e-ISSN 3083-6018

SOCIAL DEVELOPMENT: Economic and Legal Issues

https://www.eu-scientists.com/index.php/sdel

Transformation of Ukraine's Economic Policy in the Context of the War and Post-War Economy

Tymur Shostak [1 *]

[1] *State University of Trade and Economics (Ukraine). Postgraduate Student of the Department of Finance.*

*** *Corresponding Author,*** e-mail: t.s.shostak@knute.edu.ua

ARTICLE INFO

Research Article

DOI:
10.70651/3083-6018/2026.3.01

Received:
25 January 2026
Accepted:
27 February 2026
Published online:
5 March 2026

ABSTRACT

The article proposes and substantiates directions for improving risk management tools for the digital financial assets market. The study examines the inertial nature of market dynamics, the impact of the global environment, and military-induced structural shifts as basic determinants of the risk profile. It was found that market inertia compounds risks, and high dependence on external factors increases sensitivity to shocks and to the transformation of local failures into systemic crises of confidence and liquidity. The limitations of traditional regulatory approaches in ensuring effective risk control are identified, necessitating their improvement based on risk-oriented and scenario-based management. The study developed an integrated model for improving risk management tools, which combines a risk map, a two-layer system of early warning indicators, and an institutional framework for interaction between regulators and market participants. The feasibility of differentiating tools by functional frameworks (prudence, AML/CFT compliance, operational and cyber resilience, investor protection) was substantiated, which ensures proportionality of regulatory impact in accordance with the level of the risk environment. In addition, a phased model for improving risk management tools was developed, which provides for a consistent transition from the basic regulatory framework to full-fledged risk-oriented supervision using a scenario approach and stress testing. It was determined that the integration of indicator monitoring, trigger response mechanisms, and institutional coordination ensures increased risk management efficiency and adaptability of regulatory policy to changes in the external environment. The conclusions are drawn that the improvement of risk management tools for the digital financial assets market should be based on a combination of a risk-based approach, scenario analysis and international regulatory standards, which contributes to reducing systemic vulnerability, increasing transparency and building trust as a key prerequisite for legalization and sustainable development of the market.

KEYWORDS

digital financial assets, crypto-asset market, risk management, risk-based approach, market inertia, global financial environment, AML/CFT, compliance, operational resilience, cyber resilience, investor protection, scenario management, financial stability.

e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

https://www.eu-scientists.com/index.php/sdel

Вдосконалення інструментів управління ризиками ринку цифрових фінансових активів

Тимур С. Шостак [1 *]

[1] *Державний торговельно-економічний університет (Україна). Аспірант кафедри фінансів.*

*** *Автор-кореспондент,*** e-mail: t.s.shostak@knute.edu.ua

СТАТТЯ

Дослідницька

DOI: 10.70651/3083-6018/2026.3.01

Отримана: 25.01.2026 р.
Прийнята: 27.02.2026 р.
Опублікована: 05.03.2026 р.

АНОТАЦІЯ

У статті запропоновано та обґрунтовано напрями вдосконалення інструментів управління ризиками ринку цифрових фінансових активів. У ході дослідження розглянуто інерційний характер ринкової динаміки, вплив глобальної кон'юнктури та воєнно зумовлені структурні зсуви як базові детермінанти ризик-профілю. З'ясовано, що інерційність ринку формує кумулятивний ефект ризиків, а висока залежність від зовнішніх факторів підсилює чутливість до шокових впливів і трансформацію локальних збоїв у системні кризи довіри та ліквідності. Визначено обмеженість традиційних регуляторних підходів у забезпеченні ефективного контролю ризиків, що обумовлює необхідність їх вдосконалення на засадах ризикоорієнтованого та сценарного управління. У межах дослідження розроблено інтегровану модель вдосконалення інструментів управління ризиками, яка поєднує карту ризиків, двошарову систему індикаторів раннього попередження та інституційний контур взаємодії регуляторів і учасників ринку. Обґрунтовано доцільність диференціації інструментів за функціональними контурами (пруденційність, комплаєнс AML/CFT, операційна та кіберстійкість, захист інвестора), що забезпечує пропорційність регуляторного впливу відповідно до рівня ризикового середовища. Крім того, розроблено фазову модель вдосконалення інструментарію управління ризиками, яка передбачає послідовний перехід від базового регуляторного контуру до повноцінного ризик-орієнтованого нагляду із застосуванням сценарного підходу та стрес-тестування. Визначено, що інтеграція індикаторного моніторингу, тригерних механізмів реагування та інституційної координації забезпечує підвищення ефективності управління ризиками та адаптивності регуляторної політики до змін зовнішнього середовища. Сформовано висновки, що вдосконалення інструментів управління ризиками ринку цифрових фінансових активів має ґрунтуватися на поєднанні ризик-орієнтованого підходу, сценарного аналізу та міжнародних стандартів регулювання, що сприяє зниженню системної вразливості, підвищенню прозорості та формуванню довіри як ключової передумови легалізації та сталого розвитку ринку.

КЛЮЧОВІ СЛОВА

цифрові фінансові активи, ринок криптоактивів, управління ризиками, ризик-орієнтований підхід, інерційність ринку, глобальна фінансова кон'юнктура, AML/CFT, комплаєнс, операційна стійкість, кіберстійкість, інвесторський захист, сценарне управління, фінансова стабільність.

1. Introduction

The current stage of development of the digital financial asset market in Ukraine is characterized by a high level of uncertainty, which is due to a combination of internal structural imbalances and external shocks, primarily global volatility of crypto markets and the impact of martial law. The results of the simulation indicate the presence of a stable inertial dynamics of the market, its significant dependence on the global situation, as well as the significant impact of the war factor as a source of structural shifts [18].

Under such conditions, traditional approaches to risk management, focused mainly on market parameters (volatility, liquidity), are insufficient to adequately reflect the complex nature of risks.

A feature of the digital financial asset market is the multidimensional nature of risks, covering not only financial, but also institutional, regulatory, compliance risks (AML/CFT), operational and technological threats, and investor protection risks. Their interaction has a cumulative effect: an insufficient level of regulatory certainty and supervisory capacity stimulates market shadowing, increases the risks of financial dishonesty and undermines investor confidence. In addition, the situation is complicated by the high share of non-jurisdictional services and unorganized segments, which limits the effectiveness of the application of international regulatory standards.

Despite the existence of developed international approaches to the regulation of digital asset markets, their implementation in Ukraine needs to be adapted taking into account the specifics of the institutional environment and wartime conditions. The lack of a holistic system of risk management tools integrated through all channels of their implementation leads to an increase in market vulnerability, loss of capital and a decrease in its investment attractiveness.

Thus, the scientific problem of the study is the need for theoretical substantiation and practical development of a comprehensive system of risk management tools for the digital financial asset market, which will ensure an increase in its stability, transparency and manageability in conditions of increased uncertainty and multifactorial impact of external and internal risks.

2. Literature Review

Modern research in the field of improving digital financial asset market risk management tools is formed at the intersection of several scientific areas, in particular, modeling market dynamics, developing fintech ecosystems, assessing compliance risks, and analyzing the infrastructure factors of the functioning of digital assets. In this context, a significant contribution to the development of relevant approaches was made by Y. Kleban, T. Stasiuk, A. Bukhtiarova, A. Hayriyan, N. Bort, A. Semenog, T. Dmytrenko, N. Ushenko, V. Metelytsia, I. Lytovchenko, as well as S. Volosovych, M. Nezhyva, A. Vasylenko, L. Morozova, I. Napadovskyi. The scientific results of scientists cover the issues of predicting the volatility of crypto assets, the transformation of financial markets under the influence of digitalization, assessing the risks of using digital assets in illegal financial transactions, as well as the development of digital infrastructure and blockchain technologies. Their research proves that the digital financial asset market is characterized by high dynamism, nonlinearity and increased sensitivity to external and internal factors, which necessitates the improvement of approaches to risk management.

At the same time, the generalization of scientific approaches shows that the available research is mainly focused on certain aspects of risks, while the issues of forming an integrated management system that combines market, institutional, compliance, and operational and technological components remain insufficiently developed.

3. Problem Statement

The purpose of the article is to develop and substantiate the main directions for improving risk management tools for the digital financial asset market.

4. Methods and Materials

The methods and materials of the study are based on a combination of general scientific and specialized economic approaches, ensuring a comprehensive analysis of risks in the digital financial

assets market. The research employs econometric modeling to assess the inertia of market dynamics and the impact of the global financial environment and war-related factors, as well as methods of system analysis, comparison, and generalization to develop an integrated risk management model. Scenario analysis and stress testing are applied to evaluate market resilience under different operating conditions. The empirical base of the study includes academic publications, analytical reports of international organizations (BIS, FATF, FSB, IOSCO, OECD), EU regulatory frameworks (MiCA, DORA), Ukrainian legislation, and statistical and analytical data on the development of the crypto-assets market.

5. Results and Discussion

Taking into account the results of econometric modeling of the development of the digital financial assets market in Ukraine, three key risk areas have been identified along the amplification channel. First, the inertial nature of market dynamics leads to an increase in the significance of market risks due to the prolongation of volatile regimes and the complication of liquidity forecasting. sensitivity to shock effects [18, p. 117]. Thirdly, the global integration of the market causes increased operational and technological risks due to the concentration of infrastructure elements and high correlation with global risk waves [1; 4].

Accordingly, in Table 1 systematizes a map of risks with reference to their consequences and monitoring indicators. Based on the modeling, it has been established that the development of the digital financial assets market in Ukraine is characterized by a set of interrelated effects.

Table 1. DFA market risk map in Ukraine

Risk type	Sales channel	Economic effect	Monitoring indicators
Market (volatility, liquidity)	Global conjuncture → volatility → liquidity	Amplification of fluctuations in transaction volumes; elasticity to ln(GlobalMCap)=0.3549 (see clause 3.1); risk of procyclical capital outflows	Spread dynamics; liquidity indicators; Global capitalization
Institutional and regulatory	Regulatory uncertainty → migration of operations → shadowing	Consolidation of structural imbalances due to inertia (0.7484); Dominance of systemic factors	Regulatory Certainty Index (RegIndex); share of non-jurisdictional providers; Supervisory actions
Compliance (AML/CFT)	Shadowing → risks of ML/TF → reputational losses	Procyclical growth of compliance risks; hypersensitivity to shocks (WarDummy=0.2666)	Number of suspicious transactions; AML compliance indicators; Typology signals
Operational and technological	Technology incidents → failures → loss of liquidity and trust	Increasing the likelihood of cascade failures; Increased cyber risks in wartime	Frequency of cyber incidents; continuity indicators; Redundancy Level
Investor Protection / Market Integrity	Information asymmetry → fraud → loss of trust	Limitations of scaling the legal segment; capital outflow	Number of complaints; statistics of fraudulent projects; Retail Loss Indicators

Source: Compiled by the author based on [6; 9; 11; 13; 17].

In particular, the dominance of the inertial component has been empirically confirmed: about 75% of the variation in current transaction volumes is explained by their lag values, which indicates a low short-term market elasticity to changes in exogenous and endogenous factors. At the same time, a high level of dependence on the global situation has been proven, which is manifested in the statistically significant impact of the dynamics of the global capitalization of the crypto market on internal volumes of transactions.

In addition, the effect of a military-induced structural shift after 24.02.2022 has been identified, which manifests itself in an increase in transaction activity by about 30% and reflects the functional transformation of digital financial assets towards an alternative financial instrument in the context of crisis restrictions. At the same time, the statistical insignificance of most macroeconomic and regulatory variables (inflation, key policy rate, level of digitalization, regulatory certainty) in the short term has been established, which indicates their indirect or delayed nature of impact.

Further analysis showed the dominance of indirect channels of influence, within which regulatory changes are implemented through mechanisms of trust, legitimation and structural restructuring of the market. At the same time, the increased sensitivity of the market to external and regime shocks has been

proven, where global financial fluctuations and geopolitical factors are the determining drivers of instability.

Generalization of the modeling results made it possible to establish the scenario-dependent nature of further market dynamics, which is determined by the level of regulatory harmonization, in particular with MiCA approaches, and determines the variability of development trajectories within the baseline, optimistic and pessimistic scenarios.

The risk map (see Table 1) reflects the logic of their mutual reinforcement: institutional and regulatory gaps initiate compliance and operational vulnerabilities, while market and investor risks act as the final channels of losses due to trust and capital. Accordingly, scenario priority forms an adaptive management architecture: the optimistic scenario is dominated by volatility and liquidity control tools; in the pessimistic scenario, the closure of the institutional circuit of rules and supervision; in the basic sense, it is strengthening AML/CFT and operational resilience as conditions for minimizing trust losses in the face of inertia and military shocks.

The dynamics of the DFA market is determined primarily by inertia, sensitivity to the global situation and war-induced structural shifts. At the same time, "point" regulatory and macroeconomic variables in the short term do not form a significant impact, which necessitates the orientation of the monitoring system to measurable signals capable of initiating standardized management reactions.

With this in mind, the early warning system is appropriately built as a two-layer indicator panel. The core level fixes structural drivers (inertia, global conjuncture, martial law) and ensures the identification of changes in risk modes and the launch of scenario checks. The extended layer reflects the channels for risk implementation – compliance (AML/CFT), investor protection, and operational and technological vulnerabilities, due to which external shocks are transformed into local trust and liquidity problems.

The proposed architecture is consistent with international approaches. In particular, the FSB's recommendations emphasize risk-based monitoring of market and structural factors [12]; IOSCO's approaches detail market integrity and oversight requirements [15]; FATF standards define the logic of risk-based AML/CFT for virtual assets [11]; the CPMI-IOSCO guidelines form a framework for the cyber resilience of financial infrastructures [3]; DORA consolidates the process model of ICT incident management [7].

The formed system of indicators performs the function of an integration mechanism that combines the risk map with the appropriate management tools. In its structure, it is advisable to distinguish the basic (core) and extended (extended) levels of monitoring. The basic level is focused on identifying changes in the modes of market functioning due to the inertia of dynamics and the influence of external macrofactors. In particular, the key indicators include: the indicator of inertia of transaction volumes, which reflects the lag dependence and allows you to record the consolidation of unfavorable regimes; global capitalization of the crypto market as an exogenous driver of volatility and liquidity; as well as indicators of the military regime, which act as switches of structural changes and signal an increase in compliance and operational stability risks.

A separate supervisory dimension is represented by a regulatory certainty indicator, which reflects the stage of implementation of the regulatory framework and allows identifying gaps in supervisory practices that may stimulate regulatory arbitrage and shadowing operations.

The extended level of indicators is aimed at identifying the transformation of macrodynamic changes into specific risk channels. In this context, the following are subject to analysis: the share of P2P transactions as an indicator of shadowing and compliance risks; indicators of the effectiveness of AML/CFT procedures, reflecting the quality of risk scoring and the level of detection of suspicious transactions; frequency and typology of fraudulent incidents as a marker of risks for investors and confidence in the market; concentration of turnover among providers, which characterizes systemic and liquidity risks; parameters of cyber incidents and operational continuity, which reflect the technological resilience of the infrastructure; as well as liquidity indicators, including spreads and market depth.

The institutional architecture of risk management in the DFA market determines whether the identified risks and early warning signals are translated into manageable procedures capable of reducing the market's vulnerability to external shocks and internal execution failures. The established characteristics of the market's functioning, in particular its inertia and increased sensitivity to global conjuncture, determine the cumulative nature of risk materialization: delays in response and fragmentation of responsibility contribute to the fact that local violations in the field of supervision,

compliance, or operational resilience can be transformed into systemic crises of confidence and liquidity.

In such conditions, market weakness is manifested not only in the quality of norms, but primarily in the ability to enforce, through a closed risk-based cycle of interaction between regulators, supervision, financial monitoring, cyber circuit and providers.

The agreed framework of this approach is enshrined in the FSB and IOSCO recommendations on the regulation/supervision of the markets in crypto-assets and digital assets, as well as in the Policy Implementation Roadmap (IMF-FSB), where the principles of clear accountability, proportionality of requirements, evidence-based supervision and cross-border coordination are key [13; 14].

Functionally, it is advisable to describe the institutional outline as a sequence of "policy → requirements → reporting → supervision → enforcement → communication", where each link has its own result and "entrance" to the next link. At the stage of policy, risk priorities and scenario assumptions are established (based on a risk map and a two-layer panel of indicators), as well as the distribution of competencies and the order of interaction are agreed. products (in particular on liquidity management, operational and cyber resilience, risk disclosure and AML/CFT compliance), and their applicability should be aligned with the European MiCA framework and operational resilience requirements (as a regulatory benchmark of procedures) [8; 9].

At the reporting stage, indicators provide a formalized data flow: a combination of structural drivers with operational metrics of integrity, continuity, and investor protection. Further, supervision uses this data for risk-based selection of audit objects and for trigger response, which is especially important in the context of limited resources and military challenges. The state of war reinforces the importance of procedural discipline: reducing response lags, prioritizing high-risk segments, and limitations of "blind spots" (P2P channels, cross-border VASP/CASP, anonymization mechanisms), which the FATF systematically draws attention to in the context of the implementation of VA/VASP standards [11].

The stages of law enforcement and communication close the cycle: measures of influence should be proportionate and legally defined (prescriptions, restrictions on activities, suspension/revocation of authorization, financial sanctions within the competence), and public announcements should reduce the asymmetry of information and discipline the market without creating panic. For Ukraine, the problem of disclosure of information and supervisory capacity under martial law is of particular importance: the OECD emphasizes that during martial law, disclosure is limited, and the institutional strengthening of the NSSMC and the practical implementation of reforms are critical for the post-war recovery of financial markets [16].

It is important to distinguish between macro risks and micro risks in order to avoid substitution of management levels. The macro level covers systemic risks formed by the global situation and regime shocks and requires coordination at the level of financial stability and interagency interaction. The micro level covers the risks of providers and products (operational, technological, AML/CFT compliance, investor protection) and is implemented through the requirements for internal risk management, reporting, control and continuity systems activities. Such a two-tier architecture is in line with the logic of international approaches: the FSB and IOSCO set the framework for systemic oversight and market integrity, the FATF – for risk-based AML/CFT control VA/VASP, and CPMI-IOSCO formulates requirements for the cyber resilience of critical functions, benchmarks for the recovery of critical functions should be set as "permissible limits of impact" and continuity targets aligned with international guidelines on operational and cyber resilience of financial infrastructures [3; 10].

To operationalize institutional interaction, it is advisable to present a risk-based management cycle in the form of a closed loop of accountability. The cycle consists of successive links "policy → regulatory requirements → reporting and data → supervision → enforcement → communication", where the output of each link forms the input of the next. Two information "buses" – structural indicators and operational metrics of the early warning panel – provide an evidentiary basis for supervisory decisions and at the same time close the loop to the revision of policy priorities in the event of a change in risk regime.

The microprudential package is built on the principle of "Ukraine's problem → requirement → effect → verification", while the requirements are institutionally embedded in the supervisory cycle through: control procedures (audits/inspections/testing), and a set of indicators that fall into the dashboard as a basis for risk-based intervention. This architecture is consistent with the risk-based logic

of the global recommendations on the regulation and supervision of crypto-assets [13], with the principles of supervisory practice in digital asset markets [15] and with the requirements for operational (digital) resilience in the financial sector [8].

The content of the package is summarized in five contours: prudential resilience (own funds/buffers); protection of client assets and custody; operational and cyber resilience; internal control and compliance; transparency and management of conflicts of interest. The logic of proportionality is implemented as a differentiation of the intensity of requirements depending on the scale of operations, the criticality of functions and the nature of services, which corresponds to MiCA's approaches to classifying providers' services and requirements for their organization, as well as the general DORA framework for setting up ICT controls depending on the risk profile [8].

In terms of prudential stability, it is advisable to use the MiCA benchmark, where the minimum requirements for own funds/organization of the provider's activities are tied to the types of services and provide a transparent "entrance filter" for the legal segment of the market. In terms of protecting client assets, it is critical for Ukraine to prevent the mixing of client and own assets, since this channel translates the provider's operational problems into direct losses of investors; respectively, asset segregation and formalized custody procedures should be considered as a basic requirement of market reliability [9]. For operational and cyber resilience, the reference is DORA, which sets the framework for ICT risk management, incident management, digital resilience testing, and interaction with critical ICT service providers, which is correctly transferred to the critical functions of DFA providers in the context of war risks [8]. The internal control and financial integrity circuit should be aligned with the FATF's approaches to risk-based control of virtual assets and VASPs [10], and the transparency and conflicts of interest circuit should be aligned with the MiCA regulatory logic and ESMA technical standards on conflicts of interest for providers [9].

Microprudential requirements act as "micro-anchors" for system resilience: they reduce the likelihood of a cascade of loss and mistrust, and their effectiveness is operationalized through control/audit and dashboard metrics.

Market integrity tools are focused on removing empirical barriers to the legalization of the DFA segment in Ukraine – primarily the risk of trust, which manifests itself in the loss of customer funds, manipulations, a high share of non-jurisdictional offers, and persistent AML/CFT vulnerabilities. International approaches (FSB, IOSCO, IMF-FSB-G20) emphasize that effective regulation of crypto markets should combine investor protection, market integrity, and financial integrity with operational supervisory mechanisms [13].

The intensity of requirements and control procedures is determined by the risk profile of the product/client/channel and the scale of the provider's operations, which is the basic principle of the FATF for VA/VASP [11]. Relevant for legal approximation with the EU are the MiCA requirements on the conduct, organization and transparency of providers, as well as the Regulation on Information accompanying Transfers of Funds and Certain Crypto Assets (Travel Rule), which set minimum standards of traceability and the reduction of regulatory arbitration [13]. An additional argument in favor of strengthening consumer protection procedures is the warning of European supervisory authorities about the risks and limitations of actual protection in certain segments of the crypto market [6]. The Ukrainian context is verified by the availability of specialized materials of the SFMU on typologies of money laundering using virtual assets, which operationalizes risks for the domestic financial monitoring system [17].

It is advisable to structure the tools into four blocks, which should be integrated into the supervision cycle and into the monitoring system: anti-fraud and incident response; risk-based KYC/AML and interaction with financial monitoring; complaint/arbitration/reimbursement mechanisms; minimum standards for risk communication. The general logic is consistent with IOSCO's recommendations on crypto and digital assets (in particular, in terms of manipulation, conflicts of interest, supervision of trading practices, and disclosures), as well as with the FATF's approach to KYC/AML for VA/VASP [10].

Anti-fraud mechanisms should cover at least the detection of anomalous patterns (manipulations, "pump and dump", fraudulent schemes), internal escalation, temporary blocking/hold on risk triggers, and preservation of the evidence base for surveillance/law enforcement procedures. At the level of principles, such an architecture is consistent with IOSCO approaches to ensuring market integrity in

crypto markets and with the FSB logic of minimizing systemic channels of infection through manipulation and "run-dynamics" [12].

Risk-based KYC/AML should be built as a segmentation of clients and transactions by risk with an appropriate level of due diligence (CDD/EDD), detection of suspicious transactions and proper reporting to financial monitoring. For VA/VASP, this directly follows from the FATF standards and guidelines, and for practical implementation and compatibility with the European circuit, it is important to apply the requirements for information accompanying transfers (Travel Rule) [11]. The Ukrainian adaptation is based on the existing practices and documents of the SSFMU, which describe typical schemes and risk signals in transactions with virtual assets [17].

The third block – complaint/arbitration/compensation mechanisms – serves as an institutional stabilizer of trust: the presence of a standard referral channel, defined terms of consideration, fixation of the decision and the procedure for compensation in cases where the provider's liability is established, reduces secondary loss of trust and reduces the motivation of users to move to the "gray" segment. In terms of European regulation, MiCA's requirements for organizational procedures, transparency and customer protection are relevant; In addition, the ESAs' warning emphasizes the need not to overestimate investors' expectations for automatic guarantees and, accordingly, to strengthen procedural protection [9].

The fourth block – minimum standards for risk communication – should provide pre-transaction risk warnings, transparency of tariffs/spreads, compliance conditions, as well as disclosure of conflicts of interest. For the latter, it is appropriate to refer to ESMA's technical standards on conflicts of interest for CASPs in the MiCA outline [5]; for general supervisory practices to counter abuse in crypto markets, ESMA guidelines on supervisory prevention/detection practices abuse under MiCA [5]

The inertia of the DFA market dynamics, dependence on the global situation, and the structural shift of the war shock justify the transition from static risk control to a scenario-driven protocol of regulatory and supervisory actions. The basis of integration is to align three circuits: early warning (indicators of market tension, incident, compliance and complaints); stress testing of critical operations at the level of service providers and key functions (storage/transfer, order execution, service availability, KYC/AML control); a regulatory solution that transforms scenario assessment into proportionate restrictions/tightening of requirements and communication with the market. This approach is consistent with the principles of operational resilience and with the requirements for ICT incident management and continuity, as well as with recommendations for the supervision and control of risks of the crypto market [13].

In practice, scenario management should rely on a risk dashboard that aggregates: market metrics (realized volatility, drawdown, liquidity/spreads, concentrations); integrity metrics (number of fraud incidents, time of detection/elimination, customer requests); AML/CFT metrics (frequency of triggers/triggers, number of reports of suspicious transactions, share of enhanced verification); operational resilience metrics (availability of services, recovery time of critical functions, test results) [3].

Within the (optimistic/baseline/stress) scenarios, it is advisable to structure VASP/CASP stress testing into four blocks: liquidity and fulfillment of obligations to customers; cyber and ICT incidents; operational failures/continuity of critical functions; a surge in suspicious transactions and the load on KYC/AML circuits. MiCA's requirements for prudential safeguards/coverage of individual risks (in particular, loss of customer assets and failures) in combination with the FATF's risk-based standards set the regulatory framework, while test parameters should be established as supervisory expectations and internal policies of market entities [10]. The result is a willingness to rapidly scale tools according to the scenario, which reduces the likelihood of cascading trust losses, panic withdrawals, and secondary shadowing.

It is advisable to consider the package of regulatory and supervisory measures within the framework of the scenario approach to risk management of the digital financial asset market as a response profile reflecting the intensity of the use of key functional regulatory circuits, namely: prudential supervision, protection of client assets, ensuring operational and cyber resilience, KYC/AML procedures and investor protection tools. Such conceptualization ensures the proportionality of regulatory impact depending on the level of intensity of the risk environment, and also allows maintaining consistency with the system of early warning indicators and stress test results.

Within the optimistic scenario, which is characterized by controlled market growth, the level of market tension does not exceed the high percentile values of historical distributions, the incidence does not show upward dynamics, and there are no significant failures of information and communication infrastructure. Under such conditions, the minimum intensity of regulatory impact (level 1) is applied in all circuits, with the exception of investor protection instruments, which are maintained at a slightly higher level due to the need to ensure confidence in the market. Monitoring is initiated at the level of providers with subsequent reporting to regulatory authorities, while decisions are made within the powers of the NSSMC and the NBU. Control of the effectiveness of measures is based on volatility indicators, complaint dynamics, the level of customer verification, and incident response parameters.

The baseline scenario meets the conditions of moderate market tensions, which are within the upper percentile intervals, accompanied by periodic spikes in complaints and incidents, as well as an increase in reports of suspicious transactions without signs of a systemic violation of control. In this case, the intensity of application of all regulatory circuits increases to an average level (level 2), which implies a strengthening of prudential requirements, compliance procedures and operational resilience. Monitoring is carried out jointly by providers and financial monitoring bodies, and decision-making is coordinated by the NSSMC, the NBU and the SSFMU. The performance assessment is based on the completion of stress exercises, the level of service availability, the frequency of incidents, the duration of processing requests, and AML/CFT indicators.

The stress scenario reflects the implementation of shock or escalation conditions under which market tensions exceed critical percentile values, sharp capital outflows, an increase in fraudulent practices, and the occurrence of critical information infrastructure failures. Under such circumstances, the intensity of regulatory impact on all circuits increases to the maximum level (level 3), which provides for the immediate implementation of comprehensive stabilization measures. The initiation of the response is carried out by providers with simultaneous prompt notification of regulators, and coordination of measures is provided by the NSSMC, the NBU and the SSFMU with the involvement of the cybersecurity circuit. Control over the implementation of measures is carried out on the basis of indicators of critical incidents, the time of their localization, the share of detected and blocked suspicious transactions, as well as indicators of market continuity.

Thus, scenario risk management acquires a systemic character through a combination of indicator monitoring, graduated response profiles and institutionally defined coordination procedures, which ensures the adaptability of regulatory policy to changes in the external and internal environment of the digital financial asset market.

At present, the need for a phased implementation of risk management tools is obvious. The roadmap is based on a combination of three frameworks: firstly, these are the principles of international financial stability and supervisory recommendations for the crypto market, which require proportionality of regulation, transparency, risk management and the availability of shock response procedures. including customer due diligence, monitoring, reporting, and interaction with financial intelligence [10]. Thirdly, these are European regulatory requirements for crypto-assets and operational/ICT resilience, which form expectations for the organization of internal controls, incident management, and supervisory practices regarding market abuse [9]. In the national dimension, the key prerequisite for the start is legal certainty: the Draft Law 10225-d “On Amendments to the Tax Code of Ukraine and Certain Other Legislative Acts of Ukraine” on the regulation of the turnover of virtual assets in Ukraine (in particular, the Law of Ukraine “On Virtual Asset Markets”) has not yet entered into force, which determines the phased launch of the regulatory circuit. The additional context of financial market recovery and institutional capacity requirements in the post-shock transformation period is reflected in OECD analytical materials, which emphasize the role of supervision, corporate governance and investor confidence for a sustainable recovery [16]. The high penetration rate of crypto transactions in the Eastern Europe region and significant transaction volumes, including in Ukraine, reinforce the importance of integrity, supervision, and operational resilience tools as conditions for legalization and reduction of trust losses [2].

The performance indicator system should reflect controlled outputs and outcomes in five interrelated domains: regulatory market coverage (share of operations/participants in the licensed perimeter), integrity (frequency and structure of fraud and manipulation incidents, speed of detection/response), AML/CFT efficiency (quality of KYC, share of enhanced risk checks, indicators of reporting to the DSPM), operational and cyber resilience (availability of services, indicators incident

management, results of stress exercises), investor protection (dynamics of appeals, terms of consideration, restoration of rights and quality of risk communication) (Tables 2–3).

Table 2. Phase structure of implementation of risk management tools in the DFA market in Ukraine

Stage	Key tools	Responsible	Prerequisites	Horizon
1. Basic Trust Outline	Perimeter of supervision; licensing; KYC/AML; monitoring; Risk disclosure	NSSMC; NBU; DSFM	Regulatory Framework VA; tax regulation; FATF/EU	6–12 months
2. Standardization and monitoring	Reporting; risk-dashboard; incident management; stress exercises	NSSMC; NBU; DSPM; Providers	Completion of stage 1; surveillance data; DORA	12–24 months
3. Risk-based supervision	Scenarios; stress tests; turnover control; Asset Protection	NSSMC; NBU; DSPM; Providers	Chapters 1–2; MiCA/FATF	24–36 months

In order to ensure the assessment of the effectiveness of the implementation of certain stages (Table 2) and control the risks of their implementation, a system of performance indicators has been formed, which reflects both the achieved results and potential limitations. A generalization of the relevant parameters is given in Table 3.

Table 3. Performance indicators and risks

Stage	KPI	Risks	Mitigation mechanisms
1	% of the market in the perimeter; % KYC; STR; % of risk acknowledgements	Military and personnel restrictions	RBA; digitalization; Phases
2	Reporting coverage; uptime; MTTD/MTTR; % of monitoring; % EDD	Data and IT scarcity	Standardization; Proportionality
3	% RBA supervision; incidents; SLA; fulfillment of boundaries; Scenario results	Structural shocks	Threshold calibration; Script readiness

Note: KYC – customer identification/verification; AML/CFT – countering money laundering and terrorist financing; ICT – information and communication technologies; DORA/MiCA/FATF is an international framework on which the logic of requirements is based.

The sequence of stages minimizes the methodological gap between the rules and mechanisms: at the start, legalization is tied to the measurable market coverage and the performance of AML/CFT circuits; at the second stage – to data standardization, incident management and primary stress exercises; At the third stage, it leads to the full integration of scenario-driven risk management and supervisory practices, which reduces the likelihood of cascading trust losses, panic withdrawals and secondary shadowing during shock periods.

6. Conclusions

Thus, the proposed risk management system for the digital financial asset market in Ukraine, based on the results of empirical modeling of its dynamics, integrates: a risk map, a two-layer early warning panel, an institutional accountability circuit and a risk-based cycle of interaction "policy – requirements – reporting – supervision – enforcement – communication". A package of microprudential requirements, integrity tools and a scenario response protocol provides a transition from identification of risks to reproducible control procedures compatible with key international frameworks (MiCA, FATF, DORA), which increases resilience, transparency and trust in the market as a prerequisite for its legalization and sustainable development.

References

1. Bank for International Settlements. (2023). *Financial stability risks from cryptoassets in emerging market economies* (BIS Papers No. 138). https://www.bis.org/publ/bppdf/bispap138.pdf
2. Chainalysis. (2024). *Despite war and regulatory questions, crypto adoption grows in Eastern Europe driven by institutions and DeFi activity*. https://www.chainalysis.com/blog/2024-eastern-europe-crypto-adoption
3. Committee on Payments and Market Infrastructures, & Board of the International Organization of Securities Commissions. (2016). *Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements*. https://www.bis.org/cpmi/publ/d146.pdf

4. European Securities and Markets Authority. (2022). *Crypto-assets and financial stability*. https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf
5. European Securities and Markets Authority. (2025). *Guidelines on supervisory practices to prevent and detect market abuse under the Markets in Crypto-Assets Regulation (MiCA)*. https://www.esma.europa.eu/sites/default/files/2025-07/ESMA75-453128700-1039_Guidelines_on_supervisory_practices_to_prevent_and_detect_market_abuse_MiCA_.pdf
6. European Securities and Markets Authority. (2025, October 6). *EU supervisory authorities warn consumers of risks and limited protection for certain crypto-assets and providers*. https://www.esma.europa.eu/press-news/esma-news/eu-supervisory-authorities-warn-consumers-risks-and-limited-protection-certain
7. 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* (Digital Operational Resilience Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2554/oj
8. 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
9. European Union. (2023). *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. Financial Action Task Force. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
11. Financial Action Task Force. (2024). *Targeted update on implementation of the FATF standards on virtual assets and VASPs*. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2024.html
12. Financial Stability Board. (2022). *Assessment of risks to financial stability from crypto-assets*. https://www.fsb.org/wp-content/uploads/P160222.pdf
13. Financial Stability Board. (2023, July 17). *High-level recommendations for the regulation, supervision and oversight of crypto-asset activities and markets: Final report*. https://www.fsb.org/wp-content/uploads/P170723-2.pdf
14. Financial Stability Board. (2024). *G20 Crypto-asset Policy Implementation Roadmap: Status report*. https://www.imf.org/-/media/files/research/imf-and-g20/2024/imf-fsb-g20-crypto-asset-policy-implementation-roadmap.pdf
15. International Organization of Securities Commissions. (2023). *Policy recommendations for crypto and digital asset markets: Final report (FR11/2023)*. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf
16. Organisation for Economic Co-operation and Development. (2025). *Mapping Ukraine's financial markets and corporate governance framework for a sustainable recovery*. OECD Publishing. https://doi.org/10.1787/866c5c44-en
17. State Financial Monitoring Service of Ukraine. (2025). *Ryzyky ta zahrozy lehalizatsii (vidmyvannia) dokhodiv, oderzhanykh zlochynnym shliakhom, finansuvannia teroryzmu v umovakh viiskovoi ahresii rosiiskoi federatsii* [Risks and threats of money laundering and terrorist financing under conditions of the Russian Federation's military aggression]. https://fiu.gov.ua/assets/userfiles/411/%D0%A2%D0%B8%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%20%D0%94%D0%A1%D0%A4%D0%9C%D0%A3/Typology%202025_UA.pdf (in Ukrainian)
18. Volosovych, S., Nezhyva, M., Vasylenko, A., Morozova, L., & Napadovskyi I. (2024). Rynok kryptovaliutnykh aktyviv v umovakh voiennoi ahresii [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 (in Ukrainian)