Research Article

RegTech Empowerment in Decentralized Finance: From Rule Engines to Automated Compliance Supervision

De Vries Van[1,*]

Department Faculty of Electrical Engineering, Delft University of Technology, 2600 AA, Netherlands

* Corresponding author: De Vries Van

DevriesVan@gmail.com

***Abstract*:** Decentralized finance has rapidly developed through smart contracts and distributed infrastructure, enabling lending, trading, liquidity provision, and other financial activities. However, this rapid development has also led to increasing contradictions with regulatory requirements related to anti-money laundering, sanctions compliance, market integrity, and investor protection. Against this backdrop, this paper explores how RegTech can empower compliance governance in DeFi, focusing particularly on the transition from rule engines to automated compliance regulation. This paper argues that rule formalization cannot be effortlessly translated into code without loss or ambiguity; it can only be achieved to a certain extent. The effectiveness of automated regulation depends on data observability, the structure of protocol governance, and the machine enforceability of legal requirements. Research shows that RegTech can improve the traceability, transparency, and regulatory efficiency of DeFi. Considering these limitations, further research is needed on the legal, technological, and governance boundaries of automated compliance in DeFi systems.

Keywords: *RegTech, decentralized finance; rule engines; automated compliance supervision; governance;*

1. Introduction

Decentralized finance has developed from a relatively niche set of blockchain-based experiments into a more visible segment of the digital financial landscape, offering protocol-based lending, trading, derivatives, liquidity provision, and other financial functions through smart contracts rather than through traditional intermediated infrastructures[1]. BIS research has noted that DeFi seeks to replicate many economic functions of traditional finance while relying on distinctive technical arrangements such as composability, tokenization, and automated execution, and IOSCO has similarly emphasized that DeFi arrangements may involve economic activities resembling regulated financial services even when their governance and technical form differ markedly from conventional institutions[2]. This dual character, namely functional similarity combined with structural divergence, is one reason why DeFi has become so difficult to place within inherited regulatory categories[3].

At the same time, the regulatory significance of DeFi does not arise only from novelty. FATF has repeatedly stressed, in its post-2019 work on virtual assets and virtual asset service providers, that emerging market developments, including DeFi, create continuing challenges for AML/CFT implementation, especially where responsibility, control, and service provision are distributed in ways that are not easily mapped onto traditional institutional actors. IOSCO, for its part, frames DeFi as a source of market integrity and investor protection concerns, while the FSB has argued that DeFi's current scale and interconnectedness with traditional finance may still be limited in relative terms but could grow in ways that increase contagion channels and broader financial stability concerns[4]. Taken together, these assessments suggest that DeFi regulation is not simply a matter of fitting an old rulebook to a new technological object; it is also a question of whether the modalities of supervision themselves require reconfiguration.

It is against this background that RegTech becomes relevant. In more traditional financial settings, regulatory technology has often been associated with automation of compliance reporting, transaction monitoring, identity verification, screening, and

anomaly detection. Yet the DeFi environment may push RegTech into a more demanding role. If compliance obligations are to operate in systems that settle transactions continuously, execute rules through code, and disperse control across protocol developers, governance token holders, front-end operators, and external service providers, then RegTech may no longer function merely as an auxiliary back-office tool. It may need to evolve toward something closer to embedded supervisory infrastructure, situated between legal norm, technical implementation, and governance process. This possibility is analytically attractive, although it also raises difficult questions about the limits of formalization and the persistence of legal ambiguity[5].

The movement from rule engines to automated compliance supervision captures this broader shift. A rule engine, in the narrow technical sense, can encode conditions, thresholds, and responses, allowing certain compliance checks to be performed automatically[6]. But automated compliance supervision in DeFi appears to imply something more complex: the continuous translation of regulatory expectations into machine-executable logic, the integration of on-chain and possibly off-chain signals, the triggering of alerts or restrictions in near real time, and the maintenance of auditable records that may support both internal governance and external oversight. Whether this transformation is fully feasible remains uncertain. Much depends on what kind of legal requirement is at issue, how observable the relevant conduct is, and whether the protocol architecture permits intervention without undermining its claimed decentralization[7][12][21].

The present study does not proceed from the assumption that automation solves the regulatory problem of DeFi. If anything, the initial attempt to conceptualize the topic in purely technological terms proved unsatisfactory. The more closely one examines FATF's concern with attribution and control, IOSCO's emphasis on legal accountability and investor protection, or BIS and FSB discussions of structural risk and functional resemblance, the harder it becomes to maintain the view that compliance can simply be "coded in" without remainder[8][15][17][18][26]. There are zones of legal interpretation, exceptions, conflicts of jurisdiction, and governance disputes that resist straightforward machine translation. Still, it would also be too easy to conclude that because legal judgment cannot be fully automated, automation has little regulatory value. The more productive question may lie in between: to what extent, in which areas, and under what institutional conditions can RegTech meaningfully empower compliance supervision in DeFi.

The core research problem of this paper lies in the fact that DeFi has generated a regulatory object whose economic functions are legible, but whose control structure is often obscure, layered, or contested. Existing compliance models generally presuppose identifiable intermediaries, stable points of supervisory contact, and organizational structures capable of receiving instructions, implementing controls, and bearing liability[9][19][22]. DeFi complicates all three assumptions. FATF's updates repeatedly return to the difficulty of determining whether ostensibly decentralized arrangements may in fact involve persons or entities exercising sufficient control or influence to fall within regulatory scope, while IOSCO similarly stresses the importance of identifying responsible persons and functions within DeFi arrangements. This suggests that before one can ask whether compliance may be automated, one must first ask what exactly is being supervised, and who, if anyone, is in a position to operationalize supervision.

A second problem concerns translation. Legal and regulatory rules are rarely written in a form immediately suitable for machine execution. They contain open-textured standards, context-dependent judgments, proportionality requirements, and exceptions that presume interpretive discretion. A rule engine can process conditions, but only after those conditions have been formalized in a manner sufficiently stable for computation. This creates a difficult intermediate layer between law and code. If that layer is ignored, the analysis becomes naïvely technical. If it is overstated, one risks implying that no meaningful automation is possible. The present paper therefore approaches the problem as one of selective formalization rather than total translation. Some requirements may be encoded with relative clarity, while others may remain partially resistant to automation[10][25].

A third problem concerns governance outcomes. It is one thing to argue that RegTech can help monitor transactions, screen addresses, or trigger alerts. It is another to claim that these functions amount to effective compliance supervision in a robust sense. Supervision implies not only detection but also response, accountability, reviewability, and some degree of normative legitimacy.

In DeFi, automated controls may improve traceability while still producing false positives, excluding legitimate users, or shifting power toward actors who control interfaces, oracles, or governance parameters. This leads to a more nuanced research agenda. The question is not simply whether automation enhances compliance, but whether it changes the balance between transparency, control, decentralization, and legal accountability in ways that are normatively and institutionally sustainable[11][16][24].

For these reasons, the present study is guided by four interrelated questions. First, what is the conceptual role of RegTech in decentralized finance compliance. Second, how can rule engines transform regulatory requirements into machine-executable logic without collapsing the interpretive complexity of law entirely. Third, through what mechanisms might automated compliance supervision improve governance in DeFi. Fourth, what limitations, risks, and boundary conditions constrain the effectiveness of RegTech-enabled compliance architectures. These questions are not arranged in order to produce a single definitive answer. They are intended, rather, to keep open a space in which legal theory, technical design, and governance analysis can be brought into more careful relation.

Against the above background, the first objective of this paper is conceptual clarification. RegTech in DeFi should not be reduced either to compliance software in the narrow operational sense or to a broad slogan about "regulation by code." The paper seeks to specify what it means to speak of RegTech empowerment where financial functions are protocol-based, supervisory access may be indirect, and compliance depends partly on the formalizability of norms[12][21]. The second objective is mechanism analysis. Rather than treating automated supervision as a technological outcome, the paper examines the chain through which regulatory requirements are abstracted, formalized, encoded, monitored, and translated into alerts, restrictions, or governance actions. The third objective is evaluative: to assess, in a structured way, where automated compliance supervision may improve traceability, transparency, and efficiency, and where it may remain limited by legal indeterminacy, data gaps, or governance fragmentation.

The significance of the study may be considered at two levels[13][14]. At the theoretical level, it contributes to the emerging intersection of DeFi governance, RegTech, and code-mediated regulation by offering a framework that links legal normativity, technical execution, and governance outcomes. Much of the existing literature treats these dimensions separately. At the practical level, the study may help regulators, protocol designers, and market participants think more carefully about where automation is genuinely useful and where human review, legal interpretation, or institutional coordination remain indispensable. This is not a minor point. In fast-moving digital finance, the temptation to overstate technological solutionism can be strong. A more differentiated framework may be useful precisely because it neither dismisses automation nor romanticizes it.

2. Literature Review and Theoretical Foundation

The literature on decentralized finance has developed quickly, but not always coherently. Some work emphasizes DeFi's technological architecture, such as smart contracts, automated market makers, protocol composability, and token-based governance. Other studies focus more on DeFi as an economic and legal phenomenon, asking whether it reproduces traditional financial functions, whether it disintermediates or merely reconfigures intermediation, and how responsibility should be allocated when services are delivered through distributed infrastructures. BIS work is especially useful here because it resists both uncritical enthusiasm and reductive dismissal, arguing that DeFi can replicate many economic functions of traditional finance while also exhibiting vulnerabilities and governance frictions rooted in its architecture. This is relevant to the present study because it suggests that regulation cannot be approached solely as an external constraint; it is also shaped by the internal form of the system being regulated[20][23].

A second line of literature, reflected in FATF, IOSCO, and FSB materials as well as academic commentary, centers on the regulatory and supervisory difficulty posed by DeFi. FATF's treatment of DeFi within the broader virtual asset framework is especially important because it moves the debate beyond mere description and toward attribution, control, and AML/CFT accountability. IOSCO adds a different but complementary perspective by focusing on market integrity, investor protection, and

the identification of responsible persons and functions in DeFi arrangements. FSB, while somewhat more macro-prudential in orientation, highlights the possibility that DeFi's links with traditional finance may expand and thereby transform what currently appears to be a contained risk field into one with wider systemic implications. These approaches do not fully converge, but they do reveal a common difficulty: DeFi creates functions that are economically legible yet institutionally elusive.

Methodologically, this literature also displays certain limitations. Much of the policy-oriented analysis is strong on functional diagnosis but less developed in its account of how supervisory techniques might actually operate in code-mediated environments. Conversely, some technology-focused writing proposes compliance-by-design or governance-by-code without sufficiently engaging the indeterminacy of legal language and the institutional complexity of cross-border financial supervision. The present paper is situated in the space between these tendencies. It takes seriously the idea that DeFi cannot be regulated as though it were simply a disguised traditional intermediary, but it is equally cautious about the claim that decentralization renders meaningful supervision practically obsolete.

2.1 Literature Review on RegTech, Rule Engines, and Automated Compliance

RegTech literature, in its earlier and more mainstream form, largely emerged within regulated centralized financial systems. There, its core functions were typically described in terms of cost reduction, speed enhancement, data integration, regulatory reporting, transaction monitoring, and screening. In such settings, RegTech generally operated within institutions whose legal status, governance structure, and compliance responsibility were already defined. This context is important because it means that much of the classical RegTech literature implicitly presumes the very institutional stability that DeFi unsettles. What works as supervisory technology in a bank, broker, or centralized exchange may not simply transfer into a protocol environment where responsibility is distributed and intervention points are contested.

Within this broader literature, rule engines occupy a particularly interesting position. They represent an attempt to make norms operational by expressing conditions, triggers, and consequences in forms suitable for computation. In administrative and corporate compliance settings, this may be relatively manageable where obligations are threshold-based, event-driven, or strongly proceduralized. But the move from rules to rule engines should not be romanticized. The literature on legal formalization has long shown that many norms derive force precisely from context-sensitive interpretation rather than from purely fixed thresholds. For DeFi, this difficulty is magnified. A rule engine may screen addresses against sanctions lists or flag transaction patterns, but whether the resulting action constitutes adequate compliance may depend on legal scope, evidentiary sufficiency, and institutional review. Thus, rule engines should perhaps be seen as instruments of partial operationalization rather than complete legal translation.

The idea of automated compliance supervision takes the analysis one step further. It implies not merely that rules are encoded, but that monitoring, detection, response, and auditability are connected within an ongoing supervisory process. IOSCO's DeFi recommendations, though not framed in the vocabulary of rule engines, are relevant here because they emphasize achieving common regulatory outcomes, identifying responsible persons, understanding structures, and improving oversight consistency. These priorities suggest that automation, to be meaningful, must be attached to governance design and not just to technical screening. FATF's emphasis on implementation challenges, including those associated with emerging risks and Travel Rule progress, reinforces a similar point: technological compliance tools can matter, but their effectiveness depends on whether they are embedded in enforceable governance and supervisory arrangements.

2.2 Literature Review on DeFi Compliance Governance and Theoretical Foundation

Research on DeFi compliance governance has increasingly focused on the tension between decentralization and control. Some studies and policy discussions point toward wallets, interfaces, governance tokens, oracles, and analytics tools as locations where compliance functions may be introduced without fully centralizing the protocol core. Others remain skeptical, arguing that these interventions may either be evaded, prove ineffective, or reintroduce concentrated power in ways that undercut the normative

claims of decentralization. This debate is central to the present paper because it shows that compliance in DeFi is not a binary matter of either total automation or complete absence of control. It is more plausibly a layered field in which technical architecture, governance design, and legal expectations intersect unevenly.

The theoretical foundation of this paper draws on several complementary traditions. Institutional theory is useful because DeFi does not operate outside institutional pressure; rather, it exists in a contested field of regulatory expectations, legitimacy claims, and organizational adaptation. Regulatory governance theory helps explain that supervision is not merely about rules on the books but about the infrastructures, actors, and monitoring logics through which rules become effective. The "code as law" perspective remains relevant, though it requires caution. It correctly highlights that technical architectures structure behavior, yet it may overstate how fully normative complexity can be absorbed by code. A socio-technical systems perspective becomes necessary at this point, because automated compliance supervision in DeFi is best understood not as a technical layer added to law, but as an assemblage in which legal norms, computational logic, data visibility, and governance choices continuously interact.

This review leads to the central research gap. Existing literature has generated rich descriptions of DeFi risk, important policy reflections on responsible persons and regulatory outcomes, and increasingly sophisticated accounts of RegTech tools. Yet it has not sufficiently integrated these strands into a coherent explanation of how rule formalization, rule engines, and automated compliance supervision are related in DeFi. What remains underdeveloped is a mechanism-level account linking legal requirements, machine-executable representation, monitoring architecture, and governance consequences. The present paper positions itself in that gap. It does not claim to resolve the tension between law and code. What it seeks, more carefully, is to explain how that tension is operationalized, limited, and sometimes partially stabilized through RegTech in decentralized financial systems

3. Research Framework and Mechanism Analysis

The present chapter does not proceed as though the conceptual difficulties identified earlier had already been resolved. On the contrary, the movement from literature review to mechanism analysis makes those difficulties even more visible. If DeFi is functionally legible yet institutionally elusive, and if RegTech is expected to operate not in a conventional intermediary but in a protocol environment whose governance is distributed, then any explanatory framework must remain somewhat provisional. What can be done, however, is to identify a sequence of transformations through which legal expectations may be rendered partially operational. This chapter, accordingly, treats RegTech empowerment not as a singular technological event, but as a layered process extending from rule abstraction to rule formalization, from formalization to rule engines, and from rule engines to automated monitoring, response, and auditable oversight.

A first analytical distinction is necessary at the outset. Rule engines, although often invoked as if they were synonymous with automated supervision, are in fact only one component of a larger supervisory architecture. A rule engine can encode conditions, thresholds, logic trees, and trigger events. It can compare inputs with predefined compliance conditions and produce outputs, such as flags, restrictions, or escalations. Yet supervision, even in an automated or semi-automated sense, implies a broader arrangement. It requires the availability of observable data, a governance environment in which outputs can be acted upon, and some framework of responsibility through which alerts or restrictions become institutionally meaningful. This leads to further thinking that the central analytical movement is not from law directly to code, but from law to formalized representation, from representation to executable logic, and from executable logic to governance consequences.

The first stage in this sequence is rule formalization. Here the paper adopts a deliberately cautious position. Legal requirements are not naturally machine-readable. They contain open-textured concepts, proportionality standards, contextual judgments, and exceptions that frequently depend on interpretive discretion. FATF's Travel Rule framework, for instance, is more amenable to formalization than many broader principles because it concerns the transmission of specified originator and beneficiary

information, yet FATF's own reports also make clear that implementation is uneven, operationally burdensome, and affected by interoperability problems, counterparty due diligence issues, and phased implementation. What this suggests is not that formalization fails, but that it succeeds selectively. Certain obligations may be encoded with relative clarity, while others remain only partially codifiable.

A second stage is the operation of rule engines themselves. In DeFi, rule engines may screen wallet addresses, check transaction patterns against pre-set typologies, test counterparties against licensing or sanctions conditions, or verify whether transfer information has been transmitted in a manner compatible with Travel Rule obligations. The appeal of such systems lies in their speed and consistency. Unlike ex post manual review, rule engines can operate continuously and at scale. Still, consistency should not be confused with correctness. A rule engine is only as sound as the prior translation on which it depends and the data visibility it can access. When on-chain signals are incomplete, when off-chain identifiers are unavailable, or when legal conditions depend on more than observable transaction structure, automation may create an appearance of precision that exceeds its actual normative reliability.

The unevenness of formalization is visible in FATF's implementation data. In its 2025 best-practices report on Travel Rule supervision, FATF reported that the number of jurisdictions having passed legislation putting the Travel Rule in place for VASPs rose from 35 in 2023 to 65 in 2024 and 85 in 2025. The number of jurisdictions in the process of passing such legislation moved from 27 in 2023 to 15 in 2024 and 14 in 2025, while those in "none of the above" declined from 28 in 2023 to 14 in 2024 but then rose to 18 in 2025. These data do not tell us how effective implementation is, nor do they distinguish DeFi from other virtual asset contexts. Even so, they do indicate that the rule environment within which rule engines might operate is expanding, but not converging in a perfectly stable way.

Table 1. FATF-reported jurisdictional implementation of the Travel Rule for VASPs

Year	Has passed legislation	In process of passing legislation	None of the above
2023	35	27	28
2024	65	15	14
2025	85	14	18

Source: FATF, Best Practices in Travel Rule Supervision (2025), Figure 1.1.

Considering the above factors, the mere existence of rule-compatible legislation does not suffice to establish automated compliance supervision. The next stage is real-time monitoring. In theoretical terms, this is where rule engines are connected to live or near-live data streams and can produce dynamic assessments rather than static classifications. In DeFi, such monitoring may involve tracking sanctioned or high-risk addresses, evaluating transaction flows, observing liquidity movements, or identifying anomalies across front-end access and protocol interaction. The ambition is not simply to know what happened, but to detect what may require intervention while the system is still in motion. This capability is one of the most important promises of RegTech in DeFi, precisely because conventional supervisory cycles are often too slow for code-mediated markets that can reallocate value in minutes rather than weeks. Yet here again, the promise is conditional. Real-time monitoring is powerful only where relevant data are visible and where governance actors are willing and able to respond.

That response stage is analytically crucial and sometimes underdeveloped in the literature. Automated supervision is not simply monitoring plus notification. It includes the design of response pathways, which may range from warning messages and enhanced review to interface restrictions, freezing of identifiable assets, exclusion of certain counterparties, or the generation of logs for later audit and enforcement. FATF's 2024 and 2025 materials are revealing in this regard because they show that many jurisdictions are not content merely to legislate the Travel Rule; they also restrict how domestic VASPs may interact with foreign

counterparts when implementation is uneven. This suggests that automation and supervision intersect not only at the level of information transmission, but also at the level of conditional access and risk-based counterparty control.

The distribution of those response models is itself instructive. FATF's 2025 best-practices report states that, of the 85 jurisdictions that had passed legislation enacting the Travel Rule, 49 had measures in place to ensure domestic VASPs transact only with licensed, registered, Travel Rule-compliant, or otherwise risk-mitigated foreign counterparties. Among the specific measures reported, 8 jurisdictions allowed transactions only with licensed or registered foreign VASPs, 22 required foreign counterparties to be both licensed or registered and Travel Rule-compliant, 24 permitted transactions only with VASPs licensed or registered in specific jurisdictions and or compliant with the Travel Rule, and 14 allowed dealings with unlicensed or unregistered foreign VASPs only where appropriate risk mitigation steps were taken. FATF also noted that 36 jurisdictions implementing the Travel Rule placed no such limitations, and 9 jurisdictions permitted domestic VASPs to transact regardless of foreign counterparties' licensing or compliance status. These figures do not map neatly onto DeFi, but they do reveal the supervisory logic of conditional interoperability.

Table 2. FATF-reported measures restricting interactions with foreign counterparties, 2025

Measure category	Number of jurisdictions
Transactions only with licensed/registered foreign VASPs	8
Transactions only with foreign VASPs that are both licensed/registered and Travel Rule-compliant	22
Transactions with VASPs licensed/registered in specific jurisdictions and/or Travel Rule-compliant	24
Transactions with unlicensed/unregistered foreign VASPs only if risk mitigation steps are taken	14
Jurisdictions with some restrictive or mitigating measures in place	49
Jurisdictions implementing the Travel Rule that place no such limitations	36
Jurisdictions permitting transactions regardless of foreign status/compliance	9

Source: FATF, Best Practices in Travel Rule Supervision (2025), paras. 10–11.

A further stage in the framework is auditability. Automated compliance supervision, if it is to become something more than automated gatekeeping, must generate records that can be reviewed, contested, and connected to governance accountability. This is where RegTech becomes especially interesting for DeFi. Public blockchains already produce extensive transactional traceability, but traceability alone is not equivalent to compliance evidence. The relevant issue is whether automated controls can generate meaningful compliance logs, explainable triggers, and reviewable intervention histories that support both internal governance and external supervision. IOSCO's DeFi recommendations are relevant here because they do not treat oversight as merely a matter of identifying risk; they also emphasize identifying responsible persons, achieving common regulatory outcomes, requiring systems and controls, and ensuring enforcement powers remain meaningful. Automated supervision, in this sense, is valuable only if it can be linked to review and responsibility.

The framework developed in this chapter can thus be summarized, though only provisionally, as follows: regulatory requirements are abstracted into formalizable elements; those elements are encoded through rule engines; rule engines become meaningful when connected to observable data and response pathways; and automated compliance supervision emerges where monitoring, intervention, and auditability are joined within a governance structure capable of acting on them. This chain is possible, but only partially stable. It may work better for screening, sanctions compliance, transfer-information controls, and certain threshold-based

functions than for open-ended legal standards or disputes over responsibility in highly decentralized systems. For that reason, the value of RegTech in DeFi may lie not in replacing law with code, but in selectively operationalizing supervision where legal formalization, data observability, and governance capacity align sufficiently to make automation more than symbolic. Further empirical analysis is needed to test how this alignment works in concrete cases.

4. Empirical Analysis

The empirical ambition of this chapter is intentionally limited, and that limitation should be stated plainly. DeFi compliance architectures do not yet lend themselves easily to clean quantitative comparison across protocols, jurisdictions, and supervisory models. Publicly available data are often fragmentary, and what appears observable at the protocol or interface layer may not capture the deeper governance arrangements through which compliance is actually mediated. For that reason, the chapter adopts a case-based comparative approach, supplemented by official policy statistics, rather than attempting to impose an artificial large-sample causal model on a still unstable field. This is not an ideal design in the abstract, but under current conditions it may be the more intellectually defensible one.

The first case is Tornado Cash, not because it exemplifies successful RegTech, but because it reveals the limits of supervision when automation and decentralization are not accompanied by effective controls. In August 2022, the U.S. Treasury stated that Tornado Cash had been used to launder more than USD 7 billion worth of virtual currency since its creation in 2019, including over USD 455 million stolen by the Lazarus Group, more than USD 96 million from the Harmony Bridge heist, and at least USD 7.8 million from the Nomad heist. The Treasury further argued that Tornado Cash had repeatedly failed to impose effective controls designed to stop laundering activity. Whether one agrees entirely with the sanctioning approach is another matter, and later legal developments complicated the story, but the case is analytically important because it highlights what regulators may perceive when a protocol exhibits functional financial significance without corresponding supervisory friction points.

The second case is Aave Arc, which represents an attempt to construct a permissioned or semi-permissioned access model around a DeFi protocol in response to compliance concerns. According to Fireblocks' official announcement, Aave Arc launched in January 2022 as a separate deployment of the Aave V2 liquidity pool for institutions, with participating institutions becoming "whitelisted" after undergoing a rigorous customer identification process. Fireblocks stated that its framework referenced globally accepted KYC, CDD, and EDD principles, and that 30 licensed financial institutions had been approved to participate at launch. From the standpoint of the present study, Aave Arc matters not because it resolves all governance tensions, but because it shows one route by which rule-based access control, identity verification, and ongoing monitoring can be introduced without fully rewriting the protocol logic of DeFi into traditional centralized finance.

The third case is Uniswap Labs, which illustrates a different layer of compliance intervention, namely the interface layer rather than the core protocol layer. In April 2022, Uniswap Labs publicly stated that its app had blocked addresses on the OFAC sanctions list for years and, with the help of TRM Labs, was also blocking wallet addresses associated with illicit activity such as stolen funds or ransomware from interacting with the Uniswap Labs app. This case is particularly useful because Uniswap Labs itself emphasized that, given the decentralized and open-source nature of the Uniswap Protocol, it did not control user access via portals other than its own app. The compliance intervention here is thus selective and infrastructural rather than total. It targets the access surface, not the protocol as such, which suggests that automated supervision in DeFi may often be implemented through interfaces, routing layers, or ancillary services rather than solely through immutable smart contracts.

These three cases already indicate that "automated compliance supervision" is not a single model. It may appear as sanction-based supervisory escalation, as permissioned whitelisting and identity-gated participation, or as interface-level address screening and risk filtering. What unites them is not uniform design but a common movement toward embedding supervision into technical and governance layers that operate before, during, or immediately around transaction execution. This does not mean that all such

interventions are equally effective or normatively attractive. Tornado Cash suggests the costs of absent or insufficient control. Aave Arc suggests the possibilities of compliance-conscious design, but perhaps at the price of narrowing participation. Uniswap suggests that front-end screening can be operationalized, though not without raising questions about partial control, circumvention, and the relationship between protocol openness and interface governance.

Table 3. Officially reported indicators from selected DeFi-related compliance cases

Case	Officially reported quantified indicator	Supervisory relevance
Tornado Cash	More than USD 7 billion laundered since 2019; over USD 455 million linked to Lazarus; more than USD 96 million from Harmony; at least USD 7.8 million from Nomad	Illustrates supervisory escalation where effective controls were viewed as absent
Aave Arc	30 licensed financial institutions approved at launch	Illustrates permissioned participation through KYC/CDD/EDD-based whitelisting
Uniswap Labs	USD 175,000 CFTC civil monetary penalty in 2024	Illustrates continuing legal exposure around DeFi access and interface governance

Source: U.S. Treasury press release on Tornado Cash; Fireblocks press release on Aave Arc; CFTC press release on Uniswap Labs.

A further layer of evidence comes from FATF's continuing work on Travel Rule implementation, which, while not DeFi-specific, is highly relevant to the broader trajectory of automated compliance architecture in virtual asset markets. FATF reported in 2024 that, of the 80 jurisdictions that had implemented the Travel Rule or were in the process of doing so, 26 were still taking a phased approach or allowing grace periods. The same report noted that of the 65 jurisdictions that had passed Travel Rule legislation at that time, 36 had measures in place to ensure domestic VASPs were transacting only with regulated or Travel Rule-compliant counterparts or otherwise mitigating the risks, while 10 of the 65 still allowed domestic VASPs to transact with any foreign VASP regardless of licensing, compliance, or risk mitigation. These figures are important because they show not only uneven adoption but different supervisory philosophies. Some jurisdictions appear willing to structure interoperability conditionally, while others remain more permissive.

That unevenness becomes even more visible in FATF's 2025 best-practices material. By 2025, 85 jurisdictions had passed Travel Rule legislation, 14 were still in process, and 18 fell into none of those categories. Of the 85 implementing jurisdictions, 49 had measures restricting or conditioning interaction with foreign counterparties, and about half of these measures tied access to licensing, registration, Travel Rule compliance, or explicit risk mitigation. What is striking here is not only the rise in legislation, but the persistence of conditional access logic. This may be read as indirect support for the paper's argument: automated compliance supervision becomes more plausible where the supervisory environment itself shifts toward machine-checkable conditions rather than exclusively ex post enforcement. Still, one should resist over-reading the data. Jurisdictional legislation does not automatically translate into protocol-level enforcement, and VASP-centered supervision cannot be mapped one-to-one onto all DeFi arrangements.

Table 4. FATF-reported supervisory environment for Travel Rule implementation

Indicator	2024	2025
Jurisdictions that had passed Travel Rule legislation	65	85
Jurisdictions implementing or in process of implementing Travel Rule	80	99

Indicator	2024	2025
Jurisdictions taking phased approach or allowing grace periods	26	N/A
Implementing jurisdictions with restrictive or mitigating measures on foreign counterparties	36	49
Implementing jurisdictions allowing any foreign VASP regardless of status/compliance	10	9

Source: FATF, Virtual Assets: Targeted Update on Implementation of the FATF Standards (2024); FATF, Best Practices in Travel Rule Supervision (2025).

If one reads the case evidence together with the FATF policy environment, a more differentiated empirical picture begins to emerge. RegTech-enabled compliance in DeFi seems most plausible where there are identifiable intervention layers, observable data, and governance actors willing to act on automated outputs. Aave Arc reflects one such model, in which whitelisting and identity controls are built into participation. Uniswap reflects another, where the interface operates as a compliance membrane without claiming total protocol control. Tornado Cash, by contrast, became the object of direct sanction-based intervention precisely because authorities viewed the absence of effective controls as intolerable. These models differ sharply, yet all point toward the same underlying insight: compliance automation in DeFi is rarely total and is often distributed across protocol, interface, and institutional layers.

At this stage, however, interpretive caution becomes essential. It would be easy to narrate these cases as a straightforward march toward more effective automated supervision, but such a reading would likely be too smooth. Aave Arc may demonstrate the viability of whitelisting, but it also raises the question of whether permissioned access remains meaningfully DeFi in anything other than technical form. Uniswap's interface controls may show the practicality of address screening, yet they also reveal how selective such control is, given that protocol interaction can occur elsewhere. FATF's implementation data show expanding legislation, but also persistent inconsistency, phased implementation, and different counterparty philosophies. In other words, the same evidence that suggests progress also exposes fragmentation. This ambivalence should be retained rather than explained away.

For the purposes of this paper, the empirical discussion supports a limited but meaningful claim. RegTech can empower compliance supervision in DeFi, especially when rules are formalizable, relevant data are available, and intervention points exist at the protocol, interface, or governance level. Yet empowerment is not equivalent to completion. Automation may strengthen traceability, screening, and conditional access, but it does not dissolve legal ambiguity, cross-jurisdictional inconsistency, or conflicts over who is responsible within decentralized arrangements. Further research would be needed, perhaps combining protocol-level technical analysis with richer governance data, to determine more precisely where automation produces robust supervisory effects and where it remains largely symbolic. What the present evidence does show is that the movement from rule engines to automated supervision is not imaginary; it is already visible, though uneven, contested, and institutionally incomplete.

5. Conclusion

Building on the foregoing discussion, the final chapter draws the argument together without presuming that the path from rule engines to automated compliance supervision can be described as either linear or complete. What the preceding chapters have gradually indicated is that RegTech may indeed become a meaningful supervisory force in decentralized finance, yet its contribution appears to depend less on automation in the abstract than on the more demanding question of whether legal requirements can be selectively formalized, whether relevant data remain sufficiently observable, and whether protocol, interface, or governance structures provide points at which automated outputs can be translated into reviewable and institutionally

intelligible action. The theoretical analysis in Chapter 3, together with the policy evidence and case-based discussion in Chapter 4, does not eliminate ambiguity, nor does it suggest that DeFi compliance can simply be reduced to code-based enforcement. If anything, the analysis points toward a more careful conclusion: automated supervision may strengthen traceability, screening, conditional access, and certain forms of governance coordination, while still remaining constrained by legal indeterminacy, jurisdictional fragmentation, and persistent disputes over responsibility within decentralized arrangements. It is from this analytical basis that the final chapter proceeds to synthesize the principal findings of the study, reflect on their theoretical and regulatory implications, and consider the limits and future directions of RegTech-enabled supervision in the evolving architecture of decentralized finance.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The author(s) declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] *Devanga, S. V. (2025). Significance of Regulatory Technology and its Impact on Banks and Financial Institutions amongst the Growth of Decentralized Finance (Doctoral dissertation, Dublin, National College of Ireland).*

[2] *Wang, H., Sun, W., & Liu, Y. (2022). Prioritizing autism risk genes using personalized graphical models estimated from single-cell rna-seq data. Journal of the American Statistical Association, 117(537), 38-51.*

[3] *Lin, A. (2025). Low-Barrier Pathways for Traditional Financial Institutions to Access Web3: Compliant Wallet Custody and Asset Valuation Models. Frontiers in Management Science, 4(6), 80-86.*

[4] *El Khoury, R., Alshater, M. M., & Joshipura, M. (2025). RegTech advancements-a comprehensive review of its evolution, challenges, and implications for financial regulation and compliance. Journal of Financial Reporting and Accounting, 23(4), 1450-1485.*

[5] *Lin, A. (2025). Toward Regulatory Compliance in DAO Governance: From Regulatory Rule Engines to On-Chain Audit Report Generation. Journal of World Economy, 4(6), 12-20.*

[6] *Wang, H., Li, Q., & Liu, Y. (2022). Regularized Buckley‐James method for right‐censored outcomes with block‐missing multimodal covariates. Stat, 11(1), e515.*

[7] *Wu, Y. (2026). A Study on the Impact of Cross-Departmental Data Collaboration on Marketing Campaign Efficiency in Fast-Moving Consumer Goods E-commerce: The Case of PepsiCo (China)'s 7UP and Mirinda Project. Frontiers in Management Science, 5(1), 7-12.*

[8] *Martins, M. R. (2025). Artificial Intelligence in Business Strategy: How AI Driven Analytics is Reshaping Decision Making. International Journal of Humanities and Information Technology, 7(01), 63-71.*

[9] *Wang, C. (2025). Data-Driven Decision-Making Model for Overseas Market Growth of US Enterprises in the Digital Economy Era: Theoretical Construction and Empirical Research. Journal of World Economy, 4(6), 58-65.*

[10] *Lin, A. (2026). Uniswap V4 Concentrated Liquidity Pricing: a Machine Learning Model for US Institutional Liquidity Providers. Journal of Intelligence and Engineering Technology, 1(1), 19-26.*

[11] *Hao, Z. (2026). Dynamic Task Prioritization for Edge AI in Smart Cities: Balancing Latency and Energy Efficiency. Journal of Intelligence and Engineering Technology, 1(1), 60-69.*

[12] *Wu, Y. (2026). Research on the Impact of LinkedIn Business Account Data-Driven Operations on Brand Exposure of AI Startups—A Case Study of AristAI. International Academic Journal of Social Science, 2, 27-37.*

[13] Jin, Y., Li, Z., Zhang, C., Cao, T., Gao, Y., Jayarao, P., ... & Yin, B. (2024). Shopping mmlu: A massive multi-task online shopping benchmark for large language models. Advances in Neural Information Processing Systems, 37, 18062-18089.

[14] Wang, J., Tim, K. T., Li, S., Chan, T. K., & Fung, J. C. (2023). A systematic comparison of the wind profile codifications in the Western Pacific Region. Wind & structures, 37(2), 105-115.

[15] Ryabov, O., Golubev, A., & Goncharova, N. (2021, October). Decentralized Finance (DeFi) as the basis for the transformation of the financial sector of the future. In Proceedings of the 3rd International Scientific Conference on Innovations in Digital Economy (pp. 387-394).

[16] Hao, Z. (2025). Fault-Tolerant Real-Time Scheduling for Edge AI in US Critical Infrastructure. Engineering Frontiers, 1(4).

[17] Kudal, P., Dawar, S., Inamdar, V., Patnaik, A., & Rathore, T. (2024). Achieving Financial Inclusion through Blockchain-Based Decentralized Finance and the Fintech Revolution. In Sustainability Reporting and Blockchain Technology (pp. 364-375). Routledge.

[18] Sindhu, S. (2025). Blockchain-enabled decentralized identity and finance: Advancing women's socioeconomic empowerment in developing economies. Journal of Women, Innovation, and Technological Empowerment, 1(1), 19-24.

[19] Wang, C. (2026). A Study on Data-Driven Budget Optimization for US Enterprises' Cross-Border Marketing. Frontiers in Management Science, 5(1), 41-46.

[20] Wang, J., Kudagama, B. J., Perera, U. S., Li, S., & Zhang, X. (2025). Framework for generating high-resolution Hong Kong local climate projections to support building energy simulations. Physics of Fluids, 37(3).

[21] Wu, Y. (2026). Research on Dynamic Prediction Model of Brand Marketing Content ROI Based on Machine Learning. International Journal of Advance in Applied Science Research, 5(2), 31-38.

[22] Wang, C. (2025). Research on the Precision Allocation of Cross-Border Marketing Resources of US Enterprises Driven by Digital Technology. Innovation in Science and Technology, 4(11), 7-13.

[23] Mustafa, J. A. (2024). Integrating financial literacy, regulatory technology, and decentralized finance: A new paradigm in Fintech evolution. Investment Management & Financial Innovations, 21(2), 213.

[24] Hao, Z. (2026). Structure-Aware Deep Reinforcement Learning for Latency-Minimal Scheduling of Edge AI Inference on Heterogeneous Cores. Journal of Intelligence and Engineering Technology, 1(1), 50-59.

[25] Lin, A. (2026). Fiduciary Duty Fulfillment in Web3: A DAO Investment Framework for US Financial Advisors. International Academic Journal of Social Science, 2, 17-26.

[26] Ali, A., Butt, M. H., & Senturk, I. (2025). Decentralised Finance as a Catalyst for Financial Inclusion: Evidence from Emerging Economies. Policy Journal of Social Science Review, 3(7), 292-303.