

Nedyalko Valkanov**Financial Regulation and Technological Innovations –
an Indisputable Commitment or Danger of Overconfidence?**

Nedyalko Valkanov, Ph.D., is an Associate Professor at the University of Economics – Varna, Department of Finance. The author's research interests lie in the fields of financial regulation, the prevention of economic fraud, and financial crime. He is the author of the monograph "Compliance in Support of Financial Regulation", as well as other publications on regulatory compliance and anti-money laundering measures. N. Valkanov is a Certified Expert Fraud Examiner (CEFE) and a member of the management board of the Association for Counteraction to Economic Fraud (ACEF). Contact: n.valkanov@ue-varna.bg

Abstract

The ongoing digital transformation of the financial sector has significantly altered not only the financial services themselves, but also the landscape of financial regulation and supervision. This article explores the dual dimensions of technological innovations used for compliance and supervisory purposes in finance. It argues that while such developments offer efficiency and scalability, they also introduce new operational vulnerabilities that may exceed traditional financial risks in complexity and impact. The paper avoids specific regulatory case studies, focusing instead on particular conceptual points of emerging interdependencies and the potential risk of overconfidence in high-tech compliance mechanisms. It concludes by emphasizing the need for a balanced approach that fosters innovation while ensuring resilient, adaptive regulatory safeguards.

Keywords

Financial Innovations, Financial Regulations, Regulatory Technologies (RegTech), Compliance.

DOI: <https://doi.org/10.56065/FNJ2025.1.143>

Introduction

The rapid transformation of the financial landscape necessitates accounting for the growing importance of high-tech innovations in financial regulation and supervision. The shift from traditional financial services and instruments to algorithmic trading, peer-to-peer (P2P) platforms, and blockchain-based systems compels financial regulators to modernize their toolkits and supervisory practices as an indisputable imperative.

Against this backdrop, the article analyses recent trends that shape the discourse around the integration and institutional acceptance of technological innovations within financial regulation. It focuses on already emerging spheres of dependence and interdependence involving various financial institutions, critical infrastructure providers, and regulatory expertise providers (RegTech firms). Within this context, it also explores the potential risk of overconfidence in the use of advanced technological tools and innovative compliance

methods employed by regulated entities. It is argued that navigating this evolving landscape requires a careful balance between embracing innovation and maintaining robust, adaptive safeguards.

The extensive discussion of individual regulatory practices or specific legal frameworks such as MiCA, DORA, or the EU AI Act is deliberately avoided. Instead, the aim is to outline specific potentially challenging areas arising from two developments: the emergence of previously unknown functional ecosystems within the financial services sector, and the parallel evolution of the respective regulatory framework.

1. Technological Innovation as a Catalyst for Enhanced Regulation

The need for a proactive regulatory framework, in response to the changed financial landscape, requires implementation and use of a state-of-the-art technological toolkit with active application of innovative tools such as artificial intelligence, big data processing and even blockchain solutions. All of these already find partial application in ensuring regulatory compliance by different financial institutions, external regulatory service providers (RegTech) and even financial regulators themselves.

This innovation of the regulatory infrastructure can be subjected to analysis in different aspects, namely: *technological* – in relation to the specifics of the new technologies being introduced; *institutional* – regarding the types of financial intermediaries undergoing the process of technological reorganization; *product-related* – in relation to the new and renewed financial products; systemic – from the point of view of emerging new levels of interdependence and correlation between different financial service providers and different Fintech and RegTech ecosystems. Any analysis in this regard should be interdisciplinary in nature. As for the applied supervisory toolkit, it can be segmented into three categories according to the degree of application of the relevant technological innovations.

The first is that of *technological modernization* of the digital tools implemented at an earlier stage of the technological evolution, used for processing databases, communication with supervised financial institutions, risk analysis, and etc., thus allowing processing of huge volumes of financial data generated by the reporting of supervised institutions¹. An illustration of this aspect is the analysis of the information collected by financial intelligence authorities on cash, wire transfer and suspicious operations under the anti-money laundering and anti-terrorist financing legislation. For their part, financial institutions are implementing systems to automate this process by improving algorithms and machine learning techniques in order to detect and analyse the so-called “red flags” – suspicious activities that can be identified by detecting anomalies in the information arrays.

¹ Structuring and visualizing information in tabular form has been done for decades through solutions such as MS Office, SQL, Oracle databases, and others, often supplemented by machine learning algorithms. Some popular modern software solutions in this regard are Redis, PostgreSQL, MongoDB, MySQL, Microsoft SQL Server, MLDB, Apache Cassandra.

The second group of activities in this area includes the development, testing and implementation of *entirely new technologies*. Specifically, this refers to the integration of blockchain and artificial intelligence in supervisory practice. From this perspective, RegTech solutions related to the activities of regulatory agencies are separated into the category of Supervision Technology (SupTech). An example here is the successful testing by the financial regulators of Singapore and Hong Kong of shared databases used in cross-border currency transfers via blockchain networks². With the evolution of blockchain, the implementation of automated coded agreements (smart contracts) gains popularity also in regulatory context.

In the third place we can highlight the *formation of test environments* for experimenting with new products within closed ecosystems known as regulatory sandboxes. Apart from the regulators, representatives of the financial sector such as fintech companies and traditional financial institutions also participate in them. Within these controlled environments, conditions are created for the study of various innovative solutions, which may be implemented at a future point in regulatory practice.

Another systematization in this direction consists in the grouping of innovative solutions in the field of regulatory compliance in terms of functions. Thus, data processing technologies may be classified with regard to: aggregation – social, voice, identity, regulatory, market, digital; management – interpretation, guidance, security, privacy; sharing – through modelling, visualization, information consolidation, and processing – based on predictive analytics, behavioural analytics, statistical analysis, mining, research and tracking of information³.

2. Progressive Deepening of Interdependence

Technological dependence, which is already deeply embedded, could be considered from two key perspectives. *First*, today's financial service providers are almost entirely reliant on technological systems that not only support but also shape and predetermine their operational behavior. It is increasingly clear that technology plays a dominant role in the design and delivery of financial products and services. *Second*, this dependence is reflected in the growing technologization of financial products themselves. This trend spans both

² As part of the Ubin+ project, Singapore's financial authorities, in collaboration with other central banks and global institutions, are exploring the use of digital currency infrastructure for cross-border transactions. The initiative aims to test DLT-based models for foreign currency settlements, enhance interoperability and atomic settlement between platforms, and develop policy frameworks to support broader access and participation. For more, see: <https://www.mas.gov.sg/schemes-and-initiatives/ubin-plus>.

³ AI-driven technologies such as facial and voice recognition, biometric identification, and speech-to-text processing are increasingly used in digitally delivered financial services. These tools facilitate secure customer authentication (e.g., in mobile banking), enable automated support through chatbots, and assist in detecting fraud via communication analysis. Their growing adoption, however, raises regulatory concerns around data privacy, algorithmic transparency, and the robustness of consent and authentication mechanisms, prompting oversight under frameworks such as the EU's AI Act and GDPR.

traditional instruments and those introduced through innovations such as blockchain, big data analytics, and artificial intelligence, signalling a fundamental shift in the structure and accessibility of financial operations.

The lack of unified standards for “communication” between separate compliance processes carried out independently of each other in the otherwise increasingly integrated participants in the financial system is only one of the challenges arising in the emerging virtual financial ecosystems with the participation of traditional and new financial institutions. In order to visualize this process, several indicative types of ecosystems can be outlined, gravitating around:

- *Product assortment* (with the participation of all financial service providers in the form of traditional financial institutions, FinTech, BigTechs);
- *Customer base sharing* (between traditional financial institutions and their competitors in the form of FinTech and BigTechs);
- *Sharing of infrastructure* (between traditional financial institutions, FinTech, BigTechs, payment system operators);
- *Outsourcing of regulatory expertise* (between traditional financial institutions, FinTech and BigTech as its users, RegTech⁴ firms as providers and financial regulators in their role as proactive supervisors).

Each of the above ecosystems may be indicatively associated with its own degree of *interdependence risk*. Still not widely established in financial literature, this risk category refers to the potential for disruption and/or systemic failure that arises from the interconnectedness of entities, systems, or sectors—where the functioning or failure of one component significantly affects others.

In a regulatory context, it typically associates with following dimensions which can also be seen as a challenge to ensuring system stability:

- *Cross-institutional exposure* - for example, when banks, fintechs, and infrastructure providers rely on shared platforms or services or regulatory expertise providers (RegTechs);
- *Operational dependency* - reliance on third-party service providers (e.g., cloud computing, APIs, or external data sources), which can create single points of failure across multiple institutions;
- *Technological entanglement* - dependence on same critical infrastructure tools like cloud services or AI models;

⁴ The RegTech segment also provides an environment for moving to a risk-based proportional approach to effective supervision based on adequate data management. This minimizes the risks of falling into the situation of regulatory capture observed in the run-up to the global financial crisis of 2008, as well as a number of other emerging risks (Arner et al. 2017: 375).

- *Data Interconnectivity* and *data veracity* - shared data flows between institutions (e.g., open banking environments) that increase both systemic efficiency and the risk of coordinated data breaches or misinformation;
- *Regulatory spill over* and *Compliance synchronization* - rules or failures in one jurisdiction or sector impacting others due to the interconnected regulatory systems or when entities operating in multiple jurisdictions must comply with overlapping or contradictory regulatory requirements, especially in areas like AI ethics, AML, or cybersecurity⁵.

Table 1 provides a structured overview of various financial ecosystems, classified by the nature of inter-institutional collaboration and associated interdependence risks.

Table 1. Interdependence and risk of interdependence in modern financial ecosystems		
Ecosystem	Participants	Risk of interdependence
Product level	Traditional Financial Institutions (TradFin), FinTech, BigTechs	Low
Customer base sharing	Traditional Financial Institutions (TradFin), FinTech, BigTechs	Low to Moderate
Infrastructure sharing	Traditional Financial Institutions, FinTech, BigTechs, payment system operators	High
Outsourcing of regulatory expertise	Traditional Financial Institutions (TradFin), FinTech, BigTechs, RegTech, regulators	Moderate to High
Source: Own elaborations		

At the *product level*, the collaboration among traditional financial institutions (TradFin), FinTechs, and BigTechs is considered to carry low risk, suggesting relatively compartmentalized operations with minimal systemic spillover potential. However, as interactions deepen – particularly at the *customer base sharing* stage – interdependence increases to a low-to-moderate level, reflecting shared exposure to data risks and reputational contagion. The *infrastructure sharing* ecosystem is highlighted as the most vulnerable, with a high risk of interdependence. This is due to the concentration of critical services – such as cloud computing, APIs, and payment rails – often managed by a few dominant BigTech or infrastructure providers. Disruption at this level can lead to widespread operational paralysis across financial actors. Finally, *outsourcing regulatory expertise*, including reliance on RegTech and external compliance providers, introduces moderate to high risk, especially as traditional regulatory oversight becomes more technologically mediated. This dependence may obscure accountability and complicate responses to compliance failures.

⁵ We may also add, especially in the DeFi area, the *Systemic amplification risk* - the potential for small disruptions (e.g., in algorithmic trading or DeFi protocols) to propagate rapidly across interconnected platforms, amplifying market volatility and the *Governance asymmetry* - uneven distribution of control or decision-making power across actors in a shared digital ecosystem, leading to disproportionate influence or risk concentration.

Overall, this exemplary risk systematization underscores the importance of differentiated regulatory attention across ecosystem layers, highlighting where systemic safeguards are most urgently needed. The assessed higher risk of interdependence in the shared infrastructure segment can be explained by the following circumstances: regulatory requirements for providing access to information on accounts and payment operations in line with open banking (PSD regulation); the sharing of electronic channels for the sale of financial products by heavily regulated banking institutions and their lightly regulated competitors; blurring of responsibilities in implementing cyber risk protection mechanisms. In turn, vulnerabilities in the outsourcing of regulatory expertise are explained by the potential risk of overtrusting the service provider; the loss of control over sensitive information provided to the service provider; the possible lack of an alternative provider concerning certain activities.

A joint study on the subject by the Bank of England and the two UK financial regulators FCA and PRA has concluded that the financial sector's growing reliance on services provided by third parties creates risks both for individual financial intermediaries, supervisory authorities and the overall financial system (Prudential Regulation Authority 2022). According to the aforementioned study, these risks arise from a combination of various factors, including: the observed increasing dependence of financial institutions on third-party service providers, whose failure or disruption could have a systemic impact on the objectives of supervisory authorities); concentration in the provision of these services; the potential impact of the failure or disruption of these services on the stability or market integrity of the UK financial system and the viability of financial intermediaries (Prudential Regulation Authority 2022). Conversely, a KPMG study on the top ten regulatory challenges for 2025 notes that understanding the interconnections and interdependencies within and between critical business operations and services, as well as key business lines and opportunities, including third-party risks and critical technology services, is key to achieving resilience (KPMG, 2024).

Also of interest in this regard is the issue of regulating so-called *DeFi - platforms*, which operate within the broader concept of *democratisation of financial services*⁶. Regulating the democratization of finance presents a complex challenge that involves balancing broader access to financial services with the need to maintain market stability, integrity, and fairness. Key regulatory priorities include protecting inexperienced investors from fraud, misinformation, and high-risk products; addressing financial literacy gaps that contribute to poor decision-making; mitigating technological risks such as cyber threats, platform failures, and data misuse; and preserving market stability by managing systemic risks linked to speculative or unsophisticated participation. These goals are further complicated

⁶ Decentralized Finance (DeFi) enhances financial inclusion by eliminating intermediaries, fosters innovation through novel mechanisms such as liquidity pools, yield farming, and decentralized exchanges (DEXs), and enables global participation irrespective of access to traditional financial infrastructure.

by regulatory challenges, such as jurisdictional fragmentation, the rapid pace of innovation outstripping existing legal frameworks, and the enforcement difficulties posed by decentralized or pseudonymous financial environments. While the EU's Markets in Crypto-Assets Regulation (MiCA) and the Digital Operational Resilience Act (DORA) represent significant steps toward addressing these concerns, their implementation highlights the ongoing tension between fostering innovation and ensuring effective oversight in increasingly complex financial ecosystems.

3. Emerging Normative Framework

In September 2020, the European Commission introduced the EU Digital Finance Package, a strategic initiative aimed at fostering a competitive and innovative financial services sector within the European Union. This package encompasses a digital finance strategy and legislative proposals designed to enhance consumer access to innovative financial products, ensure consumer protection, and maintain financial stability (European Commission, 2020a).

Central to this initiative are two significant legislative initiatives: *the Markets in Crypto-Assets Regulation* (MiCA) and the *Digital Operational Resilience Act* (DORA). MiCA seeks to establish a harmonized regulatory framework for crypto-assets across the EU, addressing objectives such as supporting innovation, enhancing consumer protection, ensuring market integrity, and mitigating risks related to money laundering and terrorist financing (European Commission, 2020b). DORA complements this by creating a comprehensive framework for managing digital operational risks within the financial sector, focusing on resilience to ICT-related disruptions and cyber threats (European Commission, 2020c). The two aforementioned regulations partially mitigate the risk of interconnection through licensing, prudential requirements, unified supervision (under MiCA), and the ICT Risk Management Framework and third-party risk oversight (under DORA).

Despite their pioneering nature, both MiCA and DORA have been subject to critical scrutiny. MiCA's focus on centralized service providers may limit its applicability to decentralized finance (DeFi) structures, such as algorithmic stablecoins and decentralized autonomous organizations (DAOs), which remain under-regulated or ambiguously defined. DORA, while notable for imposing ICT risk management standards and third-party oversight, may encounter enforcement challenges, particularly concerning non-EU service providers and cross-border technological dependencies.

Comparative analysis reveals differing regulatory approaches in other jurisdictions. The United States employs a fragmented, enforcement-led model grounded in existing securities and commodities laws, leading to regulatory uncertainty. The United Kingdom adopts a more adaptive approach, prioritizing innovation through mechanisms like regulatory sandboxes. In contrast, Singapore's Monetary Authority (MAS) has developed an integrated and anticipatory framework, balancing oversight with innovation support.

Particularly significant is the AI Act, proposed in April 2021, which represents the world's first comprehensive attempt to regulate artificial intelligence. The Act categorizes AI applications based on risk levels and imposes corresponding obligations, aiming to mitigate ethical and operational risks while establishing a harmonized EU-wide governance model (European Commission, 2021). Given the increasing integration of AI into financial services—ranging from algorithmic trading to automated compliance—the AI Act is expected to play a central role in future financial supervision⁷.

Beyond MiCA and DORA, the European Union has introduced several additional digital regulations shaping the financial supervisory landscape. These include: *The Data Governance Act*, facilitating cross-border and cross-sector data sharing; the *eIDAS Regulation*, harmonizing digital identification and authentication standards across the EU; the *NIS II Directive*, establishing robust national cybersecurity frameworks; the *Digital Markets Act (DMA)*, promoting fair competition by curbing the dominance of large digital platforms; the *Digital Services Act (DSA)*, enhancing digital user rights and platform accountability.

4. Tech-Driven Finance: Regulation (Im)possible?

The increasing reliance on technology in financial markets has led to significant efficiency gains but also introduced new sensitivity areas that can be collectively summarized as *risk of overconfidence*. It refers to that systemic vulnerability that arises when financial institutions, regulators, or technology providers place excessive trust in technological solutions, such as AI, machine learning, or digital infrastructures, without fully understanding, testing, or governing their limitations and failure modes. In the context of financial regulation and high technology, this overconfidence can manifest in different critical ways. Some of them associate with:

- *Fragmented regulatory responsibilities* (existing EU regulations still focus on traditional financial conglomerates but largely exclude fintechs and BigTechs and thus creating regulatory blind spots amid growing partnerships between banks and technology firms).
- *Regulatory gaps for neo-banks* which are usually subjected to lighter regulatory regimes (challenging here are the insufficient participation in deposit insurance schemes, cybersecurity vulnerabilities, operational continuity, and limited experience with traditional financial risk management).
- *Lack of systemic relevance and adequate macroprudential oversight* (examples here are failures such as Wirecard (2020) and U.S. Silicon Valley and Signature banks in 2023).

⁷ The EU Artificial Intelligence Act outlines key provisions, including: the *risk-based classification of AI systems* (ranging from minimal to unacceptable risk); *strict obligations for high-risk systems*, such as transparency, data quality, and human oversight requirements; *protection of personal data and user rights*, ensuring AI does not exploit or harm users; and the establishment of *supervisory and enforcement mechanisms* led by the European Commission and national authorities, empowered to monitor, test, and sanction non-compliance.

- *Overdependence on third-party technology providers* (more often financial institutions rely on external providers for regulatory tech and critical infrastructure which dependency introduces new vulnerabilities, including operational disruptions, vendor lock-in, and resilience concerns)⁸.
- *Growing role of BigTechs* as financial services providers (global tech giants like Alphabet, Amazon, Meta, Microsoft, Tencent, etc. are constantly expanding into financial services through direct offerings or partnerships which raises questions about imposing capital and liquidity requirements akin to those applied to banks).
- *Reputational contagion in platform-based finance* (especially speaking in terms of interconnected digital ecosystems, where misconduct or failure in one firm can quickly erode public trust across the sector, amplifying systemic risk).
- *The growing importance of the risk of financial fraud and crime* (like the synthetic identity frauds, created often by generative AI).

Future updates of the regulatory framework are likely to take into account the presence of shared environments and ecosystems. An example here is the shift of focus from 'embedded banking' towards 'embedded finance' in third version of the European Payments Directive (PSD 3), which expected to come into force in 2027. An additional example is the implementation of Basel IV, which shifts regulatory emphasis from internal risk models toward standardized approaches, aiming to reduce excessive reliance on banks' proprietary algorithms and improve comparability across institutions.

Along these lines, some might ask whether capital and liquidity requirements under Basel regulations should not be extended to fintech sector and BigTechs? However, extending Basel-style rules in this direction presents major challenges. These entities often operate under different business models, are subject to lighter regulatory oversight, and leverage advanced technologies, such as AI-driven credit scoring or algorithmic lending platforms, that fall outside traditional supervisory frameworks. Applying capital and liquidity requirements designed for banks to such firms raises complex questions around proportionality, risk calibration, and enforcement, especially given their cross-sector and cross-border operations.

However, all of this is a solid basis for future discussion towards answering the question of whether recalibrating the regulatory toolkit towards emerging ecosystems and innovative financial service providers will create new levels of regulatory arbitrage between them and traditional financial institutions.

Conclusion

Driven by a dynamic and complex external environment, this transformation demands a

⁸ Monchev (2024) provides a detailed examination of approaches to countering operational risk in the fintech sector.

reassessment of the accompanying risk landscape. Emerging vulnerabilities, such as system outages, unauthorized access to user accounts, and data breaches, are seen as significant operational risks that can lead to significant damage for financial service providers and even lead to systemic risk as a result of the increasingly high levels of interconnectedness between participants in new financial ecosystems. On the other hand, high-tech innovation is being incorporated in full force into the toolkit of financial supervision. The outlines presented above illustrate the impossibility of giving primacy to any of the hypotheses as to whether it is even possible to regulate present high-tech driven financial sphere. What remains indisputable, however, is the imperative to modernize the overall regulatory infrastructure by integrating high-tech innovations, ensuring it remains responsive to the evolving complexities of the digital financial ecosystem.

References

1. Arner, D., J. Barberis, R. Buckley. (2017). *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, Northwestern Journal of International Law and Business, Vol 37, Issue 2, pp. 371-413, <https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2>
2. Cambridge SupTech Lab (2022). *State of SupTech Report 2022*, Available at: <https://www.jbs.cam.ac.uk/wp-content/uploads/2023/01/2023-ccaf-state-of-suptech-report.pdf>
3. European Commission (2020a). *Digital finance package*. Available at: https://finance.ec.europa.eu/publications/digital-finance-package_en
4. European Commission (2020b). *Proposal for a regulation on markets in crypto-assets (MiCA)*. Available at: https://finance.ec.europa.eu/digital-finance/crypto-assets_en
5. European Commission (2020c). *Proposal for a regulation on digital operational resilience for the financial sector (DORA)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0595>
6. European Commission (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>
7. KPMG (2024). *Ten Key Regulatory Challenges of 2025*, Available at: [kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/ten-key-regulatory-challenges-of-2025.pdf](https://www.kpmg.com/kpmg-us/content/dam/kpmg/pdf/2024/ten-key-regulatory-challenges-of-2025.pdf)
8. Monchev, V. (2024). Dobri praktiki za upravlenie na operatsionniya risk vav fintek sektora v epokhata na digitalnata transformatsiya [Good practices for operational risk management in the fintech sector in the age of digital transformation]. *Voenen zhurnal*, 131(4), 463–473.
9. Prudential Regulation Authority (2022). *Operational resilience: Critical third parties to the UK financial sector*. PRA Discussion Paper 3/22, Available at: www.bankofengland.co.uk/prudential-regulation/publication/2022/july/operational-resilience-critical-third-parties-uk-financial-sector