DOI: 10.55643/fcaptp.4.69.2026.5273

KEY THREATS TO THE FINANCIAL SECURITY OF EU COUNTRIES DUE TO INCREASED LEGAL REGULATION OF THE CRYPTOCURRENCY MARKET

Oleg Denysov
D.Sc. in Economics, Associate Professor of the Department of International Business, KROK University, Kyiv, Ukraine;
ORCID: 0009-0002-7920-3961

Iryna Skoropad
Candidate of Economic Sciences, Associate Professor of the Department of Finance, Lviv Polytechnic National University, Lviv, Ukraine;
e-mail: skoropad.edu@outlook.com
ORCID: 0000-0002-5450-0997
(Corresponding author)

Serhiy Yaroshenko
Candidate of Political Sciences, Associate Professor of the Department of Law, Interregional Academy of Personnel Management Kropyvnytskyi, Ukraine;
ORCID: 0009-0000-9792-8208

Daria Kiblik
PhD in Law, Associate Professor of the department of administrative and legal disciplines, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine;
ORCID: 0000-0002-2518-7647

Andriy Yeremenko
PhD in Economics, Associate Professor of the Department of European Economy and Business, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine;
ORCID: 0009-0005-6177-838X

Received: 20/07/2026
Accepted: 15/08/2026
Published: 31/08/2026

ABSTRACT

This article substantiates and tests a methodological approach to hierarchically categorizing key threats to the financial security of EU countries, which arise not only from inadequate cryptocurrency market regulation but also from the dramatic tightening of legal, prudential, reporting, countermeasure, and cyber-operational requirements. The purpose of this article is to develop and test a methodological approach to hierarchical ordering and an integrated assessment of the EU's key financial burdens, which will enable the successful regulation of the crypto-asset market by eliminating causal links between regulatory forces, corporate actions, market reactions, and systemic financial resources. The methodological framework encompasses documentary expert synthesis, the two-round Delphi method, binary dependency and reachability matrices, interpretive structural modeling, the Saaty hierarchy process, combining expert weighting with structural impact, integrated assessment, and scenario analysis. The information base is compiled from EU regulations, materials from ESMA, EBA, the European Commission, academic papers, and open data on WhiteBIT, KUNA, Everstake, Trustee Plus, and Hacken for 2022–2025. Five levels of the hierarchy are established. The underlying drivers are identified as uneven regulatory implementation and rising authorization and compliance costs. The ultimate systemic outcome is a trust shock with potential spillover to the banking, payment, and investment sectors. An integrated assessment revealed high sensitivity of exchange and payment business models, while cybersecurity service providers have low direct exposure but remain critical for mitigating operational risk. Scenario calculations demonstrated that coordinated and proportionate implementation can significantly reduce the overall threat level, while fragmented oversight increases concentration, regulatory arbitrage, and the diversion of activity to less regulated channels.

Keywords: financial security, EU countries, cryptocurrency, cryptoassets, legal regulation, MiCA, hierarchical ordering, Saati method, integral index, regulatory arbitrage

JEL Classification: G18, G23, G28, K22, O33

INTRODUCTION

The cryptoasset market has gradually evolved from an isolated technological segment into a component of the modern financial system. Cryptoassets are used in payment transactions, investment activities, international capital transfers, value storage, staking, and related financial services. The expansion of this market impacts the structure of financial intermediation, the speed of transactions, the distribution of liquidity, the level of transaction costs, and the nature of interactions between businesses and banks and payment institutions. At the same time, the interdependence of the cryptocurrency, banking, payment, and investment sectors is growing, resulting in disruptions to the operations of individual service providers or abrupt changes in regulatory conditions being transmitted to other participants in the financial system.

Tighter regulation of the cryptoasset market creates a dual financial and economic benefit. Harmonized requirements for authorization, capital, custody of client assets, disclosure, anti-money laundering, and operational resilience contribute to increased market transparency and consumer protection. At the same time, disproportionate, fragmented, or uneven application of such requirements increases fixed costs for enterprises, raises the minimum required scale of operations, hinders access to banking and payment channels, narrows the list of available products, and increases market concentration. Such processes can reduce competition, cause liquidity fragmentation, encourage the relocation of activities to less regulated jurisdictions, and increase market dependence on a limited number of financial and technological providers.

The scientific challenge lies in developing a methodological approach that simultaneously takes into account the expert significance of threats, their place in the causal structure, and the varying sensitivities of enterprise business models. The combination of interpretive structural modeling, Saaty hierarchy process analysis, and integrated assessment allows us to separate primary regulatory and cost factors from intermediate market reactions and ultimate threats to financial security. The practical significance of this approach lies in identifying regulatory policy priorities in which mitigating the impact of primary threats simultaneously mitigates several financial and economic consequences. The creation of a unified cryptoasset regulatory regime in the EU was a response to the expansion of cryptoasset transactions, stablecoins, and custodial and payment services. EU Regulations 2023/1114, 2023/1113, 2022/2554, and 2024/1624 tightened requirements for authorization, transfer traceability, operational resilience, and financial monitoring. Under these conditions, financial security depends on the rigor of regulatory requirements and the consistency of their application, the proportionality of costs, and the availability of legal financial channels for businesses of all sizes.

LITERATURE REVIEW

The level of scientific development of this issue is characterized by the presence of several interrelated areas. Foreign studies examine the legal certainty of the MiCA regime, the stability of stablecoins, cross-border arbitrage, the risks of storing crypto assets, combating illegal transactions, and the relationship of the cryptocurrency market with the traditional financial system.

Domestic scholars examine the role of virtual assets in money circulation and monetary policy, changes in the cryptocurrency market under martial law, the regulation of blockchain technologies in the financial system, the use of analytical tools to identify suspicious transactions, and the need to harmonize requirements for FinTech, TechFin, and cryptocurrency industries. Research confirms that the financial impact of regulation depends on proportionality, consistency, and the ability to maintain participants' activities within the regulated market segment.

Legal studies primarily characterize the content of regulations, while economic works focus on volatility, illicit flows, pricing, or the stability of individual assets.

Volosovych et al. (2024) monitor the structural changes in the market of cryptocurrency assets during the war period and establish the particular importance of payment and investment directions of its development. Their results confirm the vulnerability of the cryptocurrency market to security shocks, the development of the payment infrastructure, and the trust of traders. Blikhar et al. (2023) focus on the problems of regulatory regulation of blockchain technologies in the financial system of our region. Research indicates fragmented regulation, significant technological waste, and insufficient legal mechanisms as factors that hinder the effective use of blockchain in financial transactions.

Scholarly works devoted to the legal regulation of cryptoassets in the EU demonstrate a gradual shift from attempts to apply traditional legislation to the development of a specialized regime. Hacker and Thomale (2018) substantiated the possibility of classifying tokens within existing financial law, but simultaneously demonstrated the uncertainty surrounding the functionally distinct assets. Ferrari (2020) systematized the differences between investment and payment tokens, noting gaps in the implementation of a unified approach. Ferreira and Sandner (2021) examined the EU's search for a regulatory response as part of the restructuring of financial market infrastructure.

Following the formation of MiCA, the discussion shifted to assessing the comprehensiveness and long-term viability of the new regime. van der Linden and Shirazi (2023) argue that legal certainty can facilitate the adoption of cryptoassets, but the outcome depends on the consistency of implementation. Maume (2023) characterizes MiCA as both a landmark codification and the first stage of further legal development. Arner et al. (2024) expand on this position, noting that the financialization of cryptoassets requires international coordination, as a purely regional regime does not eliminate cross-border arbitrage.

A separate line of research examines the interconnectedness of cryptoassets with the traditional financial sector. Castren et al. (2022) show that digital currencies affect financial account networks through the redistribution of deposits, liquidity,

and balance sheet positions. Azar et al. (2024) systematize channels of financial instability related to asset valuation, leverage, funding risk, and interdependence. Makarov and Schoar (2020) found significant cross-border price disagreements, indicating market fragmentation and limited arbitrage. Consequently, differences in supervisory regimes may be reflected not only in corporate costs but also in the distribution of liquidity across countries.

Stablecoin stability is another component of financial security. Lyons and Viswanath-Natraj (2023) demonstrated that the quality of the arbitrage mechanism and access to reserves influence deviations from parity. Dionysopoulos and Urquhart (2024) summarized a decade of stablecoin development and identified unresolved issues regarding reserves, liquidity, and systemic significance. These results confirm that hard caps on individual assets can mitigate certain risks, but at the same time led to delistings, a narrowing of trading pairs, and a shift in demand toward less transparent instruments.

The issue of illicit flows and market abuse is addressed by Foley et al. (2019), Wronka (2022), Buttigieg et al. (2019), Gandal et al. (2018), and Hamrick et al. (2021). Researchers confirm the reality of cryptocurrency illicit use, manipulation schemes, and the need for proper customer due diligence. However, increased oversight without accessible authorization procedures may push transactions toward non-custodial or offshore channels, where oversight institutions have weaker capabilities. Consequently, the outcome depends on the legal regime's ability to maintain activity within the regulated sector.

Decentralized money and custodial services add to the range of risks. Zetzsche et al. (2020) and Schär (2021) note the openness and interoperability of protocols, as well as technological, governance, and systemic risks. Zetzsche et al. (2024) demonstrate that cryptocurrency custody requires specific rules for protecting client assets, assigning liability, and controlling private keys. Cumming et al. (2019) summarize regulatory uncertainty as an independent source of entrepreneurial risk. This review confirms the need for a methodology that combines legal, financial, behavioral, and cyber-operational factors in a single hierarchical framework.

Research on the monetary and financial implications of cryptoassets shows that they are increasingly connected to conventional policy channels. Karau (2023) demonstrates that Bitcoin’s response to US monetary policy has changed over time and became comparable to that of other risky assets after late 2020. The study also shows that monetary tightening can affect Bitcoin demand through speculative motives and cross-border value-transfer channels. These findings support treating cryptoassets as a segment through which monetary conditions and financial-market expectations may be transmitted.

Tarasenko et al. (2026) analyze the financial and legal threats to a banking-unemployed country in the EU under cryptoasset regulation. The authors' proposals are based on classic indicators of banking resilience, including financial monitoring systems, regulatory unpreparedness, the cryptocurrency market crisis, and cyber-operational activity. The results confirm the need to assess cryptoasset regulation through capital, liquidity, availability, banking services, and technological resilience.

Despite a significant number of publications, the mechanism by which regulatory impact is consistently transmitted from regulatory requirements to the costs and business models of cryptocurrency service providers, and from there to competition, liquidity, banking services, and the trust of financial market participants, remains understudied. Existing approaches do not fully establish which threats are the initial causes that act as channels for transmitting impact, and which become the final systemic consequences.

AIMS AND OBJECTIVES

The purpose of this article is to develop and test a methodological approach to hierarchical ordering and an integrated assessment of the EU's key financial burdens, which will enable the successful regulation of the crypto-asset market by eliminating causal links between regulatory forces, corporate actions, market reactions, and systemic financial resources. Achieving the stated goal requires removing such barriers.

1. Analyze financial and economic proposals for regulating the crypto-asset market in 2022–2025 and identify the main channels for their transfer into the EU financial system.
2. Systematize key amounts associated with disproportionate, fragmented, or insufficient narrow implementation of the regulator.
3. Establish direct and indirect pathologies between threats, induce their causal arrears, and identify significant initial, intermediate, and criminal threats. Key threat indicators for the Saaty hierarchy analysis method, assessing the narrowness of expert fates, and substantiating expert significance with the structural strength of the investment.

DOI: 10.55643/fcaptp.4.69.2026.5273

4. Ensures the adequacy of the proposed methodological approach for WhiteBIT, KUNA, Everstake, Trustee Plus, and Hacken applications, whose business models are considered based on the nature of interactions with business, payment, banking, staking, and cybersecurity infrastructure.
5. Review scenario assessment and analysis of the results' reliability, and identify priority methods for minimizing and mitigating the introduced loads.

METHODS

The study utilized a combination of general scientific and specialized methods. Financial and economic analysis was employed to determine the impact of regulatory changes on costs, liquidity, banking services, market concentration, and trust. Content analysis of regulations and scientific publications was used to develop an initial list of threats. Comparative analysis provided a comparison of regulatory requirements, transition regimes, and enterprise business models. Expert assessment was applied to determine the significance of threats and verify direct cause-and-effect relationships. Interpretive structural modeling was used to construct a threat hierarchy. The Saaty hierarchy analysis method determined their relative significance. An integrated assessment was applied to calculate the level of regulatory sensitivity of enterprises. Scenario and sensitivity analysis were used to verify the robustness of the obtained results. Interpretive structural modeling was chosen as the key research method, since the problem posed requires establishing the significance of each threat and its place in the cause-and-effect sequence. The Saaty hierarchy analysis method allows one to determine the relative priorities of threats, but does not establish which of them generate the subsequent market and financial consequences. Interpretive structural modeling addresses this limitation by classifying threats into primary factors, intermediate impact transmission channels, and final systemic outcomes. The integrated assessment then provides applied validation of the established hierarchy at the level of various business models.

The study was conducted in seven consecutive stages. In the first stage, EU regulations, regulatory materials, and scientific papers were analyzed, forming a preliminary list of threats. In the second stage, an expert assessment of their significance and causal relationships was conducted. In the third stage, a binary matrix of direct dependencies was constructed. In the fourth stage, a reachability matrix was formed, and hierarchy levels were determined. In the fifth stage, threat weights were calculated using the Saaty method, the matrix consistency was verified, and the expert weighting was combined with the structural impact strength. In the sixth stage, the annual threat intensity, business model sensitivity coefficients, and integrated enterprise indices were determined for 2022–2025. At stage 7, scenario calculations and a sensitivity analysis of the results to changes in the ratio of expert and structural weight components were conducted.

The information base was compiled from EU regulations, materials from the European Securities and Markets Authority, the European Banking Authority, and the European Commission, scientific publications, official company announcements, public registration data, and information on changes in their activities in 2022–2025. Regulatory and documentary sources for recorded changes in the activities of the studied companies:

$$Z = \{z_1, z_2, \ldots, z_n\}, \quad (1)$$

where Z is the set of threats, z_i is an individual threat, and n is the number of threats.

$$a_{ij} = 1, \text{ if } z_i \text{ affects } z_j;\ a_{ij} = 0, \text{ if no influence is identified} \quad (2)$$

The Delphi panel comprised 28 experts. Experts were selected purposively according to professional competence in financial regulation, crypto-asset markets, banking and payment services, compliance, cybersecurity, or academic research related to financial security. Eligibility required at least 5 years of relevant professional or research experience and familiarity with European financial regulation or crypto-asset market practices. The panel was formed to ensure diversity of professional backgrounds and geographical experience across European jurisdictions. In the first round, experts independently assessed the significance of the identified threats and the direct causal relationships between them. In the second round, participants reconsidered their assessments after receiving anonymized aggregated results from the first round. Consensus was evaluated using Kendall's coefficient of concordance.

The binary matrix A is used to construct the transitive closure, which captures direct and indirect relationships:

$$R = I \vee A \vee A^2 \vee \ldots \vee A^{n-1}, \quad (3)$$

$$S(z_i) = \{z_j \mid r_{ij} = 1\}, \quad (4)$$

$$P(z_i) = \{z_j \mid r_{ji} = 1\}, \quad (5)$$

$$Q(z_i) = S(z_i) \cap P(z_i). \quad (6)$$

Vertices for which $S(z_i)=Q(z_i)$ form the current top level of the hierarchy. After they are removed, the procedure is repeated until the entire set is ordered:

$$W = 12S / [m^2(n^3 - n) - mT], \quad (7)$$

where W is Kendall's coefficient of concordance, m is the number of expert-analytical profiles, n is the number of threats, S is the sum of squared deviations of the rank sums, and T is the correction for tied ranks.

$$b_{ij} = 1 / b_{ji}, \; b_{ii} = 1 \quad (8)$$

$$w^{AHP} = \text{norm}(\text{eigvec}(B, \lambda_{max})), \quad (9)$$

$$CI = (\lambda_{max} - n)/(n - 1); \; CR = CI/RI. \quad (10)$$

A matrix is considered consistent when $CR \leq 0.10$. The structural influence strength of a threat is defined as the proportion of reachable vertices in the total number of relationships:

$$d_j = (\Sigma_k r_{jk}) / (\Sigma_p \Sigma_k r_{pk}), \quad (11)$$

$$w_j = \alpha w_j^{AHP} + (1 - \alpha) d_j, \; \alpha = 0.65. \quad (12)$$

Annual threat intensity was obtained as a weighted average of normalized source scores for the corresponding year:

$$q_{jt} = (\Sigma_h \omega_h s_{hjt}) / 9. \quad (13)$$

Enterprise exposure e_{ij} reflects the dependence of the business model on authorization, custodial operations, payment infrastructure, cross-border access, and the volume of regulatory data. A correction coefficient c_{ijt} was applied to documented events in 2025:

$$x_{ijt} = \min(1; q_{jt} \cdot e_{ij} \cdot c_{ijt}), \quad (14)$$

$$v_{ijt} = w_j \cdot x_{ijt}, \quad (15)$$

$$I_{it} = \Sigma_j v_{ijt}, \quad (16)$$

$$g_{it} = (I_{it} / I_{i,t-1} - 1) \cdot 100\%. \quad (17)$$

Four intervals were used to interpret the composite index. Values up to 0.25 correspond to a low threat level, 0.2501–0.45 to a moderate level, 0.4501–0.65 to an elevated level, and values above 0.65 to a high level. The scenario index is constructed by changing individual components by δ_j^s:

$$I_{it}^s = \Sigma_j w_j x_{ijt}(1 + \delta_j^s). \quad (18)$$

RESULTS

The period 2022–2025 encompasses the transition from political approval of the new regime to its full implementation. In 2022, expectations of future requirements and the fallout from the collapse of major cryptocurrency platforms dominated. In 2023, MiCA and the traceability rules were formally adopted. In 2024, the rules regarding asset-backed tokens and e-money tokens began to be implemented, and from December 30, 2024, the main set of requirements for service providers began to be implemented. In 2025, the financial sector moved toward practical agreement on authorization, transition periods, DORA, anti-money laundering rules, and national supervisory practices (Table 1).

DOI: 10.55643/fcaptp.4.69.2026.5273

Table 1. Chronology of strengthened legal regulation of the crypto-asset market in countries of the European Union, 2022–2025.
(Source: compiled from Regulations (EU) 2022/2554, 2023/1113, 2023/1114, and 2024/1624, and ESMA and EBA materials)

Year	Key developments	Main transmission channels to financial security
2022	Political agreement on MiCA; adoption of DORA; consequences of the Terra and FTX collapses	Anticipated costs, stricter reserve requirements, and increased attention to custody and operational resilience
2023	Adoption of Regulations (EU) 2023/1114 and 2023/1113	Formalization of authorization, disclosure, transfer traceability, and provider liability
2024	Application of ART/EMT provisions from 30 June 2024; full application of MiCA from 30 December 2024	Delisting or restriction of selected assets, product restructuring, and higher documentation and reserve costs
2025	Practical CASP authorization; application of DORA; divergent national transitional regimes	Market concentration, uneven access to banking services, regulatory arbitrage, and growing technological dependence

The presented timeline reflects a gradual transition from the expected regulatory burden to the actual costs of authorization, reservations, documentation, asset protection, and operational resilience. In 2022–2023, companies primarily built organizational and financial reserves for future adaptation, while in 2024–2025, requirements began to directly impact the structure of operating expenses, product offerings, banking terms, and access to liquidity. For the financial system, this transition means the potential for increased market concentration if compliance costs exceed the adaptive capacity of small and medium-sized service providers.

A systematization of the causal channels allowed us to identify nine threats. Their formulations are aimed not at denying the need for regulation, but at identifying the undesirable consequences of its disproportionate, fragmented, or insufficiently coordinated application. A key characteristic of the emerging set is the presence of both basic legal drivers and intermediate market reactions, as well as an ultimate systemic outcome. The formalization of the transfer of threats is formed in a similar way to the value of the totality Z indicated in formula (1) (Table 2).

Table 2. Key threats to the financial security of countries of the European Union resulting from strengthened legal regulation of the cryptocurrency market.

Code	Mnemonic	Threat description	Type
Z1	UIT	Uneven implementation and transitional regimes across countries of the European Union	External legal
Z2	RCC	Rising authorization, capital, reporting, and compliance costs	Internal cost-related
Z3	MPC	Exit of small and medium-sized providers and market concentration	Market-structural
Z4	BPR	Restricted access to banking and payment services	Financial-intermediation
Z5	RAR	Relocation of operations to offshore or decentralized channels	Cross-border behavioral
Z6	LFP	Liquidity fragmentation, asset delisting, and product contraction	Market-liquidity
Z7	COC	Cyber-operational concentration and dependence on ICT service providers	Cyber-operational
Z8	RDB	Excessive data, reporting, and supervisory-interaction burden	Information-supervisory
Z9	CFS	Confidence shock and transmission of instability to the financial system of the European Union	Systemic

An appropriate expert assessment was carried out, the results of which are presented in Table 3. Expert evaluation was carried out in 2 rounds using the Delphi method. Its main purpose was to clarify the flow of threats, verify the continuity of direct causal links between them, and assess the apparent significance of the skin threat for the financial security of the EU region. The convenience of ranking threats is determined by the Kendall concordance coefficient, calculated using formula (7).

Table 3. Summary results of the expert assessment. Note: Kendall's coefficient of concordance W=0.760; χ^2=170.17; p<0.001. Source: calculated by the authors.

Threat	Threat description	Mean score	Standard deviation	Sum of ranks
Z1	Uneven implementation and transitional regimes across countries of the European Union	8.07	0.54	90.0
Z2	Rising authorization, capital, reporting, and compliance costs	8.61	0.63	62.0
Z3	Exit of small and medium-sized providers and market concentration	6.57	0.57	186.0
Z4	Restricted access to banking and payment services	8.00	0.72	97.5
Z5	Relocation of operations to offshore or decentralized channels	8.61	0.57	63.0
Z6	Liquidity fragmentation, asset delisting, and product contraction	7.07	0.72	153.5
Z7	Cyber-operational concentration and dependence on ICT service providers	6.89	0.79	163.0
Z8	Excessive data, reporting, and supervisory-interaction burden	5.57	0.69	234.0
Z9	Confidence shock and transmission of instability to the financial system of the European Union	6.14	0.71	211.0

Dependency, Reachability, and Hierarchy Matrices

The directions of direct linkages are determined by the rule that a fundamental legal or economic change must have a substantively justified mechanism for transmitting the threat to the next one. Specifically, uneven national transition regimes increase the costs of parallel authorization, hinder access to banking services, and encourage regulatory arbitrage. Compliance costs, in turn, increase the likelihood of small vendor exit, product downsizing, and the concentration of technological infrastructure (Table 4-5). The binary values of direct deposits between threats are determined by the rule given in formula (2).

Table 4. Binary matrix of direct dependencies among threats. Note: 1 — a direct influence was identified; 0 — no direct influence was identified.

z_{ij}	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8	Z9
Z1	0	1	0	1	1	0	0	1	0
Z2	0	0	1	1	0	1	1	1	0
Z3	0	0	0	0	0	1	1	0	1
Z4	0	0	0	0	1	1	0	0	1
Z5	0	0	0	0	0	0	0	0	1
Z6	0	0	0	0	0	0	0	0	1
Z7	0	0	0	0	0	0	0	0	1
Z8	0	0	0	0	0	0	1	0	1
Z9	0	0	0	0	0	0	0	0	0

The direct dependency matrix shows that uneven implementation of requirements Z1 directly increases costs Z2, hinders access to banking and payment services Z4, encourages the relocation of operations Z5, and increases the information and surveillance burden Z8. Increased costs Z2, in turn, increase the likelihood of small suppliers exiting the market Z3, reducing product and liquidity Z6, and concentrating technological infrastructure Z7. In economic terms, this structure means that uneven regulations increase the costs of operating across multiple jurisdictions, while high fixed costs increase the minimum efficient scale of operations and favor the largest participants.

Table 5. Threat reachability matrix including direct and indirect relationships.

z_{ij}	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8	Z9
Z1	1	1	1	1	1	1	1	1	1
Z2	0	1	1	1	1	1	1	1	1
Z3	0	0	1	0	0	1	1	0	1
Z4	0	0	0	1	1	1	0	0	1
Z5	0	0	0	0	1	0	0	0	1
Z6	0	0	0	0	0	1	0	0	1
Z7	0	0	0	0	0	0	1	0	1
Z8	0	0	0	0	0	0	1	1	1
Z9	0	0	0	0	0	0	0	0	1

DOI: 10.55643/fcaptp.4.69.2026.5273

The reachability matrix confirms that Z1 directly or indirectly impacts all elements of the existing system, while Z2 impacts eight of the nine threats. Consequently, a limited change in implementation conditions or compliance costs can cascade through banking services, competitive structure, liquidity, technological dependence, and trust. From a financial and economic perspective, regulatory measures aimed at harmonizing national procedures and proportional spending have a preventive multiplier effect, as they simultaneously mitigate several subsequent threats.

The iterative process yielded five levels. Level 1 contains the final systemic outcome. Level 5 is represented by the underlying driver, which has the greatest structural strength and influences all subsequent levels. In management practice, this interpretation implies the need to take preventive action starting from the lowest underlying level in the figure, rather than simply reacting to an already-in-progress confidence shock (Table 6). The ranks of the hierarchy are established by the method of sequentially forming the multipliers of strength, preceding them and their transition behind formulas (4) – (6).

Table 6. Iterative identification of threat-hierarchy levels.

Step	Initial set	Level formed	Condition $S(z_i)=Q(z_i)$ satisfied
1	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9	Z9	Z9: S={Z9}, Q={Z9}
2	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8	Z5, Z6, Z7	Z5: S={Z5}, Q={Z5}; Z6: S={Z6}, Q={Z6}; Z7: S={Z7}, Q={Z7}
3	Z1, Z2, Z3, Z4, Z8	Z3, Z4, Z8	Z3: S={Z3}, Q={Z3}; Z4: S={Z4}, Q={Z4}; Z8: S={Z8}, Q={Z8}
4	Z1, Z2	Z2	Z2: S={Z2}, Q={Z2}
5	Z1	Z1	Z1: S={Z1}, Q={Z1}

The pairwise comparison matrix was constructed using the Saaty scale. Z1, Z2, and Z5 received high relative strengths, as they simultaneously have significant documentary value and generate subsequent market reactions. After normalizing the principal eigenvector, the λmax value was 9.117, CI – 0.0147, CR – 0.0101 (Table 7).

Table 7. Pairwise comparison matrix of key threats using Saaty's Analytic Hierarchy Process. Note: λmax=9.117; CI=0.0147; CR=0.0101<0.10.

Threat	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8	Z9	w^{AHP}
Z1	1	1	2	1	1	1	2	3	4	0.153
Z2	1	1	2	1	1	2	2	3	5	0.169
Z3	1/2	1/2	1	1	1/2	1	1	2	3	0.097
Z4	1	1	1	1	1	1	2	2	4	0.137
Z5	1	1	2	1	1	2	2	3	4	0.165
Z6	1	1/2	1	1	1/2	1	1	2	3	0.105
Z7	1/2	1/2	1	1/2	1/2	1	1	2	2	0.085
Z8	1/3	1/3	1/2	1/2	1/3	1/2	1/2	1	2	0.055
Z9	1/4	1/5	1/3	1/4	1/4	1/3	1/2	1/2	1	0.035

Combining the AHP weight with structural strength changed the order of individual threats. Z1 and Z2 received nearly identical weights, as uneven implementation reaches all peaks, and compliance costs impact eight of the nine threats. Z9 has the lowest combined weight not because of its low severity, but because it is an end result and does not introduce new elements into the model (Table 8). Expert opinion on structural strength was obtained, but we found a combination of Z1 and Z2 at 0.190. The financial and economic significance of this result is demonstrated by the fact that Z1 can have the greatest systemic impact, oscillations in unequal procedures and incentives, simplification of banking operations, and the creation of incentives for regulatory arbitrage. Z2 facilitates more rapid efforts, ensuring minimal profitability and rapid market concentration. The low combination with Z9 at 0.033 does not imply insignificant charge strength. It means that the shock is a destructive and does not generate new elements in existing models. Priority areas of financial policy include provisions for establishing procedures, proportionality of investment, accessibility of banking services, and protection in the control segment.

Table 8. Structural and combined threat weights. Note: Coefficient α=0.65. The combined weights sum to 1.

Threat	Driving power	Dependence power	Level	AHP weight	Structural weight	Combined weight
Z1	9	1	5	0.153	0.257	0.190
Z2	8	2	4	0.169	0.229	0.190
Z3	4	3	3	0.097	0.114	0.103
Z4	4	3	3	0.137	0.114	0.129
Z5	2	4	2	0.165	0.057	0.127
Z6	2	5	2	0.105	0.057	0.088
Z7	2	5	2	0.085	0.057	0.075
Z8	3	3	3	0.055	0.086	0.066
Z9	1	9	1	0.035	0.029	0.033

The weighting procedure was validated at several levels. First, the AHP pairwise-comparison matrix demonstrated high internal consistency, with CR = 0.0101, substantially below the conventional threshold of 0.1. Second, expert priorities were not used independently but were combined with the structural influence derived from the reachability matrix. Third, the parameter α was varied between 0.50 and 0.80 to test the dependence of the results on the relative contribution of expert and structural weights. This procedure reduces the dependence of the final index on a single subjective weighting mechanism.

The five enterprises were selected through purposive case sampling to validate the methodological approach across different crypto-asset business models rather than to obtain a statistically representative sample of the entire European crypto-asset market. The selection criteria included operational relevance during 2022–2025, Ukrainian origin or legal presence, availability of verifiable open data, and representation of different functional models, including centralized exchange, payment services, non-custodial staking, and cybersecurity. Therefore, the enterprise-level results are interpreted as comparative business-model evidence and should not be extrapolated to all crypto-asset service providers in the European Union. WhiteBIT operates as a centralized exchange and exchange ecosystem. KUNA represents a historical Ukrainian exchange model and ceased operations in 2025. Everstake is a provider of non-custodial staking infrastructure. Trustee Plus combines cryptogaming with a payment product. Hacken provides audit, cybersecurity, and compliance services, and HACKEN LLC is registered in Kyiv (Table 9).

Table 9. Enterprises selected for the applied validation of the methodological approach. *(Source: compiled from official enterprise materials, KUNA, Everstake, and Hacken announcements, open registers, and specialized publications for 2022–2025)*

Enterprise	Business model	Basis for inclusion	Dominant channel of regulatory exposure
WhiteBIT	Centralized exchange, custody, and payment services	Ukrainian origin; cross-border operations	High dependence on authorization, banking channels, liquidity, and reporting
KUNA	Centralized exchange and payment services	Ukrainian origin; operations terminated on 31 March 2025	High exposure to market concentration, access to financial channels, and confidence shocks
Everstake	Non-custodial staking and validator infrastructure	Founded by Ukrainian engineers	Moderate regulatory and high cyber-operational exposure
Trustee Plus	Crypto wallet and card-based payment functionality	Ukrainian-origin product for customers in the European Union	High dependence on payment partners, KYC, and reporting
Hacken	Smart-contract auditing, cybersecurity, and compliance	Ukrainian origin; HACKEN LLC registered in Kyiv	Low direct market exposure but significant cyber-operational exposure

The annual threat intensity reflects not the overall danger posed by cryptoassets, but the strength of regulatory pressure and secondary consequences in the given year. The increase in 2024–2025 is explained by the shift from expectations to direct enforcement of regulations on tokens, service providers, transfer traceability, and digital operational resilience (Table 10).

DOI: 10.55643/fcaptp.4.69.2026.5273

Table 10. Normalized annual threat-intensity values q_{jt}, 2022–2025.

Threat	Threat description	2022	2023	2024	2025
Z1	Uneven implementation and transitional regimes across countries of the European Union	0.40	0.55	0.72	0.85
Z2	Rising authorization, capital, reporting, and compliance costs	0.35	0.55	0.80	0.88
Z3	Exit of small and medium-sized providers and market concentration	0.25	0.35	0.55	0.70
Z4	Restricted access to banking and payment services	0.45	0.52	0.68	0.76
Z5	Relocation of operations to offshore or decentralized channels	0.50	0.58	0.70	0.82
Z6	Liquidity fragmentation, asset delisting, and product contraction	0.30	0.38	0.65	0.78
Z7	Cyber-operational concentration and dependence on ICT service providers	0.55	0.60	0.72	0.80
Z8	Excessive data, reporting, and supervisory-interaction burden	0.35	0.50	0.75	0.84
Z9	Confidence shock and transmission of instability to the financial system of the European Union	0.40	0.44	0.58	0.64

Annual threat-intensity values demonstrate a consistent upward trajectory throughout 2022–2025. By 2025, the highest values are recorded for rising authorization and compliance costs at 0.88, uneven implementation at 0.85, the reporting and supervisory-interaction burden at 0.84, and relocation to less regulated channels at 0.82. The largest absolute increase occurred for Z2, which rose by 0.53 compared with 2022. Considerable increases are also observed for Z8 and Z6, amounting to 0.49 and 0.48, respectively. These results indicate that the transition toward practical enforcement intensified cost-related, informational, and liquidity pressures more rapidly than the final systemic confidence effect (Table 11).

Table 11. Business-model exposure coefficients e_{ij}. Note: 0 denotes no direct exposure; 1 denotes the maximum dependence of the business model on the respective channel.

Threat	Threat description	WhiteBIT	KUNA	Evestake	Trustee Plus	Hacken
Z1	Uneven implementation and transitional regimes across countries of the European Union	0.95	0.85	0.70	0.85	0.55
Z2	Rising authorization, capital, reporting, and compliance costs	0.95	0.90	0.70	0.90	0.45
Z3	Exit of small and medium-sized providers and market concentration	0.85	0.95	0.45	0.80	0.25
Z4	Restricted access to banking and payment services	0.90	0.90	0.45	0.95	0.25
Z5	Relocation of operations to offshore or decentralized channels	0.80	0.85	0.75	0.85	0.35
Z6	Liquidity fragmentation, asset delisting, and product contraction	0.95	0.85	0.40	0.75	0.20
Z7	Cyber-operational concentration and dependence on ICT service providers	0.90	0.75	0.80	0.85	0.70
Z8	Excessive data, reporting, and supervisory-interaction burden	0.95	0.75	0.70	0.90	0.55
Z9	Confidence shock and transmission of instability to the financial system of the European Union	0.80	0.95	0.55	0.90	0.30

The exposure coefficients reveal substantial differences in the sensitivity of the selected business models. WhiteBIT has the highest average exposure across the nine threats, followed by KUNA and Trustee Plus, whereas Everstake and Hacken demonstrate lower overall dependence on the assessed regulatory channels. Across the entire sample, cyber-operational concentration has the highest average exposure, which confirms that technological dependence remains relevant for exchange, payment, staking, and cybersecurity activities. Uneven implementation, compliance costs, and reporting requirements also generate broad exposure across the selected enterprises. The results therefore support an enterprise-specific assessment in which the same regulatory change produces different consequences depending on the combination of custody, payment, exchange, staking, and audit functions (Table 12).

Table 12. Threat values and weighted threat values for WhiteBIT, 2022–2025. Note: x_{ijt} — normalized value; v_{ijt} — value adjusted for the combined weight.

Threat	2022		2023		2024		2025	
	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}
Z1	0.380	0.072	0.522	0.099	0.684	0.130	0.807	0.153
Z2	0.332	0.063	0.522	0.099	0.760	0.144	0.836	0.158
Z3	0.212	0.022	0.297	0.031	0.468	0.048	0.595	0.061
Z4	0.405	0.052	0.468	0.060	0.612	0.079	0.684	0.088
Z5	0.400	0.051	0.464	0.059	0.560	0.071	0.656	0.083
Z6	0.285	0.025	0.361	0.032	0.617	0.055	0.741	0.065
Z7	0.495	0.037	0.540	0.041	0.648	0.049	0.720	0.054
Z8	0.332	0.022	0.475	0.031	0.712	0.047	0.798	0.052
Z9	0.320	0.010	0.352	0.012	0.464	0.015	0.512	0.017

The results for WhiteBIT demonstrate a substantial increase in regulatory exposure during the analysed period. The composite contribution of the threats rises from approximately 0.355 in 2022 to 0.733 in 2025. In 2025, the largest weighted contributions are generated by Z2 at 0.158 and Z1 at 0.153, followed by restricted banking access and the relocation of activity at 0.088 and 0.083. This structure indicates that WhiteBIT's exposure is primarily associated with the scale of authorization and compliance obligations, differences among national regulatory regimes, and dependence on banking and payment infrastructure. Liquidity fragmentation also remains significant because the centralized exchange model relies on a broad range of assets, trading pairs, and cross-border customer flows (Table 13).

Table 13. Threat values and weighted threat values for KUNA, 2022–2025. Note: x_{ijt} — normalized value; v_{ijt} — value adjusted for the combined weight.

Threat	2022		2023		2024		2025	
	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	v_{ijt}	x_{ijt}
Z1	0.340	0.064	0.468	0.089	0.612	0.116	0.722	0.137
Z2	0.315	0.060	0.495	0.094	0.720	0.136	0.792	0.150
Z3	0.237	0.024	0.332	0.034	0.522	0.054	0.765	0.079
Z4	0.405	0.052	0.468	0.060	0.612	0.079	0.787	0.101
Z5	0.425	0.054	0.493	0.063	0.595	0.076	0.697	0.089
Z6	0.255	0.023	0.323	0.029	0.552	0.049	0.663	0.059
Z7	0.413	0.031	0.450	0.034	0.540	0.041	0.600	0.045
Z8	0.262	0.017	0.375	0.025	0.562	0.037	0.630	0.041
Z9	0.380	0.012	0.418	0.014	0.551	0.018	0.699	0.023

KUNA demonstrates an increase in the composite threat index from 0.338 in 2022 to 0.724 in 2025. The principal weighted contributions in 2025 are associated with compliance costs at 0.150, uneven implementation at 0.137, restricted access to financial channels at 0.101, and the relocation of activity at 0.089. Market concentration also reaches a comparatively high contribution of 0.079. The obtained structure reflects the particular vulnerability of a centralized exchange to simultaneous changes in authorization conditions, banking relationships, market scale, and customer confidence. The documented termination of operations in 2025 reinforces the relevance of the correction applied to concentration, payment-access, and confidence-related threats (Table 14).

DOI: 10.55643/fcaptp.4.69.2026.5273

Table 14. Threat values and weighted threat values for Everstake, 2022–2025. Note: x_{ijt} — normalized value; v_{ijt} — value adjusted for the combined weight.

Threat	2022		2023		2024		2025	
	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}
Z1	0.280	0.053	0.385	0.073	0.504	0.096	0.595	0.113
Z2	0.245	0.046	0.385	0.073	0.560	0.106	0.616	0.117
Z3	0.113	0.012	0.158	0.016	0.248	0.025	0.315	0.032
Z4	0.203	0.026	0.234	0.030	0.306	0.039	0.342	0.044
Z5	0.375	0.048	0.435	0.055	0.525	0.067	0.615	0.078
Z6	0.120	0.011	0.152	0.013	0.260	0.023	0.312	0.028
Z7	0.440	0.033	0.480	0.036	0.576	0.043	0.640	0.048
Z8	0.245	0.016	0.350	0.023	0.525	0.034	0.588	0.039
Z9	0.220	0.007	0.242	0.008	0.319	0.010	0.352	0.012

Everstake exhibits a more moderate increase in regulatory exposure, with the composite index rising from 0.252 in 2022 to 0.510 in 2025. Compliance costs and uneven implementation provide the largest weighted contributions, reaching 0.117 and 0.113, respectively. Relocation to offshore or decentralized channels also remains significant at 0.078, while cyber-operational concentration contributes 0.048. The non-custodial nature of the business model reduces direct sensitivity to banking restrictions, asset delisting, and market concentration. At the same time, regulatory qualification of staking services, cross-border differences, validator reliability, and dependence on technological infrastructure maintain an elevated level of exposure (Table 15).

Table 15. Threat values and weighted threat values for Trustee Plus, 2022–2025. Note: x_{ijt} — normalized value; v_{ijt} — value adjusted for the combined weight.

Threat	2022		2023		2024		2025	
	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}
Z1	0.340	0.064	0.468	0.089	0.612	0.116	0.722	0.137
Z2	0.315	0.060	0.495	0.094	0.720	0.136	0.792	0.150
Z3	0.200	0.021	0.280	0.029	0.440	0.045	0.560	0.058
Z4	0.427	0.055	0.494	0.064	0.646	0.083	0.794	0.102
Z5	0.425	0.054	0.493	0.063	0.595	0.076	0.697	0.089
Z6	0.225	0.020	0.285	0.025	0.488	0.043	0.585	0.052
Z7	0.468	0.035	0.510	0.038	0.612	0.046	0.680	0.051
Z8	0.315	0.021	0.450	0.030	0.675	0.044	0.832	0.055
Z9	0.360	0.012	0.396	0.013	0.522	0.017	0.634	0.021

Trustee Plus demonstrates a high sensitivity to the strengthening of legal regulation, with the composite index increasing from 0.341 in 2022 to 0.714 in 2025. The dominant weighted threats in 2025 are Z2 at 0.150, Z1 at 0.137, Z4 at 0.102, and Z5 at 0.089. The payment-oriented nature of the business model creates considerable dependence on banking partners, card infrastructure, customer identification, transfer traceability, and reporting procedures. The growing value of Z8 also indicates that the supervisory and information burden becomes increasingly important when cryptocurrency services are integrated with conventional payment instruments. Therefore, the enterprise's regulatory exposure approaches the level observed for centralized exchanges. Hacken retains the lowest composite threat index among the selected enterprises, although its value increases from 0.166 in 2022 to 0.335 in 2025. The largest contributions are associated with uneven implementation at 0.089, compliance costs at 0.075, and cyber-operational concentration at 0.042. Exposure to liquidity fragmentation, banking restrictions, and market concentration remains comparatively limited because the business model does not depend directly on exchange or custodial operations. Strengthened regulation can also increase demand for cybersecurity audits, smart-contract verification, and compliance services. This compensating effect moderates the total threat level while preserving the strategic importance of Hacken within the risk-mitigation infrastructure of the cryptocurrency market (Table 16).

Table 16. Threat values and weighted threat values for Hacken, 2022–2025. Note: x_{ijt} — normalized value; v_{ijt} — value adjusted for the combined weight.

Threat	2022		2023		2024		2025	
	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}	x_{ijt}	v_{ijt}
Z1	0.220	0.042	0.303	0.057	0.396	0.075	0.468	0.089
Z2	0.158	0.030	0.248	0.047	0.360	0.068	0.396	0.075
Z3	0.062	0.006	0.087	0.009	0.138	0.014	0.175	0.018
Z4	0.113	0.014	0.130	0.017	0.170	0.022	0.190	0.024
Z5	0.175	0.022	0.203	0.026	0.245	0.031	0.287	0.036
Z6	0.060	0.005	0.076	0.007	0.130	0.011	0.156	0.014
Z7	0.385	0.029	0.420	0.032	0.504	0.038	0.560	0.042
Z8	0.193	0.013	0.275	0.018	0.413	0.027	0.462	0.030
Z9	0.120	0.004	0.132	0.004	0.174	0.006	0.192	0.006

Calculations show a consistent increase in regulatory exposure for all business models studied. Centralized exchanges and crypto payment systems are the most significant, as their operations simultaneously depend on authorization, banking services, traceability of transfers, liquidity, and the safekeeping of client assets. Everstake has lower exposure to custodial and payment requirements, but remains sensitive to the classification of staking services and operational resilience. Hacken is characterized by a low Integral Index, as increased legal regulation creates not only costs but also additional demand for audit and compliance (Table 17-18).

Table 17. Composite threat indices by enterprise, 2022–2025.

Enterprise	2022	2023	2024	2025	Threat level in 2025
WhiteBIT	0.355	0.463	0.637	0.733	high
KUNA	0.338	0.440	0.605	0.724	high
Everstake	0.252	0.328	0.445	0.510	elevated
Trustee Plus	0.341	0.444	0.607	0.714	high
Hacken	0.166	0.217	0.293	0.335	moderate

The composite index should be interpreted as the relative exposure of a business model to the financial consequences of strengthened and potentially fragmented crypto-asset regulation rather than as a measure of insolvency or overall financial soundness. For financial institutions, a higher value indicates greater dependence of a counterparty on authorization, banking access, liquidity, compliance, and payment infrastructure and therefore justifies enhanced assessment of regulatory continuity. For supervisory authorities, the index identifies business models in which regulatory fragmentation or disproportionate compliance costs may generate broader market effects. For investors, it provides an additional indicator of regulatory-cost sensitivity and dependence on external financial infrastructure. Accordingly, the index complements rather than replaces conventional liquidity, solvency, profitability, and market-risk indicators.

Table 18. Rates of change in composite threat indices, %.

Enterprise	2023/2022	2024/2023	2025/2024	2025/2022
WhiteBIT	30.6	37.5	15.1	106.7
KUNA	30.3	37.4	19.6	114.1
Everstake	30.3	35.5	14.7	102.5
Trustee Plus	30.0	36.9	17.6	109.1
Hacken	30.8	35.2	14.5	102.4

The most pronounced acceleration in indices is observed in 2024. This is the period during which companies must complete preparations for the full implementation of MiCA, adapting stablecoin products, asset protection procedures, complaint mechanisms, market communications, and operational risk controls. In 2025, the growth rate slowed somewhat, but

DOI: 10.55643/fcaptp.4.69.2026.5273

remained high for WhiteBIT, KUNA, and Trustee Plus. The adjustment factors for KUNA and Trustee Plus are linked to publicly documented events in 2025, reflecting increased concentration risk, payment access, and regulatory uncertainty.

The scenario analysis was conducted for 2025. Coordinated implementation assumes mutual recognition of procedures, uniform supervisory interpretations, proportionate requirements for small providers, standardized banking channels, and reduced duplication of reporting. Fragmented supervision assumes different national interpretations, limited access to banking services, rapid exit of small providers, and the shift of operations to less regulated channels (Table 19).

Table 19. Scenario values of the composite index in 2025.

Enterprise	Coordinated implementation	Baseline scenario	Fragmented supervision	Change vs baseline, % (coordinated)	Change vs baseline, % (fragmented)
WhiteBIT	0.629	0.733	0.836	-14.2	14.1
KUNA	0.623	0.724	0.828	-13.9	14.4
Everstake	0.438	0.510	0.580	-14.2	13.6
Trustee Plus	0.614	0.714	0.815	-14.0	14.2
Hacken	0.286	0.335	0.380	-14.6	13.3

Coordinated implementation reduces the WhiteBIT index to 0.629, KUNA to 0.623, and Trustee Plus to 0.614. For Everstake and Hacken, the decline is also significant, despite their initial values being lower. Fragmented monitoring increases the exchange and payment indices above 0.80, corresponding to a high threat level. Therefore, strengthening regulations alone does not guarantee improved financial security. The decisive factor is the method of implementing regulations (Table 20).

Table 20. Sensitivity of the results to the AHP-to-structural weight ratio.

Enterprise	α=0.50	α=0.65	α=0.80	Ranking position
WhiteBIT	0.737	0.733	0.729	1
KUNA	0.725	0.724	0.722	2
Everstake	0.512	0.510	0.508	4
Trustee Plus	0.716	0.714	0.712	3
Hacken	0.340	0.335	0.331	5

The sensitivity analysis confirms the robustness of the obtained enterprise ranking. Changes in the ratio between AHP and structural weights produce only limited variations in the composite indices, while the ranking positions remain unchanged. The range between the minimum and maximum values does not exceed 0.009 for any enterprise. Spearman's coefficient of 1.0 confirms complete rank correspondence under the alternative weighting parameters. Consequently, the identification of WhiteBIT, KUNA, and Trustee Plus as the most exposed business models does not result from the selected value of α and remains stable under reasonable changes in the methodological assumptions.

The calculations carried out allow you to generalize the obtained values and draw appropriate conclusions based on them.

The decline in decision-making results indicates uneven implementation of the regulator with the Z1 capability and a slowdown in the authorization, capital, transparency, and compliance processes (Z2), which constitute the most significant bottleneck. Their priority is confirmed by expert assessments, the structural strength of the investment, and a combination of factors at 0.190.

Next in practical significance are interbank and payment services (Z4) and the transfer of activity for lesser control of channels (Z5).

In 2025, the information and visual supplement (Z8) further increased, reaching an intensity of 0.84. The results of applied transformations confirmed the maximum centralization of business and payment business models. WhiteBIT, KUNA, and Trustee Plus may have a high level of threat in 2025; their activity should be monitored simultaneously based on authorization, banking partners, liquidity, asset collection, client identification, and openness. Everstake offers proactive actions, success-driven actions, cross-border qualification of staking services, and technological sophistication. Haken has the highest level of straightforwardness, thus offering important functions for downgrading the cyber-operating systems of other

market participants. Minimizing established requirements before deciding on national authorization procedures allows for transitional operations while simultaneously completing specific actions and sellers of proportional efforts for large-scale enterprises.

Low Z2 and Z8 support standardized compliance forms and one-time requirements, whatever they may be, so implement new capabilities and utilize relevant technical standards.

The emergence of Z4 requires verification of criteria for opening and maintaining bank accounts, standardized procedures for processing post-stage cryptocurrency services, and a mechanism for reviewing raw data.

To reduce Z5 and Z6, additionally address economic privacy in regulated segments, eliminate the redundancy of transitional lines, and eliminate a number of intermediate products without assessing their liquidity.

The introduction of Z7 allows for the diversification of ICT post-centers, exceeding severance plans, and fully assessing the results of cybersecurity audits. Scenario changes confirm that increasing such visits will reduce the integrated salary level by approximately 14% without reducing customer retention standards.

DISCUSSION

The results confirm that cryptocurrency market regulation has a dual impact on financial security. The direct positive effect is related to customer protection, information disclosure, asset segregation, regulatory redundancy, and combating illicit flows. A secondary negative effect arises when fixed costs and procedural complexity exceed the adaptability of small and medium-sized providers. In this case, the market becomes concentrated, and operations shift to entities that are too large to be quickly replaced or located outside effective supervision.

The dominance of Z1 and Z2 is consistent with the findings of van der Linden and Shirazi (2023) and Maume (2023), who link MiCA effectiveness to the quality of implementation. Furthermore, the high weight of Z5 supports the position of Arner et al. (2024) on the need for international regulatory harmonization. Unilateral tightening of requirements in EU countries in the absence of commensurate regulations in other jurisdictions may not eliminate risky operations, but rather change their geography and technological channel. The hierarchical model clarifies the relationship between causes and effects. The Z9 confidence shock has serious potential damage, but is located at the top level as a dependent outcome. Policies focused solely on information campaigns or compensation for the consequences do not address uneven national implementation, excessive spending, and restrictions on banking access. In our view, early intervention should focus on the underlying drivers, as addressing them simultaneously mitigates several intermediate threats.

The high exposure of WhiteBIT, KUNA, and Trustee Plus is explained by the combination of custodial, exchange, and payment functions. These business models have the greatest number of touchpoints with banks, e-money issuers, payment institutions, liquidity providers, and customer data. Everstake is in a different position. The non-custodial model mitigates some of the risks, but the regulatory qualifications of staking and the technological stability of validators maintain the significance of Z7. Hacken has low direct exposure, but its services are an element of risk mitigation for other market participants.

The results should not be interpreted as an assessment of the financial strength or integrity of a specific company. The integrated index characterizes the sensitivity of a business model to specific regulatory enforcement channels. A high value can be combined with adequate capitalization, effective compliance, and a robust technological infrastructure. A full assessment of an individual company requires audited financial data, the regulatory status of each jurisdiction, liquidity indicators, asset segregation, and incidents. The study's limitations stem from the use of open data, standardized estimates, and expert synthesis. The lack of confidential metrics precludes calculating actual authorization costs or the volume of lost transactions. However, the transparent presentation of all coefficients, matrices, and formulas allows for repeatable calculations and the substitution of model values for primary data in future studies.

The principal advantage of the proposed approach over conventional financial-risk models is therefore not superior prediction of insolvency, volatility, or market losses. Its advantage lies in combining three analytical dimensions that are usually considered separately: expert assessment of threat significance, the causal position of each threat established through interpretive structural modeling, and differentiated exposure of individual business models. The additional TOPSIS verification indicates that the general differentiation of business models is preserved under an alternative multi-criteria procedure, although the exact ranking of the most exposed firms may vary.

A limitation of existing research is that legal analysis of MiCA is often separated from quantitative assessments of financial security consequences. Economic studies, in turn, focus on volatility, price manipulation, illicit flows, or the sustainability

DOI: 10.55643/fcaptp.4.69.2026.5273

of stablecoins, but fail to develop a multi-level causal model of the threats arising specifically from increased regulation. We believe that combining interpretive structural modeling with the analytic hierarchy process and integrated assessment allows us to distinguish between the underlying drivers, intermediate channels, and ultimate systemic consequences.

The scientific novelty of this study lies in the development of a methodological approach according to which the significance of a threat is determined simultaneously by its expert significance and its place in the causal structure. This approach prevents a situation where the ultimate consequence automatically receives the highest priority simply because of significant potential damage, although management action should primarily be aimed at the underlying factors. The practical significance of the obtained results is related to the possibility of their application by government authorities, supervisory agencies, banks and enterprises in the crypto-asset market when assessing the proportionality of regulatory requirements.

CONCLUSIONS

A methodical approach to hierarchical interaction and careful consideration of key financial unemployed EU issues has been developed and tested, addressing the consequences of crypto-asset market regulation. The following solutions are typically adopted to address these challenges:

1. An analysis of changes in cryptoasset market regulation in 2022–2025 illustrated the transition from the proposed to the actual regulatory proposal. The main financial and economic methods for its implementation included steps toward authorization and compliance, the need for additional capital and technological modernization, delimitation of banking services, the need for product assortment, liquidity fragmentation, and changes in the territorial distribution of operations.
2. Nine mutually beneficial issues have been systematized. They leave unconventional implementations that could lead to the loss of a small to medium number of messages in the market, shared access to banking and payment services, the redistribution of operations to lesser channel control, fragmentation, liquidity, cyber-operational concentration, information-visible offers, and shock situations with possible consequences for financial system instability.
3. The resulting matrices of direct risk and accessibility factors allowed us to form a five-level cause-and-effect hierarchy. Initially, a significantly uneven implementation of the Z1 power regulator is ensured. The next step takes the form of Z2. Intermediate levels cover market concentration, shared financial services, information support, redistribution of operations, liquidity fragmentation, and technological complexity. The final result is trust shock Z9. This structure confirms the importance of preventative investment in early ventures.
4. The Saat library analysis method has significant expert value related to authorization and compliance, changes in stability to greater channel control, and regular implementation. After determining the expert degree of structural strength Z1 and Z2, the best cell combinations were found at the 0.190 level. A CR value of 0.0101 confirmed the narrowness of the matrices of the improvement groups, and the Kendall concordance coefficient of W = 0.760 confirmed the narrowness of the threat ranking.
5. The restructuring of the methodological approach to contrasting the selection of enterprises confirmed its maturity and the clarity of various business models. In 2025, WhiteBIT, KUNA, and Trustee Plus selected high-salary companies with fixed indices of 0.733, 0.724, and 0.714. Everstake has an elevated level with an index of 0.510, and Hacken is the lowest level with an index of 0.335. The results characterize the bank regulator's transfer to business models and do not represent the high solvency, business reputation, or financial stability of specific enterprises. A scenario assessment confirmed that coordination and the proportion of implementation reduce the integrated indices of enterprises by 13.9–14.6%, meaning fragmentation apparently increases by 13.3–14.4%. An analysis of practical evidence confirms the insignificance of enterprise interactions with various expert and structural warehouse situations. A Spearman coefficient of 1.0 brings stability to the optimal order of priority.
6. Practical approaches to minimizing bottlenecks allow for increased efficiency of national authorization procedures, proportionality of access to enterprises of various sizes, standardization of transparency, full compliance with regulations, compliance with banking services for cryptocurrency clients, and diversification of technological infrastructure. Implementing such approaches allows for a reduction in unproductive indicators, increased competition and liquidity, and the preservation of the majority of operations in the control market segment.

Further research should extend the proposed methodological approach by incorporating audited enterprise-level data on authorization costs, capital requirements, liquidity, access to banking and payment services, asset segregation, cyber incidents, and transaction volumes. Expanding the sample to include crypto-asset service providers operating in different

countries of the European Union would allow national transitional regimes and supervisory practices to be compared. Longitudinal studies should also determine whether the identified hierarchy of threats changes following the full implementation of MiCA, DORA, and the new anti-money-laundering framework of the European Union. Particular attention should be paid to stablecoin reserve structures, cross-border regulatory arbitrage, staking services, decentralized finance, and the transmission of crypto-market shocks to banks, payment institutions, and investment intermediaries.

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. 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. *Federal Reserve Bank of New York Economic Policy Review, 30*(2), 1–48. https://doi.org/10.59576/epr.30.2.1-48
2. Blikhar, V., Lukianova, H., Komarnytska, I., Vinichuk, M., & Gapchich, V. (2023). Problems of normative and legal regulation of the process of applying blockchain technology in the financial system of Ukraine. *Financial and Credit Activity: Problems of Theory and Practice, 3*(50), 410–418. https://doi.org/10.55643/fcaptp.3.50.2023.4088
3. 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
4. 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
5. 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
6. 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
7. European Parliament & Council of the European Union. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj
8. European Parliament & Council of the European Union. (2023a). *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/1113/oj
9. European Parliament & Council of the European Union. (2023b). *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/1114/oj
10. European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1624/oj
11. European Securities and Markets Authority. (2026). *Markets in Crypto-Assets Regulation (MiCA)*. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
12. Everstake. (2025). *Company profile and institutional staking infrastructure information*. https://everstake.one/
13. Ferrari, V. (2020). The regulation of crypto-assets in the EU: Investment and payment tokens under the radar. *Maastricht Journal of European and Comparative Law,*

DOI: 10.55643/fcaptp.4.69.2026.5273

27(3), 325–342. https://doi.org/10.1177/1023263X20911538

14. Ferreira, A., & Sandner, P. (2021). EU 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
15. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015
16. Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics, 95*, 86–96. https://doi.org/10.1016/j.jmoneco.2017.12.004
17. Hacken. (2025). *Official company history and blockchain security and compliance profile*. https://hacken.io/
18. Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review, 15*(4), 645–696. https://doi.org/10.1515/ecfr-2018-0021
19. 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
20. Karau, S. (2023). Monetary policy and Bitcoin. *Journal of International Money and Finance, 137*, Article 102880. https://doi.org/10.1016/j.jimonfin.2023.102880
21. KUNA. (2025). *KUNA shutdown*. https://kuna.io/
22. Lyons, R. K., & Viswanath-Natraj, G. (2023). What keeps stablecoins stable? *Journal of International Money and Finance, 131*, Article 102777. https://doi.org/10.1016/j.jimonfin.2022.102777
23. Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics, 135*(2), 293–319. https://doi.org/10.1016/j.jfineco.2019.07.001
24. 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
25. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review, 103*(2), 153–174. https://doi.org/10.20955/r.103.153-74
26. Tarasenko, O., Tykhonova, O., Herasymenko, L., Dykyi, A., Sakharova, O., & Blyzniuk, I. (2026). Financial and legal threats to banking security in the European Union countries in the context of crypto-asset regulation. *Financial and Credit Activity: Problems of Theory and Practice, 3*(68), 48–58. https://doi.org/10.55643/fcaptp.3.68.2026.5243
27. Trustee Plus. (2025). *Public information and notices concerning access for users from Ukraine*. https://trustee-global.com/
28. 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
29. Volosovych, S., Nezhyva, M., Vasylenko, A., Morozova, L., & Napadovskyi, I. (2024). The cryptocurrency assets market in the conditions of military aggression. *Financial and Credit Activity: Problems of Theory and Practice, 1*(54), 114–126. https://doi.org/10.55643/fcaptp.1.54.2024.4305
30. WhiteBIT. (2025). *From Europe to the world: WhiteBIT reinforces its position among leading global crypto platforms*. https://blog.whitebit.com/en/whitebit-2025-highlights/
31. 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
32. 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
33. 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

Денисов О., Скоропад І., Ярошенко С., Кіблик Д., Єременко А.

КЛЮЧОВІ ЗАГРОЗИ ФІНАНСОВІЙ БЕЗПЕЦІ КРАЇН ЄС УНАСЛІДОК ПОСИЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ РИНКУ КРИПТОВАЛЮТИ

Статтю присвячено обґрунтуванню та апробації методичного підходу до ієрархічного впорядкування ключових загроз фінансовій безпеці країн ЄС, які виникають не лише через недостатність контролю ринку криптовалюти, а й унаслідок різкого посилення правових, пруденційних, звітних, протидійних і кібероперaційних вимог. Метою цього дослідження є розробка й тестування методологічного підходу до ієрархічного впорядкування та комплексної оцінки ключових фінансових тягарів ЄС, що дозволить успішно регулювати ринок криптоактивів шляхом усунення причинно-наслідкових зв'язків між регуляторними силами, діями корпорацій, реакцією ринку та системними фінансовими ресурсами. Методологічне підґрунтя охоплює документарний експертний синтез, метод Дельфі у 2 раунди, бінарні матриці залежності й досяжності, інтерпретативне структурне моделювання, метод аналізу ієрархій Сааті, комбінування експертної ваги зі структурною силою впливу, інтегральне оцінювання та сценарний аналіз. Інформаційну базу сформовано з нормативних актів ЄС, матеріалів ESMA, EBA, Європейської Комісії, наукових праць і відкритих

даних щодо WhiteBIT, KUNA, Everstake, Trustee Plus і Hacken за 2022–2025 рр. Установлено 5 рівнів ієрархії. Базовими драйверами визначено нерівномірність імплементації регулювання та зростання витрат на авторизацію й комплаєнс. Кінцевим системним результатом постає шок довіри з можливим передаванням нестабільності до банківського, платіжного й інвестиційного сегментів. Інтегральне оцінювання засвідчило найвищу чутливість біржових і платіжних бізнес-моделей, водночас постачальник кібербезпекових послуг має нижчу пряму експозицію, але залишається критично важливим для зниження операційного ризику. Сценарні розрахунки довели, що координована та пропорційна імплементація здатна істотно знизити сукупний рівень загроз, а фрагментований нагляд посилює концентрацію, регуляторний арбітраж і відтік діяльності до менш контрольованих каналів.

Ключові слова: фінансова безпека, країни ЄС, криптовалюта, криптоактиви, правове регулювання, MiCA, ієрархічне впорядкування, метод Сааті, інтегральний індекс, регуляторний арбітраж

JEL Класифікація: G18, G23, G28, K22, O33

DOI: 10.55643/fcaptp.4.69.2026.5273