Regulation of financial markets in the European Union in the context of digitalisation

Liubov Lipych[1], Mykola Nadeiko[2]

Received: 2025-12-12
Accepted: 2026-01-15
DOI: https://doi.org/10.5281/zenodo.19360292

Abstract. The article examines the evolution and current state of the regulatory architecture of the European Union's financial markets in the context of digital transformation. The post-crisis institutional restructuring of EU financial supervision is analysed, including the establishment of the European Supervisory Authorities (EBA, ESMA, EIOPA), the formation of the Banking Union, and the introduction of the Single Rulebook concept. Key EU regulatory acts aimed at governing digital financial services are explored: the Markets in Crypto-Assets Regulation (MiCA), which for the first time globally provides comprehensive legal regulation of crypto-assets with classification into e-money tokens, asset-referenced tokens, and other crypto-tokens; the Digital Operational Resilience Act (DORA), which harmonises cybersecurity standards for the financial sector; the updated Payment Services framework PSD3/PSR, which deepens the open financial ecosystem; the AI Act, which classifies financial AI systems as high-risk; and the General Data Protection Regulation in the context of its impact on automated decision-making in finance. Regulatory approaches to fostering innovation through sandbox mechanisms, innovation hubs, and the principle of proportionality are considered. The main challenges posed by digitalisation are identified: regulatory gaps concerning decentralised finance, systemic risks of stablecoins, algorithmic bias issues, concentration of cyber risks in cloud providers, and the complexities of introducing the digital euro. The significance of the EU's regulatory experience for Ukraine as a candidate country is substantiated. The current state of implementation of European standards in Ukraine is analysed in the areas of virtual asset regulation, open banking, banking supervision, and anti-money laundering. A strategy for gradual harmonisation with opportunities for technological leapfrogging and adaptation to wartime conditions is proposed.

Keywords: financial markets, European Union, digitalisation, MiCA, DORA, crypto-assets, regulatory sandbox, open banking, digital euro, financial regulation.

[1] Doctor of Economics, Professor,
Professor at the Department of Entrepreneurship, Trade and Logistics,
Lutsk National Technical University
ORCID: https://orcid.org/0000-0002-9059-7271
[2] PhD in Economics,
Lecturer at the Department of Economics and Finance, Faculty of Economics,
Academician Stepan Demianchuk International University
of Economics and Humanities
ORCID: https://orcid.org/0000-0002-1011-3477

Introduction

Problem Statement

The digital transformation of global financial markets has accelerated markedly over the past decade. Crypto-assets, decentralised finance, algorithmic trading, and next-generation payment systems are fundamentally reshaping the landscape of financial services while simultaneously generating new systemic risks that extend beyond traditional regulatory frameworks. The European Union, as one of the world's largest financial markets, faces a strategic challenge: ensuring financial stability and consumer protection without impeding innovative development.

The relevance of this problem is heightened by Ukraine's European integration aspirations. As a candidate country for EU membership, Ukraine is obliged to adapt its financial legislation to the European acquis communautaire, which entails the implementation of a series of complex regulatory acts in the field of digital finance. This implementation takes place under martial law conditions and limited institutional resources, yet alongside a high level of societal digital readiness. A systematic analysis of the EU's regulatory experience in digital financial markets is therefore directly important for shaping effective national regulatory policy—in both its theoretical and applied dimensions.

Analysis of Recent Research and Publications

The regulation of financial markets under digitalisation conditions is studied by both European institutions and the international academic community. The UK House of Lords Committee, in a report on the post-crisis EU regulatory framework, examined the architecture of the Banking Union and the Single Rulebook concept, identifying them as the foundation of post-crisis financial stability [1]. The European Commission, in its Digital Finance Strategy of 2020, outlined a systemic approach to regulating digital financial services, providing for the creation of comprehensive rules for crypto-assets, regulatory sandboxes, and the coordination of innovation hubs through the European Forum for Innovation Facilitators (EFIF) [2].

ESMA, in its 2024 Final Report, analysed the criteria for qualifying crypto-assets as financial instruments within the meaning of MiFID II, noting a regulatory gap for a significant portion of digital assets [3]. EIOPA highlighted the requirements of the Digital Operational Resilience Act (DORA), particularly regarding ICT risk management, cyber resilience testing, and oversight of critical third-party technology providers [4]. The European Parliamentary Research Service, in a 2023 briefing, systematised the changes envisaged by the updated payment services framework PSD3/PSR, including the expansion of open API requirements and strengthened fraud protection [5].

CertiK, in a 2026 study, analysed the advantages and limitations of MiCA from an auditing perspective, notably the reserve coverage requirements for stablecoins and the boundaries of the regulation's applicability to DeFi and NFTs [6]. Wolf Theiss and CEE Legal Matters examined the introduction of open banking in Ukraine following the adoption of NBU Resolution No. 80, outlining the regulatory status of AIS/PIS providers and the compliance of these norms with PSD2 requirements [7; 8]. Goodwin, in a 2024 legal review, systematised the key provisions of the EU AI Act relevant to financial services, particularly the classification of financial AI systems as high-risk [9].

Mitchell J., in an article published in the Harvard Data Science Review, explored the prospects for credit scoring and insurance underwriting under the EU AI Act, substantiating the need for algorithmic explainability and the right of individuals to challenge automated refusals [10]. Chomczyk Penedo A., in a paper prepared for the European Banking Authority, analysed the issue of privacy in the context of the digital euro, particularly the requirements for ensuring payment confidentiality comparable to cash transactions [11]. The BIS Working Group, in a 2023 study, empirically confirmed the impact of participation in regulatory

sandboxes (using the UK FCA sandbox as a case study) on the volume of funding attracted by fintech companies [12].

The European Parliament's Research Division prepared an analytical document in 2024 devoted to BigTech finance, examining the risks of large technology companies entering the financial sector and the need to adapt antitrust regulation [13]. RUSI, in a 2025 taskforce report, investigated the issues of public–private partnerships and virtual asset regulation in Ukraine, particularly in the context of fulfilling obligations under the Ukraine Plan for harmonisation with the EU acquis [14].

Despite the substantial body of research, the questions of comprehensive analysis of the interaction among EU regulatory acts (MiCA, DORA, PSD3, AI Act, GDPR) as a holistic regulatory ecosystem, as well as strategic approaches to adapting this experience under martial law conditions and limited institutional capacity characteristic of Ukraine, remain insufficiently explored.

Formulation of the Article's Objectives

The aim of the article is a comprehensive analysis of the European Union's regulatory architecture in the field of digital financial markets and the substantiation of strategic directions for adapting this experience to Ukraine. To achieve this aim, the following objectives are set: to examine the evolution of EU regulatory frameworks from post-crisis regulation to digital adaptation; to analyse the key regulatory instruments (MiCA, DORA, PSD3, AI Act, GDPR) and mechanisms for stimulating innovation; to identify the challenges and risks that digitalisation creates for financial regulation; and to assess the current state and prospects for the implementation of European standards in Ukraine.

Results

The regulatory architecture of EU financial markets underwent fundamental changes following the 2008 global financial crisis. Supranational financial supervisory bodies were established—the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA)—and the Banking Union was realised with the Single Supervisory Mechanism (SSM) and the Single Resolution Mechanism (SRM) [1]. The Single Rulebook concept was intended to ensure the formation of a unified capital market with harmonised prudential standards and a financial passporting mechanism [1]. In 2014–2015, the EU continued reforms by adopting updated frameworks for the banking sector (CRD/CRR, BRRD), insurance (Solvency II), capital markets (MiFID II), and derivatives (EMIR), as well as launching the Capital Markets Union (CMU) project [1]. However, the implementation of CMU was hampered by national divergences in financial market development levels, tax regimes, and corporate regulation.

Post-crisis regulatory frameworks, however, proved inadequate for covering rapidly evolving digital innovations. In particular, ESMA noted in its Final Report that crypto-assets are largely not covered by the definition of "financial instruments" under MiFID II [3], creating a significant regulatory gap. The principle of "same activity—same risk—same rules" is difficult to apply to business models undergoing constant transformation. The turning point was the European Commission's Digital Finance Strategy of 2020 [2], which envisaged a shift from piecemeal gap-filling to a systemic approach: creating comprehensive rules for the crypto market, pilot regimes for distributed ledger technologies, and coordinating innovation hubs through EFIF [2].

The generalised architecture of the EU's regulatory ecosystem for digital financial markets is presented in Fig. 1.

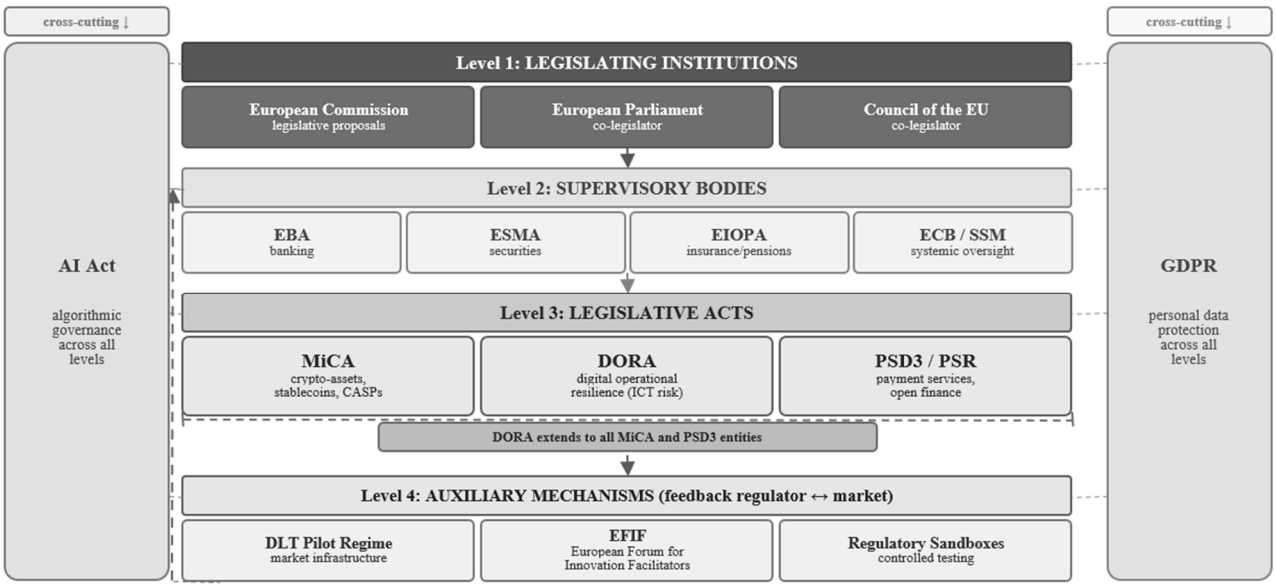

Fig. 1. Architecture of the EU's regulatory ecosystem for digital financial markets

The substantive content of EU digital financial regulation is defined by specific legislative acts. Central among them is the Markets in Crypto-Assets Regulation (MiCA), adopted in 2023. MiCA classifies crypto-assets into three categories: e-money tokens (EMT), pegged to a single fiat currency; asset-referenced tokens (ART), pegged to a basket of assets; and other crypto-tokens. The regulation establishes licensing and prudential requirements for crypto-asset service providers (CASPs), transparency requirements including disclosure in "white papers", and consumer protection. The reserve assets of stablecoins must be liquid and provide full coverage of obligations. MiCA provides legal guarantees through a passporting mechanism, but has acknowledged limitations: DeFi and NFTs formally remain outside the regulation, and their governance requires separate treatment [6]. Despite this, MiCA is recognised as the world's first comprehensive crypto-asset legislation, combining the "same activity—same risk—same rules" principle with flexible procedural instruments.

In parallel with the regulation of crypto-assets, the EU developed a framework for ensuring the digital operational resilience of the financial sector. The Digital Operational Resilience Act (DORA), mandatory from 2025, harmonises cyber resilience rules for banks, insurance companies, exchanges, and payment organisations [4]. DORA's core requirements encompass the implementation of ICT risk management frameworks, mandatory resilience testing (including Red Teaming), standardised ICT incident reporting, and thorough auditing of relationships with technology providers. Of particular significance is the provision on oversight of critical third-party ICT service providers, which allows regulators to supervise key cloud providers (AWS, Azure, Google Cloud) [4]. DORA thus closes a significant gap in the financial sector's cyber defence system.

Payment services rules are also undergoing a profound transformation. The PSD2 Directive of 2015 introduced the concept of Open Banking, granting third parties access to bank accounts via APIs. The updated PSD3/PSR framework, currently being developed by the EU, envisages a deepening of the open financial ecosystem: expanding the list of mandatory APIs, introducing additional anti-fraud measures, and establishing unified licensing requirements for fintech services [5]. Ukraine has already implemented a PSD2 analogue: NBU Resolution No. 80 of 25 July 2025 opened AIS/PIS provider access to bank accounts, which complies with PSD2/PSD3 requirements and promotes competition in the payment sector [7; 8].

The EU Artificial Intelligence Act (AI Act) classifies systems by risk level, categorising a broad spectrum of financial applications—credit scoring, insurance pricing, algorithmic

trading—as high-risk [9; 10]. For such systems, strict requirements are stipulated: bias testing, explainability of decisions (human-in-the-loop), model transparency for regulators, and complete documentation. The use of AI in lending is permitted only on condition that individuals receive explanations of decisions and can challenge refusals [10]. The AI Act thereby complements financial regulation, which has long required non-discriminatory access to credit services.

Closely linked to the AI Act is the General Data Protection Regulation (GDPR), which significantly affects digital financial services. The use of personal data in financial algorithms falls under the requirements for automated decision-making: consumers must receive information about the use of their data and give explicit consent [11]. Fintech companies are compelled to implement privacy-by-design principles, notably pseudonymisation and data aggregation, creating a systemic tension between the drive to utilise large datasets and privacy requirements.

The systematised characteristics of the analysed regulatory acts are presented in Table 1, which enables comparison of their scope, key mechanisms, and acknowledged limitations.

Table 1. Comparative characteristics of key EU regulatory acts in the field of digital finance

Regulatory act	Entry into force	Scope	Key mechanisms	Acknowledged limitations
MiCA	Phased: 06.2024 (EMT/ART), 12.2024 (CASP)	Crypto-assets (EMT, ART, other tokens); crypto-asset service providers (CASP)	CASP licensing; stablecoin reserve requirements (min. 100% coverage); white paper disclosure; passporting mechanism	DeFi and NFTs outside scope; risk of offshore arbitrage via reverse solicitation
DORA	01.2025	Banks, insurers, exchanges, payment organisations, investment funds	ICT risk management frameworks; resilience testing (Red Teaming); incident reporting; oversight of critical cloud providers	Does not extend to DeFi infrastructure
PSD3/PSR	Proposal (COM/2023/360)	Payment services, Open Banking	Expansion of mandatory APIs; enhanced fraud protection; unified licensing requirements for fintech services	Not yet adopted; inter-institutional negotiations ongoing
AI Act	Phased: 02.2025–08.2027	AI systems in finance: credit scoring, insurance, algorithmic trading	Risk-level classification; bias testing; human-in-the-loop; full model documentation	Technology evolution outpaces the regulatory base; difficulty controlling “black boxes”
GDPR	05.2018	Personal data in financial services	Explicit consent for processing; right to explanation of automated decisions; privacy-by-design	Systemic tension with BigData analytics needs in the fintech sector

Source: compiled by the authors based on [2; 4; 5; 6; 9; 11].

Beyond legislative acts, the EU’s regulatory architecture includes instruments for stimulating innovation. Regulatory sandboxes are one of the key mechanisms: the UK’s FCA launched the first sandbox in 2015, and a BIS study empirically confirmed that participation

helps fintechs attract additional funding and understand regulatory expectations [12]. At the EU level, the DLT Pilot Regime effectively serves as a sandbox for tokenised financial instruments. Innovation hubs provide advisory support to start-ups on regulatory compliance, while EFIF coordinates cross-border cooperation among national hubs [2]. The proportionality principle allows the regulatory burden to be adapted to the size and type of market participant, providing simplified licensing procedures for small fintech firms.

At the same time, the entry of large technology companies (BigTech) into financial services poses a distinct challenge. Conglomerates such as Apple, Google, and Meta integrate payment and trading services into unified ecosystems, creating significant competition for traditional banks [13]. The EU responds primarily through adjacent acts (DMA, DSA, cloud services regulation), while financial regulation has not yet established separate frameworks for BigTech, as regulators assign this issue to antitrust law and market transparency.

The described regulatory architecture, despite its comprehensiveness, cannot keep pace with all the challenges generated by the digitalisation of financial markets. Decentralised finance (DeFi)—networks of smart contracts without a centralised operator—is virtually impervious to traditional oversight due to the absence of intermediaries with clear legal responsibility. Market participants frequently remain outside MiCA licensing zones through reverse solicitation mechanisms or offshore models, creating a situation of informal regulation. Stablecoins represent a separate risk: the collapse of TerraUSD in 2022 demonstrated their potential systemic danger. MiCA has established reserve coverage requirements for stablecoins, but global stablecoins can circumvent EU rules by issuing in jurisdictions with lenient regulation, creating a risk of regulatory arbitrage [6].

Algorithmic decision-making based on artificial intelligence poses additional challenges: banking credit scoring algorithms can inadvertently produce discriminatory outcomes, and high-frequency trading with AI does not preclude flash-crash events. Cybersecurity remains a critical problem: the concentration of infrastructure in cloud providers creates a single-point-of-failure threat, while increasing automation expands the potential attack surface. DORA is aimed at addressing these issues through a cloud services oversight framework, but simultaneously the security risks of blockchain networks and DeFi protocols are growing [4].

The digital euro (CBDC) project opens new opportunities but also generates contradictions. The European Central Bank is considering the introduction of a retail digital euro currency, which could strengthen the euro's role in e-commerce but creates a range of challenges. Researchers emphasise that the digital euro must ensure a level of privacy comparable to cash transactions [11], and regulatory documents envisage it being free of charge and equivalent to cash [11]. At the same time, legislators must resolve the problem of potential disintermediation—a mass shift of funds from bank deposits to CBDC—and reconcile instant transactions with anti-money laundering (AML/KYC) requirements.

Anti-money laundering in the crypto space remains unresolved. European rules require virtual asset providers to conduct customer identification and transmit transaction information (Travel Rule), but anonymous technologies—mixers and private wallets—allow evasion of tracking. The fragmentation of supervision further complicates the situation: in the digital sphere, authority is distributed among financial regulators (ESMA, EBA, ECB), data protection bodies (EDPB), and law enforcement, creating a risk of blind spots and jurisdictional conflicts.

The examined EU regulatory experience is directly relevant to Ukraine. As a candidate country, Ukraine is obliged to adapt the financial acquis communautaire, and the "Ukraine Plan" provides, inter alia, for the alignment of virtual asset legislation with the acquis by the end of Q4 2025 [14]. In the area of crypto-asset regulation, the Law "On Virtual Assets" No. 2074-IX was adopted in February 2022; however, it has not yet fully entered into force due to the absence of implementing regulations, particularly regarding taxation [14]. Legislators are

developing draft laws to align domestic rules with MiCA, including VASP licensing, asset categorisation, and AML standards.

In the area of open banking, Ukraine has demonstrated significant progress: NBU Resolution No. 80 of July 2025 implemented PSD2 requirements, obliging banks to provide API access to accounts for licensed third parties [7; 8]. Banking reform envisages strengthening capital and prudential requirements in accordance with CRD/CRR and updating stress-testing systems, although banks do not yet have extensive experience working with digital risks to DORA standards. In the area of anti-money laundering, the NBU and NAPC are gradually adapting their norms to FATF models, while the NSSMC is developing provisions on tokenised securities following the example of the DLT Pilot Regime. The "Diia" platform demonstrates a high level of digital readiness and may serve as infrastructure for financial innovations, notably a potential e-hryvnia [11].

A summary of the state of EU standard implementation in Ukraine is presented in Table 2.

Table 2. Status of EU digital finance standard implementation in Ukraine (as of early 2026)

Area	EU standard	Ukrainian implementation	Status as of early 2026
Crypto-assets	MiCA	Law "On Virtual Assets" No. 2074-IX (02.2022); draft laws to align with MiCA (VASP licensing, categorisation, AML)	Law adopted, but implementing acts (notably tax) in development; VASP licensing not yet launched
Open banking	PSD2/ PSD3	NBU Resolution No. 80 of 25.07.2025 (AIS/PIS providers)	Effective from 01.08.2025; banks gradually deploying API interfaces
Cyber resilience	DORA	No dedicated analogue; elements of ICT requirements dispersed across NBU information security regulations	At initial stage; no holistic framework in place
Artificial intelligence	AI Act	No specific AI regulation in financial services	Not commenced
AML/CFT	AMLD/ Travel Rule	Law "On Prevention of Money Laundering"; KYC requirements, PEP checks; financial monitoring accounting for crypto risks	Basic requirements in force; adaptation to FATF-40 Recommendations ongoing
CBDC	Digital Euro Regulation	E-hryvnia research project (NBU)	Research stage; no pilot trials conducted

Source: compiled by the authors based on [7; 8; 11; 14].

Strategically, Ukraine faces a choice: gradual harmonisation, beginning with fundamental norms (AML, Open Banking, basic capital requirements), or a technological leap (leapfrogging)—implementing the most advanced standards while bypassing intermediate stages. The optimal approach appears to be a combination of both: prioritising the implementation of basic norms while simultaneously developing regulatory capacity, training expert personnel, and actively participating in international forums. Local adaptation is essential: stricter financial monitoring measures are justified under wartime conditions, while the format of innovation sandboxes requires adaptation to the specifics of a regulatory environment that faces primary structural challenges.

Conclusions

The regulatory architecture of the European Union in the field of digital financial markets has progressed from post-crisis reactive measures to the construction of a comprehensive digital regulatory ecosystem. The key elements of this ecosystem are the MiCA Regulation, which for the first time in global practice provides holistic legal regulation of crypto-assets; DORA, which harmonised digital operational resilience standards for the financial sector; the

updated PSD3 framework, which deepens the open financial ecosystem; the AI Act, which establishes requirements for algorithmic decision-making; and the GDPR, which ensures the protection of personal data in digital finance.

Despite the comprehensiveness of the EU's approach, significant gaps remain. Decentralised finance and global stablecoins largely remain outside the perimeter of current regulation. Algorithmic decision-making in finance requires further development of accountability and control mechanisms. Cyber risks associated with infrastructure concentration in cloud providers and the challenges of introducing the digital euro demand additional regulatory solutions.

For Ukraine, the EU's regulatory model is the most relevant benchmark, but it requires local adaptation taking into account the market scale, the level of technological readiness, and geopolitical risks. The optimal strategy is gradual harmonisation that combines the implementation of basic norms with the opportunities for technological leapfrogging. Promising directions for further research include the development of models for assessing the regulatory readiness of candidate countries for the implementation of digital financial acquis, as well as the analysis of the effectiveness of regulatory sandboxes in countries with limited institutional capacity.

References

1. House of Lords. European Banking Union and Single Rulebook: The post-crisis EU financial regulatory framework. *EU Financial Affairs Sub-Committee Report*. 2015. URL: https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/103/10305.htm

2. European Commission. Digital Finance Strategy for the EU (COM(2020) 591 final). *European Commission Communications*. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0591

3. ESMA. Final Report on the Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments. *ESMA Reports*. 2024. URL: https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf

4. EIOPA. Digital Operational Resilience Act (DORA). *EIOPA Publications*. 2024. URL: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

5. European Parliament Research Service. PSD3/PSR: New payment services framework. *EPRS Briefing*. 2023. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739259/EPRS_BRI(2023)739259_EN.pdf

6. CertiK. MiCA's Benefits and Limitations: An Auditing Perspective on EU Stablecoin Regulation. *CertiK Blog*. 2026. URL: https://www.certik.com/blog/micas-benefits-and-limitations-an-auditing-perspective-on-eu-stablecoin

7. Wolf Theiss. Open banking in Ukraine: AIS/PIS providers and their regulatory status. *Wolf Theiss Client Alert*. 2025. URL: https://www.wolftheiss.com/insights/open-banking-in-ukraine-ais-pis-providers-and-their-regulatory-status/

8. CEE Legal Matters. Open Banking to Launch in Ukraine on 1 August 2025. *CEE Legal Matters Briefings*. 2025. URL: https://ceelegalmatters.com/briefings/30411-open-banking-to-launch-in-ukraine-on-1-august-2025

9. Goodwin. EU AI Act: Key Points for Financial Services Businesses. *Goodwin Legal Alerts*. 2024. URL: https://www.goodwinlaw.com/en/insights/publications/2024/08/alerts-practices-pif-key-points-for-financial-services-businesses

10. Mitchell J. The Future of Credit Underwriting and Insurance Under the EU AI Act: Implications for Europe and Beyond. *Harvard Data Science Review*. 2025. Issue 7.3. DOI: https://doi.org/10.1162/99608f92. URL: https://hdsr.mitpress.mit.edu/pub/19cwd6qx/release/2

11. Chomczyk Penedo A. Digital euro: balancing privacy and regulatory compliance. *EBA Discussion Papers*. 2024. URL: https://www.eba.europa.eu/sites/default/files/2024-12/bb883c9c-1b54-4bb6-b489-aacaedc351b5/session_5_paper_1_andres_chomcyk_penedo.pdf

12. BIS. Regulatory sandboxes and fintech funding: evidence from the UK. *BIS Working Papers*. 2023. No. 901. URL: https://www.bis.org/publ/work901.pdf

13. European Parliament. BigTech Finance: Opportunities and Risks. *IPOL In-Depth Analysis*. 2024. URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/755724/IPOL_IDA(2024)755724_EN.pdf

14. RUSI. Public–Private Partnerships and Virtual Assets in Ukraine: Taskforce Report. *Royal United Services Institute Reports*. 2025. URL: https://static.rusi.org/ukraine-ppps-taskforce-second-report-august-2025.pdf