Cahill

The DeFi Control Paradox: When Compliance Controls Increase the Risk of MSB Classification

September 25, 2026

EXECUTIVE SUMMARY

This article is the first in a series examining the growing tension between the expectations of anti-money laundering ("AML") and sanctions regulators and the evolving capabilities of decentralized finance ("DeFi") architecture. U.S. regulatory frameworks are built around identifiable actors, defined control, and accountable oversight. These frameworks are often difficult to apply to DeFi systems, which are typically built on non-custodial infrastructure, distributed governance, automated execution, and, in some cases, the deliberate absence of any formal intermediary. That mismatch is becoming more consequential as protocols, foundations, interfaces, and ecosystem participants face increasing pressure to adopt sanctions, AML, and illicit-finance controls. In July 2026, the Financial Action Task Force ("FATF") published a DeFi report that, for the first time at the international level, sets out a list of indicators of control over a DeFi arrangement, several of which are the very features that compliance stakeholders are asking DeFi projects and their development teams to adopt.

This article examines the resulting control paradox (the "DeFi Control Paradox"): measures intended to reduce illicit-finance risk — including screening, blocking, geofencing, pause powers, AI-enabled compliance tools, app-store distribution limits, and token-level transfer or freeze functionality — may also strengthen the argument that a DeFi project and its development teams are exercising intermediary-like control. In the U.S., that record can increase the risk that regulators characterize the actor as a money transmitter (and thus a money services business ("MSB")), potentially triggering registration, licensing, AML program, reporting, and personal-liability obligations that many DeFi project teams are neither structured nor resourced to meet. This article focuses on U.S. federal MSB risk, although similar control questions may arise under state money transmission laws and non-U.S. regulatory regimes.

THE PRESSURE TO ADD CONTROLS

DeFi project teams are increasingly being asked to do more. Banking partners want sanctions controls; institutional users want comfort that protocol access is not facilitating illicit finance; investors, wary of enforcement actions and reputational fallout, want visibility into where risk monitoring sits in the stack; and protocol communities want consistent, credible responses to hacks, exploits, sanctioned actors, stolen funds, and reputational crises.

That pressure can be traced to identifiable sources. Illicit-finance data give counterparties a reason to ask questions, and regulated institutions are increasingly being told not to deal with DeFi arrangements whose control structure, governance, and risk controls they cannot assess. FATF's July 2026 DeFi report states that financial institutions and virtual asset service providers ("VASPs") should refrain from interacting with DeFi arrangements where FATF Standards cannot be fulfilled,[1] while the U.S. Department of the Treasury has observed that application-layer participants and operators of relayers or remote procedure call nodes are already using risk-mitigation measures such as wallet risk-rating and transaction rejection.[2]

This pressure is mounting at a time when the capabilities of DeFi platforms are evolving such that enhanced control features are technologically possible. These advances have made way for improved screening tools, sanctions oracles, wallet-risk scoring, geofencing, pause powers, identity or eligibility credentials, transfer restrictions, and freeze functionality. All of these can serve legitimate risk-management objectives, but these control functionalities are not legally neutral switches that can simply be turned on or off. They present instead an array of institutional decisions as to how they are implemented, and create a record of doing so: who selected the control, who configured it, who updates it, who can override it, who receives alerts, who makes exceptions, who can pause or freeze, and who earns revenue from the activity the control permits.

At this point the DeFi Control Paradox begins to materialize. By voluntarily implementing controls to reduce AML, sanctions, banking, institutional, or reputational risk, participants in DeFi arrangements become more vulnerable to the argument that a protocol team, foundation, decentralized autonomous organization, issuer, administrator, or affiliated front end has moved beyond providing neutral infrastructure and is exercising intermediary-like control over the movement of value. By creating better compliance controls, they step away from the protection of hands-off DeFi neutrality and become quarry for regulators that may use these efforts to bring them within enforcement frameworks. Any party involved in setting up DeFi arrangements should therefore weigh each control for both its compliance value and its classification cost — the risk that the control leads to a relevant party being characterized as an intermediary. Because of the DeFi Control Paradox, participants in DeFi arrangements would be well advised to be disciplined and strategic when designing the relevant control environments.

---

[1] FATF, *Targeted Report on Regulatory Challenges from Decentralised Finance* ¶ 59 (July 2026) ("FATF DeFi Report"), https://www.fatf-gafi.org/en/publications/Virtualassets/targeted-report-decentralised-finance-2026.html. Paragraph references are to the main text, which is numbered separately from the executive summary.

[2] U.S. Dep't of the Treasury, *Report to Congress on Innovative Technologies to Counter Illicit Finance Involving Digital Assets* 31 (Mar. 2026), https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.

THE LEGAL BASELINE: INFRASTRUCTURE OR INTERMEDIARY?

Whether U.S. regulators will treat a given project as infrastructure or as an intermediary does not depend on whether the project calls itself decentralized. It depends on the facts and circumstances of how the project actually operates. The U.S. Bank Secrecy Act's ("BSA") functional money-transmission framework supplies the legal baseline for that inquiry,[3] and further guidance comes from the Financial Crimes Enforcement Network's ("FinCEN") 2013 and 2019 virtual-currency guidance[4] and Treasury's 2023 *Illicit Finance Risk Assessment of Decentralized Finance*.[5]

The position that a project serves as a neutral infrastructure is strongest when users control their own assets and transactions execute automatically under pre-programmed code. In that model, a team may write code, publish software, maintain documentation, or support ecosystem development, but it does not decide who may use the system, approve particular transactions, take custody of user assets, or intervene in transaction flow.

The characterization of a project as an intermediary becomes stronger as those facts change. A project begins to look less like neutral infrastructure and more like an intermediary when an affiliated actor can screen or block users, control a primary interface, route transactions, update deny lists, hold admin keys, pause contracts, freeze assets, approve transfers, or collect transaction-linked fees.

No single fact necessarily decides the analysis, although some controls — particularly those that allow a platform actor to block, pause, freeze, approve, or route transactions — may weigh more heavily than others. A pause function, screening tool, deny list, or transaction fee may each serve a legitimate platform-resilience or risk-management purpose, but as those features accumulate, they may make the project look less like software that users operate for themselves and more like a person or entity controlling access, intervening in transactions, and earning revenue from value movement. The question is not simply whether compliance controls exist, but whether they show that an identifiable actor is controlling access, making transaction-level decisions, or profiting from value movement.

THE CONTROL PARADOX

DeFi project teams are sometimes pushed to adopt heightened controls because of stakeholder expectations that they do more to mitigate illicit-finance risk. Depending on where those controls sit, who operates them, and how much discretion they involve, however, the same controls can make the team look more like the regulated intermediary the architecture was designed to avoid.

The chart below illustrates how certain controls, particularly when taken in combination with one another, can create a record of access control, intervention, and revenue tied to value movement that may shape how regulators characterize the project's role.

---

[3] 31 C.F.R. § 1010.100(ff)(5)(i)(A).
[4] *See* FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013); FinCEN, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019).
[5] U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* (Apr. 2023).

Compliance objective	Control adopted	Potential classification signal
Reduce sanctions risk	Wallet screening or blocking	Indication of control over access
Respond to exploits	Pause or emergency intervention powers	Indication of retained operational authority
Recover stolen assets	Freeze, burn, reissue, or forced-transfer functionality	Indication of post-issuance asset control
Satisfy bank or investor diligence	Case-management and escalation workflows	Indication of individualized review
Support institutional users	Permissioned access or identity-based eligibility	Indication of controlled participation
Fund operations	Transaction-linked fees	Indication of business activity tied to value movement
Scale compliance	AI compliance agents	Indication of delegated operational control if the agent can block, pause, freeze, or trigger intervention

Controls also leave evidentiary byproducts — screening logs, blocked-transaction records, risk-score thresholds, vendor configurations, exception notes, governance votes, admin-key transactions, and incident-response communications — that regulators can mine for indications of control. Increasingly, regulators are likely to look past decentralization labels where the operational record suggests that an identifiable actor controls access, intervenes in transactions, or profits from value movement. FATF has said as much, observing that "[a]rrangements that present themselves as truly decentralised for marketing purposes may nonetheless be centralised in practice."[6]

That does not mean DeFi project teams should avoid controls. In many cases, avoiding controls may create a different and equally damaging record — one of indifference, reckless disregard, or willful blindness. The goal, then, is disciplined control design: adopting controls with a clear-eyed understanding of both the risk they mitigate and the record they create.

FATF'S JULY 2026 DEFI REPORT: CONTROL INDICATORS BECOME THE INTERNATIONAL BASELINE

On July 21, 2026, FATF published its *Targeted Report on Regulatory Challenges from Decentralised Finance*.[7] The report is non-binding, but the FATF Standards are the benchmark against which member jurisdictions, including the United States, are evaluated, and the report is likely to shape both non-U.S. regimes and the diligence questions

[6] FATF DeFi Report, *supra* note 1, ¶ 7.
[7] FATF DeFi Report, *supra* note 1, ¶ 12 ("As with all FATF Targeted Reports, this guidance is non-binding.").

that banks and institutional counterparties put to DeFi projects and affiliated actors. Its significance for the DeFi Control Paradox is that it converts the "control or sufficient influence" test in FATF's 2021 guidance (under which "creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangement[s]" may be VASPs) into a list of indicators, many of which describe compliance features.[8]

The report sorts DeFi arrangements into three categories: centralized arrangements with identifiable controllers, arrangements in which control exists but controllers cannot be identified, and "truly decentralised" arrangements in which no person maintains control or sufficient influence.[9] It defines control as the ability to take key decisions within the DeFi arrangement[10] and identifies on-chain and off-chain indicators of control, including upgradeable contracts, kill-switch functions, fee-setting rights, oracle control, protocol-level fee flows, permissioned pools, whitelists, upgrade keys, multisignature signing roles, front ends, wallets, and legal entities that employ core contributors, hold intellectual property, or manage treasuries.[11] Read against the framework in this article, many controls that reduce illicit-finance risk also map directly onto FATF's indicators of control.

The report therefore restates the same paradox at the international level. It encourages truly decentralized arrangements to embed AML and controls countering the financing of terrorism, while also treating upgrade rights, parameter-setting authority, permissions administration, and appointments to key governance, operational, or administrative roles as indicators of control.[12] It distinguishes disclosed emergency functions from undisclosed or unilateral access rights, but does not provide a clear test for when a disclosed pause, freeze, or circuit-breaker power becomes an indicator of control.[13] The report also recommends that jurisdictions and competent authorities use documentation, points of contact, and engagement with persons who may exercise control or sufficient influence — including admin keyholders or multisignature signers — to assess control.[14] Those steps may improve accountability, but they also have an effect on the DeFi Control Paradox by creating the record regulators will use to identify who holds meaningful authority.

The report does not address AI-enabled compliance or expressly draw the rule-based versus discretionary distinction discussed below. It does, however, underscore the importance of documentation. Contemporaneous documentation of why a control exists, who holds it, how it is disclosed, and what constrains its exercise can support the U.S. classification position and help a project respond to the control-based inquiries FATF is encouraging member jurisdictions to undertake.

NEW TECHNOLOGY IS MOVING CONTROLS DEEPER INTO THE STACK

The DeFi Control Paradox is becoming more acute because newer tools allow controls to move deeper into the DeFi stack — from the interface to the protocol, from the protocol to the token, and from human governance to AI-enabled administration. Each new tool creates another potential point of control — another place where an identifiable actor may be seen as exercising authority over access, transactions, or asset movement.

---

[8] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* ¶ 67 (Oct. 2021).
[9] FATF DeFi Report, *supra* note 1, ¶ 7.
[10] *Id.* ¶ 34.
[11] *Id.* ¶ 37.
[12] *Id.* ¶¶ 37, 52, 62.
[13] *Id.* ¶¶ 37, 53.
[14] *Id.* at 45 (Recommendation 14); *id.* ¶ 69.

In the relatively short history of DeFi, compliance controls typically operated at user access points, such as through website terms of use, IP geofencing, app-store distribution restrictions on downloads from sanctioned jurisdictions, front-end blocking, or basic wallet screening. Those control measures still matter, but technological developments now allow compliance controls to move from the interface into the protocol or the token itself. Used narrowly, these tools may operate as objective, rule-based constraints; but used more expansively (such as when configurable by an affiliated team, updated through governance, or tied to exception workflows) they may become part of a broader access-control system.

Freeze functionality is perhaps the sharpest example of how newer tools allow for control over the asset itself, in addition to control over the interface. If the issuer or other owner or controller of a token smart contract retains the ability to freeze or restrict transfers, this functionality can prove useful in responding to hacks, sanctions designations, legal process, or stolen-asset recovery. That same power, however, also creates a significant control fact: an identifiable person — such as an issuer, or a party delegated authority by the issuer such as an administrator, foundation, governance body, multisignature wallet requiring approval from multiple keyholders, or agent — can control whether the asset can move. Where a DeFi project itself holds or shares that authority, the classification implications may be more direct; where the authority resides with an unrelated token issuer, the control fact belongs primarily to that issuer rather than to the protocol using the token.

For permitted payment stablecoin issuers, the choice has been made by statute. The Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025 (the "GENIUS Act") permits an issuer to issue payment stablecoins "only if the issuer has the technological capability to comply, and will comply, with the terms of any lawful order," defines a lawful order to include one that requires the issuer "to seize, freeze, burn, or prevent the transfer of payment stablecoins issued by the person," and requires "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations."[15] Those issuers are treated as financial institutions under the BSA in any event. For non-stablecoin issuers, however, the paradox remains: a team that builds comparable freeze functionality into a protocol or a non-stablecoin token is adopting a power that Congress has so far required only of a regulated issuer. Of course permitted payment stablecoin issuers are far from decentralized, but the assets they issue and can freeze are regularly used in DeFi protocols.

AI-enabled controls are a frontier technology that may raise the same issue. An AI compliance agent — an automated tool used to monitor, score, recommend, or execute compliance-related actions — may operate as a risk-intelligence tool: monitoring blockchain data, identifying sanctions exposure, detecting mixer proximity, flagging exploit-linked funds, or producing risk explanations for users, liquidity providers, interfaces, or governance participants. Used that way, the agent may be closer to analytics than administration. The same agent can, however, be given more authority. It may adjust thresholds, route flagged transactions to reviewers, block access to a front end, update a deny list, recommend or trigger an emergency pause, or invoke smart-contract functions. The legal significance depends on what authority has been delegated to the agent, who within the protocol ecosystem delegated that authority, and who can modify, revoke, or override it. Control over the agent and the surrounding orchestration layer may itself be an important control fact. The ability to set prompts or policies, define tool permissions, adjust thresholds, determine which actions the agent may execute, or modify the conditions under which human review is required may show that an identifiable actor retains practical authority

[15] GENIUS Act, Pub. L. No. 119-27, §§ 2(16), 4(a)(5)(A), 4(a)(5)(A)(iv), 4(a)(6)(B), 139 Stat. 419, 421, 425–26 (2025) (codified at 12 U.S.C. §§ 5901(16), 5903(a)(5)(A), (a)(5)(A)(iv), (a)(6)(B)).

over the compliance function. The fact that the decision-maker is artificial is likely to add very little insulation from regulatory scrutiny, as regulators are unlikely to treat automation as equivalent to decentralization. Delegating control to an AI-enabled system may reduce human discretion, but it may nevertheless preserve, or even strengthen, evidence that the protocol has an operational control layer, particularly where an identifiable actor defines the agent's objectives, permissions, tool access, or decision boundaries, or configures the agentic harness through which those constraints are implemented and enforced.

IMPLEMENTATION MATTERS: RULE-BASED VERSUS DISCRETIONARY CONTROLS

Regulator scrutiny and the determination of whether a platform serves as infrastructure or intermediary can be significantly affected by how a platform implements control, elevating the importance of being deliberate and thoughtful when designing and implementing a suite of control measures. A distinction that may have considerable bearing on whether a platform is viewed as infrastructure or as an intermediary is whether a point of control is rule-based or discretionary, although emerging technology is bound to make this distinction more complex.

Rule-based controls operate according to predefined criteria. For example, a fixed sanctions-list screening tool that returns an allow/deny result, without human override, exception review, or discretionary escalation, is closer to an architectural constraint and more infrastructural in nature. Such a tool may still contain some record of administrative control, however — for example, stemming from how a human actor selected and deployed the control. It nevertheless creates a much different record from a system in which an alert is routed to a human reviewer who decides whether a particular user may transact.

When implementing discretionary controls, platforms should be thoughtful about configuring controls to allow for features that require human judgment, such as case-by-case review, manual exceptions, mutable thresholds, selective blocking, individualized risk determinations, or governance and committee decisions about particular users, wallets, or transactions. Discretionary features such as these are often what make infrastructure look like intermediation. The emergence of AI-powered compliance agents and programs complicates the distinction further. An AI-enabled system may be described as automated, but if it adapts thresholds, weighs open-ended factors, decides borderline cases, or initiates enforcement actions, regulators could focus on how it functionally resembles discretionary review.

TORNADO CASH: HOW CONTROL CHOICES BECOME ENFORCEMENT FACTS

The *Tornado Cash* criminal prosecution does not supply a definitive MSB rule for DeFi activity, and its mixed procedural history counsels caution. Before trial, prosecutors withdrew the failure-to-register object of the unlicensed money-transmitting-business conspiracy count and proceeded only on the theory that the business transmitted funds known to be criminally derived under 18 U.S.C. § 1960(b)(1)(C) (a statute which defines the relevant offense by reference to the transmission of criminally derived funds rather than by reference to control), and on August 6, 2025, the jury convicted on that count but deadlocked on the money-laundering and sanctions-

conspiracy counts.[16] The conviction therefore rests on knowing transmission of criminal proceeds, and it says correspondingly little about registration or MSB status as such. The government has given notice that it intends to retry the two deadlocked counts; a motion for judgment of acquittal argued on April 9, 2026 remains pending, and the retrial has been adjourned to April 26, 2027.[17] The practical significance of the case here is narrower: it shows how control facts can become enforcement facts.

Prosecutors focused on what identifiable actors allegedly built, maintained, promoted, controlled, or failed to control — using those operational and compliance choices to tell a story about the actors' role. Whether the smart contracts executed autonomously received little attention. That is why *Tornado Cash* matters for the DeFi Control Paradox: prosecutors pointed to (i) the absence of an effective know-your-customer or AML program, (ii) an interface-level sanctions-screening tool, added the day after Treasury's Office of Foreign Assets Control designated an address linked to the Lazarus Group, that was alleged to be ineffective and easy to evade, and (iii) continued control over the user interface and the relayer registry, as evidence of an identifiable actor's operational role.[18] For DeFi projects and affiliated actors designing control measures and seeking to strike the right balance in the DeFi Control Paradox, the lesson of the *Tornado Cash* prosecution is that the record matters — what the team could do, what it chose to do, and what it chose not to do. That lesson does not counsel adopting the most aggressive controls available, nor does it render any retained control fatal. It shows instead that control design creates risk in more than one direction: adopting too few meaningful controls invites enforcement risk; retaining broad discretionary control invites classification risk; and adopting ineffective or cosmetic controls risks the worst of both worlds — evidence of knowledge without meaningful mitigation.

STRIKING A BALANCE IN THE DEFI CONTROL PARADOX

Teams seeking to preserve a non-intermediary posture but maintain a resilient platform that adequately meets stakeholder expectations are faced with the challenge of choosing their control measures deliberately, with a clear understanding of which compliance risks they mitigate and the corresponding risk of signaling a more intermediary structure. The chart below poses questions that platform teams may use as a guide when striking this balance, along with certain implementation and scoping considerations that tend to signal a greater or lesser resemblance to an intermediary framework, as opposed to neutral infrastructure.

[16] *See* Letter from U.S. Att'y's Office for the S. Dist. of N.Y. to Hon. Katherine Polk Failla, *United States* v. *Storm*, No. 23 Crim. 430 (S.D.N.Y. May 15, 2025), ECF No. 144 (stating that the government "will not proceed to trial on Title 18, United States Code, Section 1960(b)(1)(B), that is, the first object of the conspiracy charged in Count Two"); *see also* Press Release, U.S. Att'y's Office for the S. Dist. of N.Y., Founder of Tornado Cash Crypto Mixing Service Convicted of Knowingly Transmitting Criminal Proceeds (Aug. 6, 2025).

[17] Order, *United States* v. *Storm*, No. 23 Crim. 430 (S.D.N.Y. Aug. 25, 2026), ECF No. 300 (adjourning the retrial to April 26, 2027 in light of the pending motion for judgment of acquittal, ECF No. 229).

[18] *See* Indictment ¶¶ 14, 26, 29-30, 33–34, 60–68, *United States* v. *Storm*, No. 23 Crim. 430 (S.D.N.Y. filed under seal Aug. 21, 2023, unsealed Aug. 23, 2023).

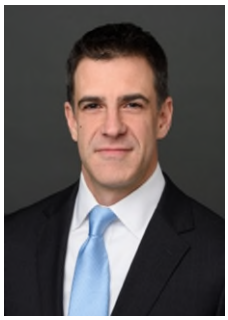
Design question	Lower classification signal	Higher classification signal
What risk is being addressed?	Tie the control measure to a specific sanctions, exploit, banking, or diligence risk	Adopt broad control measures without a defined risk or rationale
Where does the control sit?	User-side, distribution-layer, or interface-level where sufficient	Protocol-level, token-level, or administrator-level intervention
How does the control operate?	Fixed, objective, rule-based criteria	Case-by-case review, exceptions, or mutable thresholds
Who operates it?	Independent user, third party, or fixed automated process with no case-by-case override	Protocol team, affiliated front end, committee, or administrator
Can it affect asset movement?	Warning, disclosure, or limits on distribution or interface access	Blocking, pausing, freezing, burning, reissuing, or forced transfer
How is revenue earned?	Fixed software fee, licensing fee, or revenue unrelated to transaction flow	Transaction-linked fees tied to value movement
How is it documented?	Contemporaneous rationale and classification analysis	*Ad hoc* decisions, inconsistent messaging, or unexplained overrides
Is the power disclosed and constrained?	Published in protocol documentation, subject to a timelock, governance vote, or multi-party approval, with a defined scope and sunset	Undisclosed, unilateral, and immediately exercisable by an affiliated actor

The key for DeFi project teams is to select control measures that mitigate the relevant risk without unnecessarily feeding a narrative of intermediary status. Even once that balance is struck, platform teams should keep tailoring their control environment over time — through planned reviews and refreshes of controls, sunset provisions, and de-escalation measures. A control measure that is disclosed in the protocol's documentation, constrained by a timelock or a governance vote, and reviewed on a schedule reads differently, under both the U.S. framework and the FATF indicators, from one that an affiliated team can exercise unilaterally and without notice.

Within the DeFi Control Paradox, compliance architecture becomes classification architecture. Teams cannot eliminate that tradeoff, but they can recognize it, document it, and design for it. By approaching control design with the same rigor applied to any high-stakes regulatory interaction — and with the guidance of crypto-native legal counsel — DeFi projects and affiliated actors can convert what might otherwise be a source of legal exposure into a foundation for sustainable growth.

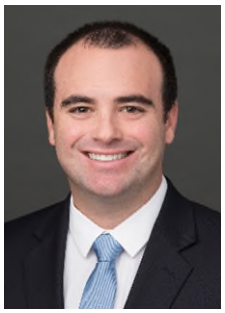
CONTACT

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to call or email authors Brockton B. Bosson (partner) at 212.701.3136 or bbosson@cahill.com, Jonathan Galea (partner) at 44.20.7947.9315 or jgalea@cahill.com, or Christopher Arkin (counsel) at 212.701.3986 or carkin@cahill.com; or email publications@cahill.com.



Brockton Bosson
Partner
212.701.3136
bbosson@cahill.com

Jonathan Galea
Partner
44.20.7947.9315
jgalea@cahill.com



Christopher Arkin
Counsel
212.701.3986
carkin@cahill.com