTOR ARE FRAGMENTED AND IMPLEMENTATION IS INSUFFICIENT 11 (2021), https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_EN.pdf [https://perma.cc/Q68F-6MLL].

[276] *See id*.

[277] *See Follow the Money, AMLA! – How to Unleash the EU's New AML Watchdog*, JACQUES DELORS CTR. (Oct. 7, 2025), https://www.delorscentre.eu/en/publications/detail/publication/follow-the-money-amla-how-to-unleash-the-eus-new-aml-watchdog [https://perma.cc/ER8G-7DA7].

robust compliance obligations on centralized service providers.[278] Its regulatory architecture presumes the existence of a central authority—an identifiable legal entity, such as an exchange, custodian, or wallet provider—that acts as an intermediary responsible for implementing AML controls and responding to supervisory oversight.[279] As demonstrated in Part III, however, DAOs directly challenge this model. Their governance structures lack the identifiable legal entities that MiCA relies on for assigning compliance obligations, leaving regulators without a clear counterpart to oversee or hold accountable.[280]

Similar structural mismatches exist with respect to the EU's AMLDs. The absence of a centralized or otherwise accountable legal entity within DAOs significantly undermines regulators' ability to enforce obligations under these directives. These EU directives presuppose the existence of centralized financial intermediaries with the legal capacity and operational infrastructure to implement compliance measures such as customer due diligence, transaction monitoring, and suspicious activity reporting.[281] This structural mismatch between the centralized assumptions of AMLD frameworks and the decentralized architecture of DAOs renders the enforcement tools embedded in the AMLDs—such as mandatory registration, licensing regimes, and direct supervisory oversight—ill-suited to address the unique AML risks they present.

A key illustration of this mismatch arises from the definition of VASPs under EU Directive 2018/843 (AMLD 5), which the European Parliament enacted on May 30, 2018, and which entered into effect on January 10, 2020.[282] Article 1(1)(c) extends EU AML obligations to entities engaged in activities such as exchanging virtual and fiat currencies, facilitating transfers between virtual assets, and providing custodial wallet services. These entities must register with national authorities and

---

[278] *See EU Supervisory Authorities Warn Consumers of Risks and Limited Protection for Certain Crypto-Assets and Providers*, EUR. BANKING AUTHORITY (Oct. 6, 2025), https://www.eba.europa.eu/publications-and-media/press-releases/eu-supervisory-authorities-warn-consumers-risks-and-limited-protection-certain-crypto-assets-and [https://perma.cc/QBM2-HSEG]; Press Release, Eur. Parliament, Crypto-assets: Green Light to New Rules for Tracing Transfers in the EU (Apr. 20, 2023), https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu [https://perma.cc/6FV9-VLQW].

[279] *See* MiCA, *supra* note 95, arts. 4, 5, 22, 23, 37, 38, 76, 81.

[280] *See generally* Luciano Quarta, *DeFi and MiCA: Another Missed Opportunity*, THE CRYPTONOMIST (Oct. 13, 2022), https://en.cryptonomist.ch/2022/10/13/defi-mica-another-missed-opportunity [https://perma.cc/5PVF-CG98]; Cristina Carata & William J. Knottenbelt, *An Analysis of the MiCA Regulation and Its Impact for Blockchain-Based Economics*, *in* MATHEMATICAL RESEARCH FOR BLOCKCHAIN ECONOMY 359 (Stefanos Leonardos et al. eds., 2024); *see also* DIRK A. ZETZSCHE ET. AL, REMAINING REGULATORY CHALLENGES IN DIGITAL FINANCE AND CRYPTO-ASSETS AFTER MICA 7 (May 2023), https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740083/IPOL_STU(2023)40083_EN.pdf [https://perma.cc/4YZN-6EKY].

[281] *See* CRYPTO-ASSET REPORT, *supra* note 40, 33–41.

[282] *See* Directive (EU) 2018/843, *supra* note 94.

implement comprehensive AML and KYC measures.[283] This definition, however, problematically presumes the existence of a centralized actor, with a clearly identifiable legal or natural person responsible for compliance.[284] When applied to DAO-like or fully decentralized protocols, this provider-centric framework may create a regulatory blind spot,[285] because it presumes an identifiable crypto-asset service provider with legal status, articles of association, AML compliance contacts, and responsible natural or legal persons subject to authorization and sanction.[286]

This distinction between centralized and decentralized frameworks becomes even more pronounced when considering EU Directive 2024/1640 (AMLD 6), which the European Parliament enacted on May 31, 2024, and which sought to strengthen the EU's AML regime by harmonizing offenses and expanding liability provisions.[287] Unlike AMLD 5, which focused on extending AML obligations to VASPs operating as identifiable intermediaries, AMLD 6 aimed to ensure that both natural and legal persons can be held accountable for ML offenses.[288] Notably, AMLD 6 introduced provisions imposing criminal liability on legal persons—such as corporations or other structured entities—where offenses are committed

---

[283] *See* EUR. BANKING AUTH., OPINION ON MONEY LAUNDERING AND TERRORIST FINANCING RISKS AFFECTING THE EU'S FINANCIAL SECTOR 2, 22 (July 28, 2023), https://eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2023/1058335/EBA%20Op%202023%2008%20Opinion%20on%20MLTF%20risks%20EBA%20REP%202023%2021.pdf [https://perma.cc/JTW7-69NQ].

[284] *See* Directive (EU) 2018/843, *supra* note 94, art. 8.

[285] *See* STEFAN BERGER, REPORT ON THE PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON MARKETS IN CRYPTO-ASSETS AND AMENDING DIRECTIVE (EU) 2019/1937 arts. 6, 30, 84, 122–23 (2022), https://www.europarl.europa.eu/doceo/document/A-9-2022-0052_EN.html [https://perma.cc/A77D-V6VD].

[286] *See Crypto Service Providers in the DeFi Space – Is Money Laundering Regulation a Dealbreaker for an Engagement in Decentralized Finance*, FIN LAW (Jan. 8, 2024), https://fin-law.de/en/2024/01/08/crypto-service-providers-in-the-defi-space-is-money-laundering-regulation-a-dealbreaker-for-an-engagement-in-decentralized-finance/ [https://perma.cc/5KBW-AZ2E].

[287] *See* Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May on the Mechanisms to Be Put in Place by Member States for the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, Amending Directive(EU) 2019/1937, and Amending and Repealing Directive (EU) 2015/849, 2024 O.J. (L 1640), art. 114, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401640 [https://perma.cc/SV9G-U8BM]; Chiara Jezerca, The Rise of Cryptocurrencies: A Tool for Money Laundering or an EU Regulatory Failure? 36–38 (Apr. 7, 2025) (unpublished manuscript) (on file with Brunel University of London); Georgios Pavlidis*, Targeted Financial Sanctions and the Evolving EU AML/CFT Framework: What's Changing and Why It Matters*, 9 BRATISLAVA L. REV. 193, 194–97 (2025).

[288] *See* Francesco Paolo Patti, *Towards a Global Anti-Money Laundering Law for Crypto-Assets*, 56 GEO. J. OF INT'L. L. 697, 716–17 (2025); Cécile Volten, Michel van Eeten & Rolf van Wegberg, *Money for Nothing, Supervision for a Fee: Investigating the Effects of the 5th Anti-Money Laundering Directive on Cryptocurrency Exchanges in the Netherlands,* EUR. J. ON CRIM. POL'Y & RSCH. 1, 3–4 (2025); *Virtual Asset Service Providers ('VASPs'),* CENT. BANK OF IR., https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/virtual-asset-service-providers [https://perma.cc/DN3V-Y7M3] (last visited Apr. 9, 2026); *see also* Directive (EU) 2024/1640, *supra* note 287, arts. 5, 7, 8.

for their benefit by stakeholders acting in a managerial capacity or resulting from a failure of supervision.[289]

Although AMLD 6's innovation closed important enforcement gaps in traditional corporate contexts, its effectiveness in addressing DAOs is limited. As noted above, DAOs lack both legal personality and centralized governance structures through which managerial liability could attach.[290] DAOs' lack of a corporate body, supervisory officers, or controlling persons undermines the AMLD's corporate liability regime, which is founded on a premise of imposing accountability on an entity for the actions of its agents.[291] As a result, even with AMLD 6's broadened enforcement and sanctions, DAOs and fully decentralized protocols may remain insulated from the directive's reach, perpetuating significant vulnerabilities in the EU's AML architecture.

Similar challenges arise in the space of transaction monitoring requirements. The EU's 2023 Transfer of Funds Regulation (the "Regulation"), designed to enhance traceability and transparency in crypto-asset transfers, forms a central component of the EU's AML framework.[292] Building on the principles of the FATF "Travel Rule," the Regulation imposes obligations on "crypto-asset service providers" to collect and transmit identifying information about the originator and beneficiary of crypto-asset transactions.[293] These measures seek to align the crypto-asset ecosystem with AML controls historically applied to traditional financial transfers, thereby mitigating risks of ML. Article 2(1) of the Regulation, however, cabins its scope to crypto-asset transfers involving at least one regulated "crypto-asset service provider."[294] This effectively excludes purely peer-to-peer transactions that bypass intermediaries—a scenario especially common in DAO-based ecosystems, where tokens are exchanged directly between users through unhosted wallets.[295]

---

[289] *See* Directive (EU) 2024/1640, *supra* note 287, art. 114.
[290] *See* David M. Grant, Eric M. Kirby & Steven Hawkins, *Decentralized Autonomous Organizations: To Statutorily Organize or Not*, 24 WYO. L. REV. 59, 69–75 (2024), https://scholarship.law.uwyo.edu/wlr/vol24/iss1/2 [https://perma.cc/7EKD-A9C6]; *see also* Directive (EU) 2018/1673, of the European Parliament and of the Council of 23 Oct. 2018 on Combating Money Laundering by Criminal Law, 2018 O.J. (L 284) 22, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673 [https://perma.cc/6PAV-CU7U].
[291] *See* Directive (EU) 2024/1640, *supra* note 287, arts. 11–13. According to the Directive, Member States are required to impose criminal liability on legal persons for money-laundering offenses committed for their benefit by persons in a leading position or made possible by a lack of supervision or control. *See id.* § 4.
[292] *See* Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May on Information Accompanying Transfers of Funds and Certain Crypto-Assets and Amending Directive (EU) 2015/849, 2023 O.J. (L 150), https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng [https://perma.cc/XSQ7-TW4E].
[293] *See id.* preemptory paras. 10–12, arts. 14–16.
[294] *See id.* art. 2.
[295] *See* Kai Wang, *Regulating Cryptocurrency Non-Custodial Service Providers Through the Bank Secrecy Act,* 4.2 U. CHI. BUS. L. REV. (2025), https://businesslawreview.uchicago.edu/print-archive/regulating-cryptocurrency-non-

The Regulation's reliance on identifiable and accountable intermediaries further poses inherent enforcement challenges in the DAO context, void of a centralized governance structure or legal entity capable of fulfilling compliance obligations.[296] Furthermore, the pseudonymous nature of blockchain transactions and the automated execution of DAO smart contracts complicate the collection and verification of originator and beneficiary information.[297] As a result, fulfilling the regulatory ambition of monitoring and tracing crypto-asset flows becomes particularly difficult in the context of fully decentralized DeFi protocols, including DAO-governed arrangements, leaving significant gaps in AML oversight and enforcement.[298]

C. *Existing Regulatory Frameworks: The Bottom Line*

As the analysis of the U.S. and EU regulatory frameworks demonstrates, existing virtual asset regulatory schemes, including AML regimes, are fundamentally ill-equipped to address the structural and jurisdictional challenges posed by DAOs. While federal and state authorities in the United States have adopted a case-driven approach, and the EU has pursued systemic legislative reforms, both jurisdictions rely on regulatory tools that presuppose centralized intermediaries and clear jurisdictional anchors. These approaches, though divergent in form, share a common limitation: they are designed for financial systems in which accountability can be imposed on identifiable entities or stakeholders within defined territorial boundaries. DAOs' decentralized, cross-border structures, by contrast, enable them to evade traditional compliance controls and exploit disparities between jurisdictional regulatory regimes. The ability to migrate governance and operations across borders exacerbates these enforcement gaps, revealing the inherent limitations of territorially bounded AML frameworks.

---

custodial-service-providers-through-bank-secrecy-act [https://perma.cc/ZB73-V6R9]; David Carlisle, *Unhosted Wallets: Crypto's Biggest Compliance Conundrum*, ELLIPTIC (July 18, 2022), https://www.elliptic.co/blog/analysis/unhosted-wallets-crypto-s-biggest-compliance-conundrum [https://perma.cc/26MP-9FY6].

[296] *See* Aniruddh Vadlamani & Sarthak Sharma, *Bridging the Divide Between DeFi and Regulators: Showcasing Decentralized Autonomous Governance as the Future for Self-Custody Wallet Regulation*, UNIV. ILL. J. L. TECH. & POL'Y 373, 377, 379, 381, 386, 389–91 (2023).

[297] *See Unlocking Compliance: AML Policies for DeFi Protocols Decoded,* FIN. CRIME ACAD. (Jan. 20, 2026), https://financialcrimeacademy.org/aml-policies-for-defi-protocols/ [https://perma.cc/L4MK-NR36].

[298] *See* EUR. BANKING AUTH., JOINT REPORT: RECENT DEVELOPMENTS IN CRYPTO-ASSETS 10–11, 19–20, 23–24, 26–28, 54–56 (2025), https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1391_Joint_Report_on_recent_developments_in_crypto-assets__Art_142_MiCA.pdf [https://perma.cc/RB9Z-VTE6]; Press Release, Eur. Banking Auth., EBA Issues Guidance to Crypto-Asset Service Providers to Effectively Manage their Exposure to ML/TF Risks (Jan. 16, 2024), https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-guidance-crypto-asset-service-providers [https://perma.cc/JF9G-B7JV].

These limitations underscore the need for coordinated international responses and highlight the critical role of global standard-setting bodies in addressing regulatory blind spots that national and regional frameworks have failed to close. Part V turns to the FATF and other international organizations to assess whether these global governance structures have managed to articulate a coherent or effective response to the regulatory challenges created by DAOs.

V. INTERNATIONAL ANTI-MONEY LAUNDERING FRAMEWORKS AND THEIR DAO BLIND SPOTS

A. *The Financial Action Task Force*

Although the FATF framework—as noted in Part II—constitutes the cornerstone of the international AML regime, its normative design presupposes a financial system populated by centralized intermediaries capable of implementing compliance obligations. This presumption is fundamentally misaligned with DAOs, which operate through pseudonymous governance and autonomous smart contracts, eliminating the institutional compliance touchpoints upon which the FATF framework depends. By displacing traditional gatekeepers, DAOs reveal a structural vulnerability in the global AML architecture that the existing FATF Recommendations cannot adequately address either conceptually or operationally.

This structural incompatibility becomes particularly evident when examining core FATF Recommendations in the context of DAO ecosystems. Recommendation 10, for example, obliges financial institutions to conduct customer due diligence and verify client identities and presupposes centralized onboarding mechanisms and identifiable account holders.[299] Similarly, Recommendation 24 mandates transparency of beneficial ownership to prevent the misuse of legal entities, thus requiring a centralized environment for proper effectiveness.[300]

DAOs, however, lack many of these compliance touchpoints, rendering customer due-diligence obligations infeasible. Furthermore, DAO governance rights are allocated through transferable tokens that can shift rapidly among pseudonymous token holders across jurisdictions without triggering conventional disclosure or reporting obligations.[301] This reality challenges the applicability of these and other FATF standards, which were designed for corporate environments where ownership

[299] *See* FATF INTERNATIONAL STANDARDS, *supra* note 89, at 66–74.
[300] *See FATF Guidance on Beneficial Ownership Recommendation 24 - Public Consultation,* FIN. ACTION TASK FORCE (Oct. 2022), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/R24-public-consultation-oct-2022.html [https://perma.cc/2A4S-GPBU].
[301] *See* SEC ACT REPORT, *supra* note 58, at 5, 8, 14–15; *see also* RISK ASSESSMENT OF DEFI, *supra* note 12, at 13–14, 29–30.

hierarchies remain relatively stable and traceable.[302] The ease with which governance tokens are transferred among pseudonymous participants within DAO dynamics undermines the core objective of beneficial ownership transparency, allowing malicious actors to obscure their identities, evade detection, and facilitate illicit financial activities.[303] Additionally, by diffusing governance rights across a globally distributed network of pseudonymous participants, DAOs frustrate the traceability of control and ownership that FATF standards presuppose, leaving regulators unable to enforce traditional disclosure obligations.[304]

This regulatory incongruity is further illustrated by Recommendation 16, the Travel Rule, which was extended in 2019 to cover VASPs. The Travel Rule, also discussed earlier in this Article, requires VASPs to collect and transmit originator and beneficiary information for virtual asset transfers exceeding either $1,000/€1,000 or the equivalent amount in local currency.[305] The Travel Rule's enforcement model relies on the presence of identifiable entities subject to regulatory oversight and capable of discharging legal obligations.[306] In decentralized ecosystems, however, this premise cannot be sustained, as no equivalent compliance infrastructure exists to operationalize the Rule's information-sharing requirements. This gap renders the provision unenforceable in DAO-mediated transactions.[307]

As discussed in preceding sections, DAO-mediated transactions typically occur outside the purview of regulated intermediaries. This structural characteristic—particularly the widespread reliance on unhosted wallets—intensifies the enforcement challenges surrounding Recommendation 16. Without an accountable entity to collect or transmit originator and beneficiary data, the Travel Rule becomes practically inapplicable, leaving a persistent compliance vacuum.[308] This deficiency is further exacerbated by divergent national approaches: While the EU requires crypto-asset service providers to verify ownership of unhosted

---

[302] *See, e.g.*, FIN. ACTION TASK FORCE, TRANSPARENCY AND BENEFICIAL GUIDANCE 3–5 (2014), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf [https://perma.cc/Y8XB-FJ3N].
[303] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 8.
[304] *See 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers,* FIN. ACTION TASK FORCE (June 2020), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/12-month-review-virtual-assets-vasps.html [https://perma.cc/2ZX3-6NTH]; *see, e.g.*, FATF RISK-BASED APPROACH, *supra* note 10, at 22–25, 50–52.
[305] *See* FATF INTERNATIONAL STANDARDS, *supra* note 89, at 17, 80–88 (Recommendation 16 and its Interpretive Note).
[306] *See id*.
[307] FIN. ACTION TASK FORCE, BEST PRACTICES: TRAVEL RULES SUPERVISION 5–10, 24–26 (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf [https://perma.cc/KA7W-RYKG].
[308] *See* Yaya Fanusie, *What FATF's Latest Guidance Means for DeFi, Stablecoins and Self-Hosted Wallets*, COINDESK (May 11, 2023), https://www.coindesk.com/policy/2021/11/09/what-fatfs-latest-guidance-means-for-defi-stablecoins-and-self-hosted-wallets [https://perma.cc/D3CA-XTWZ].

wallets above a €1,000 threshold,[309] the United Kingdom applies a risk-based approach that requires information collection only for transactions assessed as presenting elevated risks of illicit finance,[310] and the United States has yet to finalize its proposed FinCEN rule requiring reporting for unhosted wallet transactions exceeding $10,000.[311] Such regulatory fragmentation undermines consistent AML enforcement and enables DAO participants to exploit jurisdictional asymmetries, bypassing AML regulation.

The FATF's 2021 Guidance (the "Guidance") sought to address some of these challenges by clarifying that platforms labeled as "decentralized" are not exempt from AML obligations.[312] The Guidance urged regulators to identify stakeholders or entities exercising control or significant influence—such as developers, administrators, or dominant token holders—and to treat such actors as VASPs subject to compliance requirements.[313] This control-focused approach is reinforced by Recommendation 15, which calls on countries to identify and assess ML risks associated with virtual assets and VASPs.[314] Nevertheless, the Guidance and Recommendation 15 remain primarily focused on traditional compliance structures, such as cryptocurrency exchanges and other centralized service providers, and fail to address the distinctive challenges posed by DAOs.[315] Moreover, the approach is predicated on the assumption that meaningful control can be located and attributed—an assumption that fails in genuinely decentralized ecosystems where governance is diffuse and no participant exercises determinative authority.[316]

---

[309] *See* Press Release, Eur. Parliament, Crypto Assets: Deal on New Rules to Stop Illicit Flows in the EU (June 29, 2022), https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu [https://perma.cc/YA4S-9N6L].

[310] *See The UK Government's Proposal to Not Require Verification on Unhosted Wallets Likely Welcomed by Cryptocurrency Businesses,* MISHCON DE RAYA (June 28, 2022), https://www.mishcon.com/news/the-uk-governments-proposal-to-not-require-verification-on-unhosted-wallets-likely-welcomed-by-cryptocurrency-businesses [https://perma.cc/92TY-T7BX]. UK regulations require crypto businesses to assess the risk level of each transaction and collect information only when an elevated risk of illicit finance is identified. In the United States, FinCEN proposed a rule in December 2020 that would require reporting and recordkeeping for certain unhosted wallet transactions exceeding $10,000; however, as of 2025, the rule has not been finalized. *See Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets,* FIN. CRIMES ENF'T (Dec. 23, 2020), https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/requirements-certain-transactions-involving [https://perma.cc/M2M2-SCER].

[311] *See* Press Release, U.S. Dep't of the Treasury, The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions (Dec. 18, 2020), https://home.treasury.gov/news/press-releases/sm1216 [https://perma.cc/GME7-GYSZ].

[312] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 15; *see also* Fanusie, *supra* note 308.

[313] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 27.

[314] *See* FATF INTERNATIONAL STANDARDS, *supra* note 89, at 17, 78–79 (Recommendation 15 and its Interpretive Note).

[315] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 26.

[316] *See id*. at 28.

Even where developers or token holders exercise some degree of influence, attributing "control" sufficient to trigger VASP obligations can be legally tenuous. In cases of genuinely decentralized DAOs—where thousands of anonymous participants collectively hold governance tokens—FATF's attribution model may imply that each holder could be classified as a VASP.[317] This expansive interpretation, reflected in the U.S. CFTC's enforcement posture in Ooki DAO, is doctrinally impractical and likely unenforceable. Although some jurisdictions have attempted to impose compliance obligations through regulated third-party intermediaries, the FATF has acknowledged that such mechanisms are inherently difficult to implement in decentralized systems.[318] These limitations underscore the limitations of the current FATF framework in addressing DAO-mediated financial activity.

Furthermore, the absence of a globally agreed-upon definition of DAOs and consistent criteria for assessing decentralization degrees creates regulatory uncertainty and inconsistent treatment of functionally similar entities.[319] A DAO that operates a financial protocol may be classified as a VASP in one jurisdiction due to the visible involvement of a founding team or governance facilitators, thereby subjecting it to full AML compliance obligations—including customer due diligence, transaction monitoring, and reporting requirements. By contrast, another jurisdiction may conclude that the same DAO does not meet the criteria for VASP classification and thus fall outside the scope of AML oversight.

Consider, for example, ShapeShift's transformation from a centralized exchange to a DAO, which highlights how regulatory treatment of DeFi platforms may diverge across jurisdictions.[320] Before restructuring, ShapeShift operated as a custodial crypto-asset exchange and—after regulatory scrutiny in 2018—implemented KYC controls, effectively operating within the scope of the BSA framework applicable to money services businesses.[321] In 2021, however, ShapeShift announced it would dissolve its corporate structure and migrate to a DAO-based governance model, explicitly indicating that full decentralization would reduce its regulatory exposure by eliminating intermediary control over user funds.[322] As explained, pursuant to FinCEN guidance, AML obligations apply to any "person" who is engaged in the business of accepting and transmitting value for others. Thus, if a platform has no custodial control or identifiable intermediary accepting and sending value on behalf of users, classifying a

---

[317] *See id*. at 27–28.
[318] *See id*. at 40; *see also* RISK ASSESSMENT OF DEFI, *supra* note 12, at 32.
[319] *See* LAW COMM'N, *supra* note 21, at viii, 19.
[320] *See* SHAPESHIFT, https://shapeshift.com/ [https://perma.cc/B6KW-BE2H] (last visited Mar. 13, 2026).
[321] *See* Bianca Kremer, *The Second Wave of Digital Assets*, *in* BACK TO THE FUTURE: THE SIXTH REG@TECH ROUNDTABLE ON DIGITAL ASSETS (WHARTON BLOCKCHAIN & DIGIT. ASSET PROJECT, ed., 2022), https://bdap.wharton.upenn.edu/wp-content/uploads/2022/03/Reg@Tech-6-Report-Back-to-Future-Final.pdf [https://perma.cc/H6S5-D5ZT].
[322] *Id*.

fully decentralized protocol as a money-service business becomes legally contestable.[323]

By contrast, the European Union's AMLD 5 and MiCA take a more functional approach—one aligned with the FATF's VASP framework—focusing on whether an identifiable individual or entity is providing exchange services or exercising sufficient operational influence.[324] Under such an approach, the continued existence of a foundation, coordinating body, or user-facing interface associated with an ostensibly decentralized DAO could mean it is subject to VASP (or, under MiCA, "crypto-asset service provider"[325]) classification despite protocol-level decentralization. This definitional ambiguity enables DAO structures to evade uniform regulatory characterization, exacerbating international fragmentation and undermining coordinated AML enforcement. Without a shared legal standard for determining when a DAO constitutes an obligated entity, jurisdictions apply inconsistent thresholds, further eroding the coherence of the FATF framework for decentralized systems.

Importantly, these challenges are compounded by the FATF's reliance on a risk-based approach that grants jurisdictions wide discretion in assessing and addressing AML threats, resulting in fragmented and inconsistent regulatory treatment of DAOs across the globe.[326] Jurisdictions that view DAOs as high-risk financial entities may classify them as VASPs, thereby subjecting them to full compliance with FATF standards, including customer due diligence, transaction monitoring, and suspicious activity reporting.[327]

As discussed above, the United States has taken a reactive, enforcement-driven approach to applying AML rules against DAO-affiliated DeFi protocols but still lacks a dedicated regulatory framework for DAOs. The CFTC's 2022 enforcement action against Ooki DAO exemplifies this approach, treating the DAO as an unincorporated association and seeking to impose liability on token holders under existing regulatory frameworks.[328] Likewise, FinCEN has emphasized that regulatory obligations under the BSA are determined by activity rather than organizational form. Accordingly, decentralized entities such as DAOs that engage in the acceptance and transmission of value—including through software agents or smart contracts—may fall within the definition of a money transmitter and thus be required to implement an AML program pursuant to the BSA. Likewise, FinCEN has indicated that DAOs engaging in value transmission or similar activities may fall within the definition of a "financial institution" under the BSA, thus triggering mandatory AML

---

[323] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 28.
[324] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 27.
[325] *See* Regulation (EU) 2023/1113, *supra* note 292, at arts. 2, 14–16.
[326] *See generally* FATF RISK-BASED APPROACH, *supra* note 10.
[327] *See id*. at 15–20.
[328] *See* Complaint at 2–6, Commodity Futures Trading Comm'n v. Ooki DAO, No. 3:22-cv-5416 (N.D. Cal. Sep. 22, 2022); *see also* Order Granting Default Judgment at 11–13, Commodity Futures Trading Comm'n v. Ooki DAO, No. 3:22-cv-05416 (N.D. Cal. June 8, 2023).

program requirements regardless of their decentralized governance structure.[329]

In contrast, jurisdictions that perceive DAOs as lower-risk entities have adopted a functional approach that enables DAOs to operate with comparatively fewer AML compliance burdens—provided their activities do not directly involve regulated financial services. Switzerland, for instance, permits DAOs to obtain legal recognition by registering as associations or foundations under the Swiss Civil Code.[330] This structure grants DAOs formal legal personality while imposing minimal governance and reporting obligations unless the entity engages in financial intermediation, in which case full AML requirements apply.[331] Similarly, the Cayman Islands allow DAOs to register under the Virtual Asset Service Providers Act, often through foundation companies that reflect decentralized ownership structures.[332] While these DAOs must register with the Cayman Islands Monetary Authority and implement baseline AML controls, the regime remains significantly less burdensome than that of the United States, particularly during the early phase of compliance.[333]

These jurisdictional differences create an opening for regulatory arbitrage, wherein DAOs may strategically establish operations in jurisdictions characterized with weak AML frameworks, thereby circumventing stringent regulatory oversight. This regulatory arbitrage dynamic can incentivize jurisdictions to competitively lower their AML

---

[329] *See* APPLICATION OF FINCEN'S REGULATIONS, *supra* note 146, at 7–14, 18.
[330] *See* Schweizerisches Zivilgesetzbuch [ZGB] [Civil Code] Dec. 10, 1907, art. 60 [hereinafter Swiss Civil Code].
[331] *See* Press Release, FINMA, Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs) (Feb. 16, 2018), https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/ [https://perma.cc/K82Y-ZWS2]; Swiss Civil Code, *supra* note 330, arts. 60–79, 80–89.
[332] *See Cayman Islands Foundation Companies: The Ideal Vehicle for DAOs and Crypto Trading*, MOURANT (July 25, 2024), https://www.mourant.com/news-and-views/updates/updates-2024/cayman-islands-foundation-companies--the-ideal-vehicle-for-daos-and-crypto-trading.aspx [https://perma.cc/L2HQ-HEJ7]; Bradley Kruger, *DeFi, DAOs and VASPs in the Cayman Islands*, OGIER (Oct. 7, 2021) https://www.ogier.com/news-and-insights/insights/defi-daos-and-vasps-in-the-cayman-islands/ [https://perma.cc/C4C6-25AZ]; *see also* Loeb Smith, *Cayman Islands – CIMA's Review of VASPs*, LOEB SMITH: LEGAL INSIGHTS (Feb. 9, 2026), https://www.loebsmith.com/wp-content/uploads/2026/02/Legal-Insight-Cayman-Islands-CIMAs-Review-on-VASP-licensees-9-Feb-2026-004.pdf [https://perma.cc/4CPL-XSVB]; *see also* Agnes G. West, *Recommendations for Advancing US Competitiveness in the Global Digital Asset Sector*, MERCATUS CTR. GEORGE MASON UNIV. (June 29, 2022), https://www.mercatus.org/research/public-interest-comments/recommendations-advancing-us-competitiveness-global-digital-asset [https://perma.cc/4675-LJ6M].
[333] *See* FTS Admin, *The Cayman Islands Virtual Assets Framework*, FTS (Jan. 1, 2022), https://ftscayman.com/the-cayman-islands-virtual-assets-framework/ [https://perma.cc/CC7J-7TDJ]; *see also* Andrew J. Perkins, *Regulating Virtual Asset Service Providers in the Offshore World: The Cayman Islands Example* 16 L. & FIN. MKTS. REV. 266, 266–68, 270–72 (2023); *see also* Douglas S. Eakeley, et al., *Crypto-Enforcement Around the World*, 94 S. CAL. L. REV. 99, 105, 127 (2021).

standards to attract DAO operations, potentially triggering an AML regulatory race to the bottom.[334]

Notably, jurisdictional disparities are further exacerbated by the "soft law" character of the FATF framework. As a standard-setting body, the FATF lacks binding legal authority and relies primarily on peer pressure, mutual evaluations, and public listings to encourage compliance.[335] Such a governance model has resulted in uneven implementation of the Recommendations. This institutional weakness is highlighted by evidence that, as of mid-2023, fewer than one-third of assessed countries had fully enacted legislation implementing the Travel Rule, and an even smaller subset had operationalized supervisory or enforcement mechanisms.[336] In the context of DAOs, this normative fragility creates systemic vulnerabilities: jurisdictions may deprioritize enforcement against decentralized systems for political, economic, or institutional reasons, effectively creating regulatory havens. Similarly, as of mid-2023, among the fifty-three jurisdictions assessed by the FATF since 2021, most were found to exhibit major or moderate deficiencies in identifying virtual asset–related risks and applying effective AML controls.[337] As a result, the FATF's ability to coordinate a consistent and effective global response to DAO-mediated illicit activities is significantly diminished, leaving an enforcement vacuum that illicit actors are well positioned to exploit.

B. *International Monetary Fund*

The IMF has repeatedly emphasized the need for a "comprehensive, consistent, and coordinated" global approach to crypto-asset regulation, warning that fragmented or incomplete frameworks facilitate regulatory arbitrage and heighten systemic risk.[338] In its 2023 policy paper on crypto regulation, the IMF acknowledged that many participants in the crypto ecosystem—including developers, miners, and validators—do not fall within traditional legal categories, which complicates the application of existing supervisory tools.[339] These challenges are compounded by limited institutional capacity among national regulators, particularly when

---

[334] *See* FIN. STABILITY BD., THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE, *supra* note 130, at 3, 23–24.
[335] *See* Lovina E. Otudor & Mahmood Bagheri, *Legitimacy of Power Exercised by FATF Under International* Law, 31(6) J. FIN. CRIME 1289, 1290, 1295 (2024).
[336] *See* FATF TARGETED UPDATE, *supra* note15, at 4.
[337] *See* COUNCIL OF EUR. MONEY LAUNDERING AND TERRORIST FINANCING RISKS IN THE WORLD OF VIRTUAL ASSETS 6 (2023), https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 [https://perma.cc/3NKT-BAZG].
[338] Press Release, Int'l Monetary Fund, IMF Executive Board Discusses Elements of Effective Policies for Crypto Assets (Feb. 23, 2023), https://www.imf.org/en/news/articles/2023/02/23/pr2351-imf-executive-board-discusses-elements-of-effective-policies-for-crypto-assets [https://perma.cc/GJC5-TA4K].
[339] *See* INT'L MONETARY FUND, IMF POLICY PAPER: ELEMENTS OF EFFECTIVE POLICIES FOR CRYPTO ASSETS 2, 5, 7 (2023), https://www.imf.org/-/media/Files/Publications/PP/2023/English/PPEA2023004.ashx [https://perma.cc/3U84-Q58V] [hereinafter IMF POLICY PAPER].

attempting to design effective regulatory approaches for decentralized systems, discussed earlier.

While the 2023 Policy Paper does not address DAOs specifically, several of its core recommendations carry significant implications for DAO-based financial activity. The IMF's endorsement of enhanced international regulatory coordination, for example, [340] is particularly salient given the borderless architecture of DAOs and their capacity to operate outside any single jurisdiction's effective control. This aspect of DAO design intensifies the challenges identified by the IMF, especially the difficulty of applying AML obligations in the absence of clearly accountable actors.[341] As the IMF has warned, fragmented regulatory responses risk trigger a regulatory race to the bottom, with jurisdictions lowering oversight standards to attract decentralized projects and thus undermining global AML safeguards.[342]

The IMF also endorses the principle of "same activity, same risk, same regulation," urging that all entities performing equivalent financial functions be subject to comparable regulatory obligations, regardless of their organizational structure.[343] Applied to DAOs, this principle suggests that protocols facilitating lending, trading, or asset management should be held to the same standards as traditional financial institutions. Yet this assumption presumes the presence of accountable actors capable of compliance—an assumption that fails in many DAO contexts.[344]

Finally, the 2023 Policy Paper proposes a multilateral roadmap coordinated by the IMF, FATF, and the Financial Stability Board aimed at aligning national oversight of crypto-asset markets.[345] Although this effort promotes consistency, it relies on voluntary implementation by jurisdictions, many of which lack the capacity or political will to enforce stringent AML rules on DAO-based systems.[346] The roadmap reiterates the importance of enforcing existing FATF standards, yet it fails to address

---

[340] *See, e.g.*, *id.* at 2–3, 17, 33.
[341] *See, e.g.*, *id.* at 2–6, 8, 27–29.
[342] *See* Christine Lagarde, *A Regulatory Approach to Fintech*, INT'L MONETARY FUND (June 2018), https://www.imf.org/en/Publications/fandd/issues/2018/06/how-policymakers-should-regulate-cryptoassets-and-fintech-straight [https://perma.cc/8DC3-2AFF]; *see also* Kristalina Georgieva, Managing Director, Int'l Monetary Fund, Remarks at the MOEF-BOK-FSC-IMF International Conference on Digital Money: Leaving the Wild West: Taming Crypto and Unleashing Blockchain (Dec. 13, 2023), https://www.imf.org/en/news/articles/2023/12/13/sp121423-leaving-the-wild-west-kordigitalmoney [https://perma.cc/M53L-ZXGL].
[343] *See* IMF-FSB SYNTHESIS PAPER, *supra* note 149, at 2.
[344] *See* IMF POLICY PAPER, *supra* note 339, at 2–3.
[345] *See* FIN. STABILITY BD., G20 CRYPTO-ASSET POLICY IMPLEMENTATION ROADMAP: STATUS REPORT 1–3 (2024), https://www.fsb.org/uploads/P221024-3.pdf [https://perma.cc/UB3H-YAX7]. The FSB is an international standard-setting body comprising central banks, finance ministries, and supervisory authorities from the G20 economies and several additional jurisdictions, together with international financial institutions and other standard-setting bodies. It issues non-binding policy recommendations rather than directly enforceable rules. *See About the FSB*, FSB, https://www.fsb.org/about/ [https://perma.cc/5MFB-NHYA] (last visited May 1, 2026).
[346] *See* IMF-FSB SYNTHESIS PAPER, *supra* note 149, at 4–5.

how these standards can be applied in ecosystems that lack legal personhood, centralized ownership records, or designated compliance officers.[347] Notably absent is any guidance on how to operationalize core AML requirements—such as customer due diligence or suspicious activity reporting—in settings defined by pseudonymity, peer-to-peer transfers, and decentralized control.[348]

Hence, while the IMF's policy stance reinforces the need for consistent and comprehensive oversight, its current framework lacks the doctrinal tools and enforcement mechanisms necessary to address the structural features that enable DAOs to function outside the reach of traditional AML regimes. As with the FATF's approach, the IMF's regulatory vision presumes that meaningful accountability can be located within decentralized systems.[349] As previously explained, that presumption does not hold in practice—DAOs typically lack legal personhood, centralized control, or designated compliance roles, making it impossible to attach obligations to a specific entity or actor. Nor does the IMF provide practical guidance on how existing AML tools—such as customer due diligence, suspicious transaction reporting, or beneficial ownership identification—can be implemented in ecosystems dominated by unhosted wallets and pseudonymous participation.[350] Moreover, the 2023 Policy Paper overlooks the substantial enforcement challenges posed by jurisdictions that deliberately position themselves as crypto-friendly to attract DeFi activity.[351] Without resolving these structural and institutional gaps, the IMF's goal of global AML coordination will remain largely aspirational in the context of DAOs.

C. *United Nations*

The United Nations, primarily through the UN Office on Drugs and Crime (UNODC) and relevant Security Council committees,[352] has

---

[347] *See id.* at 26; *see also* FATF RISK-BASED APPROACH, *supra* note 10, at 21.
[348] *See* FATF RISK-BASED APPROACH, *supra* note 10, at 12.
[349] *See, e.g.*, IMF-FSB SYNTHESIS PAPER, *supra* note 149, at 1–6, 11–12, 35.
[350] *See generally* IMF POLICY PAPER, *supra* note 339. Instead, the Paper largely outlines high-level principles and risk frameworks for members without operationalizing how traditional AML tools like customer due diligence, suspicious transaction reporting, or beneficial ownership transparency apply in settings dominated by unhosted wallets and pseudonymous participation. *See generally id*.
[351] *See generally* IMF-FSB SYNTHESIS PAPER, *supra* note 149. The Paper describes broad policy and coordination goals without resolving how uneven national implementation or divergent regulatory approaches will be addressed. *See generally id*.; *see also* ARUSHI GOEL, PATHWAYS TO THE REGULATION OF CRYPTO-ASSET: A GLOBAL APPROACH 12–18 (2023), https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf [https://perma.cc/7SGX-KVGN].
[352] *See generally* Panel of Experts Established Pursuant to Security Council Resolution 1874 (2009), *Final Report*, U.N. Doc. S/2023/171 (Mar. 7, 2023), https://docs.un.org/en/S/2023/171 [https://perma.cc/6WC7-4DJA]; Letter dated 20 January 2020 from the Chair of the Security Council Committee Established pursuant to Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq

acknowledged the increasing use of cryptocurrencies to facilitate illicit financial activities, including ML with significant implications for global both financial stability and international security.[353] Notably, the UN Security Council has raised concerns about North Korea's use of cryptocurrency to finance illicit activities, citing evidence of state-sponsored cyberattacks on virtual asset platforms and the laundering of proceeds through privacy-enhancing decentralized tools.[354] These discussions underscore the evolving economic and security risks posed by decentralized systems, though the Council has not yet issued binding resolutions or guidance specifically targeting DAOs.[355]

The broader UN framework similarly lacks a coherent legal response to the AML risks posed by DAOs. While UNODC has developed technical resources to aid national enforcement authorities in tracking illicit flows within the digital asset ecosystem, its tools are designed primarily for systems with identifiable intermediaries, such as custodial exchanges or wallet providers.[356] As DAOs often function without these intermediaries, it becomes difficult to apply to such organizations conventional investigative techniques.

Beyond these technical constraints, the limitations of UNODC's approach stem fundamentally from its reliance on state-level

---

and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities addressed to the President of the Security Council, U.N. Doc. S/2020/53 (Jan. 20, 2020), https://digitallibrary.un.org/record/3848705?v=pdf [https://perma.cc/SN3Q-H7X3]; Letter dated 3 June 2020 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism and the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council, U.N. Doc. S/2020/493 (June 3, 2020), https://docs.un.org/en/S/2020/493 [https://perma.cc/U8DD-GHR5]; *see also Our Mandate*, U.N. SEC. COUNCIL: COUNTER-TERRORISM COMM., https://www.un.org/securitycouncil/ctc/content/our-mandate [https://perma.cc/JE7Y-WJ3C] (last visited Feb. 25, 2026).

[353] *See Global Experts Advance the Joint Fight Against Crypto-Enabled Crime*, U.N. OFF. ON DRUGS & CRIME: CORRUPTION & ECON. CRIME BRANCH (Oct. 28, 2025), https://www.unodc.org/corruption/en/news/2025-10-28_global-experts-advance-the-joint-fight-against-crypto-enabled-crime.html [https://perma.cc/HP2F-WJ4X].

[354] *See* Robert Kim, *U.N. Highlights Escalating North Korea Cryptocurrency and Sanctions Evasion Activity*, KHARON: THE BRIEF (Apr. 24, 2023), https://www.kharon.com/brief/u-n-highlights-escalating-north-korea-cryptocurrency-and-sanctions-evasion-activity [https://perma.cc/XZ9D-SFF9]; *see also UN Toolkit on Synthetic Drugs: Regulation and Supervision*, U.N. TOOLKIT ON SYNTHETIC DRUGS, https://syntheticdrugs.unodc.org/syntheticdrugs/en/frontpage.html [https://perma.cc/6MWH-VPNT] (last visited Dec. 11, 2025).

[355] *See, e.g.*, Panel of Experts Established Pursuant to Security Council Resolution 1874 (2009), *Final Report of the Panel of Experts Submitted Pursuant to Resolution 2680 (2023)*, ¶ 196 U.N. Doc. S/2024/215 (Mar. 7, 2024), https://digitallibrary.un.org/record/4041323/files/S_2024_215-EN.pdf [https://perma.cc/6Q6T-6D47].

[356] *See, e.g.*, *Cryptocurrency Investigations*, U.N. TOOLKIT ON SYNTHETIC DRUG STRATEGY, https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/cryptocurrency.html [https://perma.cc/36W8-L635] (last visited Dec. 11, 2025).

implementation. UNODC offers guidance, capacity-building support, and risk assessments, but it lacks enforcement authority and depends on national governments to incorporate its recommendations into domestic law.[357] This reliance on domestic implementation is not unique to UNODC and is shared by other international bodies, including the IMF and FATF. Unlike the IMF, however, UNODC lacks *indirect* enforcement mechanisms such as financial conditionality or surveillance-linked incentives.[358] Jurisdictions seeking to attract DeFi innovation may also lack the political incentive to regulate DAOs effectively, thereby undermining global AML objectives. As with the FATF, this decentralized enforcement model leaves critical gaps in coverage, particularly for non-jurisdictional entities like DAOs.

Without targeted strategies that address the distinct legal challenges posed by DAOs—including their lack of legal personhood, centralized control, and traceable ownership structures—the UNODC's contributions, while valuable, remain insufficient. A coordinated international framework capable of assigning accountability within decentralized governance models is therefore essential for closing the enforcement gap that DAOs exploit for illicit finance.

VI. TRANSNATIONAL COMPLIANCE WITHOUT CENTRALIZATION: A NEW GLOBAL LEGAL ARCHITECTURE FOR DAO-BASED ANTI-MONEY LAUNDERING GOVERNANCE

The preceding analysis has demonstrated that national, regional, and international AML regulatory frameworks remain fundamentally ill-suited for the decentralized and autonomous architecture of DAOs, thus undermining effective oversight, threatening global financial stability, and weakening states' ability to detect and disrupt both conventional financial crimes and national-security threats. Existing AML regimes largely depend on assumptions of centralized control, identifiable legal persons, and jurisdictionally anchored intermediaries—assumptions that do not hold in the context of DAOs, which operate through self-executing code and collective governance across borders.[359] This structural misalignment creates vulnerabilities that extend beyond regulatory or administrative lapses: the features that define DAOs—pseudonymity, jurisdictional ambiguity, absence of identifiable controllers—generate ML risks that threaten financial stability, facilitate criminal activity, and create

---

[357] *See* Augusto Lopez-Claros, *6 Strategies to Fight Corruption*, GLOB. GOVERNANCE F. (May 15, 2014), https://globalgovernanceforum.org/6-strategies-to-fight-corruption/ [https://perma.cc/2W7S-Y2AD]; *see Money Laundering, Proceeds of Crime and the Financing of Terrorism*, U.N. OFF. ON DRUGS & CRIME, *https://www.unodc.org/unodc/en/money-laundering/index.html* [https://perma.cc/W3G7-CDRP] (last visited Dec. 11, 2025).

[358] *See* Lopez-Claros, *supra* note 357; *Money Laundering, Proceeds of Crime and the Financing of Terrorism*, *supra* note 357.

[359] *See* Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, 107 GEO. L.J. 235, 245–47 (2019); *see also* Hilary J. Allen, *Sandbox Boundaries*, 22(2) VAND. J. ENT. & TECH L. 299, 300, 318 (2020).

exploitable vulnerabilities for state adversaries, terrorist organizations, and cybercriminal networks seeking to circumvent financial controls. These structural failures are compounded by jurisdictions' inconsistent attempts to classify DAOs as corporations, partnerships, or unincorporated associations—improvised efforts that attempt to force fundamentally decentralized systems into regulatory categories designed for traditional entities. This reliance on legacy classifications has produced regulatory fragmentation, enforcement asymmetries, and significant legal uncertainty that limits states' capacity to effectively combat money laundering and its associated economic, criminal, and security risks.[360]

These structural and doctrinal failures and their accompanying risks require a reconceptualization of DAO regulation, particularly in the AML context. Rather than retrofitting legacy legal classifications or enforcement models designed for intermediated finance regulators, international bodies should adopt a modular framework—drawing on principles of functional diversity and risk-based supervision articulated in existing sandbox- and crypto-asset-governance regimes.[361] This suggested framework would depart from monolithic legal treatment in favor of a graduated, risk-based system of compliance obligations—one tailored to the DAO's scale, purpose, and governance structure. Such an approach would align with global regulatory trends emphasizing proportionality, functional equivalence, and transnational cooperation.[362] By empowering national authorities to localize implementation while maintaining shared global standards, modular regulation could reconcile the tension between innovation and enforcement while improving cross-border coordination.[363]

---

[360] *See* CRISTIE FORD, INNOVATION AND THE STATE: FINANCE, REGULATION, AND JUSTICE 54–57 (2022); *see also* Lev Bromberg, Andrew Godwin & Ian Ramsay, *Fintech Sandboxes: Balancing Regulation and Innovation*, 28 J. BANKING & FIN. L. & PRAC. 314, 324–26 (2017).

[361] *See* WORLD BANK GRP., GLOBAL EXPERIENCES FROM REGULATORY SANDBOXES: FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE 16–17, 22–23 (2020), https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf [https://perma.cc/PN8S-YB2C] [hereinafter GLOBAL EXPERIENCES FROM REGULATORY SANDBOXES]; *see also* OECD, CRYPTO-ASSET REPORTING FRAMEWORKS AND AMENDMENTS TO THE COMMON REPORTING STANDARD 5–6 (2022), https://d110erj175o600.cloudfront.net/wp-content/uploads/2022/10/11115702/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf [https://perma.cc/6LF7-Q9KV]; Robert J. Shiller, *Robert J Shiller's Message to Financial Regulators: Don't Fight the last Financial Crisis*, WORLD ECON. F. (May 19, 2016), https://www.weforum.org/stories/2016/05/robert-j-shillers-message-to-financial-regulators-dont-fight-the-last-financial-crisis/ [https://perma.cc/KJB9-EQHB] (observing that financial regulation tends to be backward-looking, often reacting to the narratives and structures of the previous crisis rather than those emerging from technological change).

[362] *See* Brummer & Yadav, *supra* note 359, at 261; *see also Recommendation of the Council on the Governance of Digital Identity*, OECD (July 8, 2023), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491 [https://perma.cc/7E9Y-2HT5].

[363] *See* FORD, *supra* note 360, at 65–68; OECD, INTERNATIONAL STANDARDS FOR AUTOMATIC EXCHANGE OF INFORMATION IN TAX MATTERS: CRYPTO-ASSET REPORTING

The institutional architecture for implementing such a framework, however, remains a complex challenge, requiring deeper research and examination. While the FATF possesses established authority in AML standard-setting, its demonstrated limitations in coordinating effective virtual asset regulation suggest that a fundamentally reformed approach—potentially involving an enhanced FATF mandate; multi-stakeholder coordination mechanisms, including the Organization for Economic Co-operation and Development (OECD) and Bank for International Settlements (BIS); or entirely new institutional arrangements—may be necessary. Determining the appropriate institutional structure, whether through reformed bodies or a new multilateral mechanism, requires assessing how to ensure effective coordination while avoiding the implementation failures that have marked FATF's oversight of VASPs and DeFi.

International institutions that are not traditionally focused on AML play an important role in scaffolding such frameworks. For instance, the BIS, through its Committee on Payments and Market Infrastructures, has advanced oversight principles grounded in proportionality, systemic risk, and technological resilience.[364] These principles underpin the BIS's Principles for Financial Market Infrastructures, which emphasize graduated oversight based on market impact rather than legal form—aligning with the modular logic needed for DAOs.[365] BIS research also addresses DeFi governance and proposes supervisory models decoupled from formal legal entities, focusing on transaction flows and systemic connectivity—key regulatory dimensions for DAOs.[366]

Similarly, the OECD may provide critical normative support. While not a direct AML regulator, the OECD's leadership in digital governance—evidenced by, for example, its Recommendation on the Governance of Digital Identity, Principles on Artificial Intelligence, and Framework for the Disclosure of Crypto-Assets—advocates for technological neutrality, interoperability, and proportional oversight.[367] These frameworks offer

---

FRAMEWORK AND 2023 UPDATE TO THE COMMON REPORTING STANDARD 14–17 (2023), https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/international-standards-for-automatic-exchange-of-information-in-tax-matters_ab3a23bc/896d79d1-en.pdf [https://perma.cc/76L3-NHU6] [hereinafter OECD CRYPTO FRAMEWORK].

[364] *See generally* COMM. ON PAYMENTS & SETTLEMENT SYSS. & TECH. COMM. OF THE INT'L ORG. OF SECS. COMM'NS., PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURES (2012), https://www.bis.org/cpmi/publ/d101a.pdf [https://perma.cc/287W-R8FG].

[365] *See id*. at 12–14, 126–32.

[366] *See* Press Release, Bank of Int'l Settlements, BIS Innovation Hub, DeFi Risk and Regulation (Jan. 25, 2022), https://www.bis.org/press/p220125.htm [https://perma.cc/8LA8-8Y8P].

[367] *See Recommendation of the Council on Artificial Intelligence*, OECD (May 3, 2025), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [https://perma.cc/8EW8-F2AE]; OECD CRYPTO FRAMEWORK, *supra* note 363, at 8–9, 12, 14–16, 17–21, 23, 26–27, 29–49; OECD, Recommendation of the Council on the Governance of Digital Identity (Adopted by the Council at Ministerial level on 8 June 2023), Doc. No. C/MIN(2023)8/FINAL (June 8, 2023), https://one.oecd.org/document/C/MIN(2023)8/FINAL/en/pdf [https://perma.cc/6EE6-UEBY]. Empirical evidence indicates substantial adherence to OECD recommendations

useful analogues for DAO regulation in areas such as pseudonymous identity verification and automated compliance systems. Additionally, the OECD's success in coordinating tax compliance via the Common Reporting Standard illustrates its capacity to harmonize standards across jurisdictions—an institutional competency that could similarly enhance AML alignment in the DeFi ecosystem.[368]

To give concrete form to the Article's proposed modular framework, the following section outlines its foundational regulatory architecture, grounded in principles of technology neutrality, functional proportionality, and transnational coordination. This framework remains exploratory, offering a preliminary map of regulatory possibilities rather than a definitive blueprint. It is intended to guide future doctrinal development and policy experimentation. The emphasis on technology neutrality ensures that regulatory obligations apply based on function and risk rather than the underlying technological design, preserving space for innovation while maintaining compliance integrity.[369]

Rather than imposing rigid, one-size-fits-all mandates, the model is structured around four interdependent components designed to address DAOs' functional diversity and risk profiles. The first component introduces a system of tiered KYC/AML obligations, calibrated to each DAO's transactional volume, governance structure, and exposure to illicit finance. The second component proposes embedding early-warning triggers into DAO infrastructures to facilitate automated, real-time compliance responses. The third component highlights DAO-focused regulatory sandboxes, allowing for structured experimentation and

---

by both member and non-member economies through documented national implementation. Data shows that that a large majority of adhering countries have incorporated the principles into national AI strategies, legislation, or regulatory guidance, while OECD peer-review reports on digital government and identity frameworks document concrete reforms aligned with OECD recommendations across multiple jurisdictions. *See The OECD.AI Policy Navigator*, OECD, https://oecd.ai/en/dashboards/policy-initiatives [https://perma.cc/8TT3-3BPX] (last visited Dec. 11, 2025); *see also* Lucia Russo & Noah Oder, *How Countries Are Implementing the OECD Principles for Trustworthy AI*, OECD.AI (Oct. 31, 2023), https://oecd.ai/en/wonk/national-policies-2 [https://perma.cc/TV54-TF7K]; OECD, *The State of Implementation of the OECD AI Principles Four Years On*, OECD ARTIFICIAL INTELL. PAPERS 11–14 (2023), https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/10/the-state-of-implementation-of-the-oecd-ai-principles-four-years-on_b9f13b5c/835641c9-en.pdf [https://perma.cc/E8B5-YHU6].

[368] The Common Reporting Standard is an OECD-developed multilateral framework for tax transparency under which participating jurisdictions require financial institutions to identify non-resident account holders and automatically exchange financial account information with the relevant foreign tax authorities. Since its adoption in 2014, the CRS has been implemented by more than a hundred jurisdictions and has become the global baseline for cross-border tax information exchange. *See Tax Transparency Resource Centre*, OECD, https://www.oecd.org/en/topics/sub-issues/international-standards-on-tax-transparency/tax-transparency-resource-centre.html [https://perma.cc/G7UQ-8ZVW] (last visited Feb. 24, 2026); *see also* OECD CRYPTO FRAMEWORK, *supra* note 363, at 3, 8–9, 90–92.

[369] *See, e.g.*, Nizan G. Packin, *Emerging Compliance in the Generative Decentralized Era,* 19 BROOK. J. CORP. FIN. & COM. L. 83, 91–95, 97–102, 106–09, 112 (2024).

supervisory insight under bounded conditions. The fourth and final component establishes accountability and coordination mechanisms, addressing legal attribution in decentralized systems and promoting cross-protocol risk monitoring to support cross-jurisdictional enforcement. These four foundational components are operationalized through and manifested in seven specific regulatory pillars that work together to create a flexible, scalable, and internationally adaptable framework that aligns decentralized innovation with AML enforcement imperatives.

A. *Pillar One: Tiered KYC/AML Obligations*

The first pillar of the proposed modular framework is a system of tiered KYC/AML obligations, calibrated to reflect the DAO's transactional volume, governance structure, and degree of exposure to illicit finance, including ML. Instead of implementing uniform identity verification requirements—an approach often infeasible for decentralized communities—this model would impose progressively stringent obligations based on objective, risk-sensitive thresholds.[370] For instance, DAOs managing substantial treasuries or offering financial services comparable to regulated entities could be mandated to adopt community-approved KYC mechanisms or incorporate decentralized identity protocols. Conversely, small-scale, low-risk DAOs with limited financial throughput could qualify for lighter oversight, similar to safe harbors.[371] This risk-proportionate approach reflects FATF's risk-based methodology principle.[372] Crucially, this framework does not exempt DAOs from accountability and instead tailors obligations to actual risk levels, thus fostering innovation while ensuring alignment with AML objectives.

B. *Pillar Two: Automated Early-Warning Triggers*

The second pillar involves embedding early-warning triggers within DAO governance and operational systems to identify and respond to emerging financial and compliance risks in real time. These triggers would rely on quantifiable indicators—such as sudden treasury movements, unusual gas-fee fluctuations, rapid token issuance, or significant deviations in smart-contract activity—that could signal increased ML or fraud risks.[373] A useful implementation model comes from recent proposals for an Early-Warning Index (EWI) designed to anticipate financial distress in decentralized crypto entities.[374] This index aggregates three metrics:

---

[370] *See* John W. Bagby & Nizan G. Packin, *RegTech and Predictive Lawmaking: Closing the RegLag Between Prospective Regulated Activity and Regulation,* 10 MICH. BUS. & ENTREPRENEURIAL L. REV. 127, 156–58 (2021).

[371] *See* Chang H. Tsai, Ching F. Lin & Han W. Liu, *The Diffusion of the Sandbox Approach to Disruptive Innovation and Its Limitations*, 53(2) CORN. INT'L L.J. 261, 281–83 (2020).

[372] *See* GLOBAL EXPERIENCES FROM REGULATORY SANDBOXES, *supra* note 361, at 11–12, 16; *see, e.g.*, FATF RISK-BASED APPROACH, *supra* note 10, at 70–74.

[373] *See* Bagby & Packin, *supra* note 370, at 143–45, 169–71.

[374] *See* Murad Farzulla & Andrew Maksakov, *ASRI: An Aggregated Systemic Risk Index for Cryptocurrency Markets: A Unified Framework for Monitoring DeFi-TradFi*

TreasuryRatio (treasury to liabilities), Volatility (standard deviation of gas fees over thirty days), and HolderChurn (weekly decline in token holders)—into a composite score. For example, a DAO may adopt the formula:

EWI = 0.5 * TreasuryRatio + 0.3 * Volatility + 0.2 * HolderChurn.

Under this scheme, a DAO that crosses a predetermined threshold (e.g., EWI > 0.7) would automatically trigger predefined compliance protocols such as a temporary transaction freeze, increased internal transparency measures, alerts to designated authorities, or activation of a rescue mechanism.[375] Integrating this kind of weighted, quantitative alert system would allow regulators and DAO communities to detect financial or ML risk upstream while preserving automation and decentralization.

These mechanisms could be implemented through self-executing smart contracts to maintain decentralization while adding compliance responsiveness.[376] This approach echoes the prudential logic underlying liquidity and leverage thresholds in traditional finance, yet is adapted to the programmability and transparency features unique to blockchain ecosystems.[377] Drawing on reg-tech innovations used in sandbox environments across the Canada, Singapore, and United Kingdom—where authorities have piloted transaction-monitoring systems that use quantitative risk indicators, automated alerts, and threshold-based escalation to enhance AML and fraud detection—this system would promote automation, transparency, and real-time adaptability, capabilities essential for upstream supervision of rapidly evolving decentralized entities.[378]

Interconnection Risk 28, 54 (Working Paper, Jan. 2026), https://arxiv.org/abs/2602.03874 [https://perma.cc/TVQ5-55U3]; *see also* Lotfi Mahiddine, The Decentralized Monetary Index—Risk (DMIR): An Early Warning System for Central Banks in a Decentralized Financial Landscape 2, 4 (Aug. 25, 2025) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5394133 [https://perma.cc/BGF6-FQWE]; Ji Liu et al., *Risk Monitor System for Blockchain-Based Security Issuing System*, ELEC. COM. RSCH. 1, 3, 15 (June 20, 2025), https://link.springer.com/article/10.1007/s10660-025-09999-7 [https://perma.cc/RV2N-TFCG].

[375] *See* Liu et al., *Risk Monitor System*, *supra* note 374, at 14–18; Farzulla & Maksakov, *supra* note 374, at 30–31, 35.

[376] *See* FORD, *supra* note 360, at 142–44.

[377] *See* Brummer & Yadav, *supra* note 359, at 278–79.

[378] *See* Ross P. Buckley et al., *Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond*, 61 J.L. & POL'Y 55, 60–62 (2020); *see also* FIN. STABILITY BD., THE USE OF SUPERVISORY AND REGULATORY TECHNOLOGY BY AUTHORITIES AND REGULATED INSTITUTIONS: MARKET DEVELOPMENTS AND FINANCIAL STABILITY IMPLICATIONS 1–3 (2020), https://www.fsb.org/uploads/P091020.pdf [https://perma.cc/BHH6-R9MV]; *see* Joseph Ibitola, *Can Innovation and Regulation Coexist in the Future of AML?*, FLAGRIGHT (Aug. 13, 2025), https://www.flagright.com/post/can-innovation-and-regulation-coexist-in-the-future-of-aml [https://perma.cc/652T-66DU]; *see also Pay.UK's Fraud Detection Pilot Exceeds Expectations, Detecting Over £112m Worth of Fraud*, PAY.UK (May 30, 2024),

C. *Pillar Three: DAO-Specific Regulatory Sandboxes*

The third pillar introduces DAO-specific regulatory sandboxes, designed to facilitate structured experimentation within clearly defined legal and compliance boundaries. Such sandboxes have demonstrated effectiveness in jurisdictions like the Canada, Singapore, and United Kingdom, where they allow experimental financial innovations to operate temporarily under relaxed regulatory oversight, monitored by authorities equipped to assess both technical and systemic risks.[379] For example, the UK Financial Conduct Authority's Regulatory Sandbox provides a controlled environment in which firms can test innovative financial products and technologies—including data-analytics, distributed-ledger, and AI-enabled tools—under supervisory oversight.[380] Similarly, Singapore's Monetary Authority of Singapore operates a FinTech Regulatory Sandbox that allows financial institutions and fintech firms to trial novel financial products and services within defined regulatory guardrails. This framework enables supervisors to observe associated risks and compliance challenges.[381] In Canada, securities regulators have established regulatory sandbox initiatives and innovation hubs that permit fintech firms to pilot innovative products and services, including through

https://www.wearepay.uk/pay-uks-fraud-detection-pilot-exceeds-expectations-detecting-over-112m-worth-of-fraud/ [https://perma.cc/5QVV-W6TN]; Joseph Ibitola, *Guide to Real-Time AML for Singapore Payment Processors*, FLAGRIGHT (Nov. 12, 2025), https://www.flagright.com/post/guide-to-real-time-aml-for-singapore-payment-processors [https://perma.cc/B5MU-UFLP] (last updated Jan. 29, 2026); Elizabeth Sale & Victoria Graham, *The Carrot: Payments Canada Publishes Real-Time Rail Participation Guide for Payment Service Providers*, OSLER (Nov. 21, 2025), https://www.osler.com/en/insights/updates/the-carrot-payments-canada-publishes-real-time-rail-participation-guide-payment-service-providers/ [https://perma.cc/E9UR-WV4V]; Jude Pinto, *Canada's Real-Time Rail: Collaborating for the benefit of the payment ecosystem*, PAYMENTS CAN. (Sep. 3 2025), https://www.payments.ca/canadas-real-time-rail-collaborating-benefit-payment-ecosystem [https://perma.cc/XET8-LPGS].

[379] *See, e.g.*, *The Canadian Securities Administrators Launches a Regulatory Sandbox Initiative,* CAN. SEC. ADMINS. (Feb. 23, 2017), https://www.securities-administrators.ca/news/the-canadian-securities-administrators-launches-a-regulatory-sandbox-initiative/ [https://perma.cc/TQ4K-DNTN]; *Overview of Regulatory Sandbox*, MONETARY AUTH. OF SING., https://www.mas.gov.sg/development/fintech/regulatory-sandbox [https://perma.cc/K7KA-4E4H] (last visited May 1, 2026*); Regulatory Sandbox Accepted Firms*, FIN. CONDUCT AUTH. (Mar. 27, 2022) https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms [https://perma.cc/2MV2-CTEF] (last updated Mar. 9, 2026); *Digital Securities Sandbox (DSS)*, https://www.bankofengland.co.uk/financial-stability/digital-securities-sandbox [https://perma.cc/3Y5A-G2YC] (last visited May 1, 2026).

[380] *See Regulatory Sandbox*, FIN. CONDUCT AUTH., https://www.fca.org.uk/firms/innovation/regulatory-sandbox?utm_s.com [https://perma.cc/9VC8-QZ5Q] (last visited Dec. 11, 2025).

[381] *See FinTech Regulatory Sandbox*, MONETARY AUTH. OF SING., https://www.mas.gov.sg/development/fintech/regulatory-sandbox?utm_source.com [https://perma.cc/F85A-WGAX] (last visited Dec. 11, 2025).

time-limited exemptive relief or regulatory guidance, while regulators assess consumer-protection and market-integrity risks.[382]

For DAOs, these environments allow testing of governance models, automated compliance protocols, and cross-border financial instruments within supervised settings. Importantly, participation in these sandboxes may require minimum standards—such as smart-contract auditability, tokenomics transparency,[383] or engagement with third-party compliance tools—that incentivize baseline operational standards.[384] Such measures would allow regulators to gather real-time data on DAO behavior, improving insights into systemic risks in decentralized constructs.[385] Broadly, DAO-focused sandboxes could serve as hubs for regulatory capacity-building and international knowledge-sharing, especially if multilateral organizations like the OECD or BIS develop evaluative criteria supporting performance assessment and cross-border interoperability.[386]

D. *Pillar Four: Functional Attribution and Decentralized Accountability*

The fourth pillar addresses the challenge of legal attribution in decentralized systems, where the absence of identifiable actors impedes the enforcement of AML obligations. To remedy the fact that DAOs often lack legal personality and operate through pseudonymous or decentralized governance arrangements, the model proposes an attribution framework

---

[382] *See CSA Financial Innovation Hub*, CAN. SEC. ADM'RS, https://www.securities-administrators.ca/csa-activities/csa-finhub/?utm_source.com [https://perma.cc/J99L-XJGJ] (last visited Dec. 11, 2025); *The Canadian Securities Administrators Launches a Regulatory Sandbox Initiative,* CAN. SEC. ADM'RS. (Feb. 23, 2017), https://www.securities-administrators.ca/news/the-canadian-securities-administrators-launches-a-regulatory-sandbox-initiative/?utm_source.com [https://perma.cc/73Y8-CSS3].

[383] Tokenomics refers to the economic design of a blockchain-based token, encompassing its issuance schedule, distribution mechanisms, supply management, and incentive structures that are intended to influence user behavior and network participation. *See Tokenomics,* COINMARKETCAP, https://coinmarketcap.com/academy/glossary/tokenomics [https://perma.cc/J4KV-6AMD] (last visited Dec. 11, 2025); CoinGecko, *What Is Tokenomics? Understanding Crypto Fundamentals*, COINGECKO (Aug. 29, 2022), https://www.coingecko.com/learn/what-is-tokenomics-understanding-crypto-fundamentals.

[384] *See* GLOBAL EXPERIENCES FROM REGULATORY SANDBOXES, *supra* note 361, at 22–24; IVO JENÍK & SCHAN DUFF, HOW TO BUILD A REGULATORY SANDBOX: A PRACTICAL GUIDE FOR POLICY MAKERS 12 (2020), https://digitalfinance.worldbank.org/sites/default/files/2022-11/How-to-Build-a-Regulatory-Sandbox-A-Practical-Guide-for-Policy-Makers.pdf [https://perma.cc/QN5R-7R4T]; Camille Walsh, *Everything You Need to Know About Regulatory Sandboxes*, STATE POL'Y NETWORK (Oct. 12, 2021), https://spn.org/what-is-a-regulatory-sandbox/ [https://perma.cc/AE4V-HJYY].

[385] *See* Lev Bromberg, Andrew Godwin & Ian Ramsay, *Fintech Sandboxes: Achieving a Balance Between Regulation and Innovation*, 28 J. BANKING & FIN. L. & PRAC. 314, 329–31 (2017).

[386] *See* Cristie Ford & Quinn Ashkenazy, *The Legal Innovation Sandbox*, 72 AM. J. COMPAR. L. 557, 558–61 (2024), https://academic.oup.com/ajcl/article/72/3/557/8102983 [https://perma.cc/T4HH-Z2BF].

that would identify responsibility based on functional roles within the DAO—such as the authority to propose, approve, or execute transactions affecting treasury flows or protocol operations. This role-based approach draws from established doctrines in corporate and securities law, including beneficial ownership principles and the control-person standard.[387] For DAOs, it may enable the designation of liable parties even in the absence of formal officeholding or contractual authority. Importantly, attribution under this model would rest on demonstrable influence rather than formal status, thereby limiting the ability of DAOs to shield illicit conduct behind decentralized governance design. More broadly, such a framework would support the development of enforcement pathways aligned with due process and international recognition, especially when integrated into standards developed by bodies such as the FATF and OECD.

E. *Pillar Five: Cross-Protocol Risk Signaling and Supervisory Coordination*

The fifth pillar addresses the challenges posed by the transnational and cross-protocol nature of DAO operations, which frequently span multiple blockchains, decentralized applications, and jurisdictions. This fragmentation disperses transactional activity across platforms without unified oversight, complicating efforts to detect and prevent ML.[388] To address these regulatory blind spots, the fifth pillar promotes the development of interoperable risk-signaling mechanisms between DAOs and related entities, including exchanges, cross-chain bridges, and custodial services.

For regulators, these mechanisms would support the identification of high-risk activity—such as movement of illicit proceeds across governance layers or manipulation of DeFi instruments through arbitrage. Importantly, participation in compliance frameworks, such as safe harbors or regulatory sandboxes, could be conditioned on engagement with supervisory alliances or risk-sharing networks modelled on national financial-intelligence units. By enabling structured information exchange across decentralized systems, this approach helps reduce operational silos and support a coordinated regulatory response to complex laundering schemes. More broadly, standardized risk-signaling could contribute to an international supervisory infrastructure for DeFi, especially if developed in coordination with multilateral organizations or public-private enforcement partnerships.

F. *Pillar Six: Compliance-Linked Reserve and Bonding Mechanisms*

---

[387] *See, e.g.*, *Assessing Compliance with BSA Regulatory Requirements*, FFIEC: BSA/AML INFOBASE, https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/03 [https://perma.cc/T9N4-FGH6] (last visited May 1, 2026).

[388] *See* Parts I & II, *supra*.

The sixth pillar draws on longstanding regulatory techniques using insurance, bonding, or capital reserves to mitigate residual legal risk in financial systems. In the DAO context, this approach would support the development of compliance-linked reserve mechanisms—such as bonding pools or mutual-coverage funds—designed to provide compensation in the event of AML violations.[389] These mechanisms do not displace legal liability but serve as structured financial backstops, enabling DAOs to demonstrate risk discipline and allowing regulators to evaluate compliance readiness.[390] For DAOs, participation in such reserve systems could be voluntary but rewarded with favorable treatment in sandbox admission, enforcement discretion, or access to cooperative-oversight regimes.[391] Importantly, these reserve structures do not rely on traditional insurers or centralized guarantors.[392] Instead, they express a principle of embedded restitution—allocating accountability internally through governance processes and codified reserve rules. Broadly, these mechanisms reflect an evolving model of financial accountability in decentralized environments, aligning restitution incentives with DAO specific technical and legal structure.[393]

G. *Pillar Seven: Jurisdictional Harmonization and Transnational Enforcement Frameworks*

The seventh and last pillar addresses the jurisdictional indeterminacy that hampers AML enforcement against DAOs operating across borders. This pillar responds to that gap by promoting a harmonized, criteria-based framework for legal accountability across jurisdictions, grounded in shared criteria for DAO classification, risk exposure, and regulatory recognition.[394] Rather than relying on the formal domiciles of a DAO's participants, jurisdictional attribution would be based on objective indicators—such as the location of the DAO's treasury governance, the concentration of economically meaningful participants, or its primary locus of economic activity.[395] This approach draws from foundational principles in international regulatory cooperation, including functional equivalence and mutual recognition, which underpin frameworks such as the OECD's regulatory-alignment initiatives[396] and FATF's cross-border AML standards.[397] For DAOs, compliance with these criteria could enable access

---

[389] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 35–37.
[390] *See* GLOBAL EXPERIENCES FROM REGULATORY SANDBOXES, *supra* note 361, at 23–25.
[391] *See* Buckley et al., *supra* note 378, at 83–84.
[392] *See* Zetzsche, Arner & Buckley, *Decentralized Finance (DeFi)*, *supra* note 79, at 195–96.
[393] *See* THE TOKENISATION OF ASSETS, *supra* note 58, at 28–30.
[394] *See* Zetzsche, Arner & Buckley, *Decentralized Finance (DeFi)*, *supra* note 79, at 196–98.
[395] *See* RISK ASSESSMENT OF DEFI, *supra* note 12, at 13–15.
[396] *See* OECD, *Regulatory Reform*, https://www.oecd.org/en/topics/regulatory-reform.html [https://perma.cc/Y6MK-CF6X] (last visited Dec. 11, 2025).
[397] *See* FATF INTERNATIONAL STANDARDS, *supra* note 89, at 118 (Recommendation 38 and Interpretive Note).

to multilateral safe-harbor regimes or coordinated-sandbox participation, thereby creating legal clarity while preserving operational flexibility.

Importantly, this pillar would support consistent enforcement pathways across legal systems, reduce incentives for jurisdictional arbitrage, and strengthen the international community's ability to respond to decentralized ML risks. Such improvements would build on existing cross-border cooperation mechanisms through which national authorities already exchange financial intelligence, coordinate supervisory responses, and pursue joint enforcement actions.[398] For example, regulators could formalize DAO-specific information-sharing protocols under existing Financial Intelligence Unit networks—particularly through the Egmont Group's Secure Web platform, which already enables over 182 Financial Intelligence Units exchange suspicious transaction intelligence in real time.[399] Expanding Egmont typology exercises to address DAO governance tokens, treasury wallets, and cross-chain bridge structures would allow member jurisdictions to develop shared red-flag indicators for decentralized ML typologies.

More broadly, such a framework could facilitate transnational supervisory collaboration, particularly if developed under the auspices of the OECD, FATF, or BIS.[400] As noted above, the success of this proposed modular framework hinges on resolving fundamental questions about institutional coordination and the appropriate division of responsibilities between international standard-setters and national implementers.

***

Figure 2, *infra*, synthesizes the chapter's proposed regulatory responses into a coherent seven-pillar framework designed to recalibrate and fortify AML enforcement in DAO ecosystems.

Figure 2: Modular Regulatory Architecture for DAO-Based AML Enforcement

#	Pillar	Key concept	Mechanism	Objective
1.	Tiered KYC/AML obligations	Risk-based identity compliance	Scaled requirements based on	Ensure proportional compliance

[398] *See, e.g.*, GLOBAL EXPERIENCES FROM REGULATORY SANDBOXES, *supra* note 361, 17–18; *see generally* EGMONT GRP. OF FIN. INTEL. UNITS, PRINCIPLES FOR INFORMATION EXCHANGE BETWEEN FINANCIAL INTELLIGENCE UNITS (2025), https://egmontgroup.org/wp-content/uploads/2022/07/EG-Principles-for-Information-Exchange-Revised-July-2025.pdf [https://perma.cc/F8R5-P2JJ]; *see also* FATF RECOMMENDATIONS, *supra* note 90, at 27–30 (Recommendations 36–40).

[399] *See About the Egmont Group*, EGMONT GRP. OF FIN. INTEL. UNITS, https://egmontgroup.org/about/ [https://perma.cc/2MMQ-2CR7] (last visited Dec. 11, 2025).

[400] *See* THE TOKENISATION OF ASSETS, *supra* note 58, at 26–29.

			DAOs size, function and risk	while preserving innovation
2.	Embedded Early Warning Signs	Automated risk detection	Quantitative metrics (e.g., EWI formula) in smart contracts	Enable real-time, upstream response to ML threats
3.	DAO-Specific Regulatory Sandboxes	Structured legal experimentation	Conditional, monitored regulatory waivers	Test compliance mechanisms in controlled environments
4.	Functional Legal Attribution	Role-baes responsibility	Assign accountability based on governance influence	Enable enforcement without formal legal identity
5.	Interoperable Risk Signaling	Cross-platform compliance coordination	Information-sharing across DAOs, exchanges and bridges	Detect and prevent cross-protocol laundering activity
6.	Compliance linked Reserve Systems	Financial risk mitigation	DAO-governed insurance or bonding pools	Provide restitution and demonstrate risk discipline
7.	Harmonized Jurisdictional Framework	Transnational accountability	Shared classification and recognition criteria	Reduce legal uncertainty and prevent regulatory arbitrage

VII. CONCLUSION

The emergence of DAOs represents not merely a technological development but a foundational shift in organizational and financial architecture. By displacing centralized intermediaries with code-based governance and pseudonymous participation, DAOs upend AML enforcement assumptions that require identifiable actors, jurisdictionally anchored operations, and centralized compliance infrastructure. This structural inversion exposes core limitations in existing national, regional, and international AML regimes that depend on legal and institutional hierarchies that DAOs fundamentally dissolve.

As this Article has shown, attempts to apply traditional legal categories and frameworks to DAOs have produced inconsistent results, thereby creating persistent enforcement gaps. Likewise, international standard-setting bodies such as the FATF and the IMF have recognized

AML risks posed by DeFi finance but have yet to produce meaningful responses tailored to DAO-specific architectures. This regulatory inertia has created a compliance vacuum exploited by sophisticated actors, including transnational criminal networks and sanctioned entities, who leverage DAOs' structural opacity and cross-jurisdictional design to move illicit funds with reduced detection risk, with implications extending from financial integrity to national security.

In response, this Article has proposed a modular regulatory framework grounded in principles of functional proportionality, technological neutrality, and transnational coordination. Its core pillars—tiered KYC/AML obligations, automated early-warning triggers, and DAO-specific regulatory sandboxes—are designed to tailor regulatory requirements to the unique risk profile and governance structure of each DAO. This approach seeks to avoid the pitfalls of overly broad surveillance and regulatory under-enforcement by replacing uniform mandates with flexible, risk-sensitive standards. Additional components—including attribution mechanisms for assigning functional accountability, cross-protocol risk signaling, reserve-based financial backstops, and a jurisdictional harmonization model—further articulate how AML enforcement can adapt to DAO-specific risks without undermining core decentralization values.

Crucially, this model does not require extensive institutional reinvention. Rather, it offers a realistic pathway for incremental adaptation by embedding modular strategies within existing multilateral institutions. FATF, for instance, could extend its risk-based guidance to address pseudonymous governance or introduce treasury-based compliance tiers. The IMF could incorporate DAO vulnerabilities into macroprudential monitoring regimes such as its Financial Sector Assessment Programs. UNODC could develop capacity-building tools tailored to smart-contract compliance and decentralized infrastructure. In these ways, the modular framework respects national sovereignty while promoting convergence on baseline AML expectations—thereby reconciling legal accountability with decentralized innovation.

The regulatory challenges DAOs pose are not transitory. As these entities increasingly mediate capital formation, protocol governance, and financial intermediation, the costs of continued doctrinal and institutional misalignment are expected to rise. AML enforcement that ignores the architectural realities of decentralization risks irrelevance; yet, a regulatory model that reflexively suppresses innovation in the name of compliance may undermine the participatory and resilient potential of DAOs. This Article has argued that modularity offers a principled middle path—one that preserves flexibility, enforces accountability, and restores coherence to a global AML system strained by the borderless nature of decentralized technologies.