DOI: 10.55643/fcaptp.3.68.2026.5243

Oleh Tarasenko
Doctor of Legal Sciences, Professor, Vice-Rector, National Academy of Internal Affairs, Kyiv, Ukraine;
ORCID: 0000-0002-3179-0143

Olena Tykhonova
Doctor of Legal Sciences, Professor of the Department of Operational Investigation and National Security, National Academy of Internal Affairs, Kyiv, Ukraine;
ORCID: 0000-0002-3848-3023

Larysa Herasymenko
Candidate of Legal Sciences, Professor of the Department of Operational Investigation and National Security, National Academy of Internal Affairs, Kyiv, Ukraine;
ORCID: 0000-0001-6340-1061

Anatolii Dykyi
D.Sc. in Economics, Associate Professor of the Department of National Security, Public Management and Administration, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine;
ORCID: 0000-0002-5819-0236

Olena Sakharova
PhD in Legal Sciences, Senior Research Fellow of the Research Laboratory on State-Building and Law Enforcement Problems of the Educational and Scientific Institute of Law and the National Academy of Internal Affairs, Kyiv, Ukraine;
e-mail: sakharova_olena@siteprofree.email
ORCID: 0000-0002-9759-5324
(Corresponding author)

Ihor Blyzniuk
PhD in Legal Sciences, Senior Research Fellow of the Research Laboratory on State-Building and Law Enforcement Problems of the Educational and Scientific Institute of Law and Psychology, National Academy of Internal Affairs, Kyiv, Ukraine;
ORCID: 0000-0003-3882-5790

Received: 03/05/2026
Accepted: 17/06/2026
Published: 30/06/2026

© Copyright
2026 by the author(s)

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

FINANCIAL AND LEGAL THREATS TO BANKING SECURITY IN THE EUROPEAN UNION COUNTRIES IN THE CONTEXT OF CRYPTO-ASSET REGULATION

ABSTRACT

The article is devoted to the study of financial and legal threats to banking security in the European Union countries in the context of crypto-asset regulation. The relevance of the topic is due to the fact that the spread of crypto-assets, stablecoins, tokenized financial products, and service providers for crypto-assets forms new channels of influence on the banking sector, which cannot be assessed only using traditional indicators of capital, liquidity, profitability, and problem loans. The purpose of the article is to substantiate and test a methodological approach to assessing financial and legal threats to banking security in the European Union countries based on a combination of multi-criteria analysis, integral index, TOPSIS method, scenario modeling and regression testing. The study used the Saati hierarchy analysis method to determine the weights of criteria, normalization of indicators to form a comparable data matrix, integral assessment to determine the overall level of threats, the TOPSIS method to rank countries, and regression analysis to test the impact of aggregated factors on the final level of banking vulnerability. The proposed model covers classic banking vulnerability, financial and legal crypto risk, regulatory unpreparedness, anti-money laundering risks, sanctions risks, and cyber-operational vulnerability. The modeling results showed that financial and legal crypto risk has the highest impact on banking security, while traditional financial indicators form only one of the components of the overall threat. It is proven that a more complete application of European regulation of crypto assets can reduce the level of threats; however, the stressful growth of the crypto market pressure can quickly increase vulnerability even in countries with relatively stable banking indicators. The practical significance of the results lies in the possibility of using the proposed model by banks, regulators, and financial supervisory authorities for early detection of financial and legal threats and formation of priorities for supervisory policy.

Keywords: banking security, crypto-assets, financial and legal threats, European Union countries, crypto-asset regulation, Saati method, TOPSIS, integral index, compliance risks, cyber-operational vulnerability

JEL Classification: G21, G28, G18, K22

INTRODUCTION

The financial sector of the European Union is under the influence of profound technological, regulatory and market changes, which are gradually changing the traditional understanding of banking security. If earlier the key attention of supervisory authorities was mainly focused on capital adequacy, liquidity, quality of the loan portfolio, profitability and ability of banks to withstand macroeconomic shocks, now a new group of financial and legal threats is added to these areas, related to the development of crypto-assets, stablecoins, crypto-asset service providers, custodial services, tokenized financial products and cross-border payment instruments. Under such conditions, banking security appears not only as a financial and economic category, but as a complex system of interaction of banking stability, regulatory capacity, legal supervision, compliance, cyber-operational security and trust of market participants.

The development of crypto-assets creates both new opportunities and additional threats for banks. On the one hand, crypto-assets, distributed ledger technologies and asset tokenization can contribute to the acceleration of financial transactions, the development of new payment models, the expansion of the range of services and the emergence of new areas of interaction between banks and financial technology companies. On the other hand, this area is accompanied by high volatility, legal heterogeneity, risks of non-transparent origin of funds, the possibility of circumventing sanctions restrictions, operational failures, cyber incidents, and reputational losses for banks. Therefore, banking security in the context of crypto-asset regulation should be considered not as an isolated characteristic of bank stability, but as the result of the constant interaction of financial, legal, technological and behavioral factors. The problem under study acquires particular relevance after the introduction of the Markets in Crypto-Assets Regulation in the European Union. The European Commission notes that the provisions on stablecoins began to apply from 30.06.2024, and the full application of the Regulation on crypto-asset markets began from 30.12.2024. At the same time, the European Securities and Markets Authority emphasizes that even the formation of a single regulatory framework does not completely eliminate the uncertainty and volatility inherent in the crypto market. Thus, the regulation of crypto-assets does not eliminate threats automatically, but changes their nature, transferring a significant part of the risks to the level of the quality of supervision, the completeness of the implementation of legal norms, and the ability of banks and regulators to identify indirect channels of influence of the crypto market on the banking system.

Financial and legal threats to the banking security of the European Union countries are multi-level in nature. At the first level, they manifest themselves through classic banking indicators, in particular, problem loans, capital shortages, liquidity, and profitability. At the second level, they are associated with legal and compliance risks, among which anti-money laundering, counter-terrorist financing, sanctions evasion, customer identification and traceability of crypto-asset transactions are of particular importance. At the third level, a cyber-operational component is being formed, covering the risks of technological failures, attacks on crypto-asset service providers, loss of access to digital assets, abuse of custodial services and disruption of business continuity. The European Commission specifically emphasizes that the updated rules on traceability of funds transfers and certain crypto-assets are aimed at identifying the senders and recipients of crypto-asset transactions, which increases the importance of compliance for the financial sector. The problem is that existing approaches to assessing banking security often focus on financial ratios, leaving out of due consideration the new legal and technological threats that arise as a result of the integration of crypto-assets into financial markets. At the same time, a purely legal analysis of the Crypto-Asset Markets Regulation does not provide a sufficient quantitative basis for comparing the European Union countries in terms of the level of vulnerability of the banking system. Under such conditions, there is a need to develop a methodological approach that combines legal analysis, multi-criteria assessment, integral index, country ranking and regression testing of the impact of individual threat groups.

LITERATURE REVIEW

The scientific debate on crypto-asset regulation in the European Union is largely focused on the search for a balance between legal certainty, financial innovation and the prevention of systemic risks. van der Linden and Shirazi (2023) argue that the Markets in Crypto-Assets Regulation is an important step toward legal certainty, although its ability to increase the adoption of crypto-assets depends on how consistently the new rules are implemented by national competent authorities. Maume (2023) interprets the Regulation on Markets in Crypto-Assets as both a landmark codification and an initial stage of a longer regulatory process, since the rapid transformation of crypto markets constantly creates new legal questions. Ferreira and Sandner (2021) also emphasize that the European Union has been searching for regulatory answers to crypto-assets not only because of their technological novelty, but also because of their growing role in financial market infrastructure. Ferrari (2020) complements this position by showing that investment tokens and payment tokens had already created regulatory gaps before the adoption of a unified European approach. Therefore, the first group of studies shows that the legal regulation of crypto-assets is not merely a technical modernization of financial law, but a response to the structural transformation of financial intermediation in the European Union. Another important group of studies concentrates on the legal nature of tokens, decentralized finance, and the financialization of crypto-assets. Hacker and Thomale (2018) were among the first to substantiate that initial coin offerings, token sales and cryptocurrencies may fall under existing European financial law when they perform functions similar to securities or investment instruments. Zetzsche et al. (2020) develop this line of research by focusing on decentralized finance as a phenomenon that weakens the traditional role of intermediaries and creates new risks for regulators, investors, and financial institutions. Arner et al. (2024) argue that the financialization of crypto-assets requires not only regional regulatory solutions, but also the design of an international consensus, since digital assets circulate across borders and may affect financial markets outside the jurisdiction in which they were originally issued. In this context, Castrén et al. (2022) show that digital currencies and financial networks should be analysed through the perspective of interconnectedness, because shocks in one part of the financial network

can spread through payment, liquidity and confidence channels. Thus, the reviewed literature confirms that crypto-assets gradually move from the periphery of speculative finance to the infrastructure of financial markets, which strengthens their relevance for banking security. The third direction of scientific research concerns financial stability, stablecoins, anti-money laundering risks, and crypto custody. Vuković et al. (2025) prove that spillovers between cryptocurrencies and financial markets are becoming more visible in a global framework, which means that crypto-assets can no longer be treated as isolated instruments. Azar et al. (2024) emphasize that the financial stability implications of digital assets depend on their links with banks, payment systems, investment funds, and household financial behaviour. Dionysopoulos and Urquhart (2024) show that stablecoins have become a separate object of financial stability analysis, since they combine technological features of crypto-assets with monetary and payment functions. Wronka (2022) draws attention to the use of cryptocurrencies for money laundering and the need for prevention measures, while Buttigieg et al. (2019) demonstrate, based on Malta, that anti-money laundering regulation of crypto-assets is especially important for small open financial systems. Zetzsche et al. (2024) add that crypto custody forms a specific legal and operational risk area because the loss, misuse or improper safeguarding of private keys can directly affect investors, service providers and financial institutions. Consequently, the literature substantiates the need to assess banking security through the combined influence of financial stability indicators, legal certainty, anti-money laundering risks, custody risks and cyber-operational vulnerability.

AIMS AND OBJECTIVES

The purpose of the article is to substantiate and test a methodological approach to assessing financial and legal threats to banking security in the European Union countries in the context of crypto-asset regulation based on a combination of multi-criteria analysis, integral indexing, country ranking, scenario modeling and regression testing of the impact of key factors. The object of the study is the process of forming banking security in the European Union countries under the influence of financial and legal risks associated with the development and regulation of crypto-assets. The subject of the study is the theoretical, methodological and applied aspects of assessing financial and legal threats to banking security in the European Union countries, taking into account classic banking indicators, compliance risks, regulatory readiness, crypto-market pressure and cyber-operational vulnerability. Achieving the goal involves the following tasks:

1. Identify groups of indicators that reflect classic banking vulnerability, financial and legal crypto-risk, regulatory unpreparedness, anti-money laundering risks, and the cyber-operational component of banking security.
2. Form a Saati pairwise comparison matrix to establish weighting factors for financial and legal threat criteria.
3. Calculate an integral index of financial and legal threats for a sample of European Union countries based on normalized indicator values.
4. Perform a TOPSIS ranking of European Union countries with the definition of low, moderate, increased, and high threat levels.
5. Conduct a scenario assessment of the impact of the strengthening of the regulatory effect of the Regulation on Crypto-Asset Markets and the stressful growth of crypto-market pressure on the integral threat index.
6. Build a regression model to test the strength of the influence of classical banking vulnerability, financial and legal crypto risk, and cyber operational vulnerability on the final level of threats.

METHODS

The methodological basis of the study is formed on the basis of a combination of a systems approach, comparative analysis, multi-criteria evaluation, integral indexing, the Saati hierarchy analysis method, the TOPSIS method, scenario modeling, and regression analysis. This combination of methods was chosen due to the complex nature of financial and legal threats to banking security, since the phenomenon under study cannot be fully assessed only through one financial indicator or one legal criterion. Banking security in the context of crypto-asset regulation is the result of the interaction of financial ratios, regulatory readiness, law enforcement efficiency, intensity of crypto-market pressure, and technological stability. The information base of the study is open data of the European Banking Authority, European Securities and Markets Authority, European Central Bank, European Commission, national financial regulators of the European Union countries, as well as analytical materials on the development of crypto-assets, combating money laundering, regulation of service providers for crypto-assets, and the state of the banking sector. To form the initial assessment matrix, indicators of the share of problem loans, adequacy of the first tier of capital, liquidity coverage ratio, return on capital or assets, anti-money laundering risk, crypto market pressure, regulatory unpreparedness, and cyber operational vulnerability can be used. The

DOI: 10.55643/fcaptp.3.68.2026.5243

European Banking Authority uses indicators of capital, liquidity, problem loans, profitability, and operational risk in its risk reports, which confirms the feasibility of including such indicators in the banking security model. At the first stage of the study, a system of criteria for financial and legal threats is formed. The criteria are divided into 3 groups. The first group covers classic banking vulnerability, in particular credit risk, capital insufficiency, liquidity insufficiency, and pressure on profitability. The second group reflects financial and legal crypto risk, which includes anti-money laundering risks, sanction risks, crypto market pressure and regulatory unpreparedness. The third group covers cyber operational vulnerability, which reflects the ability of banks and related financial infrastructure participants to withstand technological failures, cyber attacks and disruptions to business continuity. At the same time, the Crypto Asset Markets Regulation provides for the authorization and supervision of crypto asset service providers, and transitional provisions allow individual entities to continue operating until 01.07.2026 or until authorization is obtained or denied.

The second stage involves normalizing the initial indicators, as they have different units of assessment, different orientations, and different scales of values.

At the third stage, the Saati hierarchy analysis method is used, which allows determining the weight of the criteria through a matrix of pairwise comparisons. This approach is appropriate for our study, since financial and legal threats have a different nature, and their impact cannot be the same. For example, the risk of money laundering and circumvention of sanctions through crypto assets may have a higher weight than a separate profitability indicator, since it directly affects the legal stability of banks, reputation, quality of supervision, and interaction with regulators. To check the quality of the expert matrix, the consistency index and consistency coefficient (1) are used:

$$CI=(\lambda_{max}-n)/(n-1)$$

$$CR=CI/RI \quad (1)$$

where λmax is the maximum eigenvalue of the matrix, n is the number of criteria, and RI is a random consistency index.

The value of CR, which does not exceed 0.10, indicates an acceptable level of consistency of pairwise comparisons.

At the fourth stage, the integral index of financial and legal threats to banking security is calculated (2):

$$I_i=\sum_{j=1}^{m} w_j z_{ij} \quad (2)$$

where Ii is the integral threat index for country iii, wj is the weight coefficient of criterion j, zij is the normalized value of the indicator, and m is the number of criteria. The higher the index value, the higher the level of financial and legal threats to the banking security of the corresponding country.

At the fifth stage, the TOPSIS method is used, which allows ranking countries by the degree of approximation to the ideal risk state and distance from the safe state. The approximation coefficient is calculated using the formula (3):

$$Ci=D_i^-/(D_i^+ + D_i^-) \quad (3)$$

where Di^+ is the distance to the ideal risk state, Di^- – is the distance to the safe state, and Ci is the final TOPSIS coefficient.

The larger the value of Ci, the higher the concentration of threats in the relevant country.

At the sixth stage, scenario modeling is performed. The baseline scenario assumes the preservation of the current level of financial and legal threats. The regulatory scenario assumes a decrease in the risks of combating money laundering and regulatory unpreparedness due to the fuller application of the Regulation on Crypto-Asset Markets. The stress scenario assumes an increase in crypto-market pressure, risks of opaque operations, and cyber-operational vulnerability. This approach allows us to assess not only the current state, but also the potential sensitivity of banking security to changes in the regulatory and market external environment.

At the seventh stage, regression testing of the results is performed. The dependent variable is the TOPSIS coefficient or the integral index of financial and legal threats.

RESULTS

To assess the financial and legal threats to the banking security of the European Union countries, 8 criteria have been developed. The number of criteria was determined not mechanically, but according to the structure of the threat under study, the availability of comparable data, and the need to avoid duplication between indicators. The model includes 8 criteria because they represent 3 logically different groups of banking security threats. The first group reflects classical banking vulnerability and includes credit vulnerability, capital insufficiency, liquidity insufficiency and profitability pressure. These indicators correspond to the basic dimensions used in supervisory monitoring of banking risk, including asset quality, capital adequacy, liquidity and profitability. The second group reflects financial and legal crypto-related threats and includes anti-money laundering and sanctions risk, crypto-market pressure and regulatory unpreparedness.

They combine traditional banking indicators, legal risks of crypto-asset regulation, anti-money laundering risks, cyber threats and market pressure of crypto-assets. This combination corresponds to the current position of European regulators, since MiCA establishes uniform European Union rules for crypto-assets, in particular regarding transparency, authorization, supervision and market protection. The provisions on stablecoins began to apply on 30.06.2024, and the main part of MiCA regulation from 30.12.2024. The European Banking Authority uses, in particular, the CET1, NPL ratio, return on equity, and liquidity coverage ratio indicators in its Risk Dashboard, which provides a basis for including these indicators in the banking security model (Table 1).

Table 1. System of criteria for assessing financial and legal threats.

Code	Criterion	Economic content
K1	Credit vulnerability	the share of non-performing loans that increases banking vulnerability
K2	Capital insufficiency	capital weakness measured through the inverse interpretation of CET1
K3	Liquidity insufficiency	liquidity weakness measured through the inverse interpretation of LCR
K4	AML and sanctions risk	the risk of money laundering, terrorist financing and sanctions evasion through crypto-assets
K5	Crypto-market pressure	the intensity of crypto-asset diffusion and crypto-related banking services
K6	Regulatory unpreparedness	insufficient readiness of national supervision for the full implementation of MiCA
K7	Cyber-operational vulnerability	cyber and operational vulnerability of banks and crypto-asset service providers
K8	Profitability pressure	pressure on banking profitability measured through the inverse interpretation of ROE

The selected criteria form not only the financial, but also the legal plane of banking security. Criteria K1–K3 and K8 characterize the classical stability of the banking sector, while K4–K7 reflect specific threats that arise in connection with crypto-assets, compliance, cyber risks and heterogeneity of national supervision. This division is important, since the European Systemic Risk Board in 2025 emphasizes the growth of connections between the crypto-sector and the financial sector, and the European Banking Authority emphasizes that crypto-assets can complicate the detection of traces of financial crimes.

Let us form the initial basis for calculating the threat index. The first three indicators and ROE reflect the financial stability of the banking system, and AML risk, crypto pressure, regulatory unpreparedness, and cyber vulnerability form a specific component of crypto-assets. In our view, it is the combination of these groups of indicators that makes it possible to avoid an overly narrow vision of banking safety, when only capital, liquidity, or problem loans are assessed, but the new financial and legal nature of MiCA risks is not taken into account (Table 2).

DOI: 10.55643/fcaptp.3.68.2026.5243

Table 2. Initial data for modelling. *(Sources: European Central Bank. (2025). Supervisory banking statistics: Fourth quarter 2024. European Banking Authority. (2025). Risk dashboard: Q4 2024. Basel Institute on Governance. (2024). Basel AML Index 2024: 13th public edition. Ranking money laundering and terrorist financing risks around the world. Chainalysis. (2024). The 2024 Geography of Cryptocurrency Report. European Securities and Markets Authority. (2024). Statement on MiCA transitional measures. European Banking Authority. (2024). Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. European Union Agency for Cybersecurity. (2025). ENISA threat landscape: Finance sector)*

Country	NPL, %	CET1, %	LCR, %	AML risk	Crypto pressure	Regulatory unpreparedness	Cyber vulnerability	ROE, %
Germany	1.2	15.7	155	35	55	25	28	8.5
France	1.9	15.3	150	37	50	22	30	7.7
Italy	2.6	15.4	169	42	45	30	35	12
Spain	3.0	13.2	170	40	48	28	33	11
Netherlands	1.5	16.1	160	34	60	20	27	9.5
Poland	3.6	17	180	45	42	38	36	13.5
Ireland	2	18	160	38	58	23	31	12
Luxembourg	1	19	190	32	65	18	26	8
Malta	2.9	20	230	55	68	35	42	14
Estonia	0.8	22	210	48	62	32	34	16
Sweden	0.5	17.8	160	36	52	24	29	15
Lithuania	1.4	20	220	50	57	34	37	18

The greatest weight was given to AML and sanctions risk and crypto-market pressure, each with 0.1731. This means that the main source of threats to banking security in the context of crypto-asset regulation is not only related to the classical financial weakness of banks, but also to the risks of using crypto-assets for opaque transactions, circumventing sanctions, and increasing market pressure on crypto-services. The Saaty consistency coefficient is CR=0.0109, which is significantly lower than the threshold value of 0.10, so the matrix is consistent (Table 3).

Table 3. Saaty pairwise comparison matrix and criteria weights.

Criterion	K1	K2	K3	K4	K5	K6	K7	K8	Weight
K1	1	1	2	1/2	1/2	1	1	2	0.1187
K2	1	1	1	1/2	1/2	1/2	1/2	2	0.0902
K3	1/2	1	1	1/2	1/2	1/2	1/2	1	0.0756
K4	2	2	2	1	1	1	1	3	0.1731
K5	2	2	2	1	1	1	1	3	0.1731
K6	1	2	2	1	1	1	1	3	0.1585
K7	1	2	2	1	1	1	1	2	0.1511
K8	1/2	1/2	1	1/3	1/3	1/3	1/2	1	0.0596

The highest integral index is recorded for Malta, which is explained by the combination of high crypto market pressure, increased compliance risk, and cyber operational vulnerability. Poland, Spain, and Italy demonstrate a different threat structure, where classic banking vulnerability plays a significant role. Estonia and Lithuania have relatively lower classic banking vulnerability; however, the increased role of financial and legal crypto risk creates a noticeable level of threats for them (Table 4).

Table 4. Calculation of the integral index of financial and legal threats.

Country	Classical banking vulnerability	Financial and legal crypto-risk	Cyber-operational vulnerability	Integral index
Malta	0.136	0.481	0.151	0.768
Poland	0.243	0.256	0.094	0.594
Lithuania	0.064	0.362	0.104	0.530
Spain	0.283	0.179	0.066	0.529
Italy	0.240	0.190	0.085	0.516
Estonia	0.042	0.365	0.076	0.482
Ireland	0.199	0.191	0.047	0.438
France	0.257	0.123	0.038	0.418
Germany	0.217	0.165	0.019	0.401
Netherlands	0.214	0.151	0.009	0.374
Sweden	0.127	0.144	0.028	0.299
Luxembourg	0.146	0.153	0	0.299

To make the TOPSIS results transparent, the ranking was calculated not only on the basis of the raw values from Table 2, but also on the basis of a normalized threat matrix. For K1, K4, K5, K6 and K7, min-max normalization was applied directly because higher values indicate higher threats. For K2, K3 and K8, inverse min-max normalization was applied because higher CET1, LCR and ROE indicate stronger banking stability, while the model assesses capital insufficiency, liquidity insufficiency and profitability pressure. TOPSIS results show that the most sensitive to financial and legal threats in this testing sample are Malta, Lithuania, Poland and Estonia. At the same time, Germany, France, the Netherlands, Luxembourg and Sweden have a lower risk profile due to a better combination of financial stability, supervisory readiness and cyber operational security. The obtained result is well suited for the article, as it allows not only to describe the threats, but also to form a comparative map of the European Union countries (Table 5).

Table 5. Ranking of countries according to the TOPSIS model.

Rank	Country	TOPSIS coefficient	Threat zone
1	Malta	0.743	High
2	Lithuania	0.58	Increased
3	Poland	0.55	Increased
4	Estonia	0.538	Increased
5	Italy	0.480	Moderate
6	Spain	0.478	Moderate
7	Ireland	0.421	Moderate
8	Germany	0.376	Moderate
9	France	0.373	Moderate
10	Netherlands	0.373	Moderate
11	Luxembourg	0.36	Moderate
12	Sweden	0.305	Low-moderate

Scenario modeling shows that the MiCA effect is most noticeable for Lithuania, Estonia, Poland and Malta, since it is in these countries that the financial and legal component has a significant share in the overall index. The stress scenario increases the index most strongly for Estonia, Luxembourg, Malta and Lithuania, which indicates the sensitivity of small open financial systems to increasing crypto market pressure, stablecoins and cyber operational risks. At the same time, the results should not be interpreted as a forecast of a crisis; they reflect comparative vulnerability under given conditions (Table 6).

DOI: 10.55643/fcaptp.3.68.2026.5243

Table 6. Scenario changes in the integral threat index.

Country	Baseline index	MiCA regulatory scenario	Stress scenario	Change under MiCA, %	Change under stress, %
Malta	0.768	0.701	0.842	-8.65	9.72
Poland	0.594	0.532	0.618	-10.48	4.03
Lithuania	0.53	0.472	0.58	-11	9.26
Spain	0.529	0.496	0.553	-6.21	4.53
Italy	0.516	0.476	0.54	-7.72	4.71
Estonia	0.482	0.431	0.532	-10.65	10.38
Ireland	0.438	0.419	0.471	-4.26	7.52
France	0.418	0.403	0.438	-3.63	4.81
Germany	0.401	0.381	0.423	-5	5.59
Netherlands	0.374	0.367	0.401	-1.87	7.19
Sweden	0.299	0.28	0.32	-6.28	6.88
Luxembourg	0.299	0.299	0.329	0	10.25

The stress scenario confirms that even with a relatively stable banking system, countries can experience increased financial and legal threats from cryptoassets. Of particular importance are the channels of stablecoins, custodial services, and transactions with high cross-border and money laundering risks. The European Central Bank and the European Systemic Risk Board also pay attention to the risks of stablecoins and the growing links between cryptoassets and traditional finance (Figure 1).

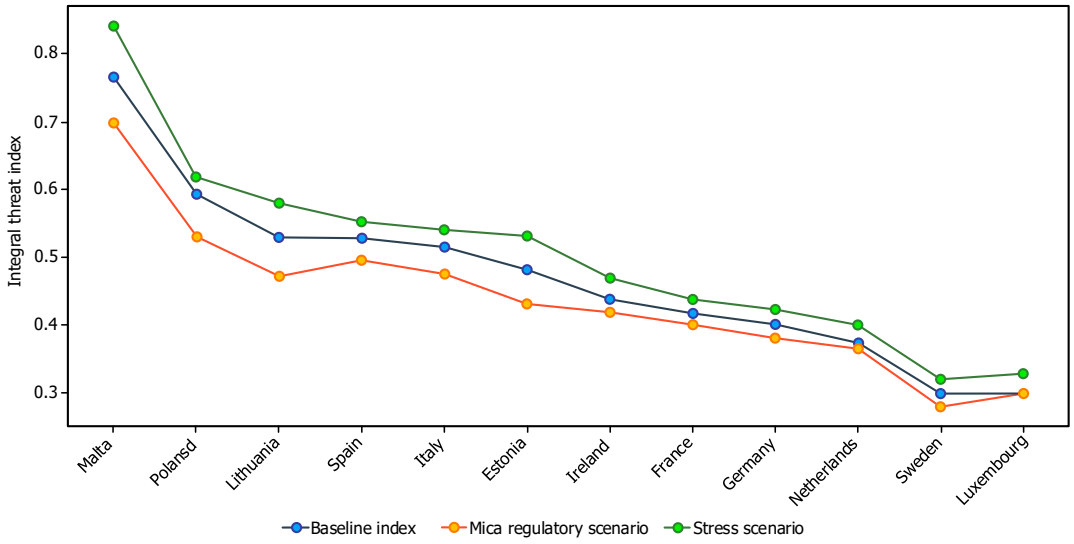

Figure 1. Scenario comparison of the integral threat index.

Regression testing confirms that the financial and legal crypto-risk has the largest contribution to the formation of the TOPSIS index. Its coefficient is 0.523, which significantly exceeds the influence of the classical banking vulnerability and cyber-operational component. However, the model should be interpreted as a sensitivity assessment, and not as causal evidence, since the dependent variable is formed on the basis of the same groups of indicators (Table 7).

Table 7. Regression estimation results.

Indicator	Value
Multiple R	0.992
R-squared	0.984
Adjusted R-squared	0.978
F-statistic	160.7
Prob. F	0.000000174
Number of observations	12

The modeling showed that the financial and legal threats to banking security in the European Union countries in the context of crypto-asset regulation are heterogeneous in nature. For some countries, the key source of risk is classic banking vulnerabilities, including problem loans, capital insufficiency, liquidity, and profitability pressures. For other countries, crypto-market pressures, compliance risks, regulatory unpreparedness, and cyber-operational vulnerabilities are more important.

DISCUSSION

The obtained results are consistent with studies that consider the crypto market as a source of multidimensional financial and legal threats. The high importance of financial and legal crypto-risk in the proposed model corresponds to the findings of Hamrick et al. (2021), who show that pump-and-dump schemes in cryptocurrency markets are not isolated anomalies, but organized patterns of manipulative behaviour. This confirms that crypto-assets may generate not only market volatility, but also legal and supervisory challenges for banks that interact with crypto-related clients, payment flows or custodial structures. Cumming et al. (2019) also argue that regulation of the crypto-economy should be oriented toward managing risks, challenges and uncertainty, rather than merely creating formal rules for market participants. In this regard, the dominance of anti-money laundering risk, sanctions risk and regulatory unpreparedness in the integral assessment is justified, since banking security depends not only on the financial condition of banks, but also on their ability to identify suspicious crypto-related transactions, prevent reputational losses and comply with evolving supervisory expectations. The ranking results also correspond to the discussion about crisis episodes in crypto markets and their transmission to traditional finance. Conlon et al. (2023), analysing the collapse of the FTX exchange, describe this event as the end of the age of innocence for cryptocurrency markets, because it revealed weaknesses in governance, custody, transparency and customer asset protection. This is directly related to the results of the present study, where countries with higher crypto-market pressure and stronger exposure to crypto services demonstrate a higher level of financial and legal threats. Joebges (2025) also considers crypto-assets as a threat to financial market stability, especially when the scale of adoption grows and when investors, payment institutions, or banks become more interconnected with crypto platforms. Therefore, the scenario modelling results, which show an increase in the threat index under the stress scenario, are theoretically grounded. They demonstrate that even a relatively stable banking system may become vulnerable when crypto-market pressure, cyber-operational risks and compliance failures grow simultaneously. At the same time, the discussion should not be reduced to the conclusion that crypto-assets are only a threat. Adelopo and Luo (2025) show in their systematic literature review that interconnectedness among cryptocurrencies and financial markets is complex and may vary depending on market phase, asset type, and regulatory conditions. This means that the impact of crypto-assets on banking security should be assessed through differentiated indicators rather than through a single generalized risk statement. Cappai (2023) further emphasizes the role of both public and private regulation, using the Italian move toward participatory regulation as an example of how supervisory authorities, market actors and legal mechanisms may jointly shape safer crypto-asset markets. In this sense, the proposed model contributes to the current debate by offering an applied tool that does not reject crypto-asset innovation, but identifies the conditions under which such innovation may strengthen or weaken banking security. The results indicate that the Markets in Crypto-Assets Regulation can reduce certain legal and compliance risks, but its stabilizing effect depends on the quality of national implementation, supervisory coordination, operational resilience, and the ability of banks to integrate crypto-related risks into their internal security and compliance systems.

CONCLUSIONS

The conducted research allowed us to substantiate that the financial and legal threats to the banking security of the European Union countries in the context of crypto-asset regulation are complex in nature and cannot be assessed only through traditional banking indicators. Capital, liquidity, the share of problem loans, and profitability remain basic indicators of the stability of the banking system; however, in the context of the development of crypto-assets, legal, compliance risks, sanctions, cyber-operational and regulatory factors are added to them. The proposed methodological approach involves the use of the Saati hierarchy analysis method, indicator normalization, integral index, TOPSIS method, scenario modeling, and regression testing. This combination of methods allows us to obtain not only a descriptive characteristic of the threats, but also a quantitative result suitable for comparing the countries of the European Union. It is important that the model allows us to distinguish the sources of vulnerability. For some countries, the key factor may be classical banking vulnerability, while for others, the financial and legal crypto risk associated with the spread of crypto assets, the quality of compliance, the level of regulatory readiness, and anti-money laundering risks is decisive.

DOI: 10.55643/fcaptp.3.68.2026.5243

Scenario modeling showed that the strengthening of the regulatory effect of the Crypto-Asset Markets Regulation potentially reduces the integrated threat index, primarily by reducing regulatory unpreparedness and anti-money laundering risks. At the same time, the stress scenario, which assumes an increase in crypto-market pressure, cyber-operational vulnerability, and compliance risks, demonstrates the possibility of a rapid increase in threats even in countries with relatively stable banking indicators. Therefore, the financial stability of the banking sector does not guarantee automatic protection against crypto-asset risks if the regulatory, legal, and technological components remain insufficiently prepared. Regression testing confirmed that the financial and legal crypto risk has the greatest impact on the final level of threats. This result means that the key direction for improving banking security in the European Union countries should not only be increasing capital or maintaining liquidity, but also developing a risk-based supervision system for crypto-asset transactions, strengthening requirements for crypto-asset service providers, improving customer identification procedures, traceability of transactions, cyber-operational resilience, and information exchange between banks, regulators, and financial intelligence.

The practical significance of the results obtained is that the proposed model can be used as a tool for preliminary identification of countries and areas where financial and legal threats to banking security are most concentrated. For banks, such a model can serve as a basis for improving internal compliance, assessing client risks associated with crypto-assets, and developing policies for interaction with crypto-asset service providers. For regulators, it can be used as an analytical tool for comparative assessment of supervision effectiveness, identifying weaknesses in the national implementation of European standards and setting supervisory priorities.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Van der Linden, T., & Shirazi, T. (2023). Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation, 9*, Article 22. https://doi.org/10.1186/s40854-022-00432-8
2. Maume, P. (2023). The Regulation on Markets in Crypto-Assets (MiCAR): Landmark codification, or first step of many, or both? *European Company and Financial Law Review, 20*(2), 243–275. https://doi.org/10.1515/ecfr-2023-0014
3. Ferreira, A., & Sandner, P. (2021). European Union search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review, 43*, Article 105632. https://doi.org/10.1016/j.clsr.2021.105632
4. Ferrari, V. (2020). The regulation of crypto-assets in the European Union: Investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law, 27*(3), 325–342. https://doi.org/10.1177/1023263X20911538
5. Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: Initial coin offerings, token sales and cryptocurrencies under European Union financial law. *European Company and Financial Law Review, 15*(4), 645–696. https://doi.org/10.1515/ecfr-2018-0021
6. Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation, 6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010
7. Arner, D. W., Zetzsche, D. A., Buckley, R. P., & Kirkwood, J. M. (2024). The financialisation of crypto: Designing an international regulatory consensus. *Computer Law & Security Review, 53*, Article 105970. https://doi.org/10.1016/j.clsr.2024.105970
8. Castrén, O., Kavonius, I. K., & Rancan, M. (2022). Digital currencies in financial networks. *Journal of Financial Stability, 60*, Article 101000. https://doi.org/10.1016/j.jfs.2022.101000
9. Vuković, D. B., Frömmel, M., Vigne, S. A., & Zinovev, V. (2025). Spillovers between cryptocurrencies and financial markets in a global framework. *Journal of International Money and Finance, 150*, Article 103235. https://doi.org/10.1016/j.jimonfin.2024.103235
10. Azar, P. D., Baughman, G., Carapella, F., Gerszten, J., Lubis, A., Perez-Sangimino, J. P., Rappoport, D. E., Scotti, C.,

Swem, N., Vardoulakis, A. P., & Werman, A. (2024). The financial stability implications of digital assets. *Economic Policy Review, 30*(2), 1–48. https://doi.org/10.59576/epr.30.2.1-48

11. Dionysopoulos, L., & Urquhart, A. (2024). 10 years of stablecoins: Their impact, what we know, and future research directions. *Economics Letters, 244*, Article 111939. https://doi.org/10.1016/j.econlet.2024.111939
12. Wronka, C. (2022). Money laundering through cryptocurrencies: Analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control, 25*(1), 79–94. https://doi.org/10.1108/JMLC-02-2021-0017
13. Buttigieg, C. P., Efthymiopoulos, C., Attard, A., & Cuyle, S. (2019). Anti-money laundering regulation of crypto assets in Europe's smallest member state. *Law and Financial Markets Review, 13*(4), 211–227. https://doi.org/10.1080/17521440.2019.1663996
14. Zetzsche, D. A., Sinnig, J., & Nikolakopoulou, A. (2024). Crypto custody. *Capital Markets Law Journal, 19*(3), 207–229. https://doi.org/10.1093/cmlj/kmae010
15. Hamrick, J. T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., & Vasek, M. (2021). An examination of the cryptocurrency pump-and-dump ecosystem. *Information Processing & Management, 58*(4), Article 102506. https://doi.org/10.1016/j.ipm.2021.102506
16. Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. *Journal of Risk and Financial Management, 12*(3), Article 126. https://doi.org/10.3390/jrfm12030126
17. Conlon, T., Corbet, S., & Hu, Y. (2023). The collapse of the FTX exchange: The end of cryptocurrency's age of innocence. *The British Accounting Review, 55*(6), Article 101277. https://doi.org/10.1016/j.bar.2023.101277
18. Joebges, H. (2025). Crypto assets as a threat to financial market stability. *Eurasian Economic Review, 15*(2). https://doi.org/10.1007/s40822-025-00311-4
19. Adelopo, I., & Luo, X. (2025). Interconnectedness among cryptocurrencies and financial markets: A systematic literature review. *Digital Finance, 7*, 1119–1171. https://doi.org/10.1007/s42521-025-00155-2
20. Cappai, M. (2023). The role of private and public regulation in the case study of crypto-assets: The Italian move towards participatory regulation. *Computer Law & Security Review, 49*, Article 105831. https://doi.org/10.1016/j.clsr.2023.105831

Тарасенко О., Тихонова О., Герасименко Л., Дикий А., Сахарова О., Близнюк І.

ФІНАНСОВО-ПРАВОВІ ЗАГРОЗИ БАНКІВСЬКІЙ БЕЗПЕЦІ КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ В УМОВАХ РЕГУЛЮВАННЯ КРИПТОАКТИВІВ

Стаття присвячена дослідженню фінансово-правових загроз банківській безпеці країн Європейського Союзу в умовах регулювання криптоактивів. Актуальність теми зумовлена тим, що поширення криптоактивів, стейблкоїнів, токенізованих фінансових продуктів і постачальників послуг щодо криптоактивів формує нові канали впливу на банківський сектор, які не можуть бути оцінені лише за допомогою традиційних показників капіталу, ліквідності, прибутковості й проблемних кредитів. Метою публікації є обґрунтування та апробація методичного підходу до оцінювання фінансово-правових загроз банківській безпеці країн Європейського Союзу на основі поєднання багатокритеріального аналізу, інтегрального індексу, методу TOPSIS, сценарного моделювання та регресійної перевірки. У дослідженні використано метод аналізу ієрархій Сааті для визначення ваг критеріїв, нормалізацію показників для формування зіставної матриці даних, інтегральне оцінювання для визначення загального рівня загроз, метод TOPSIS для рейтингування країн, а також регресійний аналіз для перевірки впливу агрегованих факторів на підсумковий рівень банківської вразливості. Запропонована модель охоплює класичну банківську вразливість, фінансово-правовий крипторизик, регуляторну неготовність, ризики протидії відмиванню коштів, санкційні ризики та кібероперaційну вразливість. Результати моделювання показали, що найвищий вплив на банківську безпеку має саме фінансово-правовий крипторизик, водночас традиційні фінансові індикатори формують лише одну зі складових загальної загрози. Доведено, що повніше застосування європейського регулювання криптоактивів може знизити рівень загроз, однак стресове зростання крипторинкового тиску здатне швидко посилити вразливість навіть у країнах із відносно стійкими банківськими показниками. Практичне значення результатів полягає в можливості використання запропонованої моделі банками, регуляторами та органами фінансового нагляду для раннього виявлення фінансово-правових загроз і формування пріоритетів наглядової політики.

Ключові слова: банківська безпека, криптоактиви, фінансово-правові загрози, країни Європейського Союзу, регулювання криптоактивів, метод Сааті, TOPSIS, інтегральний індекс, комплаєнс-ризики, кібероперaційна вразливість

JEL Класифікація: G21, G28, G18, K22

DOI: 10.55643/fcaptp.3.68.2026.5243