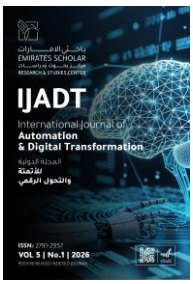

International Journal of Automation and Digital Transformation
Vol 5 Issue 1 (2026)
Pages (54 - 73)

Available at
www.emiratesscholar.com

FINTECH AS REGULATORY NIHILISM: Disruption, Strategic Non-Compliance and Sandbox as a containment device

Michele Trifiletti
PhD Student - Department of Social Sciences UCAM - Universidad Católica de Murcia (Spain) - Senior Officer and MLRO at an international financial institution; specialist in anti-money laundering, compliance, and fintech; lecturer and scholar of Islamic Banking and Finance
*Corresponding author: michele.trifiletti@libero.it

ARTICLE HISTORY

Received: 27 Jan 2026.
Accepted: 28 Feb 2026.
Published: 24 Jun 2026.

PEER - REVIEW STATEMENT:

This article was reviewed under a double-blind process by independent reviewers.

HOW TO CITE
Trifiletti, M. (2026). FINTECH AS REGULATORY NIHILISM: Disruption, Strategic Non-Compliance and Sandbox as a containment device. International Journal of Automation and Digital Transformation, 5(1), 54-73.
https://doi.org/10.54878/skb87278

ABSTRACT

This paper makes a unifying argument: a significant share of FinTech innovation is structured as "regulatory nihilism" – a strategic behavior of intentional devaluation of existing normativity when it hinders time-to-market, scalability, and network rent-grabbing. This nihilism is not taken here in a metaphysical sense, but as an institutional translation of a philosophical core: the loss of binding force of values/forms, replaced by performative logics (adoption, growth, liquidity, engagement). In the absence of governance tools capable of operating with times and granularities compatible with digital markets, selective non-compliance becomes rational for the innovator and destabilizing for the system.

The main contribution is twofold. First, it proposes a conceptual framework that integrates genealogy of nihilism (Jacobi, Nietzsche, Heidegger) with institutional theory and "code-as-law", formulating the construct of regulatory nihilism as: (i) arbitrage and forum shopping; (ii) temporal non-compliance ("move fast, regularize later"); (iii) cosmetic compliance; (iv) fragmentation of responsibility along the digital stack. Second, he argues that the regulatory sandbox represents – within a certain perimeter – the only realistic tool for containing nihilistic disruption, since it converts anti-institutional energy into experimentation under constraints, observable data and exit rules.

Methodology: interdisciplinary theoretical analysis and institutional comparison of sandbox models (FCA-UK, MAS-Singapore, BCB-Brazil) and the European framework (DLT Pilot Regime; MiCA; DORA). The paper develops a set of testable hypotheses and a design grid to assess efficacy, risks (capture, moral hazard, cyber) and transfer conditions from experiment to market.

Keywords: *FinTech; DeFi; Regulatory sandbox; Regulatory arbitrage; Code-as-law; Institutional nihilism; RegTech; SupTech.*

Introduction:

In the public lexicon, "disruption" is often celebrated as a creative rupture: innovating means reducing costs, improving the user experience, including the unbanked. However, in the financial industry, disruption is not neutral: it affects stability, protection of savings, market integrity and systemic trust. When innovation is built "against" the rule – and not "inside" the rule – conflict becomes structural. Many FinTechs have taken competitive advantage from moving at the margins, taking advantage of gray areas, differences between jurisdictions, and enforcement delays. The result is a dynamic that this paper defines as regulatory nihilism: the norm is not treated as an ex-ante constraint, but as a friction to be circumvented, postponed or reinterpreted ex post.

The thesis does not imply that all FinTechs are 'anti-regulation' by nature, nor that innovation is incompatible with protection. Rather, he argues that in high-speed digital contexts (APIs, platforms, DLT/crypto) a perverse balance is created: (i) selective non-compliance is rational for those seeking scale; (ii) traditional enforcement is often late or binary (allows or prohibits); (iii) the ex ante regulation is likely to be either too rigid or too slow; (iv) the system absorbs risk until a critical event emerges (run, hack, fraud, data loss) and then reacts discontinuously and costly.

In this framework, regulatory sandboxes take on a role that goes beyond pro-innovation rhetoric: they become containment and adaptive governance devices. The sandbox allows experimentation under constraints, defining quantitative limits (customers/volumes), safeguards, disclosure, reporting and -above all - an exit path (full authorization or orderly termination). In other words, it converts a potential transgression into an observable and controllable institutional process.

1.1 Research applications and contributions

RQ1. In what forms does FinTech disruption manifest itself as strategic non-compliance and what mechanisms make it rational?

RQ2. How can the philosophical concept of nihilism be translated into an institutional construct applicable to law and financial regulation?

RQ3. In what sense is the sandbox a containment device (and not just a promotional one) and what conditions determine its effectiveness?

RQ4. How does the problem change in the presence of DLT/crypto/DeFi, where accountability and territoriality are weakened?

RQ5. What design choices (eligibility, caps, disclosure, reporting, exit) minimize arbitrage, capture and moral hazard?

Contributions: (i) strict definition of "regulatory nihilism" as an analytical category; (ii) causal mechanism linking micro incentives (time-to-market) to macro risks (systemic confidence); (iii) comparative grid and operational propositions for 'data-native' sandboxes; (iv) integration of the EU case through DLT Pilot Regime, MiCA and DORA, as an architecture that links experimentation to operational resilience and ICT risk governance.

1.1. Specific answers to research questions

RQ1. In what forms does FinTech disruption manifest itself as strategic non-compliance and what mechanisms make it rational?

FinTech disruption manifests itself as strategic non-compliance when innovation is designed to achieve scale and speed advantages by shifting (or avoiding) the regulatory burden away from economically equivalent financial functions. The behavior is rational because it combines first-mover advantage and increasing returns from the network with regulatory typing delays,

information asymmetries and often ex post enforcement.

The recurring operating forms are:

- Arbitrage and forum shopping: choice of jurisdictions, licenses or lighter corporate forms for the same economic activity.
- Temporal non-compliance: launch in the gray area to build user base and negotiating power ('move fast, regularize later').
- Cosmetic compliance: obligations oriented towards perception (disclosure and UX) rather than substance (suitability, governance, controls).
- Fragmentation of accountability: cloud/API outsourcing, partnerships with licensed parties, multi-entity structures that disperse responsibilities.
- Replacement of the rule with the architecture (code-as-law): own technical constraints, not equivalent to legal ones.

RQ2. How does the philosophical concept of nihilism translate into an institutional construct applicable to law and financial regulation?

The translation is functional: FinTechs are not attributed a doctrine, but a practical outcome like modern nihilism is identified: devaluation of the foundation and replacement of the legitimation criterion with performance. Jacobi thematizes the erosion of reality as a content of truth; Nietzsche describes the devaluation of values and the shift towards power/result logics; Heidegger connects nihilism and technology as a reduction of meaning to what is calculable and available.

In institutional terms, this becomes the loss of binding force of the rule as an ex-ante constraint and replacement with market metrics (adoption, growth, liquidity). Operationally, regulatory nihilism is defined as intentional devaluation of existing normativity when it hinders time-to-market and scale, achieved through arbitrage, postponement of compliance, cosmetic compliance, and fragmentation of accountability.

RQ3. In what sense is the sandbox a containment device and what conditions determine its effectiveness?

The sandbox contains because it converts potential transgression into an institutional contract of experimentation: limited operating space in exchange for observable constraints, safeguards, reporting, and exit rules. It is therefore not a simple pro-innovation derogation, but adaptive governance oriented towards control and learning.

The conditions of effectiveness are:

- Credible perimeter: caps on customers, volumes and duration, with effective ability to interrupt the test.
- Non-negotiable safeguards (customer protection, security, AML/CFT where relevant) and technical measures proportionate to the risk.
- Standardized reporting and mandatory post-mortem: the sandbox must produce reusable evidence (guidance, standards).
- Mandatory exit: full authorization or orderly termination; avoid indefinite permanence ('sandbox laundering').
- Anti-capture safeguards: transparency, justification of decisions, conflict management, program audit.

RQ4. How does the problem change with DLT/crypto/DeFi, where accountability and territoriality are weakened?

With DLT/crypto/DeFi, regulatory nihilism tends to intensify because the regulated object is more difficult to typify, the value chain is global and disintermediated, liability can be 'without a subject' (smart contract) or mediated by interfaces and providers, and the irreversibility of transactions increases the ex-post damage. It follows that the sandbox must move towards observability and technical risk control:

- Code audit and change management (versioning, upgradeability, admin keys).
- Telemetry and on-chain monitoring with liquidity, concentration and anomaly indicators.
- Controls on oracles and bridges (main vectors of accidents) and management of technical dependencies.
- Emergency governance and stop/pause procedures compatible with user protection.
- Consistency with ICT and third-party resiliency requirements (DORA-like logic) already in the testing phase.

RQ5. What design choices minimize arbitrage, capture, and moral hazard in sandboxes?

The most effective choices make the sandbox unexploitable as arbitrage, not interpretable as a 'sticker' and productive of regulatory outputs. In practice:

- Public and motivated eligibility: replicable criteria and statistics on admissions/rejections with reasons.
- Stringent and graduated caps; user segmentation (retail/professional) and exposure limits.
- Clear disclosure on the experimental nature and refund/escrow mechanisms when applicable.
- Comparable reporting (standard formats) and post-mortem/lessons learned obligation.
- Defined and time-boxed exit path; No indefinite renewals without public motivation.
- Anti-capture governance: reviewer rotation, independent committees, conflict registers, external audits.
- Minimum security and resilience requirements (cyber testing, incident response, third-party management).

2. THEORETICAL FRAMEWORK: FROM PHILOSOPHICAL NIHILISM TO REGULATORY NIHILISM

Theoretical clarification: in the following we explicitly distinguish between (a) *regulatory arbitrage* and (b) *regulatory nihilism*. Regulatory arbitrage is a tactical behavior: the operator identifies asymmetries, gaps or "folds" in the applicable discipline (jurisdictional, definitional or perimeter) and exploits them to minimize constraints and costs, while recognizing the rule as a source of external legitimacy. Regulatory nihilism is conceptually more radical: it is not equivalent to mere disobedience, but to the devaluation of the norm as a source of meaning and order, replaced by the idea that technological performance - code (software), protocols, and metrics - is ontologically superior to the law because it is more efficient, verifiable, and calculable. In this perspective, legality is reinterpreted as temporary 'friction' that the technical system can circumvent, compress or render irrelevant; legitimacy no longer derives from the State, but from the ability of the code to produce measurable outcomes (scalability, resilience, automation) and to impose a new form of immanent normativity (rule-by-code).

2.1. Genealogy of Nihilism: Jacobi, Nietzsche, Heidegger

The term "nihilism" enters the modern European lexicon with the late eighteenth-century polemical use and with F. H. Jacobi's critique of post-Kantian idealism: the accusation is that a philosophy that dissolves reality into representation produces a 'nihilistic' outcome, that is, the loss of consistency of the world as a content of truth. This matrix is relevant because it introduces a typical trait of modern nihilism: it is not a simple negation, but an erosion of the foundations of legitimation.

With Nietzsche, nihilism becomes a historical diagnosis: the "death of God" means the collapse of the transcendent sources of value and the devaluation of the final horizons. The

Nietzschean formula ("the purpose is missing; the answer to why is missing; all values are devalued") should not be read as a slogan, but as a structure: when a system of values loses strength, action tends to orient itself towards substitutive criteria (power, immediate utility, performative success).

Heidegger interprets nihilism as the fulfillment of Western metaphysics and connects it to technology: modernity reveals the real as an available fund (Bestand), measurable and usable. Technique is not a set of tools, but a mode of relationship that privileges calculability and domination. In this perspective, nihilism is not the absence of rules, but the reduction of meaning to what is operationalized.

2.2. Institutional translation: nihilism as a devaluation of normativity

Transposition to the regulatory field requires methodological caution. The paper does not attribute an explicit philosophy to FinTechs but identifies a functionally equivalent dynamic: the devaluation of normativity as an ex-ante constraint. In law, the rule is not just command; it is also a promise of predictability, protection and trust. When operators treat rules as obstacles to be circumvented (rather than coordinates of legitimation), there is a 'practical collapse' of the foundation: the rule remains written but loses performative effectiveness.

Proposed operational definition: Regulatory nihilism is a set of strategies by which an innovative firm maximizes growth and scale by escaping, in whole or in part, the regime of responsibility and control provided for equivalent financial functions. It is recognizable through four recurring vectors: (1) arbitrage and forum shopping; (2) temporal non-compliance; (3) cosmetic compliance; (4) fragmentation of responsibility.

2.3. The link with 'code-as-law': when the rule is replaced by the architecture

2.4. The transition from legal regulation to architectural regulation (code-as-law) strengthens the plausibility of the category. In digital platforms, constraints and incentives are embedded in the software: terms of service, UI/UX, pricing algorithms, smart contracts, settlement mechanisms. The legal norm retains strength but competes with a level of technical rules that operates in real time and often without negotiation. Here the Heideggerian core emerges: what matters tends to become what is measurable/implementable. Compliance is transformed into parameters, and values (proportionality, equity, adequacy) risk being 'degraded' if not translatable into code.

3. CAUSAL MECHANISM: WHY NON-COMPLIANCE IS RATIONAL AND WHY IT IS DESTABILIZING

3.1. Microeconomic incentives: time-to-market, network effects and real option

Many FinTech models are platform-based: growth generates increasing returns (network effects), reduces unit costs and builds lock-ins. In this scenario, speed is a strategic asset. Full and immediate compliance with rules designed for traditional intermediaries may be incompatible with competitive dynamics. The result is an opportunistic rationality: the company maximizes the real option of expansion today and internalizes compliance costs tomorrow, when the user base and collection allow legal and capital costs to be incurred.

3.2. Inverse information asymmetry and enforcement delay

The regulator faces a problem of knowledge: the innovator knows technology, risk and architecture; The authority learns by incomplete and delayed signals. This creates inverse information asymmetry and makes late enforcement more likely. When the intervention arrives, the company may already be systemically relevant or, on the contrary, it may dissolve (insolvency, exit,

foreign jurisdiction), leaving externalities on consumers and the market.

3.3. Macro outcomes: erosion of regulated trust and downward competition

If selective non-compliance generates competitive advantage, the system produces downward competition: incumbents are pressured to 'loosen' controls, replicate aggressive UX or outsource functions to reduce costs. In this way, regulatory nihilism does not remain confined to FinTechs: it infects the competitive structure and reduces the credibility of the legal system. The result is an increase in risk (conduct, operational, cyber) and, in cases of high scale, potential impacts on financial stability.

4. REGULATORY SANDBOXES: FROM PRO-INNOVATION RHETORIC TO INSTITUTIONAL RESTRAINT

4.1. Central thesis: the sandbox as a non-compliance conversion device

If the problem is strategic non-compliance that exploits delays and ambiguities, containment requires a tool capable of operating 'in real time' and with granularity comparable to that of innovation. The sandbox offers exactly that: it allows experimentation with targeted waivers but, in return, imposes observable constraints (caps), safeguards, disclosure, reporting, and a liability regime. The key step is that the transgression is traced back to a legitimized and controlled perimeter.

4.2. Why are traditional enforcement and rulemaking not enough

Ex-post enforcement is often binary: sanction or prohibition. This can be effective against fraud and abuse, but it is less suitable for ambiguous innovations where the problem is to define the regulated object. Ex ante regulation, on the other hand, takes a long time and risks stiffening. The sandbox fills the gap: it produces regulatory learning and allows for proportionate control before the mass market.

4.3. Empirical evidence: sandbox and access to capital

A quantitative line of evidence on the UK case suggests that sandbox entry can improve access to capital and business outcomes. Cornelli et al. document that sandbox entry is associated with increased capital raising and likelihood of funding, as well as improved survival rates and patent activity (Cornelli et al., BIS Working Paper 901; SSRN version). These results are consistent with the interpretation of the sandbox as a credible signal of quality and as a reduction in the regulatory uncertainty perceived by investors.

5. BENCHMARKING: FCA (UK), MAS (SINGAPORE), BCB (BRAZIL), EUROPEAN UNION

5.1. FCA - United Kingdom

The British model defines the sandbox as a testing space with real customers under regulatory control. A distinctive feature is the emphasis on safeguards and consumer detriment: limits on exposures and volumes, enhanced disclosure and reporting are calibrated to the risk profile. The sandbox thus operates as a containment channel: it admits experimentation, but makes observable and 'interruptible' what, outside the fence, would manifest itself as competitive non-compliance.

5.2. MAS - Singapore

Singapore combines a case-by-case sandbox with a fast lane (Sandbox Express) for standardizable categories. Express reduces time-to-market and offers predefined parameters (duration, caps, categories), balancing disruption control and program scalability. In terms of regulatory nihilism, a fast and predictable lane reduces the incentive to 'run outside' the perimeter.

5.3. BCB - Brazil

Brazil has set up a controlled testing environment with rules on admission,

duration, operating limits, and information requirements. The design emphasizes the controllability of the perimeter and the possibility of intervention by authority: experimentation as an institutional contract, not as an indefinite suspension of the rule.

5.4. European Union: DLT Pilot Regime, MiCA, DORA

In the European context, sandbox logic is embedded in EU-level instruments. The DLT Pilot Regime (EU Reg. 2022/858) establishes a pilot regime for DLT-based market infrastructures, allowing for targeted derogations within thresholds and conditions. MiCA (EU Reg. 2023/1114) introduces a horizontal framework for crypto-assets: application from 30 December 2024, with rules on ART and EMT applicable from 30 June 2024. DORA (EU Reg. 2022/2554) imposes digital operational resilience with application from 17 January 2025. The combination of these tools binds experimentation to structural requirements of ICT governance, protection and resilience.

SIZE	DESIGN CHOICE	RISK IF WEAK	METRICS/OUTPUTS
ELIGIBILITY	Innovation + expected benefit + need for testing + readiness	Arbitrage and opportunistic selection	Admission rate; Grounds for rejection
PERIMETER (CAPS)	Customer limits/volumes/duration; User categories	Premature scales; consumer detriment	Accidents; complaints; breach caps
SAFEGUARDS	Disclosure; escrow; capital add-ons; Cyber Testing	Moral hazard; consumer damage	Remediation; audit findings
REPORTING	Standard datasets and reports; Mandatory post-mortem	No regulatory learning	Guidance produced; Standard
EXIT	Full authorization or orderly termination	'Sandbox laundering'	Time-to-license; drop-out
ANTI-CAPTURE	Transparency; reviewer rotation; conflicts; Audit	Privileges; Capture	Audit governance; Decision variance
ICT COHERENCE	ICT and third-party governance (DORA-like)	Systemic cyber risk	Incident reporting; testing; concentration

6. DESIGN GRID: WHEN THE SANDBOX REALLY CONTAINS REGULATORY NIHILISM

If strategic non-compliance is assumed to be an integral part of disruption, then the sandbox must be designed not as a "space of tolerance", but as a device for bringing innovation back within a perimeter of responsibility. In institutional terms, the sandbox only works if it transforms a competitive advantage based on circumvention (or referral) into an advantage based on verifiable quality, data and transferability. Hence a rule of method: any derogation or flexibility granted must have an equivalent in terms of (i) controllability; (ii) protection; (iii) production of evidence.

6.1. Operational objectives and KPIs: from the "pro-innovation" programme to the "pro-evidence" programme

A containment-oriented sandbox program must spell out measurable goals. In the

absence of KPIs, the sandbox risks becoming a reputation channel or arbitrage accelerator. There are four recommended objectives: protection, stability/operation, fair competition and regulatory learning. Ex-ante and ex-post indicators must be associated with each objective.

Protection: number and severity of claims, reimbursement rate, expected losses (EL) and realized losses.

Stability/operationality: ICT/cyber incidents, downtime, process failures (e.g. reconciliations), liquidity/collateral stress.

Fair competition: evidence of equivalence-of-regulation with respect to similar functions, reduction of advantages due to gray areas.

Learning: published guidance/standards, dataset reuse, typing times (from experimentation to rule/authorization).

6.2. Eligibility: test-necessity and 'functional equivalence'

Admission criteria are the first barrier against regulatory nihilism. Eligibility must avoid two extremes: (i) admitting projects that could already operate under ordinary rules (sandbox as a shortcut); (ii) reject truly new innovations because they do not fall under pre-existing taxonomies. A criterion with four cumulative thresholds is proposed:

- Substantial innovation (not mere re-packaging): new risk model, new channel, new architecture or new combination of functions.
- Verifiable expected benefit: measurable efficiency, inclusion, cost reduction, improved transparency or resilience.
- Need for testing in a controlled environment: regulatory/technical uncertainty that makes the full ex ante authorization disproportionate.
- Minimal readiness: governance, risk management, security, reporting and remediation capabilities (not an immature 'prototype').

A crucial element is functional equivalence: if the activity produces economic effects similar to a regulated service (payments, deposit, credit, placement, custody), then the sandbox must impose equivalent safeguards on the main risks, albeit with proportionality (limits and duration).

6.3. Perimeter and caps: making transgression 'low intensity'

The cap is the tool with which the sandbox neutralizes the advantage of 'growing first and then regularizing'. Without credible caps, the sandbox becomes a license of scale. Caps must be multi-dimensional and dynamic (step-up):

- Customer caps: maximum number of customers, segmentation (retail/professional), eligibility criteria and suitability.
- Exposure caps: ceiling per client, total ceiling, leverage limits or maturity mismatch.
- Time caps: defined duration and intermediate milestones (go/no-go).
- Geographical caps: jurisdictional perimeter, geofencing where applicable, controlled acquisition channels.
- Product caps: limitation of risky features (e.g. margins, auto-rollover, volatile collateral) until validation.

The step-up design allows you to gradually increase the limits when control thresholds are reached (audit completed, incident rate below threshold, compliance data pipeline working). This aligns incentives: growth in exchange for evidence.

6.4. Safeguards: protection as the 'internal cost' of the experiment

If the sandbox must contain regulatory nihilism, protection cannot be entrusted only to disclosure. A combination of informational, economic and technical safeguards is needed:

- Strengthened and understandable disclosure: experimental nature, specific risks, absence of guarantees, complaint and reimbursement mechanisms.
- Economic protection mechanisms: escrow, segregation of funds, loss limits, remediation funds, insurance where available.
- Risk governance: conflict policy, customer treatment, incentives and commissions, complaint management, anti-fraud.
- Proportionate but effective AML/CFT controls (for on-/off-ramp and cross-border transfers).
- Technical security: penetration testing, secure development lifecycle, vulnerability management and incident response.

In the Nietzschean logic of the devaluation of values, 'protection' risks being treated as an external cost. The sandbox must make it an internal cost and a condition of permanence in the program.

6.5. Data-native reporting: what is not measured is not governed

The sandbox produces public value only if it produces data. Reporting cannot be a narrative fulfillment; It must be a standardized and auditable data pipeline. A three-tier model is recommended:

1. Baseline dataset (minimum common): volumes, customers, pricing/fees, operational events, complaints, remediation, key risk metrics.
2. Risk-specific dataset: credit metrics (PD/LGD), payments (failure rate), custody (asset segregation), market/investment (suitability).
3. Technical dataset (ICT/cyber): incidents, vulnerabilities, recovery times, third-party dependencies, change logs.

4. Post-mortem is mandatory: each test must produce a final report with results, incidents, remediation and recommendations, even (especially) when the test fails. Bankruptcy is regulatory information.

6.6. Exit: the point at which the sandbox proves to contain

The most important condition against sandbox laundering is a credible exit. The exit must be defined from the beginning as a binary and verifiable path: full authorization or ordered termination. Containment is only real if cessation is practicable and non-destructive.

5. Ex-ante exit plan: licensing requirements, timeline, compliance deliverables, and conditions for extending (only exceptionally).
6. Orderly termination: data portability, return of funds, closing positions, customer communication and wind-down supervision.
7. Transferability: explicit mapping between experimental control and ordinary requirement (how the test 'translates' into compliance).

6.7. Program governance: anti-capture and competitive symmetry

The sandbox concentrates discretionary power. To avoid capture and favouritism, the programme must adopt institutional controls: public criteria, committees with mixed competences, rotation of evaluators, conflict registers and regular external audits. The goal is to maintain competitive symmetry: the sandbox must not create regulatory rents but reduce non-compliance revenues.

6.8. Integration with the EU architecture: ex-ante coherence (MiCA/DORA/DLT Pilot)

In the European perimeter, the sandbox cannot be thought of as a regulatory island. For crypto and DLT activities, the test must already be designed in line with the structural requirements: (i) governance and whitepaper/disclosure (MiCA logic); (ii) digital operational resilience and ICT third-party management (DORA logic); (iii) constraints of

the pilot regime for DLT market infrastructures. This reduces the incentive to 'jump' from experimentation to a non-compliant market.

7. DLT/crypto/DeFi: when regulatory nihilism becomes 'architectural'

DeFi and DLT pose a structural problem to the traditional sandbox logic: the absence or fragmentation of the responsible legal entity (no single 'operator', distributed governance, open-source development, admin keys or DAOs) makes it difficult to replicate the implicit "Enterprise Authority ↔" contractual model. It follows that, for DeFi cases, the sandbox must evolve from a procedural perimeter (derogation/caps/reporting) to *embedded supervision*: supervision capability embedded in the infrastructure itself.

Operationally, embedded supervision can be implemented in two complementary ways: (i) the sandbox as a monitoring 'layer' that integrates on-chain and off-chain telemetry with standardized data schemas and automated controls; (ii) the sandbox as a node (or service) that interacts with the network/protocol through monitoring smart contracts (e.g., regulatory oracles or contract-hooks) capable of reading events, flows and risk parameters in near real time (liquidity, leverage, exposures, upgrades, anomalous movements). In this paradigm, the "contract" of the sandbox is not only legal, but also technical: constraints and caps can become executable rules (policy-as-code), with stop, throttling or wind-down triggers that can be activated on predefined conditions.

The audit of the code, in this context, takes on an epistemic as well as a technical meaning. In a 'nihilistic' environment—where external normativity is rejected and the superiority of calculation is affirmed—the audit (static/dynamic analysis, formal verification where possible, independent review, bug bounty) becomes the main device for re-establishing a form of verifiable 'truth': not so much compliance with an external rule, but the ex ante verifiability of the properties of the system (safety, liveness, access control, upgradeability, key management) and the ex-post traceability of deviations. In other words, the audit is the place where the code's claim to self-sufficiency is tested and made translating into liability.

7.1. Why DeFi amplifies non-compliance

In DeFi, the devaluation of the norm can take a radical form: the implicit idea that the rule is replaceable by the protocol. This is a fully 'Heideggerian' declination: what matters is what can be implemented in the code. The regulatory consequence is threefold: absence or ambiguity of the responsible party; composability that multiplies interdependencies; Mutation speed via upgrade/fork.

8. Widespread accountability: Developers, governance token holders, DAOs, front-end operators, and infrastructure providers have partial roles.
9. Composability: a risk in one protocol (oracle/bridge) spreads to many others (technical contagion).
10. Irreversibility: ex post is often ineffective; We need prevention and containment ex ante.

7.2. Regulatory leverage points: from the 'subject' to the 'system'

A sandbox for DLT/DeFi ecosystems must define ex-ante the control points where accountability and observability can be imposed:

11. Front-end and distribution: KYC/controls were required, disclosure, geofencing, non-deceptive UX design.
12. On/off-ramp and custody: requirements on segregation, governance, AML/CFT and incident management.
13. Code audit and assurance: minimum requirements for independent audit, bug bounty, vulnerability disclosure.

14. Oracles and bridges: stress testing and technical dependency control, compromise response plans.
15. Emergency governance: Clear procedures on pauses, upgrades, key revocation, and user communications.

7.3. Data-native sandbox and embedded supervision

To overcome the observability deficit, the sandbox should experiment with embedded supervision models: reporting requirements embedded in the same architecture (standard on-chain events, claims, logs). This reduces supervisory costs and makes compliance timelier. The condition is to prevent embedded supervision from becoming pure meaningless metricization: metrics must map real risks (liquidity, concentration, vulnerability, manipulation) and not just volumes.

8. RISKS AND FAILURE MODE: HOW AND WHY A SANDBOX CAN FAIL

8.1. Sandbox as regulatory arbitrage

Typical failure mode: the sandbox is perceived as a reduced license and becomes an internal forum shopping tool. Mitigations: strict eligibility, functional equivalence, stringent caps and mapping of requirements to ordinary authorization.

8.2. Reputational 'sticker' and moral hazard towards consumers

If the public interprets admission as a safety certification, the risk of over-adoption and harm increases. Mitigations: standardized disclosure, exposure limits, escrow/remediation, and consistent public disclosure (sandbox is not a guarantee).

8.3. Capture, favouritism and distortions of competition

Informational proximity can produce cognitive capture: the regulator adopts the narrative of the innovator and constructs ad hoc exceptions. Mitigations: Program governance, reviewer rotation, external audits, publication of justifications and decision statistics.

8.4. Operational and cyber risk: transferring risk from the laboratory to the market

In cloud-based and API-based ecosystems, an incident can propagate quickly. If the sandbox does not include minimum ICT requirements, the experiment can become a systemic event. Mitigations: Minimum DORA-like requirements (incident reporting, testing, third-party management, continuity).

8.5. Transferability problem: 'learning' without translating

A sandbox can generate data but not generate rules: learning without translation. Mitigations: obligation of regulatory outputs (guidance, Q&A, technical standards) and internal processes that transform evidence into regulatory or supervisory intervention.

9. TESTABLE HYPOTHESES AND EMPIRICAL DESIGN: OPERATIONALIZATION AND IDENTIFICATION

This section is included to make the thesis of the article scientifically falsifiable and, therefore, assessable according to the standards of indexed journals. In particular, the qualification of FinTechs as forms of "regulatory nihilism" (intentional non-compliance as a lever of growth/disruption) requires a shift from the theoretical-philosophical framework to an empirical design that specifies: (i) units of analysis; (ii) observable variables; (iii) causal identification strategies in the presence of self-selection and selection by sandbox programs; (iv) falsification criteria. For terminological clarity, we use: RQ = Research Question; H = hypothesis; IV = Independent Variable; DV = Dependent Variable. The empirical methods are referred to with standard acronyms: DiD = difference-in-differences; PSM = propensity score matching; CEM = coarsened exact matching; RD = regression discontinuity.

Specification of sources (to strengthen replicability and empirical soundness). For H1 (temporal non-compliance), 'grey starts' can be measured by triangulating: (i) databases of enforcement actions and official communications from authorities (e.g. SEC and CFTC for USA; FCA for UK; and, where available, EU national registers) with extraction of dates, cases and subject matter of the survey; (ii) product launch and go-to-market histories reconstructed from public sources (press releases, changelogs/app releases, web archives, and industry/tech news) to identify discrepancies between date of operation and authorization status; (iii) licensing registers and public registers to verify authorization times and any jurisdictional migrations. For matching/PSM, in addition to sector and country, covariates must include at least: pre-sandbox funding (amount and stage), age of the company, pre-admission traction, and proxies of the technical profile of the team (share of engineering/security roles, experience in critical infrastructures, open-source track record), so as to isolate the 'certification' effect of the sandbox from readiness and intrinsic quality.

To consolidate the contribution on academic standards, the empirical section must (i) make the proposed causal link falsifiable; (ii) define units of analysis, variables and measurable proxies; (iii) explicitly address the problem of selection (endogeneity) typical of sandbox programs. The formulation of 'H + measurement + data + identification strategy' is therefore adopted.

9.1. RQ Map → Hypothesis

RESEARCH QUESTION (RQ)	RELATED HYPOTHESES	EMPIRICAL OBJECT (SYNTHESIS)
RQ1 **(forms and rationality of non-compliance)**	H1-H2	Incentives and proxies of strategic/temporal non-compliance; relationship with arbitrage and 'grey' start-up.
RQ3 **(sandbox as containment)**	H3-H5	Effects of design (caps, reporting, exit) on detriment, accidents, transferability and exit outcomes.
RQ4 **(DLT/DeFi)**	H6	Technical assurance (audit, on-chain telemetry) and reduction of incidents/losses.
RQ5 **(Anti-Arbitrage /Capture /Moral Hazard)**	H7-H8	Transparency, anti-capture governance and ICT requirements (DORA-like) as determinants of effectiveness and resilience.

1.1. Assumption

Main unit of analysis: company candidate/admitted to the sandbox (micro level) and sandbox cohort (meso level). Time horizon: 6-24 months from admission (or rejection decision) for funding and growth outcomes; the entire testing period for incidents and compliance

HYPOTHESIS	STATEMENT	IV (PROXY)	DV (PROXY)	FORGERY / NOTES (SELECTION)
H1	Incentives (network effects, first-movers) → greater temporal non-compliance.	Network effects (user growth, referrals, two-sided metrics), platform-based, market concentration.	'Grey' launches measured via triangulation: (a) enforcement actions/letters and regulatory communications (SEC/CFTC/FCA and similar registries); (b) product launch dates (press release, app release/changelog, web archives, tech news); (c) status and timing of authorization from licensing registries; (d) jurisdictional migration and changes of dismissed partners.	No reports once checked by sector/country and readiness (prefunding, age, traction, technical team profile).
H2	Multi-size caps + stop authority → reduction of consumer detriment.	Severity index caps + stop authority.	complaints/1,000; losses per customer; chargebacks; accidents; remediation and timing.	DV unchanged or worsened with tighter caps.
H3	Admission to the sandbox as a signal → more funding and better survival.	Dummy admission + timing; Strict requirements.	Funding 6/12/24 months; round probability; hazard failure; time-to-license.	Selection correction: matching/PSM; EF cohort/sector.
H4	Standard + post-mortem reporting → more output and less ex post heterogeneity.	Reporting maturity index (dataset, auditability, post-mortem).	Output (guidance/Q&A/standard); variance conditions; orderly exit.	Output does not grow or variance increases.
H5	Time-boxed exit + ex ante	Time-box; public exit	Test duration; renewals; exit with wind-down;	Duration does not decrease and

	criteria → less sandbox laundering.	criteria; limitation of renewals; internal enforcement.	repeated re-entry.	renewals remain high.
H6	DLT/DeFi: Code audit + telemetry → fewer incidents/losses.	Independent audit, bug bounty, telemetry, change management.	Exploits/incidents; downtime; losses; liquidity anomalies; detection/response.	Accidents are not decreasing or increasing.
H7	Anti-capture → greater fairness and credibility.	Anti-capture index (transparency, audit, rotation, conflicts).	HHI admissions; appeals; post-exit revocation/remediation.	Concentration/disputes do not improve.
H8	'DORA-like' ICT requirements → resilience and continuity.	Minimum requirements (incident reporting, testing, TPRM, BC/DR).	Accidents; MTTR; downtime; vulnerability; provider concentration.	No systematic improvement or deterioration.

1.2. Identification data and strategies

The main methodological risk is endogeneity: sandboxes select companies that are more ready (selection) and companies choose whether to apply (self-selection). A multi-method design with triangulation is recommended.

METHOD	MAIN USE	ASSUMPTIONS/MITIGATIONS	REQUIRED DATA
DiD	Pre/post outcomes: admitted vs not admitted.	Parallel trends; FE; placebo and pre-trend tests.	Admission/rejection dates; outcome; covariate enterprise.
Matching /PSM/CEM	Build comparable ex ante control.	Selection-on-observables; balancing; sensitivity. Recommended covariates: pre-sandbox funding (amount/stage), pre-traction, company age, and technical team profile (engineering/security) to isolate the 'certification' effect.	Stadium, sector, prefunding, country, team size.

RD	Take advantage of cutoff scoring/thresholds.	No handling; density testing; Robustness bandwidth.	Score, threshold, outcome, covariates.
Event study	Dynamics around the event (announcement/admission) .	No anticipation; shock checks; Multiple windows.	Funding/user time series; event dates.
Survival	Hazard failure and time-to-license.	Censorship; hazard specification; time-variant covariates.	Dates of birth/termination; licensing; accidents.
Text-as-data	It encodes conditions and severity/maturity indices.	Coding reliability; inter-coder validation.	Sandbox documents; conditions; reports.
Process tracing	Causal chain on incidents (DLT/DeFi).	Triangulation sources; verifiable histories.	Audit; incident reports; on-chain data; governance logs.

9.3.1. Enforcement Proxies: Fines and Sanctioning Actions (2023-2024)

REGULATOR	PERIOD	PERIMETER PROXY	METRICS	SYNTHETIC VALUE	USE IN THE MODEL
SEC (USA)	2023-2024	Crypto/digital assets	No. of shares; Estimated penalties	46 (2023), 33 (2024); ~$2.89 billion (2023), ~$4.98 billion (2024)	Context (pressure) and outcome (ex post containment).
CFTC (USA)	FY2024	Digital assets (including cases)	Monetary relief (total)	>USD 17.1bn (FY2024)	Proxy intensity enforcement/deterrent capacity.
FCA (UK)	2022/23-2023/24	Baseline enforcement (context)	Penalties: n. and amount	£199.3m (2022/23); ~£42m (2023/24)	Cross-country institutional control.

2. POLICY RECOMMENDATIONS: SANDBOX AS AN 'INSTITUTIONAL CONTRACT' AGAINST REGULATORY NIHILISM

This section translates the theoretical-empirical result into actionable policy implications. If the "regulatory nihilism" of FinTechs is interpreted as a structural incentive to operate in the gray area (until full compliance becomes necessary), then the regulatory sandbox cannot be treated as a mere temporary derogation, but as an "institutional contract" that conditions experimentation to greater observability, accountability and reversibility. The recommendations are then expressed in an operational form (responsible actor, instrument, trade-off and internal enforcement mechanism) to avoid generic conclusions. Main acronyms: RegTech = regulatory technology (technological solutions for compliance); SupTech = supervisory technology; KPIs = Key Performance Indicators; MoU = Memorandum of Understanding; SLA = Service Level Agreement; HHI = Herfindahl-Hirschman Index (concentration index); ICT = Information and Communication Technologies; BC/DR = Business Continuity/Disaster Recovery; MTTR = Mean Time To Recovery. EU references cited: MiCA = Markets

in Crypto-Assets Regulation; DORA = Digital Operational Resilience Act; DLT = Distributed Ledger Technology; DeFi = Decentralized Finance.

KPI reinforcement: in addition to micro outcomes (share of companies that obtain licenses, incident rates, remediation), a key indicator of sandbox success is measurable *regulatory learning*: number of guidelines, Q&A, technical standards and ex ante interpretative or regulatory changes produced by the authority starting from the test evidence; publication times; degree of reuse of evidence in subsequent cases (reduction of decision variance). EU/DORA consistency: The sandbox can also serve as a controlled environment to test, in a proportionate manner, Business Continuity/Disaster Recovery and incident reporting—anticipating and making more efficient the adoption of Digital Operational Resilience (DORA) requirements for critical ICT operators and providers, prior to the full operation of the presidia at scale.

The recommendations follow the logic of 'containment = fair incentives + accountability + observability'. To make them implementable, each is formulated with: (i) the responsible actor; (ii) implementation tool (sandbox condition, guide, authorization requirement); (iii) trade-off and proportionality clause; (iv) enforcement mechanism within the sandbox (reduction of caps, stop, early exit).

Test Design (Micro): Conditions of Admission and Risk Management

R	ACTOR	TOOL	TRADE-OFF / PROPORTIONALITY	INTERNAL ENFORCEMENT
R1	Authority/Program	Multi-dimensional caps + step-ups on milestones.	Slows growth; Scalable low caps and clear milestones.	Reduction of caps or stop on thresholds/violations.
R2	Authority; RegTech/mentor	Readiness checklist as a gate to real customers.	Early-stage barrier; pre-sandbox dry-run → live testing.	Suspension if readiness degrades.
R3	Conducted Authority	Substantive protection: disclosure + loss limits; escrow; remediation; SLA complaints.	Cost; graduated thresholds for risk and segment.	Refund/compensation; early exit.
R4	Authority; SupTech	Data-native reporting (standard dataset + ICT) + post-mortem; API.	Costs; common minimum + modularity.	No reporting: step-up freeze; then stop.

2.1. Programme Governance (meso): anti-capture, transparency and competitive symmetry

R	ACTOR	TOOL	TRADE-OFF / PROPORTIONALITY	INTERNAL ENFORCEMENT
R5	Authority/Program	Decision-making transparency: criteria, statistics, KPIs.	Confidentiality: aggregated/anonymized disclosure.	Audit and periodic review of criteria.
R6	Authority; independent audit.	Anti-capture: rotation, conflicts, committees, audits, support/decision separation.	Bureaucracy: standardization and digitize.	Review of anomalous decisions; public reporting.
R7	Prudential authority/conduct	Functional equivalence and fair competition.	Risk over regulation: caps/duration instead of full requirements immediately.	Equivalence test in exit; conditional license.

9.2. Overall architecture (macro): coordination, SupTech and EU coherence

R	Actor	Tool	Trade-off / Proportionality	Internal Enforcement
R8	Authority + network	MoU and data-sharing; recognize evidence (not stickers).	Complexity: Minimum data set + common taxonomy.	Mutual alerts on violations/migrations.
R9	Authority; Data Drives	Sandbox as a SupTech/standards lab (APIs, data schemas, metrics).	Risk metricization: metrics linked to real and reviewed risks.	Standard as a step-up/exit condition.
R10	NCA+ESAs (EU)	Ex-ante consistency with MiCA/DORA/DLT Pilot already in the testing phase; integration of minimum operational resilience requirements (incident reporting, business continuity testing, ICT third-party management) as step-up conditions.	Start-up barrier: proportionate DORA-like requirements + maturation pathway; Use the sandbox to test BC/DR and incident reporting flows before fully extending obligations.	Exit/subordinate license; stop if ICT risk is not managed.

9.3. Implementation Note: Avoid 'Sandbox as Rule Suspension'

The most common mistake is treating the sandbox as a temporary suspension of rules. With a view to containing regulatory nihilism, the sandbox must instead be a form of regulation by evidence: targeted derogations only when they increase observability and reduce externalities. The guiding principle is: no flexibility without a corresponding increase in controllability (data, caps, liability, exit).

10. CONCLUSION

This work has brought FinTech disruption back to an often-eluded theoretical knot: innovation can produce value precisely because it suspends, postpones or circumvents the rule. Defining this dynamic as regulatory nihilism makes it possible to link micro incentives (time-to-market and network rents) to macro risks (trust, protection, operational stability) and to explain why traditional enforcement struggles to govern high-speed digital markets. The sandbox emerges as a containment device because it converts transgression into controlled and data-driven experimentation, imposing caps, safeguards, reporting and credible exits. In DLT/crypto/DeFi contexts, however, containment requires evolution: technical observability, code audits, and minimum ICT resilience requirements, otherwise the sandbox risks certifying what it cannot govern. The conclusion is operational: it is not enough to 'sandbox'; It is necessary to design sandboxes as institutions of learning and accountability, capable of depriving non-compliance of its competitive advantage and transforming disruption into legitimate innovation.

REFERENCES

Ahern, D. M. (2020). Regulators nurturing FinTech innovation: Global evolution of the regulatory sandbox as opportunity-based regulation. European Business Organization Law Review, 21, 1-49. https://doi.org/10.2139/ssrn.3552015

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of FinTech: A new post-crisis paradigm? Georgetown Journal of International Law, 47(4), 1271-1319. https://doi.org/10.2139/ssrn.2676553

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), 371-413. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1817&context=njilb

Banco Central do Brasil (BCB). (2020). Resolução BCB N° 29, de 26 de outubro de 2020 (Regulatory Sandbox). https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=29&tipo=Resolu%C3%A7%C3%A3o+BCB

Baudrillard, J. (1994). Simulacra and simulation (S. F. Glaser, Trans.). University of Michigan Press. (Original work published 1981).

Carr, K. L. (1992). The banalization of nihilism: Twentieth-century responses to meaninglessness. SUNY Press.

Commodity Futures Trading Commission (CFTC). (2024, December 4). CFTC releases FY 2024 enforcement results (Press Release No. 9011-24). https://www.cftc.gov/PressRoom/PressReleases/9011-24

Cornelli, G., Doerr, S., Gambacorta, L., & Merrouche, O. (2020). Inside the regulatory sandbox: Effects on fintech funding (BIS Working Papers No. 901). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3753901

Cornelli, G., Doerr, S., Gambacorta, L., & Merrouche, O. (2021). Regulatory sandboxes and fintech funding: Evidence from the UK (BIS Working Papers No. 901). Bank for International Settlements. https://www.bis.org/publ/work901.pdf

Cornerstone Research. (2024). SEC cryptocurrency enforcement: 2023 update. https://www.cornerstone.com/insights/reports/sec-cryptocurrency-enforcement-2023-update/

Cornerstone Research. (2025). SEC cryptocurrency enforcement: 2024 update. https://www.cornerstone.com/wp-content/uploads/2025/01/SEC-Cryptocurrency-Enforcement-2024-Update.pdf

Ehrentraud, J., Ocampo, D. G., Garzoni, L., & Piccolo, M. (2020). Policy responses to FinTech: A cross-country overview (FSI Insights No. 23). Bank for International Settlements. https://www.bis.org/fsi/publ/insights23.pdf

European Parliament. (2020). Regulatory sandboxes and innovation hubs for FinTech (IPOL Study 652752). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU%282020%29652752_EN.pdf

European Supervisory Authorities (EBA, EIOPA, ESMA). (2023). Update on the functioning of innovation facilitators - innovation hubs and regulatory sandboxes (ESA 2023 27, December 11, 2023). https://www.esma.europa.eu/sites/default/files/2023-12/ESA_2023_27_Joint_ESAs_Report_on_Innovation_Facilitators_2023.pdf

Financial Conduct Authority (FCA). (2017). Regulatory sandbox: Lessons learned report (Cohorts 1 and 2). https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf

Financial Conduct Authority (FCA). (2023). Annual report and accounts 2022/23. https://www.fca.org.uk/publication/annual-reports/annual-report-2022-23.pdf

Financial Conduct Authority (FCA). (2024). Annual report and accounts 2023/24. https://www.fca.org.uk/publication/annual-reports/annual-report-2023-24.pdf

Galimberti, U. (2007). L'ospite inquietante: Il nichilismo e i giovani. Feltrinelli.

Givone, S. (2015). Storia del nulla. Laterza.

Heidegger, M. (1953). Die Frage nach der Technik. In Vorträge und Aufsätze. Neske.

Heidegger, M. (1961). Nietzsche (Vols. 1-2). Neske.

Jacobi, F. H. (1799). Sendschreiben an Fichte (Letter to Fichte). In Fichtiana (modern editions).

Leopardi, G. (1997). Zibaldone. (Critical editions).

Monetary Authority of Singapore (MAS). (2018). FinTech regulatory sandbox guidelines (updated February 19, 2018). https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox/FinTech-Regulatory-Sandbox-Guidelines-19Feb2018.pdf

Monetary Authority of Singapore (MAS). (2019). Sandbox Express guidelines (August 7, 2019). https://www.mas.gov.sg/-/media/MAS/Smart-Financial-Centre/Sandbox-Express/Sandbox-Express-Guidelines-7-Aug.pdf

Nietzsche, F. (1882). Die fröhliche Wissenschaft.

Nietzsche, F. (1883-1885). Also sprach Zarathustra.

Nietzsche, F. (1887). Zur Genealogie der Moral.

Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology. Official

Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

Severino, E. (1995). L'essenza del nichilismo. Adelphi.

Trifiletti, M. (2025). The challenge of integrating Artificial Intelligence in Anti-Money Laundering. Journal of Economics, Finance and Management (JEFM), 4(3), 777-788.

Vattimo, G. (2003). Nihilism and emancipation: Ethics, politics, law. Garzanti.

Volpi, F. (2004). Il nichilismo. Laterza.

World Bank. (2020). Global experiences from regulatory sandboxes. https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2017). From FinTech to TechFin: The regulatory challenges of data-driven finance. NYU Journal of Law & Business, 14, 393-446. https://doi.org/10.2139/ssrn.2959925

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203. https://doi.org/10.1093/jfr/fjaa010