GLOBAL COINS, GLOBAL CRIME

Jiaying Jiang[*]

The crypto ecosystem enables rapid, borderless value transfer but also facilitates money laundering at an unprecedented scale. In response, the Financial Action Task Force (FATF) has extended its anti-money laundering (AML) framework to virtual assets, bringing Virtual Asset Service Providers (VASPs) within regulatory scope, adopting a risk-based approach to regulating crypto activities, and implementing the Travel Rule to enhance transparency in crypto transactions.

These efforts are significant, but insufficient. FATF's framework remains anchored in an intermediary-based model, which fails to capture a growing share of crypto activity occurring outside such intermediaries, including peer-to-peer transactions, decentralized finance, and infrastructure-layer processes that govern how transactions are propagated and executed. As illicit actors migrate toward these channels, the effectiveness of the existing framework correspondingly declines. This Essay argues that AML regulation must move beyond intermediaries and toward infrastructure. Specifically, it proposes a framework that combines a normative reorientation toward financial infrastructure, the embedding of compliance through technical tools and system design, and the use of economic incentives to reinforce compliance outcomes. It further calls for institutional adaptations to recalibrate global AML governance for distributed systems.

INTRODUCTION 34

I. THE RISE OF GLOBAL CRYPTO MONEY LAUNDERING 39

A. Growth and Industrialization 40

B. Laundering Infrastructure and Techniques.....41

II. THE FATF FRAMEWORK AND ITS EXPANSION TO CRYPTO 42

---

[*] Associate Professor of Law, University of Florida Levin College of Law. I am grateful to the following individuals for their valuable insights, which helped shape this Essay: Jussi Aittola, Sebastian Bode, Ben Buergi, Raul Carrillo, Sam Elfarra, Nick Furneaux, Linda Jeng, Lockhart Karl, Liat Shetret, Lev Menand, Alexandar Moser, Gal Sagie, Felix Shipkevich, Bjorn Wahlstrom, and Kai Wang, as well as to other participants at the University of Florida Levin College of Law Junior Faculty Workshop, the Northeastern Junior Scholars Conference, the Financial Regulation Section of the 2025 Association of American Law Schools' Annual Meeting, and the Blockchain and Fintech Program at Rutgers Center for Corporate Law and Governance for their thoughtful feedback. I would also like to thank my research assistants, Nicholas Miguel Luhrsen and Hanuel Kim, for their excellent research support.

A. New Glossary Definitions 43
B. Risk-Based Approach 44
C. The Travel Rule 46
III. THE LIMITS OF INTERMEDIARY-BASED AML: A STRUCTURAL MISMATCH 48
A. Trust Architectures 48
B. The Mismatch 49
IV. TOWARD INFRASTRUCTURE-AWARE AML GOVERNANCE 51
A. From Intermediaries to Infrastructure 51
1. Normative Reframing 51
2. Embedding Compliance in Infrastructure Design 52
3. Economic Incentives 54
B. Institutional Adaptations 55
CONCLUSION 56

INTRODUCTION

According to estimates by the United Nations, between 2 percent and 5 percent of global GDP—amounting to $800 billion to $2 trillion—is laundered each year.[1] In 2024, INTERPOL identified money laundering as the second-highest global crime threat facing its member countries, just behind drug trafficking.[2] As financial activity increasingly migrates to digital and decentralized networks, illicit actors have likewise adapted, exploiting the unique features of the crypto ecosystem to move and conceal criminal proceeds.[3] In 2025, a single North Korean-linked network reportedly processed billions of dollars in stolen crypto through a global web of brokers, mixers, and cross-chain transactions, illustrating how crypto

1. *Improving Regional Investigations on Money Laundering and Asset Recovery*, U.N. OFF. ON DRUGS & CRIME (Nov. 18, 2024), https://www.unodc.org/roca/en/NEWS/news_2024/november/improving-regional-investigations-on-money-laundering-and-asset-recovery.html [https://perma.cc/YL2Z-TMNR]. Additionally, the Federal Bureau of Investigation (FBI) reports that "every year, more than $300 billion in concealed transactions is moved around the United States, according to a U.S. Department of the Treasury report on money laundering and terrorist financing threats." *Combating the Growing Money Laundering Threat: Specialized FBI Unit Focuses on Disrupting Professional Money Launderers*, FBI (Oct. 24, 2016), https://www.fbi.gov/news/stories/combating-the-growing-money-laundering-threat (on file with the *Fordham Law Review*); *see also Money-Laundering*, U.N. OFF. ON DRUGS & CRIME (Apr. 2018), https://www.unodc.org/e4j/en/organized-crime/module-4/key-issues/money-laundering.html [https://perma.cc/D5LT-2XYT].

2. *See* FIN. ACTION TASK FORCE, EGMONT GRP., INTERPOL & U.N. OFF. ON DRUGS & CRIME, INT'L CO-OPERATION ON MONEY LAUNDERING DETECTION, INVESTIGATION, AND PROSECUTION HANDBOOK 19 (2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/International-Cooperation-ML-Detection-Investigation-Prosecution.pdf.coredownload.pdf (on file with the *Fordham Law Review*).

3. U.S. DEP'T OF THE TREASURY, 2026 NATIONAL MONEY LAUNDERING RISK ASSESSMENT 49–50 (2026), https://home.treasury.gov/system/files/246/2026-NMLRA.pdf [https://perma.cc/9BD7-VSZD] [hereinafter NMLRA (2026)].

money laundering has evolved from isolated activity into a coordinated, industrialized system.[4]

Illicit crypto transactions now occur at a large and rapidly expanding scale. Global crypto transaction volume exceeded $10 trillion in 2024, with illicit flows reaching roughly $40–50 billion and rising to an estimated $155 billion by 2025.[5] This growth reflects not only increased adoption but also a structural shift toward more professionalized laundering networks. State-sponsored actors, organized crime groups, and specialized laundering services now operate within interconnected ecosystems, often sharing infrastructure and techniques.[6] Chinese-language money laundering networks (CMLNs) alone processed over $16 billion in illicit inflows in 2025, while stablecoins accounted for approximately 84 percent of illicit transaction volume, underscoring their role as the dominant medium for cross-border value transfer.[7]

At the same time, the techniques and infrastructure of crypto laundering have become more complex and resilient. Illicit actors rely on centralized exchanges as entry and exit points but also increasingly exploit decentralized tools and channels such as cross-chain bridges, decentralized exchanges, and mixers to fragment transaction trails and evade detection.[8] Cross-chain laundering volumes have surged past $21 billion, while mixers continue to

4. *See North Korea and the Industrialization of Cryptocurrency Theft*, TRM LABS (Dec. 18, 2025), https://www.trmlabs.com/resources/blog/north-korea-and-the-industrialization-of-cryptocurrency-theft [https://perma.cc/KZB8-2P3M]. For purposes of this Essay, "cryptocurrency" (or "crypto") refers to blockchain-based digital assets that use cryptographic techniques to validate and record transactions on distributed ledgers without centralized intermediaries. The "crypto ecosystem" refers more broadly to the network of technologies, platforms, and actors that support the creation, transfer, storage, and exchange of such assets, including blockchains, smart contracts, wallets, exchanges, and related service providers. *See, e.g.*, FIN. ACTION TASK FORCE, VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2019, updated 2021) https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*).

5. TRM LABS, 2025 CRYPTO CRIME REPORT (2025), https://www.trmlabs.com/resources/reports/2025-crypto-crime-report [https://perma.cc/PGL6-SELL] [hereinafter TRM LABS, 2025 CRYPTO REPORT]; CHAINALYSIS, 2025 CRYPTO CRIME REPORT 4 (2025), https://go.chainalysis.com/2025-Crypto-Crime-Report.html [https://perma.cc/T6DW-HH8S] [hereinafter CHAINALYSIS, 2025 CRYPTO REPORT]; CHAINALYSIS, 2026 CRYPTO CRIME REPORT 3 (2026), https://www.chainalysis.com/reports/crypto-crime-2026/ [https://perma.cc/987S-GCNL] [hereinafter CHAINALYSIS, 2026 CRYPTO REPORT]; TRM LABS, 2026 CRYPTO CRIME REPORT (2026), https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report [https://perma.cc/XMY9-WNQF] [hereinafter TRM LABS, 2026 CRYPTO REPORT].

6. *See* CHAINALYSIS, 2026 CRYPTO REPORT, *supra* note 5, at 4–5, 7, 22.

7. *Id.* at 9; TRM LABS, 2026 CRYPTO REPORT, *supra* note 5.

8. U.S. DEP'T OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 17–18, 35 (2023) https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [https://perma.cc/6NPN-LQRW]; FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 8 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf (on file with the *Fordham Law Review*) [hereinafter FATF, UPDATED GUIDANCE (2021)]; ELLIPTIC, STATE OF CROSS-CHAIN CRIME IN 2025 31, 35 (2025), https://www.elliptic.co/insights/the-state-of-cross-chain-crime-2025/ (on file with the *Fordham Law Review*).

obscure billions in illicit funds despite enforcement actions.[9] These channels and tools collectively form a layered laundering architecture that connects a wide range of illicit activities—from ransomware and fraud to sanctions evasion and state-sponsored hacking—into a shared, global financial network.[10] As illicit actors increasingly exploit pseudonymity, decentralized systems, and cross-chain infrastructure, they expose the limitations of existing AML frameworks and raise fundamental questions about their ability to combat money laundering in the crypto space.

The Financial Action Task Force (FATF) has responded by undertaking the most comprehensive effort to extend AML standards to the crypto ecosystem.[11] FATF introduced the concept of Virtual Asset Service Providers (VASPs), bringing key intermediaries within regulatory scope.[12] It also developed a risk-based approach, calibrating obligations to the level of money-laundering risk, under which obligations attach to activities rather than to formal labels.[13] FATF has further applied the Travel Rule to virtual asset transfers, requiring VASPs to collect and transmit counterparty information, thereby extending a core transparency mechanism from traditional finance.[14] Together, these measures establish a global baseline for regulating crypto activities and improve traceability within the crypto ecosystem.

This Essay acknowledges the importance of FATF's efforts but argues that FATF's framework is structurally misaligned with the architecture of distributed systems. FATF's approach remains fundamentally intermediary-centric, attaching obligations to entities that act "for or on behalf of" users.[15] This model works effectively when transactions pass through centralized exchanges or custodial providers, but it breaks down when value is transferred through peer-to-peer transfers, decentralized applications, and cross-chain networks. Increasingly, critical aspects of transaction execution, including propagation, ordering, and inclusion, are controlled not by traditional intermediaries but by infrastructure-layer actors

9. *See* David Lopez Kurtz, *Cross-Chain Crime Hits $21 Billion*, CROKE FAIRCHILD DUARTE & BERES (July 21, 2025), https://crokefairchild.com/2025/07/cross-chain-crime-hits-21-8-billion/ [https://perma.cc/W64V-H955]; ELLIPTIC, *supra* note 8, at 8.

10. *See* CHAINALYSIS, *2026 Crypto Report*, *supra* note 5, at 4–5, 7, 22; FATF, UPDATED GUIDANCE (2021), *supra* note 8, at 8. *See generally* TRM LABS, 2026 CRYPTO REPORT, *supra* note 5.

11. *See* INT'L MONETARY FUND & FIN. STABILITY BD., IMF-FSB SYNTHESIS PAPER: POLICIES FOR CRYPTO-ASSETS 26, 30–32 (2023), https://www.fsb.org/uploads/R070923-1.pdf [https://perma.cc/BDS4-ZTRT].

12. FIN. ACTION TASK FORCE, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 7 (2024), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html (on file with the *Fordham Law Review*) [hereinafter FATF, TARGETED UPDATE (2024)].

13. FATF, UPDATED GUIDANCE (2021), *supra* note 8, at 25, 28, 31, 36.

14. *Id.* at 55–58.

15. *Id.* at 4–6 (noting that the key elements required to qualify as a VASP are "acting as a business for or on behalf of another person" and providing or actively facilitating VA-related activities).

such as wallet interfaces, remote procedure call (RPC) providers, sequencers, and block builders.[16] These actors do not fit within existing definitions of VASPs, yet they exercise meaningful control over whether and how transactions are executed and finalized. As illicit actors migrate toward these channels, the effectiveness of intermediary-based AML regulation diminishes.

To address this structural gap, this Essay proposes a shift from an intermediary-based model to an infrastructure-aware AML framework. This framework includes a normative reframing that shifts attention to financial infrastructure, the embedding of compliance through technical tools and system design, and the use of economic incentives to reinforce compliance outcomes. It further calls for institutional adaptations to recalibrate global AML governance for distributed systems. Such adaptations require reconfiguring cooperation from jurisdictional reciprocity to data-layer interoperability and transforming joint analysis and investigations into processes of collective sensemaking.

This Essay contributes to the growing literature on global AML governance by adding to the debate over FATF's effectiveness. Prior scholarship has largely focused on ambiguity in terminology,[17] high

16. *See generally* Philip Daian et al., *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*, *in* 2020 IEEE SYMP. ON SEC. AND PRIV. (2020); Lioba Heimbach, Lucianna Kiffer, Christof Ferreira Torres & Roger Wattenhofer, Ethereum's Proposer-Builder Separation: Promises and Realities (Sep. 24, 2023) (unpublished manuscript) (on file with the *Fordham Law Review*).

17. *See* BYUNGKYON LIM, GARY E. MURPHY & ZHENYA LEBEDEV, DEBEVOISE & PLIMPTON LLP, FATF GUIDANCE ON AML REGULATIONS POSES SIGNIFICANT CHALLENGES TO CRYPTO INDUSTRY, DEBEVOISE & PLIMPTON LLP 2 (2019), https://www.debevoise.com/insights/publications/2019/07/fatf-guidance-on-aml-regulations-poses [https://perma.cc/C8YR-STPG] (pointing out that the broad definition of "virtual assets" creates confusion by failing to differentiate between payment, investment, and asset tokens); Peter Van Valkenburgh, *The Long-Awaited FATF Crypto Guidance Is Not as Bad as It Could Have Been, but Still Flawed*, COIN CTR. (Oct. 28, 2021), https://www.coincenter.org/the-long-awaited-fatf-crypto-guidance-is-not-as-bad-as-it-could-have-been-but-still-flawed [https://perma.cc/AR6C-F2HQ] (arguing that FATF's guidance is overly broad and unclear, particularly regarding multisignature wallets, Decentralized Finance ("DeFi") platforms, and governance tokens). While wallet providers holding only backup keys likely fall outside the framework, the phrase "actively facilitates the transfer" introduces uncertainty, and its replacement of "facilitates" offers little improvement. *Id.*

compliance costs,[18] financial exclusion,[19] political biases,[20] limited enforcement power,[21] and sunrise issues.[22] This Essay builds on these critiques by locating FATF's limitations in the structural realities of decentralized financial systems. It highlights the role of underlying technological infrastructures, which is often underexamined or misunderstood by regulators and law enforcement, yet central to detecting and disrupting illicit activity, and reveals a foundational mismatch between these infrastructures and the assumptions embedded in the existing AML framework.

In addition to its conceptual contributions, this Essay offers a set of practical pathways for regulators, policymakers, and industry participants seeking to address money laundering in distributed systems. Rather than relying solely on extending existing intermediary-based rules, it identifies concrete leverage points within blockchain infrastructure, such as RPC providers, wallet interfaces, sequencers, and validators, where compliance functions can be meaningfully implemented. It also outlines how technical tools, including programmable compliance modules, on-chain analytics, and

18. *See KYC Compliance for Banks: Addressing the Cost*, FENERGO (July 4, 2024), https://resources.fenergo.com/blogs/kyc-compliance-for-banks-addressing-the-cost (on file with the *Fordham Law Review*) (explaining that implementing Know Your Customer (KYC) verification, customer due diligence, transaction monitoring, and suspicious activity reporting requires costly advanced technological solutions, legal expertise, and continuous regulatory updates).

19. Financial institutions, aiming to minimize regulatory risk or cut ties with clients and sectors deemed high-risk, often isolate legitimate businesses and individuals who lack alternative banking options. Rather than manage risks, financial institutions avoid them altogether. De-risking disproportionately affects smaller and more financially isolated economies, emerging market economies, and conflict zones. *See* Georgios Pavlidis, *The Dark Side of Anti-Money Laundering: Mitigating the Unintended Consequences of FATF Standards*, 2 J. ECON. CRIMINOLOGY 1, 1–4 (2023).

20. *See* ROYAL UNITED SERVS. INST., THE FUTURE OF THE FINANCIAL ACTION TASK FORCE: IMPROVING THE LEAST BAD OPTION? 4 (2024) (finding that political biases within FATF raise concerns, particularly regarding its governance structure, which allows countries in the Global North to dominate decision-making and marginalizes perspectives from the Global South, potentially risking member withdrawals); *see also* Gerald Kilimo, *The Good, the Bad and the Ugly of FATF*, BOTHO EMERGING MKTS. GRP. (Mar. 2024), https://www.bothogroup.com/blog/fatf [https://perma.cc/F58Q-Q7UT] (arguing that internal governance is influenced by member governments pressuring for national placements in key roles, casting doubt on FATF's impartiality, particularly in its treatment of developing countries).

21. *See* NOTABENE, THE STATE OF CRYPTO TRAVEL RULE COMPLIANCE REPORT 68, 82 (2024) (on file with the *Fordham Law Review*) (identifying that FATF is an international organization and therefore has limited enforcement power, as it cannot impose sanctions directly and relies instead on member states to implement and enforce its rules. This dependence weakens FATF's authority, as compliance varies significantly among countries, creating loopholes that sophisticated money launderers can exploit by operating in jurisdictions with weaker enforcement).

22. *See id.* at 67. The Travel Rule varies across jurisdictions, resulting in inconsistent compliance, a challenge known as the "sunrise issue." *Id.* at 80. When implementing new requirements on a global scale, they tend to "rise" at different times around the world, just as the sun does. *Id.* The Sunrise Period refers to the period during which the Travel Rule is not yet fully implemented across jurisdictions, thus creating regulatory gaps and asymmetrical compliance across different regions. *Id.*

privacy-preserving verification mechanisms can be integrated into system design and how market-based incentives can reinforce compliant behavior. By translating abstract regulatory challenges into actionable design and governance strategies, this Essay aims to bridge the gap between AML objectives and the operational realities of decentralized financial ecosystems.

This Essay proceeds as follows. Part I examines the rise of global crypto money laundering, highlighting its scale, evolving techniques, and increasing institutionalization across transnational networks. Part II analyzes the international regulatory framework led by FATF, focusing on its extension of AML obligations to VASPs. Part III identifies the structural limitations of this framework, arguing that its intermediary-centric approach fails to capture a growing share of crypto activity occurring outside traditional gatekeepers. Part IV proposes an infrastructure-aware model of AML governance.

I. THE RISE OF GLOBAL CRYPTO MONEY LAUNDERING

Money laundering refers to the process of concealing the illicit origins of funds so that they appear legitimate if discovered.[23] It is traditionally understood to operate through three stages: placement, in which illicit proceeds are introduced into the financial system; layering, in which transactions are structured to obscure the source and ownership of funds; and integration, in which laundered funds are reintroduced into the economy as seemingly lawful assets.[24]

The emergence of crypto fundamentally alters the infrastructure through which these stages are executed. This part explores how the crypto ecosystem reshapes money laundering. First, it demonstrates that illicit activity in crypto markets has expanded in absolute scale and evolved from fragmented, opportunistic practices into increasingly industrialized and professionalized networks. Second, and most importantly, it argues that this transformation reflects an infrastructural turn: the core functions of placement, layering, and integration are not only mediated by identifiable intermediaries but are increasingly executed through decentralized financial infrastructure.

---

23. Sarah Jane Hughes, *"Gatekeepers" Are Vital Participants in Anti-Money-Laundering Laws and Enforcement Regimes as Permission-Less Blockchain-Based Transactions Pose Challenges to Current Means to "Follow the Money*," 27 GEO. MASON L. REV. 1, 10 (2019). The UN Vienna 1988 Convention Article 3.1 describes money laundering as "[t]he conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions." U.N. OFF. ON DRUGS & CRIME, *supra* note 1.

24. *White-Collar Crime*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/white-collar-crime (last visited Oct. 10, 2026) (on file with the *Fordham Law Review*).

A. Growth and Industrialization

Illicit activity in crypto markets, while often described as a small share of overall transaction volume, has expanded in absolute terms to a scale that is economically and institutionally significant. In 2024, total crypto transaction volume exceeded $10 trillion, with illicit transactions estimated at roughly $40–50 billion.[25] Although the proportional share of illicit activity has fluctuated over time—declining from earlier peaks and varying across market cycles—the nominal value of illicit flows has continued to grow alongside broader adoption of digital assets.[26] More recent estimates suggest that by 2025, illicit crypto activity reached approximately $155 billion, nearly tripling within two years.[27]

Beyond its growth in scale, crypto money laundering has undergone a deeper organizational transformation. What initially appeared as fragmented, opportunistic activity conducted by individual actors has evolved into increasingly systematized and professionalized networks.[28] North Korean cyber operations, for example, have developed highly coordinated laundering infrastructures that integrate hacking, asset aggregation, obfuscation, and liquidation into a continuous process.[29] Specialized units conduct large-scale exploits, after which stolen assets are routed through layered transaction pathways before being converted into more liquid forms.[30] Importantly, parts of this process are increasingly outsourced to external networks that specialize in specific laundering functions, reflecting a move toward modular and scalable operational design.[31]

Another example is CMLNs. CMLNs function as high-volume clearing systems, connecting illicit actors with over-the-counter brokers, underground banking infrastructures, and informal value transfer mechanisms.[32] Rather

25. *See* TRM LABS, 2026 CRYPTO REPORT, *supra* note 5; CHAINALYSIS, 2025 CRYPTO REPORT, *supra* note 5, at 4.

26. TRM LABS, 2026 CRYPTO REPORT, *supra* note 5 (reporting that illicit crypto volume reached $158 billion in 2025 while illicit volume as a share of total volume fell from 1.3 percent in 2024 to 1.2 percent in 2025).

27. CHAINALYSIS, 2026 CRYPTO REPORT, *supra* note 5, at 3; TRM LABS, 2026 CRYPTO REPORT, *supra* note 5.

28. COMPLYADVANTAGE, THE STATE OF FINANCIAL CRIME 2026 31–32 (2026) (on file with the *Fordham Law Review*).

29. *North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion*, CHAINALYSIS (Dec. 18, 2025), https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/ [https://perma.cc/E22W-LH5Z]; TRM LABS, 2025 CRYPTO REPORT, *supra* note 5; TRM LABS, 2026 CRYPTO REPORT, *supra* note 5.

30. TRM LABS, 2026 CRYPTO REPORT, *supra* note 5 (describing how North Korean operators conduct major crypto thefts and then route stolen assets through chain hops, bridges, intermediary wallets, OTC brokers, and other layered laundering pathways before liquidation into more liquid assets such as Tron USDT).

31. *See* TRM LABS, 2026 CRYPTO REPORT, *supra* note 5.

32. *Chinese Language Money Laundering Networks Emerge as Major Facilitators of the Illicit Crypto Economy, Now Driving 20% of Laundering Activity*, CHAINALYSIS (Jan. 27, 2026), https://www.chainalysis.com/blog/2026-crypto-money-laundering/ [https://perma.cc/56UD-S4JX].

than operating as isolated intermediaries, they provide integrated services that facilitate the movement and conversion of funds across jurisdictions, currencies, and asset types.[33] CMLNs now process about 20 percent of known illicit crypto laundering activity, and this growth has been 7,325 times faster than illicit inflows to centralized exchanges since 2020.[34] CMLNs processed $16.1 billion in inflows in 2025, which equals roughly $44 million per day, across 1,799 active on-chain wallets.[35]

Taken together, these developments indicate that crypto money laundering increasingly resembles a mature industry, characterized by repeatable processes, scalable infrastructures, and networked coordination across actors and jurisdictions. Such an industry also produces convergence across illicit activities. Rather than operating through distinct financial channels, actors ranging from terrorist organizations and ransomware groups to fraud networks and state-sponsored hackers increasingly rely on the crypto ecosystem to move and monetize illicit proceeds.[36] The common thread is not the underlying crime, but the laundering layer that follows. In this sense, industrialization not only scales laundering activity but also standardizes it, enabling diverse actors to plug into the same infrastructure.

B. Laundering Infrastructure and Techniques

The industrialization of crypto money laundering is closely tied to a more fundamental transformation: the relocation of laundering functions from identifiable intermediaries to the technological infrastructure that governs transaction execution. In traditional finance, the stages of placement, layering, and integration are typically mediated by institutions such as banks, payment processors, and other regulated entities.[37] These institutions serve as chokepoints for monitoring and enforcement.[38] By contrast, in the crypto ecosystem, these functions are increasingly performed through distributed systems that enable, route, and transform transactions without requiring centralized control.[39]

Different components of the crypto ecosystem now perform distinct infrastructural roles within the laundering lifecycle. Centralized exchanges continue to function as key gateways between fiat and digital assets,

33. *Id.*
34. *Id.*
35. *Id.*
36. CHAINALYSIS, 2026 CRYPTO REPORT, *supra* note 5, at 4–7.
37. NMLRA (2026), *supra* note 3, at 35 ("Banks remain a key vector through which criminals seek to move funds given the sheer volume of financial activity in the banking sector."); *id.* at 57 ("Money launderers use [these] platforms to layer and integrate illicit proceeds from predicate crimes."); *id.* at 65–66 (describing transaction laundering in which illicit payments are routed through merchant accounts and the payment system, and discussing the roles of payment processors, card networks, and banks).
38. *Id.* at 64 ("[D]ue to the reliance on the highly regulated financial services sector to conduct transactions, there are measures in place, such as [customer due diligence] and suspicious activity reporting, at covered financial institutions that help to mitigate illicit finance risks in the legal sector.").
39. *Id.* at 53 (describing tools criminals use to make it difficult to trace assets).

facilitating entry and exit points for illicit funds.[40] At the same time, stablecoins have emerged as dominant value-transfer rails, offering price stability, deep liquidity, and rapid settlement across borders.[41] Their widespread adoption has made them the preferred medium for moving illicit value at scale, particularly in sanctions evasion and transactional financial crime.[42]

Beyond these gateways and value rails, a growing set of decentralized tools enables the fragmentation and obfuscation of transaction trails. Cross-chain bridges,[43] decentralized exchanges,[44] and swap protocols[45] allow actors to move assets across blockchain networks, exploiting interoperability to complicate tracing and attribution. Crypto mixers further obscure transaction provenance by pooling and redistributing funds, weakening the link between source and destination addresses on otherwise transparent ledgers.[46] Together, these systems create layered pathways through which illicit funds can be routed, transformed, and concealed without reliance on a single controlling entity.

What distinguishes this infrastructural configuration is not merely the availability of new tools and channels, but the redistribution of functional control over transaction execution. The capacity to move, transform, and obscure value is embedded directly within the architecture of the system, rather than concentrated in regulated intermediaries.

II. THE FATF FRAMEWORK AND ITS EXPANSION TO CRYPTO

Internationally, FATF serves as the global standard-setting body for anti-money laundering and countering the financing of terrorism

40. U.S. DEP'T OF THE TREASURY, *supra* note 8, at 34–35.

41. FIN. ACTION TASK FORCE, TARGETED REPORT ON STABLECOINS & UNHOSTED WALLETS: PEER TO PEER TRANSACTIONS 11–13 (2026), https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/targeted-report-on-stablecoins-and-unhosted-wallets.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*); *Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale*, CHAINALYSIS (Jan. 8, 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction [https://perma.cc/P9LH-VJFX] [hereinafter Chainalysis Team].

42. Chainalysis Team, *supra* note 41 (explaining that stablecoins now account for 84 percent of illicit transaction volume because of their easy cross-border transferability, lower volatility, and broader utility).

43. EUROPOL, CRYPTOCURRENCIES: TRACING THE EVOLUTION OF CRIMINAL FINANCES 9–10 (2021), https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (select "downloads") (on file with the *Fordham Law Review*); ELLIPTIC, *supra* note 8, at 8.

44. ELLIPTIC, *supra* note 8, at 8.

45. *Id.*

46. 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 [https://perma.cc/YYS9-RVZP]; Press Release, U.S. Dep't of Just., Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer that Processed Over $3 Billion of Unlawful Transactions (Mar. 15, 2023), https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed-over-3 (on file with the *Fordham Law Review*).

(AML/CFT).[47] These standards comprise Recommendations, Interpretive Notes, and relevant definitions from the glossary.[48] FATF collaborates with its forty member countries and regional organizations to ensure the effective implementation of these standards.[49] Although FATF's standards are not legally binding, they provide an influential framework widely adopted by various jurisdictions through national legislation.[50]

With the rise of cryptocurrencies, FATF has adapted its standards to address the specific risks they pose. This part highlights the key components of the FATF's AML/CFT framework, focusing on the new glossary definitions, the Risk-Based Approach, and the Travel Rule.

A. New Glossary Definitions

Recommendation 15 is a key component of the FATF framework, addressing the risks associated with new payment methods and emerging technologies.[51] The 2018 update to Recommendation 15 reflected FATF's acknowledgment of the growing role of cryptocurrencies in the global financial system by introducing two new glossary definitions: "virtual asset (VA)" and "virtual asset service provider (VASP)."[52]

A VA is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes.[53] VAs do not include digital representations of fiat currencies, securities, or other financial assets that are already covered elsewhere in the FATF Recommendations.[54] A VASP means:

> any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
> - exchange between virtual assets and fiat currencies;
> - exchange between one or more forms of virtual assets;
> - transfer of virtual assets;

47. *Who We Are*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/en/the-fatf/who-we-are.html (last visited Oct. 10, 2026) (on file with the *Fordham Law Review*).

48. *See The FATF Recommendations*, FIN. ACTION TASK FORCE (June 2026), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (on file with the *Fordham Law Review*).

49. *Who We Are*, *supra* note 47.

50. NOTABENE, *supra* note 21, at 16.

51. FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS 17 (2012, updated 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Feburary%202025%20FATF%20Recommendations.pdf (on file with the *Fordham Law Review*) [hereinafter FATF, INTERNATIONAL STANDARDS]. This document has undergone periodic updates. The original version was published in 2012; Interpretive Note to Recommendation 15 regarding VASPs was introduced in the 2019 update, followed by further revisions in 2021, 2023, and 2025, with the 2025 version being the most recent. *See generally id.*

52. FATF, UPDATED GUIDANCE (2021), *supra* note 8, at 8.

53. *Id.* at 109.

54. *Id.*

- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[55]

This update ensures that VASPs are brought under the same regulatory scrutiny as traditional financial institutions. These entities must now adhere to the same AML/CFT standards, including licensing, registration, and ongoing supervision by competent authorities.[56]

The Interpretive Note to Recommendation 15, adopted in June 2019, provides detailed guidance on how the FATF requirements should apply to VAs and VASPs.[57] The Interpretive Note clarifies that VASPs are subject to the full range of preventive measures, including customer due diligence, recordkeeping, and the reporting of suspicious transactions.[58] Furthermore, it mandates that VASPs must be licensed or registered in the jurisdiction where they operate and that authorities must take steps to prevent criminals from owning or controlling VASPs.[59]

B. Risk-Based Approach

The cornerstone of the FATF's AML/CFT framework is the Risk-Based Approach, which requires jurisdictions and regulated entities to identify, assess, and mitigate money-laundering and terrorist-financing risks, rather than applying uniform rules across all activities.[60] This approach reflects a shift from rule-based compliance toward a dynamic system in which regulatory intensity is calibrated to the level of risk presented.

This framework imposes several baseline obligations. First, countries must conduct national risk assessments to develop a comprehensive understanding of risks within their financial systems and allocate supervisory resources accordingly.[61] Second, they are expected to impose enhanced due

---

55. *Id.*

56. FATF, INTERNATIONAL STANDARDS, *supra* note 51, at 17.

57. FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS & VIRTUAL ASSET SERVICE PROVIDERS 55 (2019), https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (on file with the *Fordham Law Review*).

58. *See id.*

59. *Id.*

60. FIN. ACTION TASK FORCE, RISK-BASED SUPERVISION 5, 8 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Risk-Based-Supervision.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*) [hereinafter FATF, Risk-Based Supervision (2021)]; FIN. ACTION TASK FORCE, UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS & VIRTUAL ASSET SERVICE PROVIDERS, *supra* note 57, at 7; FIN. ACTION TASK FORCE, GUIDANCE ON PROLIFERATION FINANCING RISK ASSESSMENT AND MITIGATION 5 (2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*); FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL CURRENCIES 6 (2015), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*) [hereinafter FATF, GUIDANCE (2015)].

61. *See* FATF, Risk-Based Supervision (2021), *supra* note 60, at 12–13.

diligence and stricter controls in higher-risk scenarios, while permitting simplified measures where risks are demonstrably lower.[62] Third, the Risk-Based Approach requires institutional coordination: Under Recommendation 2, jurisdictions must establish mechanisms to facilitate cooperation among regulators, law enforcement, and policymakers.[63] Finally, effective implementation depends on supervision and enforcement. Recommendations 26 and 27 require that regulated entities be monitored by competent authorities with powers to inspect, compel information, and impose proportionate and dissuasive sanctions.[64]

FATF has extended this general framework to VAs through its 2019 Interpretive Note to Recommendation 15 and subsequent guidance.[65] These materials clarify that VASPs fall within the scope of AML/CFT obligations and must be licensed or registered in relevant jurisdictions.[66] Countries may also require foreign VASPs that offer services in their jurisdictions to comply with local regulatory requirements.[67] As in the traditional financial system, VASPs are expected to implement risk-based controls, including customer due diligence, monitoring, and reporting, tailored to the risks associated with their activities.[68]

Applying the Risk-Based Approach in the crypto context requires translating its general principles into a technologically distinct environment. FATF guidance identifies several risk factors specific to virtual assets, including pseudonymous transactions, non-face-to-face business relationships, and exposure to unknown or unverified counterparties.[69] These features can increase opacity and complicate traditional customer identification and transaction monitoring processes. Accordingly, jurisdictions and VASPs are expected to incorporate these factors into their risk assessments and adopt enhanced safeguards where necessary.

The Risk-Based Approach also requires attention to Decentralized Finance ("DeFi") when assessing risk.[70] FATF acknowledges that regulating DeFi

62. *See* FATF, GUIDANCE (2015), *supra* note 60, ¶ 23, at 8; FATF, Risk-Based Supervision (2021), *supra* note 60, at 32–34.

63. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶ 110, at 41.

64. *See id.* ¶ 142, at 47.

65. *See id.* ¶¶ 98–99, at 37–38.

66. *See* FATF, INTERNATIONAL STANDARDS, *supra* note 51, ¶ 3, at 78.

67. *See id.* ¶ 3, at 78.

68. *See id.* ¶ 10, at 14, ¶ 5, at 78.

69. *See id.* ¶ 15 at 71.

70. FATF's updates between 2021 and 2023 reflect an effort to expand its AML/CFT framework to address risks posed by DeFi. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 67–68, at 27, ¶ 69, at 28; FIN. ACTION TASK FORCE, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, ¶¶ 31–34, at 19–20 (2022), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*) [hereinafter FATF, TARGETED UPDATE (2022)]; FIN. ACTION TASK FORCE, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, ¶¶ 37–43, at 28–32 (2023) https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf (on file with the *Fordham Law Review*) [hereinafter FATF, TARGETED UPDATE (2023)].

presents significant challenges.[71] Many DeFi arrangements lack a clearly identifiable operator, and control may be distributed across developers, governance token holders, or autonomous code, making it difficult to enforce compliance obligations.[72] FATF also highlights risks associated with anonymity, cross-border accessibility, and the absence of traditional account-based relationships.[73]

FATF does not create a wholly new regulatory category for DeFi. Instead, FATF reaffirms that its existing definition of a VASP remains the central organizing concept.[74] Under this framework, the critical inquiry is not whether an arrangement is labeled "DeFi," but whether any person or entity exercises "control or sufficient influence" over the protocol.[75] Where such control or influence exists, those actors may be treated as VASPs and are therefore subject to AML/CFT obligations.[76] At the same time, the Risk-Based Approach requires regulators and regulated entities to account for technological features in DeFi that may elevate risk, thereby warranting enhanced due diligence and closer monitoring.[77]

C. The Travel Rule

The Travel Rule originated in the traditional financial system as part of AML regulation governing wire transfers.[78] Codified in Recommendation 16 of the FATF framework, wire transfers were defined "as any transaction carried out on behalf of an originator through a [financial institution] by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary [financial institution], irrespective of whether the originator and the beneficiary are the same person."[79] The rule requires financial institutions to transmit identifying information about the originator and beneficiary of a transfer so that such information "travels"

71. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 68–69, at 28; FATF, TARGETED UPDATE (2022), *supra* note 70, ¶¶ 30–34, at 19–20; FATF, TARGETED UPDATE (2023), *supra* note 70, at 4, ¶¶ 37–42, at 28–30, ¶ 56, at 35.

72. *See* FATF, TARGETED UPDATE (2023), *supra* note 70, at 4, ¶¶ 37–41, at 28–29, ¶ 56, at 35.

73. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 1–9, at 7–9, ¶¶ 63–71, at 26–28, ¶¶ 154–55, at 50; FATF, TARGETED UPDATE (2022), *supra* note 70, ¶¶ 30–43, at 19–22, 25; FATF, TARGETED UPDATE (2023), *supra* note 70, ¶¶ 33–52, at 27–34, ¶¶ 53–57, at 35.

74. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 57–70, at 25–28; FATF, TARGETED UPDATE (2022), *supra* note 70, ¶¶ 33–34, at 19–20; FATF, TARGETED UPDATE (2023), *supra* note 70, ¶¶ 38–41, at 28–29.

75. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 57–76, at 25–29, ¶¶ 93–94, at 36; FATF, TARGETED UPDATE (2022), *supra* note 70, ¶ 33, at 19–20; FATF, TARGETED UPDATE (2023), *supra* note 70, ¶ 40, at 29.

76. FATF, TARGETED UPDATE (2023), *supra* note 70, ¶¶ 39–41, at 29–30.

77. *See id.* at ¶¶ 39–41, at 28–30.

78. *See* FATF, INTERNATIONAL STANDARDS, *supra* note 51, ¶ 16, at 17 (requiring financial institutions to include originator and beneficiary information with wire transfers, ensure that such information remains with the transfer throughout the payment chain, and monitor transfers for missing information).

79. FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶ 176, at 56.

with the transaction.[80] The objective is to enhance traceability, facilitate sanctions screening, and enable law enforcement to reconstruct financial flows.[81] As VAs gained prominence, FATF extended this requirement to VA transfers through its Interpretive Note to Recommendation 15.[82]

To comply with the Travel Rule, VASPs must first identify the counterparty institution and conduct due diligence before initiating transactions and sharing any information to establish a certain level of trust in the counterparty.[83] Second, VASPs must collect information about the counterparty's customer.[84] The level of information collection can vary by jurisdiction.[85] For example, in Estonia, VASPs are not required to collect beneficiary names, whereas in Singapore, such information is mandatory.[86] Third, VASPs need to assess the risk associated with the counterparty's customer, which involves sanctions screening to ensure compliance with relevant regulations.[87] Lastly, VASPs must securely transmit customer information to the counterparty institution and make it available upon request to appropriate authorities.[88] Countries should require that VASPs and other obliged financial institutions maintain the required originator and beneficiary information, and submit it to beneficiary institutions.[89]

When a transaction involves an unhosted or self-hosted wallet—meaning no counterparty VASP is present—the application of the Travel Rule shifts in an important way. Because there is no intermediary on the other side from whom information can be transmitted, the originating VASP must obtain the required originator and beneficiary information directly from its own customer.[90] This includes identifying the customer initiating the transfer as well as collecting information about the beneficiary associated with the self-hosted wallet, to the extent available.[91] The VASP must treat the unhosted wallet as a source of counterparty risk and assess that risk using information provided by its customer and other available data.[92] This may include, where appropriate, verifying aspects of the beneficiary information, applying sanctions screening, and evaluating whether the transaction exhibits higher-risk characteristics.[93]

80. FATF, INTERNATIONAL STANDARDS, *supra* note 51, ¶ 8, at 81.
81. *See id.* ¶ 8, at 81.
82. *See id.* ¶ 7, at 79; *see also* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶ 178, at 56.
83. *See* FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 196–99, at 62–64.
84. *See id.* ¶¶ 197–99, at 62–64.
85. *See* NOTABENE, *supra* note 21, at 23, 72–74.
86. *See id.* at 95.
87. *Id.* at 21.
88. FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶ 188, at 60.
89. *Id.* at 57, 59.
90. *See id.* ¶ 295, at 86.
91. *See* NOTABENE, *supra* note 21, at 20.
92. *See id.*
93. *See id.*

III. THE LIMITS OF INTERMEDIARY-BASED AML: A STRUCTURAL MISMATCH

While scholars have long debated FATF's effectiveness, the existing literature has primarily focused on state capacity and institutional compliance.[94] This Essay shifts the analysis to the decentralized financial architecture, asking whether FATF's enforcement model remains viable in such architecture. It argues that FATF's fundamental weakness lies in its reliance on the presence of trusted intermediaries to enforce compliance, an assumption that becomes increasingly untenable as financial activity migrates to decentralized environments.

A. Trust Architectures

The concept of trusted intermediaries can be understood through Professor Kevin Werbach's typology of trust architectures.[95] Professor Werbach explains that trust in economic systems is not monolithic, but organized through four primary architectures.[96] First is peer-to-peer trust, which arises from direct interpersonal relationships and reputational signals, typical of small communities or repeated interactions.[97] Second is Leviathan trust, grounded in centralized authority, where institutions such as governments enforce rules and guarantee compliance through law and coercion.[98] Third is intermediary trust, which relies on private trusted actors, such as banks, clearinghouses, or payment platforms, which sit between parties and facilitate transactions by providing verification, custody, and enforcement.[99] Finally, Werbach identifies distributed trust, exemplified by blockchain systems, where trust is embedded in technical protocols and consensus mechanisms rather than centralized authorities.[100]

This framework is particularly useful for analyzing financial regulation: Traditional AML regimes, such as U.S. AML laws, are largely designed around intermediary trust, assuming the presence of identifiable gatekeepers capable of monitoring transactions and enforcing compliance.[101] By contrast, blockchain networks shift elements of trust toward distributed

---

94. *See supra* notes 17–22 and accompanying text.

95. *See generally* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (Sandra Braman ed., 2018). In this book, Werbach distinguishes among peer-to-peer, Leviathan, intermediary, and distributed trust, each representing a distinct architecture through which trust is established and maintained. *See generally id.*

96. *See id.* at 25–31.

97. *See id.* at 26.

98. *See id.* at 27.

99. *See id.* at 27–28.

100. *See id.* at 28–31. Distributed trust is also referred to as "trustless trust," a term coined by Reid Hoffman. *Id.*

101. Jiaying Jiang, *Crypto Money Laundering*, 41 BERKELEY TECH. L.J. 199, 231 (2026) ("Current laws and regulations continue to rest on the assumption that there is always a centralized entity responsible for compliance. This assumption is evident in statutory text, regulatory interpretation, and enforcement actions."); *see also* 31 U.S.C. § 5312(a)(2) (The Anti-Money Laundering Act's definition of "financial institution": a person who engages as a business).

architectures, thereby weakening regulatory models that depend on stable, institutionally anchored intermediaries.[102]

B. The Mismatch

On closer examination, one positive aspect of the FATF framework is that many of its rules acknowledge decentralized elements of the crypto ecosystem. For example, FATF intentionally defines VASPs by activity rather than by labels, acknowledging that crypto ecosystems do not map neatly onto traditional institutional categories.[103] Instead of regulating exchanges or banks, FATF regulates entities that conduct certain functions (custody, transfer, exchange), recognizing that decentralized systems can fragment roles across actors.[104] FATF has also repeatedly acknowledged the existence of peer-to-peer transfers and self-hosted wallets, which operate without intermediaries.[105] In defining VASPs, the framework intentionally excludes DeFi applications when they function solely as software platforms,[106] and it does not treat non-fungible tokens as virtual assets when they are used as collectibles.[107]

While it is promising that FATF acknowledges the features and complexities of decentralized ecosystems and attempts to regulate accordingly, it has not gone far enough. In practice, many of its rules and suggested regulatory tools continue to gravitate toward an intermediary-based trust model. For example, FATF requires VASPs to be licensed or registered in the jurisdiction in which they are established, premised on the assumption that there exists an identifiable legal or natural person who can be held accountable for compliance.[108]

A similar intermediary-centric logic is embedded in FATF's approach to customer due diligence and beneficial ownership identification. FATF guidance presumes that a regulated entity is both capable of and responsible for establishing the identity of transacting parties.[109] This presupposes not only that identity can be reliably anchored in off-chain documentation, but

---

102. *See* Jiang, *supra* note 101, at 229 ("The crypto industry emerged around the concept of 'trustless trust,' where cryptographic, decentralized protocols, rather than intermediaries, guarantee the integrity of transactions and relationships. In contrast, the existing legal framework attempts to bring the crypto industry back to an intermediary trust system, forcing it into a structure that undermines its core principles."); Carla L. Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343, 1350 (2024) ("U.S. regulatory regimes demand, and even encourage, centralization that [blockchain] technology itself obviates.").

103. FATF, UPDATED GUIDANCE (2021), *supra* note 8, ¶¶ 25–26, at 13, ¶¶ 29–30, at 15, ¶¶ 45–52, at 22–23.

104. *See id.* ¶¶ 45–54, at 22–24.

105. *See id.* ¶¶ 37–43, at 18–21.

106. *See id.* ¶ 76, at 29.

107. *See id.* ¶ 53, at 24.

108. *See id.* ¶ 125, at 43.

109. *See* FATF, INTERNATIONAL STANDARDS, *supra* note 51, ¶¶ 2–8, at 78–79 (stating potential requirements for VASPs to "identify, assess, and take effective action to mitigate their money laundering, terrorist financing and proliferation financing risks" without acknowledging the limits of VASPs' capabilities in identifying transacting parties).

also that a designated intermediary can verify, update, and vouch for that information over time. In decentralized environments, however, identity is often fragmented, pseudonymous, or dynamically constructed across multiple protocols.

FATF's reliance on intermediaries is also evident in its emphasis on transaction monitoring and suspicious activity reporting. These requirements assume that regulated entities occupy a privileged observational position, enabling them to detect anomalous behavior and flag illicit activity.[110] This assumption holds in traditional finance, where intermediaries have comprehensive visibility into customer accounts and transaction flows.[111] In contrast, crypto transaction activity is often distributed across wallets, protocols, and chains, with no single actor possessing full visibility.[112]

Finally, FATF's broader enforcement architecture continues to rely on jurisdictionally anchored entities as points of leverage for regulation. Its recommendations assume that national authorities can supervise, audit, and sanction identifiable actors within their territorial reach.[113] This jurisdiction-based enforcement model aligns with intermediary institutions that have a clear legal presence, a well-defined governance structure, and a nexus to a specific state. However, many crypto infrastructures, such as decentralized protocols, validator networks, or Decentralized Autonomous Organization governance, do not map neatly onto such jurisdictional boundaries.

All these examples show how FATF's rules consistently recenter regulatory authority around identifiable actors, introducing a layer of functional centralization and reinforcing reliance on regulated intermediaries as the primary points of control within the ecosystem. This approach creates a structural tension with decentralized systems and helps explain why the existing framework is ineffective at combating money laundering in the crypto space.

---

110. *See id.* at 14 (presupposing that VASPs, like traditional financial intermediaries, can develop customer risk profiles, continuously compare observed transactions against expected customer behavior, and identify deviations as potentially suspicious).

111. *See* 12 C.F.R. § 21.11(c) (2024) (requiring national banks to file a Suspicious Activity Report (SAR) upon detecting transactions that may involve money laundering); 31 C.F.R. § 1020.320 (2024) (paralleling the Financial Crimes Enforcement Network's SAR obligation for banks).

112. *See* Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, *Decentralized Finance*, 6 J. FIN. REGUL. 172, 185–86 (2020) (observing that in decentralized networks "multiple entities provide parts of a service and clients are similarly spread around the globe," such that "markets and individual providers lose importance as supervisory access and control points," and concluding that neither entity-based nor function-based supervisory approaches can be effectively applied).

113. *See* FATF, INTERNATIONAL STANDARDS, *supra* note 51, ¶¶ 3–8, at 78–79 (requiring VASPs to be licensed or registered and subject to inspection, information-compulsion, and sanctions by competent authorities).

IV. TOWARD INFRASTRUCTURE-AWARE AML GOVERNANCE

This part sketches a path forward for AML governance in decentralized environments. At the outset, it is important to recognize that not all blockchain or crypto projects are meaningfully decentralized.[114] Many so-called decentralized systems, or DeFi, remain highly centralized in design, governance, and operation, such as centralized stablecoin issuers and centralized crypto exchanges.[115] In such settings, the traditional intermediary-based regulatory approach remains feasible, as identifiable entities can serve as compliance gatekeepers.[116]

This Essay focuses on the more challenging category of projects that are meaningfully decentralized and proposes an infrastructure-aware AML framework. This framework consists of two components: a normative reframing that shifts attention from intermediaries to financial infrastructure, and institutional adaptations that recalibrate global AML governance for distributed systems.

A. From Intermediaries to Infrastructure

This Essay advances three dimensions—conceptual, technical, and economic—to shift attention from intermediaries to infrastructure. First, it proposes a normative reframing: shifting AML regulation from intermediaries to infrastructure-layer actors with functional control over the transaction lifecycle. Second, it argues that compliance must be embedded directly into financial infrastructure through technical tools and system design. Third, it emphasizes that these technical mechanisms should be complemented by economic incentives aligned with compliance outcomes.

1. Normative Reframing

As Part III concludes, regulatory frameworks premised on stable gatekeepers and trusted intermediaries face structural limits in decentralized environments. To address this mismatch, AML governance should shift toward an infrastructure-aware model that targets functional control over the transaction lifecycle.[117] Rather than asking whether a VASP exists, the

114. *See* Jiang, *supra* note 101, at 234, 237–38 (analyzing decentralization across three key dimensions—development, governance, and operation—and finding that some projects remain highly centralized, only one achieves maximum decentralization, and many fall somewhere in between, blending elements of centralization and decentralization to varying degrees).

115. *See id.* at 236–37 ("[D]evelopment refers to who builds the project, which addresses the relationship between developers and projects . . . . [G]overnance refers to control or influence over a project after deployment . . . . [O]peration refers to whether the project outsources critical functions or processes to third parties.").

116. *See id.* at 255.

117. *See generally* Raphael Auer, *Embedded Supervision: How to Build Regulation into Decentralised Finance* (CESifo, Working Paper No. 9771, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4127658 (on file with the *Fordham Law Review*) (proposing that supervision be built directly into the architecture of decentralized markets rather than imposed through intermediaries).

relevant inquiry should be whether an actor controls critical stages of the transaction lifecycle, including propagation, ordering, and inclusion. This framing redefines the basis for allocating AML obligations.

In contemporary blockchain systems, such control is exercised by a range of infrastructure-layer participants, including RPC providers that relay transactions, wallet interfaces that shape user interactions, sequencers that determine which transactions are included in rollups, and block builders or validators that influence ordering and execution.[118] These actors do not fit neatly within existing VASP definitions.

However, these actors are better positioned to combat money laundering because their control operates at the point of transaction formation and execution, rather than after the fact. Unlike traditional intermediaries, which often rely on ex post monitoring and reporting, infrastructure-layer participants can influence whether, how, and under what conditions transactions are propagated, ordered, or finalized.[119] Moreover, because many of these actors sit at coordination bottlenecks, they possess a vantage point that aggregates activity across users, protocols, and chains. Targeting these sites of functional control therefore offers a more effective means of disrupting illicit financial flows in decentralized systems than relying solely on intermediary-based regulation at the application layer.

2. Embedding Compliance in Infrastructure Design

Building on this reframing, operationalizing the shift requires allocating compliance responsibilities across the transaction stack. Each category of infrastructure actor should be subject to obligations calibrated to its role.

RPC providers, for example, can implement risk-based filtering, rate-limiting, or flagging mechanisms at the point of transaction propagation, particularly for known illicit addresses or sanctioned entities. Wallet interfaces can embed ex ante compliance features such as address screening, transaction simulation with risk scoring, and user warnings for high-risk transfers. Sequencers and block builders can incorporate policy-aware ordering rules, such as excluding transactions linked to sanctioned addresses or prioritizing compliant flows.[120]

---

118. *See generally* Daian et al., *supra* note 16 (demonstrating how ordering, inclusion, and execution are loci of operational control exercised by miners and, now, block builders); Heimbach et al., *supra* note 16 (empirically documenting the emergence of builders, relays, and proposers as distinct infrastructure actors following the Merge).

119. *See* Andrew Allen, *Solana - When Mainnet?*, COINBASE (Sep. 9, 2022), https://www.coinbase.com/developer-platform/discover/insights-analysis/solana-when-mainnet (on file with the *Fordham Law Review*) (describing RPC- and validator-level controls that affect transaction routing and processing).

120. *See generally* ANDERS BROWNWORTH, JON DURFEE, MICHAEL JUNHO LEE & ANTOINE MARTIN, FED. RSRV. BANK N.Y., REGULATING DECENTRALIZED SYSTEMS: EVIDENCE FROM SANCTIONS ON TORNADO CASH (2024), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1112.pdf [https://perma.cc/3CL8-8TDW] (documenting that U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)-compliant Maximal Extractible Value (MEV)-Boost relays systematically excluded Tornado

To ensure that compliance is not merely optional but systematically embedded, these obligations must be translated into infrastructure-level design requirements. This approach builds on the emerging concept of "compliance-by-design," under which regulatory requirements are incorporated directly into technological architecture and automated processes.[121] In the decentralized context, such an approach could take the form of open, auditable modules that integrate sanctions screening, anomaly detection, and reporting hooks directly into widely used clients, software development kits, and node software.

For example, standardized compliance libraries could be incorporated into wallet software or RPC endpoints, while block-building software could include configurable policy engines reflecting jurisdictional requirements. Crucially, these mechanisms should be interoperable and modular, allowing different jurisdictions or networks to adapt them without fragmenting the underlying infrastructure. Privacy-enhancing technologies can also play a role, enabling selective disclosure or zero-knowledge compliance proofs that reconcile AML objectives with user privacy.[122]

A central challenge, however, lies in governance: who sets these rules and who enforces them in a decentralized environment. Here, a hybrid model is likely to emerge. Standard-setting bodies (e.g., FATF) can articulate high-level functional expectations, while technical standards organizations, open-source communities, and industry consortia translate these into implementable specifications. Enforcement, in turn, becomes layered and distributed. States may impose legal obligations on infrastructure providers (e.g., major RPC providers or wallet developers), while networks themselves may adopt protocol-level constraints or social norms—for instance, through client defaults, validator coordination, or slashing conditions tied to prohibited behavior. In this model, compliance is neither purely external (state-imposed) nor purely internal (code-based), but emerges from the interaction between regulatory mandates, technical design, and network governance.[123]

Cash-linked transactions from block inclusion following the August 2022 sanctions designation).

121. *See* BANK FOR INTERNATIONAL SETTLEMENTS, PROJECT MANDALA: SHAPING THE FUTURE OF CROSS-BORDER PAYMENTS COMPLIANCE 1, 8 (2024) (describing "compliance-by-design" as "a systematic approach to integrating regulatory requirements into automated tasks and processes").

122. *See* Jiang, *supra* note 101, at 205, 247 (proposing a zero-knowledge-proof-based digital identity system for "decentralized digital infrastructure" for AML, permitting users to prove verified status without exposing underlying personal data, and thus reconciling AML obligations with the privacy norms of decentralized systems).

123. *See generally* LAWRENCE LESSIG, CODE: VERSION 2.0 (2006) (theorizing that regulation in networked environments emerges from the interaction of law, architecture, markets, and norms); PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE (2018) (analyzing how states may regulate blockchain-based systems through law, social norms, market forces, and code, including by regulating end users, intermediaries such as exchanges, miners, hardware manufacturers, and the code itself, so that legal mandates are carried out through technical design); Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is*

3. Economic Incentives

Technical embedding alone is insufficient without economic alignment. In decentralized systems, compliance must also be reinforced through market-based mechanisms that shape behavior via incentives rather than solely through legal compulsion. At the transaction and asset level, one emerging dynamic is the development of "compliance premiums," where assets or transactions that meet certain standards, such as being screened or traceable, gain preferential access to liquidity, institutional capital, or critical infrastructure.[124] Conversely, noncompliant flows may face economic frictions, including higher fees, reduced composability, or exclusion from major platforms.

At the infrastructure level, economic incentives can operate directly on the providers that facilitate transactions. Infrastructure providers themselves may compete on compliance quality, offering compliance-enhanced or "institutional-grade" services that attract more users.[125] These incentive structures could be reinforced through protocol-level mechanisms. Existing proof-of-stake systems already use staking, slashing, and reward allocation to incentivize desired validator behavior and penalize misconduct.[126] Similar mechanisms could be adapted to compliance objectives: Validators or sequencers that adhere to compliance standards could receive greater delegation or order flow, while noncompliant actors could face penalties, exclusion, or reputational loss.

Over time, these technical and market mechanisms generate a form of endogenous regulation, where compliance becomes a condition of participation in economically valuable segments of the ecosystem. In this way, AML governance is reconstituted not as an external overlay imposed on decentralized systems, but as an internal feature of their architecture and incentive structure, aligning regulatory objectives with the operational logic of DeFi.

Code, 21 FIRST MONDAY (Dec. 2016), https://firstmonday.org/ojs/index.php/fm/article/view/7113 [https://perma.cc/63AR-NZV3] (explaining the interdependent relationship between law and technology and how technological architectures can increasingly serve as mechanisms for implementing and enforcing legal rules).

124. *See* David Duong, *Growth of the Liquid Staking Market*, COINBASE (Nov. 7, 2022), https://www.coinbase.com/institutional/research-insights/research/market-intelligence/growth-of-the-liquid-staking-market (on file with the *Fordham Law Review*) (observing that enterprise-grade compliance may be a prerequisite for institutional participation and that a premium may attach to instruments incorporating KYC/AML features).

125. *See* Brady Turner, *Building the Future of Institutional Staking: Figment's 2024 Review and 2025 Vision*, FIGMENT (Jan. 24, 2025), https://www.figment.io/insights/building-the-future-of-institutional-staking/ [https://perma.cc/ZU8C-LWAH] (marketing compliance-enhanced validator services as a premium and providing customizable offerings for institutional clients).

126. For example, Ethereum itself explains the economic structure very clearly: Validators receive rewards for actions that benefit the network, incur penalties for failures, and can have their stake "slashed" for malicious conduct. Ethereum expressly describes slashing as a mechanism for economically disincentivizing harmful validator behavior. *See Validator FAQs*, STAKING LAUNCHPAD, https://launchpad.ethereum.org/en/faq [https://perma.cc/AY74-EE4G] (last visited Aug. 26, 2026).

B. Institutional Adaptations

Recalibrating global AML governance for distributed systems also requires institutional adaptations. By institutional adaptations, this Essay means changes to the machinery of cooperation through which AML rules and standards are applied across borders—the formats, channels, and analytical arrangements that connect authorities and relevant actors to one another. Two adaptations are especially important, and each takes a core function of traditional cooperation and translates it into the technical architecture of distributed systems.

The first adaptation reengineers cooperation architectures from jurisdictional reciprocity to data-layer interoperability. Traditional AML governance relies heavily on reciprocity-based exchanges—whether through Financial Intelligence Unit networks, mutual legal assistance, or bilateral trust relationships—where information is requested, shared, and validated across sovereign boundaries.[127] It emphasizes the importance of standardized templates, secure communication channels, and clear contact points to make these exchanges efficient and reliable.[128] Informal communication channels can supplement these mechanisms by allowing authorities to exchange information more quickly and iteratively when investigations evolve rapidly.[129]

In distributed systems, these insights can be operationalized by embedding standardized data schemas and compliance interfaces directly into financial infrastructure, for example: interoperable wallet attribution standards, machine-readable compliance signals, shared blockchain analytics layers, or Application Programming Interface based reporting mechanisms. Instead of relying solely on ex post requests between authorities, governance can shift toward ex ante harmonization of data formats and observability, reducing the institutional friction involved in identifying, preparing, and sharing information for subsequent analysis.

The second adaptation moves from information exchange to collective sensemaking.[130] The traditional insight comes from joint investigations, which allow authorities to pool data, coordinate methodologies, and generate richer insights than any authority could achieve independently.[131] This collaborative function becomes particularly important in distributed systems, where illicit financial activity may unfold across multiple blockchains, protocols, infrastructure layers, and jurisdictions, while the data necessary to reconstruct that activity remains fragmented among different authorities and private actors.

Translating this model into distributed systems points toward shared analytical environments, such as federated data platforms or privacy-preserving computation systems, which enable multiple authorities

127. *See* FIN. ACTION TASK FORCE ET AL., *supra* note 2, at 8–10.
128. *See generally* FIN. ACTION TASK FORCE ET AL., *supra* note 2, at 13, 33–35.
129. *Id.* ¶¶ 3–4, at 3, ¶¶ 3–4, at 9–12, ¶¶ 70–72, at 32.
130. *See id.* at 17–20.
131. *Id.* ¶¶ 36–40, at 17–18.

and relevant actors to analyze transaction patterns collaboratively without centralizing sensitive data in a single repository. These arrangements could also facilitate more continuous and iterative collaboration among regulators, law enforcement, blockchain analytics firms, infrastructure providers, and protocol developers as illicit activity evolves. By combining otherwise fragmented data and analytical perspectives, participants could identify connections, reconstruct transaction pathways, and detect broader patterns of illicit activity that remain invisible when each actor analyzes only its own portion of the financial ecosystem.

In sum, recalibrating global AML governance for distributed systems requires translating core insights from traditional international cooperation—standardization, informal agility, and joint analysis—into technologically mediated, infrastructure-aware governance models. These two adaptations address distinct but complementary dimensions of this challenge: data-layer interoperability creates the technical conditions for information to be standardized, shared, and observed across fragmented systems, while collective sensemaking enables authorities and other relevant actors to analyze that information jointly and reconstruct patterns that no single participant can see alone. Together, they shift cooperation from episodic exchanges among discrete institutions toward more continuous and technologically integrated forms of coordination and analysis.

CONCLUSION

FATF's AML framework was built for a world of intermediaries. Crypto is not that world. To effectively identify and disrupt the actors behind crypto-enabled illicit finance, AML governance must move beyond its traditional reliance on regulated gatekeepers and instead engage directly with the infrastructures through which value flows. An infrastructure-aware AML framework is therefore not optional; it is essential. Building such a framework requires more than incremental technological upgrades; rather, it demands a conceptual shift in how compliance is understood and operationalized, alongside coordinated legal and institutional adaptation, as outlined in this Essay.

Future research can deepen this agenda along several dimensions. First, it should further explore how technical architectures, such as digital identity and programmable compliance, can be integrated into regulatory design without undermining privacy and innovation. Second, future research should examine more deeply how global stakeholders can operationalize shared analytic infrastructures (such as jointly governed data layers, interoperable compliance nodes, or transnational investigative sandboxes) that enable not only real-time information exchange but also synchronized risk assessment, attribution, and coordinated intervention across jurisdictions. Third, it should further examine diverse models for operationalizing economic incentives that can mobilize stakeholders across the ecosystem to collectively combat money laundering, including mechanisms that align individual strategic behavior with system-wide compliance objectives. Together, these lines of

inquiry can help build a more resilient model of global AML governance for the crypto era.