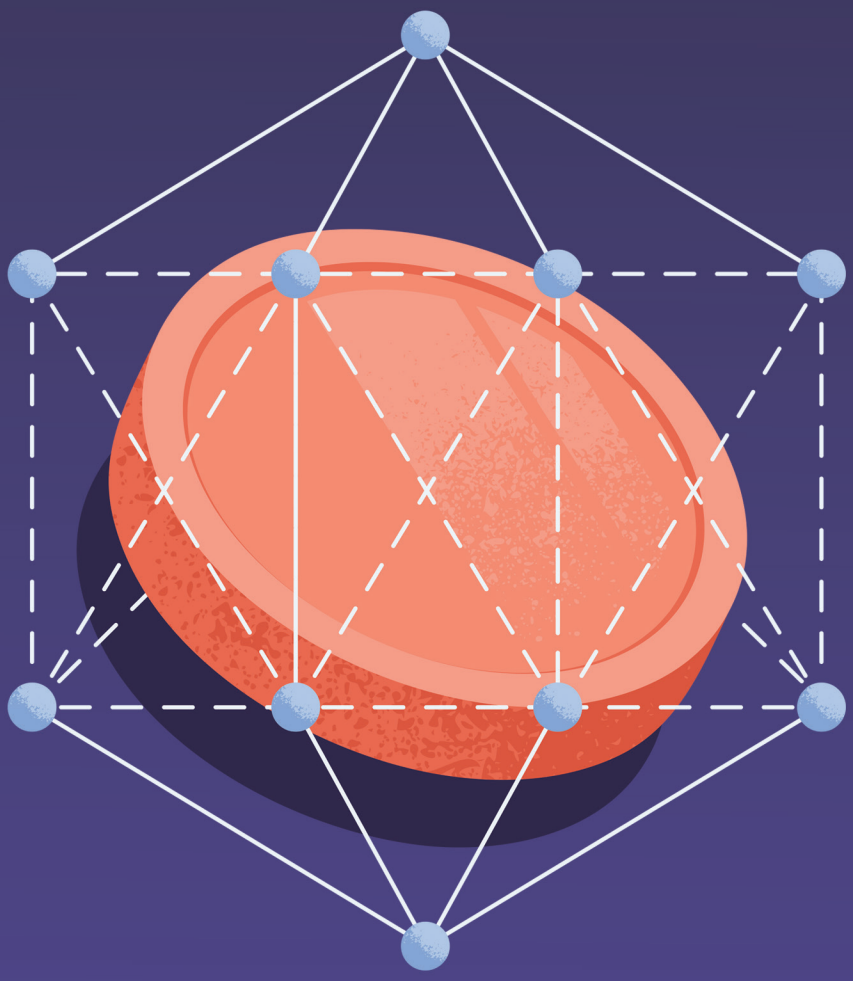
Centre for International
Governance Innovation

CIGI Paper No. 355 – May 2026

Regulating Compliance in a World of Decentralized Finance

Steven L. Schwarcz and Jack Tiedemann



Centre for International
Governance Innovation

CIGI Paper No. 355 — May 2026

Regulating Compliance in a World of Decentralized Finance

Steven L. Schwarcz and Jack Tiedemann

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

President, CIGI Paul Samson
Research Director, Digital Economy Odun Olowookere
Director, Programs Dianna English
Program Manager Grace Wright
Publications Editor Christine Robertson
Publications Editor Lynn Schellenberg
Graphic Designer Sami Chouhdary

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
cigionline.org

Table of Contents

About the Authors

Steven L. Schwarcz is a senior fellow of the Centre for International Governance Innovation, the Stanley A. Star Distinguished Professor of Law and Business at Duke University, and founding director of Duke's interdisciplinary Global Financial Markets Center. His areas of research and scholarship include insolvency and bankruptcy law, international finance, capital markets, systemic risk, corporate governance and commercial law. He holds a bachelor's degree in aerospace engineering (summa cum laude) and a juris doctor degree from Columbia Law School. Prior to joining Duke, he was a partner at two of the world's leading law firms, a visiting lecturer at Yale Law School and a lecturer in law at Columbia Law School. He has been a distinguished professor or fellow at numerous universities and an adviser to the United Nations. One of the world's most highly cited scholars in his fields, Steven is a fellow of the American College of Bankruptcy and the American College of Commercial Finance Lawyers, a founding member of the International Insolvency Institute, a former business law adviser to the American Bar Association and a member of P.R.I.M.E. Finance's Panel of Recognized International Market Experts in Finance.

Jack Tiedemann is a current third-year student, soon to graduate with a juris doctor degree, at Duke University School of Law. His studies and scholarship primarily focus on financial markets, bankruptcy and decentralized finance. He will be joining Sullivan & Cromwell's New York office in the fall of 2026.

Acronyms and Abbreviations

AML	anti-money laundering
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CCPs	central counterparties
CFT	countering the financing of terrorism
DeFi	decentralized finance
FATF	Financial Action Task Force
FSB	Financial Stability Board
IOSCO	International Organization of Securities Commissions
TradFi	traditional finance

Executive Summary

Decentralized finance (DeFi) promises cheaper, faster and more accessible financial services by replacing traditional regulated intermediaries with software protocols and smart contracts. But removing those intermediaries also removes the practical chokepoints for implementing modern financial regulation: customer identification and screening, disclosure, recordkeeping, operational safeguards and incident reporting. This paper argues that the core compliance challenge in DeFi is therefore a governance problem: regulators should focus less on DeFi's underlying computer code and more on the control points where compliance duties could realistically be assigned, supervised and enforced. Identifying those control points could be challenging, however, because DeFi responsibilities are dispersed across software developers, governance structures, parties that interface with investors and third-party service providers. To address that challenge, the paper proposes a layered regulatory strategy comprising four complementary approaches: identifying and regulating gateway intermediaries that facilitate access to DeFi services; prescribing the compliance obligations those intermediaries should assume; establishing targeted governance standards for smart contracts and the oracle and data inputs on which they depend; and applying shadow-banking-type safeguards to constrain spillover channels between DeFi and the traditional financial system. No single approach would be sufficient on its own; their combined effect would reconstruct, at workable control points, the most critical accountability and oversight functions that DeFi displaces. Properly designed and implemented, this strategy could help to preserve DeFi's efficiency benefits while cost-effectively restoring regulatory protection and accountability.

Introduction

Modern finance is a system of delegated trust. In traditional finance (TradFi), parties are able to routinely transact with strangers — across jurisdictions and time zones, and notwithstanding profound information asymmetries — because regulated intermediaries specialize in providing verification, enforcement and risk management (Nakamoto 2008, 1). Those services are not incidental; they are the institutional scaffolding that makes large-scale finance governable.

Consider three familiar functions. A wire transfer of funds is not merely "messaging": banks authenticate instructions, maintain account ledgers, screen for fraud and sanctions and settle through payment systems.[1] In commercial finance, issuers of letters of credit substitute institutional assurance for counterparty trust by requiring documentary conditions for payment.[2] And in securities markets, central counterparties (CCPs) manage counterparty exposure through margining, netting and centralized risk governance.[3] Institutional intermediaries charge fees for performing these valuable functions. Private parties cannot easily, cost-effectively or reliably reproduce these functions through bilateral contracting (Diamond 1984, 393–95, 401–7).

This paper focuses on DeFi, which seeks to provide financial services and products without traditional institutional intermediaries. Although the United States Department of the Treasury (2023, 1–2) notes that there is no single agreed definition of DeFi, the term generally refers to financial activity conducted on shared digital ledgers (blockchains) — distributed, cryptographically secured databases designed to record and verify transactions in a tamper-resistant way (Nakamoto 2008, 2–3) — or other computer-code-based systems that operate through preset rules or protocols. These protocols are often implemented through smart contracts, meaning computer code that automatically carries out specified actions when predefined conditions occur, without further human intervention (United States Department of the Treasury 2023, 1; International Organization of Securities Commissions [IOSCO] 2023, 4; Levi and Lipton 2018).

Advocates of DeFi emphasize its ability to reduce intermediation costs and speed up the execution of financial transactions. While cautioning against illicit-finance risks, the United States Department of the Treasury (2023, 12) likewise notes that DeFi transactions could speed settlement and reduce

1 See *Uniform Commercial Code* art 4A (2022) [UCC]; *Bank Secrecy Act*, 31 USC §§ 5311–5336.

2 See UCC, *supra* note 1, art 5.

3 See *Dodd-Frank Wall Street Reform and Consumer Protection Act*, Pub L No 111-203, § 725(a)(1), 124 Stat 1376, 1676 (2010) (codified at 7 USC § 2(h)(1)) [*Dodd-Frank Act*].

certain costs. However, lowering intermediation costs by bypassing financial intermediaries can shift financial activity away from traditional regulation, creating regulatory arbitrage: financial activity migrates from nodes, or points, where law traditionally attaches (banks, broker-dealers and CCPs) toward a protocol-based (that is, based on preset rules) environment that is harder to supervise in practice (Financial Stability Board [FSB] 2023, 1–3).

This paper argues that DeFi can be economically valuable, but its displacement of traditional institutional intermediaries can impair financial regulation, thereby reducing accountability and other legal protections. Regulators therefore should treat DeFi as a governance problem and examine how to reconstruct core compliance functions, such as screening, monitoring, disclosure and operational controls, at workable control points that remain visible to supervisors (United States Department of the Treasury 2023, 1–3; FSB 2023, 1–3, 2024, 1–2).

The paper first maps DeFi's principal risk channels to three system-protective objectives that pervade modern financial regulation: monetary integrity and national security; market integrity and customer/investor protection; and macroprudential stability — that is, stability of the financial system. It then evaluates four regulatory approaches aimed at restoring attribution, integrity controls and macroprudential intervention capacity while preserving DeFi's efficiency gains: regulating functional controllers ("second-best" intermediaries), requiring supervised gateways for economically significant access, regulating smart contracts and their data dependencies, and applying shadow-banking-style constraints as interconnections grow. Finally, the paper addresses the cross-border coordination problem that DeFi intensifies.

Non-Compliance Risks of DeFi

DeFi is attractive in significant part because it can reduce transaction costs associated with traditional intermediary-based finance. By replacing regulated intermediaries with code-mandated execution, DeFi can offer faster settlement, broader access and lower explicit fees (United States Department of the Treasury 2023, 12). In TradFi, however, many of the "costs" of intermediation arise from governance functions through which law protects the system — screening and monitoring, documentation, operational controls and risk management — that are difficult to reproduce reliably or cost-effectively at scale through bilateral contracting (Nakamoto 2008, 1). When activity migrates away from intermediaries, regulators can lose practical points of supervision and enforcement, and those governance functions may be performed incompletely or not at all (Born et al. 2022; United States Department of the Treasury 2023, 1–3).

Those governance functions track three familiar public objectives. First, monetary integrity and national security: laws on anti-money laundering (AML) and countering the financing of terrorism (CFT) impose customer due diligence, monitoring and reporting duties on the intermediaries (Financial Action Task Force [FATF] 2025).[4] Second, market integrity and customer/investor protection: federal securities and commodities laws reduce fraud and manipulation, and protect customers through registration, disclosure, custody safeguards and market surveillance; among other things, these tools presuppose identifiable intermediaries.[5] Third, macroprudential stability: post-2008 financial-crisis prudential and market-infrastructure regulation seeks to dampen bank runs and reduces fire sales and financial contagion by constraining leverage and liquidity mismatches and by imposing resilience and liquidity requirements on banks and other systemically important financial institutions and infrastructures (Basel Committee on Banking Supervision [BCBS] 2011).[6]

DeFi strains each of these objectives through two linked mechanisms: attribution failure and automated procyclicality. Attribution failure is the practical inability to identify a responsible party (an obligated intermediary, a venue operator or a controller) against whom legal duties can attach and be enforced. Pseudonymity — using fictitious names to hide the user's legal identity — is central to this problem: DeFi activity often runs through wallet addresses — fictitious public identifiers

4 See *Bank Secrecy Act*, *supra* note 1, and implementing regulations.

5 See *Securities Act of 1933*, 15 USC §§ 77a–77aa [*Securities Act*]; *Securities Exchange Act of 1934*, 15 USC §§ 78a–78qq [*Securities Exchange Act*]; *Commodity Exchange Act*, 7 USC §§ 1–27f.

6 See *Dodd-Frank Act*, *supra* note 3.

used to send and receive crypto-assets (United States Department of the Treasury 2023, 33–34). Responsibility is also dispersed across multiple control layers (for example, developers who can upgrade code, governance participants who can change parameters, and interface operators and third-party service providers), leaving no single actor with obvious end-to-end accountability (ibid., 12–14; FATF 2021, 67). As a result, regulators may not know, for example, whom to obligate to conduct AML/CFT screening or to hold accountable for breaches — an especially acute problem because existing compliance regimes typically presuppose an identifiable "obligated entity" (United States Department of the Treasury 2023, 1–3; Born et al. 2022; FATF 2025).

The United States Department of the Treasury (2023, 1) emphasizes that the most significant illicit-finance risk in DeFi is not necessarily the technology itself but "a lack of implementation of [AML/CFT]…controls by DeFi services," including by actors who may already have obligations under existing law. It also notes that DeFi's attribution failure is not necessarily absolute; depending on how a DeFi activity is structured, there may be an identifiable controlling organization and actors who can implement (though they might try to evade) compliance. That observation also explains why cross-border implementation gaps matter: the AML/CFT regime is only as strong as its weakest link, and if some jurisdictions (or service providers operating therefrom) do not implement baseline controls, illicit actors can route activity through those channels to reduce detection and frustrate cooperation and enforcement (FATF 2021). Attribution failure can likewise undermine market integrity and investor/customer protection. (References hereinafter to investors will include customers and any other parties paying for DeFi goods or services.) When investors cannot identify responsible parties, fraud is easier to commit, disputes are harder to resolve and losses are harder to recover even when legal rights exist in theory (Born et al. 2022; United States Department of the Treasury 2023, 1–3). The IOSCO (2023, 4) emphasizes that DeFi arrangements commonly involve multiple actors and technical dependencies, making the allocation of responsibility central to market integrity and investor-protection analysis. In practical terms, DeFi does not necessarily eliminate control; it can relocate it. Functions that are exercised through visible, regulated intermediaries in TradFi may instead be exercised through less visible "control levers" embedded in code, governance processes or data dependencies — for example, permissions to modify or replace deployed code, authority to change economically significant parameters (such as collateral requirements, fees or liquidation thresholds), or influence over critical inputs (especially price feeds) on which smart contracts rely (United States Department of the Treasury 2023, 12–14). When these levers sit with developers, governance insiders, interface operators or data providers rather than with supervised intermediaries, investors may not appreciate who can upgrade or correct code, change risk parameters or pause the execution of smart contracts (see below) — precisely the information that matters most during financial stress (ibid., 4).

Automated procyclicality is the second mechanism that strains the aforesaid public objectives. Smart contracts drive this procyclicality by automatically executing specified actions when predefined conditions occur. Among other concerns, this can convert individually rational behaviour into correlated stress events.

DeFi lending illustrates this risk. DeFi lending platforms typically rely on collateral and encode liquidation rules that trigger when collateral values fall. The Bank for International Settlements (BIS) explains that DeFi platforms cannot normally gather borrower information the way banks do and therefore rely heavily on collateral rather than underwriting borrower creditworthiness in making lending decisions (Aramonte et al. 2022, 2). As a result, a sharp drop in the price of a common collateral asset can concurrently put multiple loans into default, triggering forced selling of the collateral — which pushes prices down further and induces additional liquidations (ibid., 2–3; FSB 2023, 1–3). As DeFi lending grows in volume and interconnections with regulated institutions deepen, these dynamics can become a fire-sale channel with spillovers into broader banking and financial markets (FSB 2023, 1–3).

In the DeFi context, procyclicality is reinforced because smart contracts are often linked: contract A may trigger liquidation and thereby affect contract B, which in turn affects contract C, and so on (United States Department of the Treasury 2023, 11; Duley et al. 2023, 2). Oracles and other shared data inputs are a key conduit. Smart contracts cannot directly observe market prices, interest rates or other real-world facts on their own; instead, they typically rely on third-party "oracle" mechanisms

that collect external (outside the blockchain) price data and feed it into the contract (FSB 2024, 18–20). If an oracle input deviates from the asset's true market value, the contract may liquidate not only mechanically but also on a false premise (ibid., 19–20). The risk can compound because many DeFi services reuse the same oracle or price feed. If a distorted price is published — whether through thin markets, data failures or manipulation — multiple smart contracts may liquidate simultaneously, producing correlated liquidations and spillovers across linked services (United States Department of the Treasury 2023, 11; Deng et al. 2024, 2, 10; Duley et al. 2023, 2, 5). Authorities have warned that this is also a broader concentration and correlation channel: reliance on a small number of shared third-party providers (including data and model vendors) can create common-mode failures and synchronized responses under stress (FSB 2024, 18–20, 24; IOSCO 2025, 40–41). Oracle and data-input dependency is therefore a vulnerability that is relevant to each of the regulatory approaches discussed below, not only to direct smart-contract regulation.

The risk of procyclicality is magnified by DeFi's informational architecture. In TradFi, many economically important terms are centralized and legible: set out in contracts, rulebooks, disclosures and supervised books and records. In DeFi, by contrast, those terms are often embedded in layers of computer code and settings: the deployed smart-contract logic, the parameters that govern how smart contracts respond to price inputs, and the governance mechanisms that can update the code or change the settings (United States Department of the Treasury 2023, 12–14; IOSCO 2023, 15–16, 27). Even though much of this information is public in a technical sense, it can be difficult for non-specialists to locate, interpret and verify, creating a correlated information asymmetry when seemingly standalone smart contracts are linked to one another by virtue of using the same inputs (BIS Innovation Hub 2023, 3, 5–6; United States Department of the Treasury 2023, 11–12). To address this difficulty, market participants increasingly rely on interpretive tools, including AI-enabled systems, to translate technical information into economic understandings that can enable risk and compliance judgments (IOSCO 2023, 39–40, 56; FSB 2024, 18–20; IOSCO 2025, 40–41). That reliance, however, can inadvertently concentrate risk if widely used AI or other tools yield false or misleading interpretations that propagate across the market (FSB 2024, 18–20, 24; IOSCO 2025, 40–41).

In summary, DeFi provides a useful, less expensive alternative to intermediary-based TradFi, but the absence of regulated intermediaries and the automatic execution of smart contracts can impose public costs. The paper next examines how regulation could help to mitigate those costs while attempting to respect DeFi's benefits.

Analyzing Possible Regulatory Approaches

The discussion has framed DeFi's compliance challenges as institutional problems: DeFi can remove or obscure intermediaries as points of regulatory accountability and as decision makers to monitor and control the execution of smart contracts. The paper next treats DeFi regulation as somewhat of an engineering problem — how to rebuild points of regulatory accountability and responsible decision making, thereby enabling meaningful government supervision even when DeFi transactions settle on computerized networks (United States Department of the Treasury 2023, 1–3; FSB 2023, 1–3). Because smart contracts execute automatically once programmed conditions are met, the paper later evaluates each regulatory approach not only as an identity-and-controls framework but also as a way to add credible oversight — and, when necessary, limited emergency brakes — around automatic actions that could otherwise amplify stress.

This paper's analysis takes into account, and is partly informed by, efforts already under way for regulating crypto-assets. Several jurisdictions have begun to regulate the access points through which DeFi connects to the traditional financial system. In the United States, the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), signed into law in July 2025, established a framework for payment stablecoins and directed the United States Department of the Treasury (2026, 1–3) to assess innovative tools for detecting illicit finance involving digital assets. The department's resulting March 2026 report to Congress highlights digital identity tools — including verifiable credentials and privacy-preserving mechanisms — as a potentially valuable compliance infrastructure for regulated institutions and digital asset service providers (ibid.,

22–24). The European Union's Markets in Crypto-Assets Regulation likewise imposes authorization and conduct requirements on crypto-asset service providers.[7] These emerging approaches might apply to DeFi by connecting intermediary-based regulation to smart-contract governance and macroprudential safeguards. Taken together, the four approaches discussed below could form such a framework.

Intermediary identification and gateway regulation (the first two approaches) would establish who should be accountable and what compliance duties should attach. Smart-contract governance (the third approach) would address risks inherent in automated execution — procyclicality, oracle failure and the absence of discretionary judgment — that persist even when intermediaries are supervised. Shadow-banking-type protections (the fourth approach) would constrain the channels through which DeFi stress can spill into the broader financial system. No single layer would be sufficient on its own; their combined effect, however, would be to reconstruct, at workable control points, the core regulatory functions that disintermediation displaces.

To the extent that DeFi's cost advantages over TradFi partly reflect regulatory avoidance rather than genuine efficiency, that advantage alone would not justify continued regulatory forbearance; the public objectives served by financial regulation, including macroprudential stability and the prevention of illicit finance, would apply regardless of the technology used to deliver financial services. At the same time, if DeFi's efficiency benefits are genuine — faster settlement, broader access and lower explicit fees — any regulation should be proportionate and designed to try to preserve those benefits. The objective of regulatory policy should be to maximize competition and efficiency subject to prudential constraints, not to insulate incumbents from disruptive entry (United States Department of the Treasury 2023, 12; FSB 2023, 1–3).

Identifying and Regulating Second-Best Intermediaries

One approach would be to regulate the people and firms that, as a practical matter, enable and control DeFi activities. The United States Department of the Treasury (2023, 2) emphasizes that DeFi services often are not meaningfully ownerless; many retain a controlling organization or centralized governance features notwithstanding the decentralization rhetoric. The IOSCO (2023, 4) likewise explains that DeFi arrangements typically involve multiple actors and dependencies, making responsibility allocation — including the identification of accountable persons — feasible.

Because DeFi's defining compliance challenge is the lack of an accountable intermediary, a practical starting point is to require or encourage institutional intermediation at key access points. In essence, regulators would focus on a limited set of supervised "gateways" that provide a jurisdictional and operational nexus, including custodians or wallet providers that effectively hold or control customer assets; stablecoin issuers and other entities that can control minting, redemption or transfer restrictions; bridge operators that route assets across chains (that is, cross-chain bridges that lock assets on one blockchain and issue corresponding representations on another) (FSB 2023, 20); and investor-facing interfaces that facilitate user access to protocols (United States Department of the Treasury 2023, 2; IOSCO 2023, 4).

More generally, if institutional intermediaries are reintroduced as gateways for DeFi access, they should be required to implement core compliance functions — customer identification and screening, recordkeeping, reporting and investor due diligence — under applicable AML/CFT and financial-stability frameworks (FATF 2025, 2021; United States Department of the Treasury 2023, 1–3). They should also be expected to screen against sanctions lists, an area the United States Department of the Treasury (2023, 6–7) flags as a central deficiency in current DeFi practice. Those requirements would align DeFi more closely with the market's existing governance architecture, without attempting to impose bank-like obligations directly on permissionless code (IOSCO 2023, 4).

That pairing would mirror the basic architecture of US public-company regulation: periodic disclosure is not merely informational but is backed by enforcement tools that make noncompliance

7 EC, *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937*, [2023] OJ, L 150/40, arts 59–72, online: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>.

costly. For example, certain contracts that are made or performed in violation of federal securities law may be unenforceable.[8] Similarly, regulation could condition the enforceability of smart contracts on compliance, creating concrete commercial consequences that could supplement after-the-fact penalties.

Requiring Institutional Intermediation

Identifying gateway intermediaries and prescribing their compliance obligations are two components of a single regulatory strategy: the first establishing who should be accountable, and the second specifying what that accountability should require in practice. They are presented separately in this subsection and the one immediately preceding it for analytical clarity, but they function as an integrated framework — neither is effective without the other. Under the second prong of this two-layered approach, institutional gateway intermediaries (described above) would be required to provide core compliance functions that permissionless systems may not supply on their own (FATF 2025, 2021; United States Department of the Treasury 2023, 1–3). These intermediaries should identify customers, implement AML/CFT screening and sanctions controls, maintain records, and report significant operational incidents to supervisors (United States Department of the Treasury 2023, 6–7; FSB 2021, 3). They also should provide plain-language governance disclosure (including what external data inputs the system relies on) and make clear which parties control upgrades, parameter changes and emergency halts. And where an intermediary effectively holds customer assets (or controls private keys on the customer's behalf), it should follow custody and safeguarding practices familiar from TradFi, including asset segregation, operational resilience and complaint-handling procedures (IOSCO 2023, 37–38).

In practice, requiring institutional intermediation would target the practical access points through which most investors interact with DeFi — namely, investor-facing websites and apps and the venues where crypto-assets are exchanged. That strategy assumes an economically meaningful limited number of such access points and available evidence supports the premise. For example, in an Organisation for Economic Co-operation and Development sample of Uniswap v3 liquidity pools, the top quintile accounted for more than 90 percent of observed trading volume (Nassr, Kostika and Melachrinos 2024, 15). The United States Department of the Treasury (2023, 15) likewise notes that DeFi activity is concentrated and therefore may be susceptible to supervision through gateways. This kind of concentration matters for compliance design because regulators need not "solve" every corner of DeFi to reduce risk meaningfully. This paper therefore emphasizes access-point regulation rather than attempting to regulate the underlying public blockchain ledger itself, as discussed below.

Regulating Smart Contracts Directly

The preceding approaches address who should be regulated and what obligations should attach. This subsection addresses a distinct set of risks (automated procyclicality, oracle vulnerability and the absence of human judgment in execution) that inhere in the smart-contract code itself and that persist even when intermediaries are identified and supervised. Regulating DeFi by monitoring smart contracts and transactions directly on chain is sometimes framed as an alternative to intermediary-based regulation. Public blockchains record transfers and contract interactions in a transparent time-stamped ledger, which can support surveillance and *ex post* analysis (Yaga et al. 2018, 13, 33; United States Department of the Treasury 2023, 9). That visibility could, in principle, be paired with disclosure requirements that make protocol risk mechanics legible — for example, who can change code or parameters, what data inputs a contract relies on, and how liquidation or pause functions are triggered — thereby reducing information asymmetry and improving monitoring (United States Department of the Treasury 2023, 12–14; IOSCO 2023, 4). Yet on-chain transparency does little, by itself, to solve attribution and enforcement: the ledger identifies addresses and contract calls, not accountable legal persons, and wallet addresses are often pseudonymous (United States Department of the Treasury 2023, 32–33).

Accordingly, a workable smart-contract regulatory strategy typically attaches to identifiable off-chain access points where identity, control or convertibility concentrates. These include entities that hold or manage users' private keys and execute transactions on their behalf (custodians or hosted-

8 See *Securities Exchange Act, supra* note 5, § 29(b), 15 USC § 78cc(b); § 13(a), 15 USC § 78m(a).

wallet providers), issuers of widely used fiat-pegged tokens that control minting and redemption into bank money (stablecoin issuers), businesses that convert between bank deposits and crypto-assets (fiat on- and off-ramps), and user-facing web or app front ends that route users into protocols (interface operators) (United States Department of the Treasury 2023, 32–33; FATF 2025, 2021, 67; World Economic Forum 2023, 10). These access points are natural regulatory anchors because they can identify customers, set the terms of access and implement compliance and risk controls that are difficult to impose on pseudonymous addresses alone — including conditioning use on disclosure, restricting interactions with particular contracts and requiring safeguards where protocols embed high-speed liquidation triggers. The March 2026 report to Congress issued by the United States Department of the Treasury (2026, 22–24) explains that emerging digital identity tools — such as verifiable credentials and privacy-preserving verification mechanisms — may further reduce the cost and friction of meeting attribution requirements at these access points.

The value of smart-contract regulation can be illustrated through the example of liquidation-driven stress. Smart contracts execute automatically as programmed when their initial conditions are satisfied (Ethereum Foundation 2026). In DeFi lending, a smart contract will automatically liquidate posted collateral once it falls below a preset threshold — often expressed as a collateral-to-debt (or loan-to-value) ratio — because the contract is programmed to protect lenders through prompt seizure and sale rather than discretionary workout. Sirio Aramonte and his co-authors (2022, 3–4) describe how these "liquidation ratio" triggers permit third-party liquidation once collateral depreciates below a specified level. That design departs from supervised lending's basic prudential intuition that repayment should come first from the borrower's cash flow, with asset liquidation treated as a secondary, value-destructive backstop — what bankers sometimes describe as "two ways out" (Office of the Comptroller of the Currency 2025, 9; Schwarcz 2023, 970 n. 11). A purely ratio-based trigger can therefore force liquidation even where the borrower's ongoing cash flow would rationally support continued performance, triggering potentially imprudent and value-destructive liquidations.

This risk of imprudent liquidation is further complicated by how collateral is priced in smart contracts. Smart contracts cannot directly "see" market prices; they typically rely on oracles, or mechanisms that supply price data from designated sources in a form the contract can use (Deng et al. 2024, 3–4). However, an oracle can be "wrong" in the same basic ways any market-data feed can be wrong: it can be stale (updating too slowly in a fast-moving market); unrepresentative (drawing from a thin or dislocated venue so that a small trade or brief spike looks like a real clearing level); or corrupted (because the reference market is manipulated or the data are distorted in transmission) (ibid., 4–5). A TradFi analogue is a margining or liquidation system that triggers automatically off a single reference quote that is delayed, taken from an illiquid venue or briefly "off market": the mechanism can operate exactly as designed while acting on a bad input. If the oracle input deviates from the asset's true market value, the contract may liquidate not only mechanically but also on a false premise.

The Bank of Canada finds that the "out-of-the-box" risk settings in several major smart-contract lending protocols — in other words, the standard configuration choices that determine when liquidations trigger and how the system responds when oracle prices move — often do not adequately protect against meaningful oracle errors. Xun Deng et al. (2024, 10) note that oracle deviations can cause protocols to violate basic safety constraints at least temporarily, such as over-collateralization. They also caution that some commonly proposed quick fixes, including adding delays to price updates, may be "insufficient or even detrimental" because they can increase the gap between the posted price and the market price in fast-moving conditions (ibid., 11, 18).

Smart-contract liquidations thus can become systemic: forced sales push prices down, which triggers more liquidations across correlated collateral and interconnected protocols, producing liquidation cascades. Such cascades can be triggered or amplified by incorrect oracle valuations, creating negative feedback loops in which price-impactful liquidations mechanically beget further liquidations (Lehar and Parlour 2022, 8–9; Aramonte et al. 2022, 4–5).

The regulatory response should therefore be framed in macroprudential terms: *ex ante* safeguards to reduce the probability of liquidation cascades, paired with *ex post* stabilizers to limit cascade dynamics when *ex ante* safeguards fail. *Ex ante* safeguards could focus on the integrity of oracles and price inputs. Smart contracts should clearly

specify which oracles they may use and which reference markets those oracles can draw from, and those design choices should be disclosed in clear, concise and non-technical terms so that users can understand how price reliability depends on reference-market quality (IOSCO 2023, 40). Smart contracts also could require information redundancy: more than one market price source or a defensible aggregation method, so that no single information source can unilaterally trigger liquidation. Furthermore, smart contracts could be programmed to require "sanity checks" that reject stale, discontinuous or clearly implausible prices as determined by the protocol's design assumptions; evidence suggests that oracle deviations can defeat over-collateralization protections and that common mitigations can be inadequate (Deng et al. 2024, 10–11).

Ex ante safeguards could reduce, but not eliminate, the imprudent execution of smart contracts, particularly in fast-moving markets or during deliberate attacks. Accordingly, regulation should also contemplate *ex post* "emergency brakes" aimed at slowing liquidation cascades once stress conditions are detected. On the compliance side, such an emergency freeze may resemble mechanisms already used in traditional markets to dampen panic dynamics. TradFi uses "circuit breakers" that pause trading and allow the system to absorb information when markets become disorderly (New York Stock Exchange 2026, 1–2). DeFi protocols could be designed to implement a functionally similar response by temporarily suspending specified executions (including liquidations) or withdrawals when predefined stress triggers are met, for example, where oracle-reported volatility breaches a threshold, thereby creating a window for investors to post additional collateral, repay loans or exit through more orderly channels rather than through a liquidation cascade (ibid., 1–2).

A framework that pairs *ex ante* safeguards with *ex post* "emergency brakes" requires monitorability. Regulators must be able to determine on a continuing basis which smart-contract code a covered DeFi service in fact uses, and whether that code (or its risk settings) has changed. Therefore, a robust regulatory framework should impose a modest inventory and audit trail: a covered intermediary should maintain an up-to-date public list of the contracts it relies on, together with a basic change log and incident record, sufficient for supervisors to verify that the service is operating through compliant code and controls (BIS Innovation Hub 2023). Initiatives such as Project Atlas, which fuses on-chain and off-chain data to support central bank analysis of crypto-asset flows, illustrate the kind of supervisory infrastructure that could support such monitorability. To be clear, this paper does not propose that regulators audit every deployed smart contract; the multiplicity and complexity of such contracts would make comprehensive review impracticable. The approach should instead be targeted: it should focus on the highest-risk features of smart contracts (liquidation triggers, oracle dependencies and emergency-halt mechanisms) that are used by or through regulated intermediaries, rather than attempting to police the entire on-chain ecosystem.

The framework must also anticipate evasion. If an intermediary can frustrate oversight by splitting a product across nominally separate contracts, interfaces or labels — or by routing activity through undisclosed modules — then conditioning intermediated access will predictably underreach. Regulators should therefore define the regulated intermediary functionally, treating integrated components as a single product for disclosure and accountability purposes, and should attach meaningful consequences to nondisclosure.

Applying Shadow-Banking-Type Protections

"Shadow banking" refers to non-bank credit intermediation, typically provided by hedge funds, private equity/credit funds or money market funds. The problem is that shadow banking can create bank-like vulnerabilities, including leverage, liquidity mismatch and runnable structures, outside the traditional regulated banking sector (Pozsar et al. 2012, 1–3). In the run-up to the 2008 financial crisis, significant non-bank credit intermediation contributed to runs and forced asset sales, which amplified losses and transmitted stress back into financial markets and institutions (ibid.). Regulators responded by (among other things) restricting bank connections to non-bank risk and imposing stronger liquidity and redemption controls on systemically important non-banks (BCBS 2011; Securities and Exchange Commission 2014).

Although it differs from shadow banking, DeFi can replicate certain shadow-banking risks, especially as DeFi and TradFi activities become more connected (FSB 2023, 1–3). Like shadow banks, DeFi platforms can engage in maturity and liquidity

transformation, facilitate leverage and create structures from which participants can withdraw rapidly — but without the capital buffers, liquidity backstops or supervisory oversight that post-crisis reforms imposed on their non-bank counterparts (Pozsar et al. 2012, 1–3; FSB 2023, 7–9). The parallel is particularly consequential as interconnections deepen: when regulated institutions hold DeFi-related assets, provide funding to DeFi participants or rely on DeFi platforms for settlement or yield, stress originating on chain can transmit into the banking system through the same exposure and funding channels that shadow banking exploited before 2008 (FSB 2023, 1–3; Aramonte et al. 2022, 4–5). Because those transmission channels are familiar, so too is the regulatory logic: vulnerabilities outside the regulatory perimeter (shadow banking and DeFi) become systemic once they are connected to institutions inside it (TradFi).

At least two shadow-banking lessons can inform DeFi regulation. First, regulators should treat bank and market-infrastructure interconnections as potential spillover channels. Shadow-banking reforms reduced the ability of non-banks to externalize risk onto banks, such as restricting consolidated exposures involving bank backstops and funding links that can pull "non-bank" losses into the banking sector (Pozsar et al. 2012, 1–3). Similarly, regulators might wish to consider limiting banking exposure to DeFi-related assets (BCBS 2011).

Another shadow-banking lesson that regulators might consider is restricting liquidity mismatches and runnable structures (Pozsar et al. 2012, 1–3). Money market fund reforms are a possible template: US and EU rules now impose liquidity buffers and other tools to slow redemptions and reduce fire-sale pressure.[9] If, for example, regulators require supervised institutional intermediation of DeFi activities, they may wish to also consider imposing capital and liquidity requirements on those intermediaries (FSB 2023, 1–3).

Cross-Border Coordination and Jurisdiction

Identifying Cross-Border Complications

DeFi intensifies a perennial question in regulating cross-border financing: Which government is, or should be, responsible for regulating a given transaction? DeFi's decentralization disperses the usual territorial signals that help to allocate authority. DeFi developers may be in one jurisdiction, governance token holders and customers dispersed globally, investor interfaces hosted elsewhere, and smart-contract execution occurring in a computerized network without any clear geographic centre (IOSCO 2023, 4; FSB 2023, 1–3).

Cross-border inconsistency invites regulatory arbitrage. If some jurisdictions treat key DeFi actors as outside their regulatory perimeter, illicit finance and high-risk activities will tend to migrate to those jurisdictions, eroding regulatory effectiveness (FATF 2021). Jurisdictional fragmentation can also impair regulation by fostering inconsistent reporting, making it harder for supervisors to observe common exposures, and delaying or obscuring responses to shared stress events, which can allow automated liquidations to cascade through interconnected markets (FSB 2023, 1–3).

Resolving Cross-Border Complications

Cross-border regulatory jurisdiction should follow function: DeFi regulation should apply to oracles and other identifiable actors who control interfaces, hold administrative keys or upgrade authority, or that control key data feeds, rather than to the fiction of locating "the protocol" territorially (United States Department of the Treasury 2023, 2; IOSCO 2023, 45). Once these actors are identified, supervisory cooperation can proceed through familiar regulatory tools, including information sharing, coordinated examinations, joint investigations and parallel enforcement actions (FATF 2025, 2021).

Requiring supervised gateway intermediaries could further reduce jurisdictional uncertainty by

9 See *Money Market Fund Reform; Amendments to Form PF*, 79 Fed Reg 47736 (2014); EC, *Regulation (EU) 2017/1131 of the European Parliament and of the Council of 14 June 2017 on money market funds*, [2017] OJ, L 169/8, online: <https://eur-lex.europa.eu/eli/reg/2017/1131/oj/eng>.

supplying a clear regulatory nexus. Home-country supervisors could impose baseline integrity controls and reporting, while other jurisdictions could condition access to local customers on equivalence or mutual recognition frameworks (FATF 2025, 2021). More generally, nations should seek to impose minimum common standards for smart-contract protocols, code-and-data governance and inputs, and auditing and disclosure of DeFi activities. The logic tracks familiar efforts at international regulatory convergence in banking: shared baselines are meant to strengthen the soundness and stability of cross-border finance and to ensure that minimum standards are applied consistently across countries, thereby diminishing competitive inequality (BCBS 1988, para. 3). Post-crisis Basel III reforms likewise emphasize common global capital and liquidity rules as a floor for resilience (BCBS 2011, para. 1). In DeFi, a comparable floor would reduce incentives to jurisdiction-shop and improve interoperability if stress propagates across DeFi platforms (IOSCO 2023, 4; FSB 2023, 1–3).

Conclusion

DeFi's promise is straightforward: by replacing financial intermediary functions with oracle-inputted data and code-mediated execution, DeFi can lower costs and widen access to finance. But that same disintermediation can displace the compliance and stability functions that make modern finance governable.

An appropriate regulatory regime should therefore strive to preserve DeFi's benefits while reconstructing the types of constraints that help to ensure monetary integrity, customer/investor protection and financial stability. To that end, regulators need to focus on DeFi's workable control points: the people, firms and mechanisms that facilitate DeFi activities and that regulators could actually supervise. While these control points might not always be easily identified, they are — or at least can be made — identifiable.

Acknowledgements

The authors gratefully acknowledge that this CIGI paper greatly benefits from the forthcoming article by Gina-Gail S. Fletcher, Veronica Root Martinez and Steven L. Schwarcz, "Regulating DeFi Platforms," *Minnesota Law Review* 111.

Works Cited

Aramonte, Sirio, Sebastian Doerr, Wenqian Huang and Andreas Schrimpf. 2022. "DeFi lending: intermediation without information?" BIS Bulletin No. 57. June 14. www.bis.org/publ/bisbull57.pdf.

BCBS. 1988. *International Convergence of Capital Measurement and Capital Standards*. July. www.bis.org/publ/bcbs04a.pdf.

— — —. 2011. *Basel III: A global regulatory framework for more resilient banks and banking systems*. December 2010 (rev. June 2011). www.bis.org/publ/bcbs189.pdf.

BIS Innovation Hub. 2023. *Project Atlas: Mapping the world of decentralised finance*. October. www.bis.org/publ/othp76.pdf.

Born, Alexandra, Isabella Gschossmann, Alexander Hodbod, Claudia Lambert and Antonella Pellicani. 2022. "Decentralised finance — a new unregulated non-bank system?" In *Macroprudential Bulletin* 18. July. www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html.

Deng, Xun, Sidi Mohamed Beillahi, Cyrus Minwalla, Han Du, Andreas Veneris and Fan Long. 2024. *Analysis of DeFi Oracles*. Bank of Canada Staff Discussion Paper 2024-10. July 9. https://doi.org/10.34989/sdp-2024-10.

Diamond, Douglas W. 1984. "Financial Intermediation and Delegated Monitoring." *Review of Economic Studies* 51 (3): 393–414. https://doi.org/10.2307/2297430.

Duley, Chanelle, Leonardo Gambacorta Rodney Garratt and Priscilla Koo Wilkens. 2023. "The oracle problem and the future of DeFi." BIS Bulletin No. 76. September 7. www.bis.org/publ/bisbull76.pdf.

Ethereum Foundation. 2026. "Introduction to smart contracts." February 25. https://ethereum.org/en/developers/docs/smart-contracts/.

FATF. 2021. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. October. www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html.

— — —. 2025. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*. Updated October. www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

FSB. 2021. *Cyber Incident Reporting: Existing Practices and Next Steps for Broader Convergence*. October 19. www.fsb.org/uploads/P191021.pdf.

— — —. 2023. *The Financial Stability Risks of Decentralised Finance.* February 16. www.fsb.org/uploads/P160223.pdf.

— — —. 2024. *The Financial Stability Implications of Artificial Intelligence.* November 14. www.fsb.org/uploads/P14112024.pdf.

IOSCO. 2023. *Final Report with Policy Recommendations for Decentralized Finance (DeFi).* Final Report FR/04/2023. December. www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf.

— — —. 2025. *Artificial Intelligence in Capital Markets: Use Cases, Risks, and Challenges.* Consultation Report CR/01/2025. March. www.iosco.org/library/pubdocs/pdf/IOSCOPD788.pdf.

Lehar, Alfred and Christine A. Parlour. 2022. "Systemic fragility in decentralized markets." BIS Working Paper No. 1062. December. www.bis.org/publ/work1062.pdf.

Levi, Stuart D. and Alex B. Lipton. 2018. "An Introduction to Smart Contracts and Their Potential and Inherent Limitations." Harvard Law School Forum on Corporate Governance, May 26. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf.

Nassr, Iota Kaousar, Eleftheria Kostika and Anastasia Melachrinos. 2024. "Concentration of DeFi's liquidity: Evidence from Decentralised Exchanges (DEXs) and Automated Market Makers (AMMs)." Organisation for Economic Co-operation and Development Working Paper on Finance, Insurance and Private Pensions No. 49. https://dx.doi.org/10.1787/4ed08440-en.

New York Stock Exchange. 2026. "Market-Wide Circuit Breakers FAQ." February. www.nyse.com/publicdocs/nyse/NYSE_MWCB_FAQ.pdf.

Office of the Comptroller of the Currency. 2025. *Commercial Loans Comptroller's Handbook (Section 206).* www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/commercial-loans/index-commercial-loans.html.

Pozsar, Zoltan, Tobias Adrian, Adam Ashcraft and Hayley Boesky. 2012. *Shadow Banking.* Federal Reserve Bank of New York Staff Report No. 458. Revised February 2012 (original July 2010). www.newyorkfed.org/medialibrary/media/research/staff_reports/sr458.pdf.

Schwarcz, Steven L. 2023. "Next-Generation Securitization: NFTs, Tokenization, and the Monetization of 'Things.'" *Boston University Law Review* 103: 967–1003. www.bu.edu/bulawreview/files/2023/10/SCHWARCZ.pdf.

Securities and Exchange Commission. 2014. "Money Market Fund Reform; Amendments to Form PF." *Federal Register* 79 (157): 47736–7983. www.federalregister.gov/documents/2014/08/14/2014-17747/money-market-fund-reform-amendments-to-form-pf.

United States Department of the Treasury. 2023. *Illicit Finance Risk Assessment of Decentralized Finance.* April. https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

— — —. 2026. *Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets.* March. https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.

World Economic Forum. 2023. *Pathways to the Regulation of Crypto-Assets: A Global Approach.* White Paper. May. www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf.

Yaga, Dylan, Peter Mell, Nik Roby and Karen Scarfone. 2018. *Blockchain Technology Overview.* National Institute of Standards and Technology Internal Report 8202. October. https://doi.org/10.6028/NIST.IR.8202.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
cigionline.org