Сучасні макроекономічні тренди та тенденції

Modern macroeconomic trends and tendencies

https://doi.org/10.26565/2786-4995-2026-2-12
UDC: 336.71:004.056:338.23

Kovalenko Victoria
D.Sc. in Economics, Professor of the Department of Banking,
Odesa National Economic Universit, Odesa, Ukraine;
e-mail: kovalenko-6868@ukr.net
ORCID ID: 0000-0003-2783-186X
Sheludko Sergii
Ph.D. in Economics, Associate Professor,
Head of the Analytical and Methodological Support Unit,
Pivdenny Bank PJSC, Odesa, Ukraine;
e-mail: s.szeludko@gmail.com
ORCID ID: 0000-0003-0636-4940
Serhieieva Olena
PhD (Economics), Associate Professor, Department of Banking
Odesa National Economic University, (Odesa, Ukraine)
e-mail: lenasergeeva2007@ukr.net
ORCID ID: 0000-0002-5523-3894

Digital instruments of monetary and prudential policy in ensuring the cybersecurity of the financial space

Abstract. In the context of the unprecedented pace of digital transformation and the escalation of geopolitical risks, traditional methods of monetary regulation require a fundamental reconsideration.

Problem statement. The evolution of cyber threats – from financial fraud to complex operations involving artificial intelligence – poses significant risks to macroeconomic stability. The development of an integrated protection system based on central bank digital currencies (CBDCs) and SupTech instruments constitutes a critical prerequisite for preserving financial sovereignty, particularly for Ukraine in the context of European integration and martial law.

Unresolved aspects of the problem. The theoretical substantiation and development of practical recommendations for integrating advanced digital instruments (CBDC, artificial intelligence, distributed ledger technology (DLT), and SupTech) into monetary and prudential policy mechanisms in order to form a comprehensive cybersecurity framework for the financial sector remain insufficiently addressed.

Purpose of the article. The purpose of this article is to provide a theoretical substantiation and to develop practical recommendations for integrating modern digital instruments (such as artificial intelligence, blockchain technologies, and SupTech) into monetary and prudential policy mechanisms in order to establish a comprehensive cybersecurity system for the financial sector.

The study is grounded in a systemic approach to analysing the coordination of regulatory policies. The methodology includes comparative legal analysis (comparing the models of the e-hryvnia and the Digital Euro), structural and functional modelling (two-tier CBDC architecture), and scenario analysis to identify cyber risks (including DDoS attacks and smart contract vulnerabilities) and methods for their mitigation.

Presentation of the main material. A model of hybrid coordination has been developed, in which cybersecurity is integrated directly into the mechanism of monetary transmission. It has been demonstrated that the programmability of the e-hryvnia and the application of Zero-Knowledge Proofs (ZKP) technologies enable the automation of prudential supervision while preserving user privacy. Global case studies (China, the European Union, and the Bahamas) have been analysed, and the specific features of the Ukrainian e-hryvnia project have been identified as instruments for enhancing transparency and cyber resilience.

For the first time, it is proposed to consider a central bank digital currency not only as a means of payment but also as an active element of the cyber-prudential system, enabling the dynamic adjustment of liquidity and limits under conditions of real cyberattacks. The concept of convergence between SupTech and RegTech systems based on unified distributed ledgers has been further developed.

The proposed architectural model and cyber-risk matrix may be utilised by the National Bank of Ukraine in the finalisation of the e-hryvnia project and in the development of digital operational resilience standards in accordance with the DORA regulation.

Conclusions. It has been demonstrated that digitalisation transforms the regulator into an architect of a secure financial environment. Further research will focus on the interoperability of CBDCs across countries and the role of artificial intelligence in preventing manipulation in digital asset markets.

Keywords: *e-hryvnia, monetary policy, prudential supervision, cybersecurity, CBDC, SupTech, smart contracts, financial stability, DLT, ZKP.*

Formulas: 0; fig.: 2, tabl.: 4, bibl.: 22

JEL Classification: E52, G21, G28, O33

For citation: Kovalenko Victoria, Sheludko Sergii, Serhieieva Olena. Digital instruments of monetary and prudential policy in ensuring the cybersecurity of the financial space. Financial and Credit Systems: Prospects for Development. №2(21) 2026. P. 154-166. https://doi.org/10.26565/2786-4995-2026-2-12

Introduction. The current stage in the development of the global financial system is characterised by an unprecedented pace of digital transformation. The transition from traditional banking models to ecosystems based on open banking and the integration of artificial intelligence have fundamentally altered the nature of financial operations. According to the International Monetary Fund [1], the financial sector remains the most vulnerable target for cybercriminals. During the period 2024 – 2026, an evolution of threats has been observed – from simple fraud to complex operations involving artificial intelligence. Cyber risk has ceased to be a purely technical issue and has become a critical determinant of macroeconomic stability. The potential destabilisation of payment systems as a result of cyberattacks may trigger a “digital panic” and an instantaneous outflow of capital.

Traditional supervisory methods based on retrospective analysis no longer correspond to the speed of the digital environment. The use of SupTech (Supervisory Technology) instruments enables regulators to conduct real-time monitoring, detecting anomalies within milliseconds. At the same time, the implementation of regulatory standards such as the Digital Operational Resilience Act (DORA) establishes a legal framework for ensuring digital operational resilience, in which cybersecurity becomes a mandatory prudential requirement.

Particular importance is attached to the development of central bank digital currencies (CBDCs). The architecture of CBDCs enables cybersecurity mechanisms (such as programmable limits and the automatic blocking of suspicious flows) to be embedded directly into the monetary layer of the system. This creates a new paradigm of monetary policy in which security constitutes an inherent property of money itself.

For Ukraine, the relevance of this topic is further reinforced by the necessity to counter hybrid threats and to integrate into the European Union’s single digital market. The development of a cybersecurity system based on advanced technologies constitutes a key condition for maintaining confidence in the national financial system under conditions of persistent external challenges.

Literature Review. The issue of employing digital instruments in monetary and prudential policy to ensure cybersecurity in the financial sector has attracted significant attention from leading international institutions and scholars. The transformation of central bank functions and the coordination of their policies in the digital era remain at the centre of both Ukrainian and international academic discourse. This problem area has been addressed in the scholarly works of prominent researchers.

Of fundamental importance are the studies by Bharath A. et al. [2], which substantiate the role of CBDC architecture as a mechanism for risk absorption. The authors demonstrate that the programmability of financial assets enables the implementation of “intelligent filters” for anomaly detection at the protocol level. The technological foundations of retail and wholesale CBDC models were established in the works of R. Auer and R. Böhme [3], which are critically important for

verifying the e-hryvnia model. A mathematical framework for designing digital currencies with consideration of user preferences was proposed by A. Agur et al. [4].

The impact of CBDCs on international capital flows and currency stability has been examined by M. Ferrari et al. [5]. In turn, M. Bordo and A. Levin [6], together with R. Rupeika-Apoga [7], emphasise the transition of central banks towards the active management of digital liquidity. An important cautionary perspective is presented by V. Brühl [8], who analyses potential losses within the banking sector and proposes compensatory models to support the stability of spreads.

Changes in the risk profile of banking institutions under conditions of digital transformation are examined by Qiaoying Ding and Wensheng He [9]. Within the Ukrainian academic discourse, M. Stetsko [10] highlights the necessity of balancing financial innovation with economic security, while I. Ninyuk [11] substantiates the need for artificial intelligence models to forecast macroeconomic challenges.

The concept of a "single registry" and the application of SupTech tools for supervising tokenised assets are elaborated in reports by the Bank for International Settlements (BIS) [12]. Issues of macroprudential resilience to large-scale attacks are addressed in reports of the European Systemic Risk Board (ESRB) [13], whereas the Bank of England [14] focuses on adaptive machine learning algorithms designed to prevent flash crashes. The relationship between the digitalisation of monetary policy and banks' investments in cybersecurity has been empirically demonstrated in the study by Yawen Li et al. [15].

Despite the substantial body of research, an integrated approach to the interaction between monetary and prudential policy within a unified cybersecurity framework requires further development, which determines the relevance of this study.

Purpose, objectives and research methods. The purpose of the article is to provide a theoretical substantiation and to develop practical recommendations for integrating modern digital instruments (such as artificial intelligence, blockchain technologies, and SupTech) into the mechanisms of monetary and prudential policy in order to establish a comprehensive cybersecurity system for the financial sector.

To achieve this purpose, the following objectives are to be accomplished:

1. To classify digital threats to the stability of the monetary system.
2. To analyse the effectiveness of SupTech instruments in detecting systemic cyber risks.
3. To propose a model of interaction between the regulator and commercial banks based on distributed ledger technologies.

Object of the study – the process of ensuring cybersecurity and financial stability under conditions of economic digitalisation.

Subject of the study – the set of digital instruments (SupTech, RegTech, artificial intelligence, and blockchain technologies) applied within the framework of monetary and prudential policy to minimise cyber risks.

In the course of the study, a комплекс of scientific research methods was employed, which ensured the robustness and reliability of the conclusions obtained:

1. Systemic approach – applied to determine the correlation between monetary regulation instruments and prudential supervision tools within a unified financial stability ecosystem.
2. Comparative legal analysis – employed to conduct a comparative assessment of the regulatory models of the e-hryvnia and the Digital Euro in the context of the requirements of the DORA Regulation.
3. Structural–functional modelling method – used in the development of a two-tier CBDC architecture and the algorithms governing the interaction of SupTech solutions.
4. Scenario analysis – applied to identify potential cyber risks and to develop strategies for their proactive mitigation.

Research results. The traditional paradigm of monetary regulation is primarily based on indirect instruments of influence. However, the implementation of CBDCs transforms the very nature of money, converting it into an active component of a preventive security system. The key mechanisms underpinning this transformation include the following:

Programmability and smart contracts. Unlike fiat currency, CBDCs enable the regulator to integrate logical conditions directly into the transactional layer. In the event of a large-scale cyberattack, the central bank would be capable of activating an "adaptive isolation mode", under which operational limits are dynamically adjusted in accordance with the level of threat in real time.

Real-time liquidity monitoring. The application of artificial intelligence algorithms for the continuous semantic processing of monetary flows enables the differentiation between natural market volatility and anomalous patterns resulting from malicious cyber activities (for example, flash loan attacks).

In view of the above, the priority of cyber resilience should be embedded directly at the stage of designing regulatory requirements (Tab. 1).

Table 1. Comparative characteristics of traditional and digital prudential instruments

Category	Conventional instrument	Digital instrument (2026)	Advantage for cyber resilience
Reporting	Quarterly discrete reporting (static formats)	Real-time API data streams	Proactive detection of network anomalies
Reserves	Liquidity ratio requirements	Dynamic liquidity buffers	Adaptation of capital to the intensity of cyberattacks
Identification	Paper-based KYC procedures	Self-Sovereign Identity (SSI)	Cognitive protection of personal data

Source: developed by the authors based on [1; 16]

Under conditions of pervasive digitalisation, financial stability is determined by the continuity of payment systems. The coordination model of the National Bank of Ukraine's policy is currently evolving from the control of interest rates towards the management of cybersecurity standards for critical infrastructure (Fig. 1).

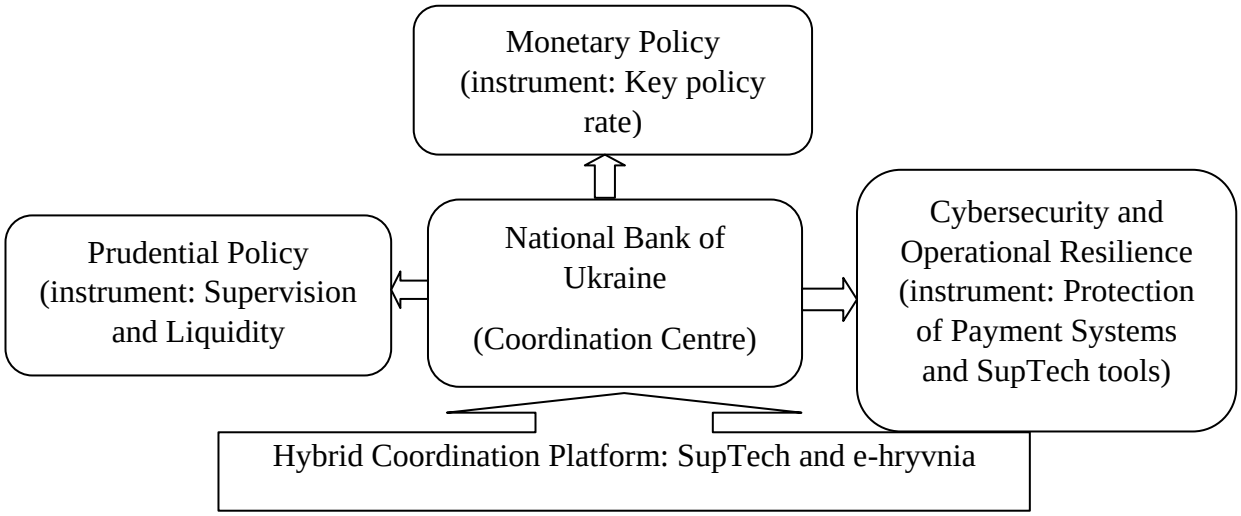

Figure 1. Hybrid model of policy coordination at the National Bank of Ukraine within the digital economy
Source: developed by the authors based on [4; 10; 17]

The proposed hybrid coordination model is based on the synergy between traditional instruments and operational resilience technologies. Within this architecture, cybersecurity ceases to function as an isolated service component and becomes integrated into the mechanism of monetary transmission. The effectiveness of the monetary impulse is now directly dependent on the uptime of

digital channels; any disruptive impact on infrastructure blocks the transmission mechanism, rendering regulatory policy ineffective.

To verify the proposed models, it is appropriate to conduct a comparative analysis of international experience (Tab. 2).

Table 2. Comparative analysis of global CBDC projects: architecture and privacy

Country / Project	Currency name	Type	Technology	Level of anonymity and privacy	Primary objective
China	e-CNY	Retail	Two-tier (Tier 2)	Managed anonymity – full regulatory control over all data	Liquidity control and displacement of private monopolies
Eurozone	Digital Euro	Retail	Hybrid (DLT+)	High for offline transactions – full anonymity of small-value payments (similar to cash)	Payment system autonomy within the EU
Bahamas	Sand Dollar	Retail	DLT / Blockchain	Multi-level – anonymity depends on wallet limits (Tier 1/2/3)	Financial inclusion in remote territories
Ukraine	e-hryvnia	Universal	Blockchain (Stellar)	Transparent monitoring – combination of privacy with the capability for financial oversight	Transparency of public expenditure and anti-corruption measures
Switzerland	Project Helvetia	Wholesale	DLT (R3 Corda)	Transaction confidentiality – restricted to licensed banks only	Efficiency of interbank settlements

Source: developed by the authors based on [2; 8; 15; 17].

The conducted analysis makes it possible to identify several key regularities in the development of global central bank digital currency projects. Most countries (including China and the European Union) tend to adopt a two-tier model, whereby the central bank issues the currency, while commercial banks and financial intermediaries are responsible for distribution and customer servicing. This arrangement helps to prevent deposit outflows from the banking system.

In the Digital Euro and e-hryvnia projects, particular attention is devoted to achieving a balance between payment privacy and AML/KYC requirements. In contrast to China's e-CNY, where the degree of state control is maximal, European and Ukrainian projects envisage a higher level of anonymity for small-value retail transactions. Projects such as Project Helvetia demonstrate the advantages of wholesale CBDCs for international settlements. They enable the reduction of transaction settlement times from days to seconds, thereby minimising settlement risks.

CBDC projects have clearly diverged according to political and institutional models. In democratic jurisdictions (such as the European Union and Ukraine), emphasis is placed on the protection of personal data in accordance with GDPR requirements, which necessitates the development of advanced cryptographic protocols to ensure the anonymity of small-value transactions. By contrast, the Chinese model of "controlled anonymity" effectively implies transparency of all transactions for the regulator, thereby strengthening the role of monetary policy as an instrument of social oversight.

To achieve a high level of anonymity (as envisaged in the Digital Euro project), Zero-Knowledge Proofs (ZKP) technologies are employed. These allow the legitimacy of a transaction to be verified without disclosing the identity of the sender, constituting a key digital instrument within modern payment architectures.

For Ukraine, the programmability function is of critical importance. It enables the implementation of targeted use of funds (for example, social transfers that can be spent only on

specific categories of goods), which automatically reduces the risks of fraud and misallocation of public funds, thereby strengthening the financial security of the state.

Recent studies indicate that offline functionality in CBDC systems is becoming a standard component of cybersecurity architecture. In the event of a large-scale cyberattack targeting internet infrastructure, the capability to perform digital payments via Bluetooth or NFC without network access (as envisaged in the architectures of the e-hryvnia and the Digital Euro) constitutes a key element of economic resilience [3; 18–19].

When designing central bank digital currencies, central banks worldwide face the challenge of selecting an appropriate interaction model between the regulator, banking institutions, and end users. According to the classification proposed by Auer and Böhme (2020), architectural solutions directly influence both cybersecurity levels and the risks of financial disintermediation.

CBDC architectural models may be examined at three distinct levels:

1. *Single-tier (Direct) model*. In this model, the central bank maintains accounts for all users directly. Its defining feature is the maximum level of state control; however, it imposes a substantial operational burden on the regulator's infrastructure. A high degree of vulnerability to centralised cyberattacks is also observed. As noted by J. Nijsse and A. Pinto, this model effectively neutralises transaction privacy, as the state is capable of observing every transaction in real time [18].
2. *Two-tier (Intermediated) model*. This represents the most widespread approach, adopted for the e-CNY and the Digital Euro. The central bank issues the currency, while commercial banks (intermediaries) perform KYC procedures and maintain digital wallets. The advantages of this model include the preservation of the existing banking structure and the distribution of operational risks. According to the Bank for International Settlements (BIS) report [12], the two-tier structure demonstrates greater resilience to system failures, as customer data are distributed across multiple financial institutions.
3. *Hybrid model (e-hryvnia)*. The Ukrainian e-hryvnia project предусматривает the possibility of both direct access and intermediary-based interaction, with a particular emphasis on distributed ledger technology (DLT). This approach enables the provision of "transparent monitoring" while maintaining operational efficiency [20].

As emphasised by P. Cipollone [19] in reports concerning the Digital Euro, algorithmic liquidity management constitutes a key instrument of prudential supervision in next-generation payment systems. This mechanism helps to prevent situations in which a cyber incident affecting a single institution propagates instantly across the entire financial network. The implementation of Zero-Knowledge Proofs (ZKP) within two-tier models is becoming a standard practice in democratic jurisdictions. Research by J. Nijsse and A. Pinto demonstrates that this instrument enables regulators to verify compliance with transaction limits and tax obligations without accessing personal wallet data, thereby meeting confidentiality requirements in the digital environment [18].

Unlike many other countries, the e-hryvnia in Ukraine carries not only economic but also socio-security significance, namely:

✔ transparency of public expenditure – the use of the e-hryvnia for social transfers (for example, subsidies or assistance to internally displaced persons) enables monitoring of the targeted use of funds through programmability features;

✔ cross-border payments – the creation of a rapid and cost-efficient transfer channel, which is particularly important given the large number of Ukrainian citizens residing abroad;

✔ development of virtual asset markets – the e-hryvnia is expected to serve as a foundational instrument for a regulated virtual asset market, functioning as a reliable regulator-backed stablecoin;

✔ cyber resilience – the establishment of an alternative payment network capable of functioning in the event of disruptions to traditional banking systems.

The implementation of the e-hryvnia project by the National Bank of Ukraine represents one of the most advanced examples of CBDC deployment in Eastern Europe. Unlike many jurisdictions that view digital currencies solely as payment instruments, Ukraine incorporates a broader functional framework, extending from social policy implementation to cybersecurity assurance.

The Ukrainian e-hryvnia project shares a common philosophy with the European Digital Euro, but differs in emphasis due to the specific features of the domestic economy (Tab. 3).

Table 3. Comparative analysis of the Ukrainian e-hryvnia and the Digital Euro projects

Comparison parameter	e-hryvnia (NBU)	Digital Euro (ECB)
Primary driver	Combatting the shadow economy and enhancing expenditure transparency	Protection of monetary sovereignty from foreign BigTech actors
Role of intermediaries	Banks and fintech companies as active wallet operators	Banks as the sole legitimate distributors
Programmability	Focus on smart contracts: support for "targeted" money	Minimal: funds are intended to remain universal
Confidentiality	Controlled transparency for AML procedures	Maximum anonymity for small-value payments (similar to cash)

Source: developed by the authors based on [8; 16; 19–21].

According to recent publications [19] and statements by the NBU [21], both projects are guided by a "do no harm" principle for commercial banks. This entails the implementation of holding limits for digital currency (e.g., up to 3,000 units per person) to prevent mass deposit outflows.

As noted by M. Stetsko [10] and I. Ninyuk [11], the Ukrainian case exhibits greater flexibility regarding the use of smart contracts. This allows the implementation of a "programmable money" model, in which a transaction executes automatically only upon the occurrence of a specified condition (e.g., confirmation of goods delivery recorded in the ledger), significantly reducing credit risks within the economy.

Comparative analysis of the NBU and ECB architectural solutions demonstrates the common adoption of a two-tier (intermediated) model, which minimises the risk of disintermediation in the banking sector [19]. However, the Ukrainian case is distinguished by deeper integration of smart contracts, enabling the programmable money function for state transfers – an option not available in the more conservative Digital Euro model.

A further aspect of the e-hryvnia's relevance is its cyber resilience. In the event of potential failures in centralised systems, the use of a DLT-based platform ensures continuity of payments, thereby satisfying the requirements of the European Digital Operational Resilience Act (DORA) regarding operational resilience [16].

The implementation of the e-hryvnia creates a "single point of entry" for potential malicious actors, necessitating the development of a multi-layered security system. According to the classification by Bharath A., Paduraru A., and Gaidosch T. [2], the primary cyber risks within a CBDC ecosystem and methods for their mitigation in the Ukrainian context can be grouped into three categories:

1. *Infrastructure-level risks (Systemic Risks)*. Massive DDoS attacks targeting nodes (validators) of the distributed ledger could potentially paralyse the national payment system. Mitigation is achieved through the deployment of a decentralised DLT architecture. Unlike traditional databases, the e-hryvnia ledger is replicated across multiple geographically distributed nodes (NBU, state-owned banks, certified EU cloud services). This ensures system viability even if a portion of servers is taken offline.

2. *Smart contract and algorithmic risks*. Vulnerabilities in smart contract code could lead to unauthorised issuance or theft of digital assets. Countermeasures include mandatory multi-layered code audits and the application of formal verification (mathematical proof of algorithm

correctness). As outlined in the DORA standards, any changes to the e-hryvnia protocol must pass through sandbox environments before deployment to the live network.

3. *Privacy and data leakage risks*. User deanonymisation via Big Data analysis on the blockchain poses threats to citizens' personal security. The implementation of Zero-Knowledge Proofs (ZKP) and homomorphic encryption addresses these concerns. These digital instruments allow regulators to verify the legitimacy of transactions without accessing personal data of senders or recipients, provided that transaction amounts do not exceed the established prudential limits (Tab. 4).

Table 4. Matrix of Cyber Risks and Prudential Response Instruments

Type of Risk	Mitigation Instrument	Role of the Regulator (NBU)
Double spending	DLT consensus algorithm	Real-time monitoring of ledger integrity
Compromise of client wallets	Multi-signature (multi-sig) and biometrics	Establishment of limits on single transactions
Insider attacks	Role-Based Access Control (RBAC)	Prudential supervision of banks' operational staff

Source: developed by the authors based on [8; 16; 20; 21]

The analysis of the e-hryvnia case demonstrates that the cybersecurity of a digital currency is not a static condition but rather a dynamic process of coordinating monetary and prudential instruments. A key determinant of resilience is interoperability with international security systems. As emphasised by V. Kovalenko, the synchronisation of e-hryvnia protection protocols with European cybersecurity standards will enable Ukraine to become part of a unified secure financial space within the EU, thereby minimising the risks of cross-border cyber incidents [17].

Based on the above, the authors propose an architectural model for integrating digital SupTech and RegTech instruments with monetary policy to ensure cyber resilience.

The proposed architecture illustrates the interaction between two levels of the financial system (macro- and micro-levels) and demonstrates how digital instruments contribute to ensuring cyber resilience.

Discussion. The findings of the conducted study bring to the fore a number of debatable issues concerning the transformation of the financial system architecture under the influence of digital instruments of monetary and prudential policy (Fig. 2).

A fundamental issue in this debate remains the tension between payment anonymity and the requirements of financial monitoring. In contrast to the model of "managed anonymity" implemented in China, the European and Ukrainian approaches require adherence to high standards of personal data protection. As noted by R. Cipollone [19], the design of modern CBDCs should move beyond the binary choice between full anonymity and total surveillance. The implementation of programmable privacy through zero-knowledge proof (ZKP) technologies enables the realisation of a "privacy-by-design" concept that complies with the requirements of the DORA Regulation [16] while simultaneously ensuring prudential supervision.

A critical aspect of the discussion concerns the impact of the digital hryvnia on the deposit base of commercial banks. Opponents of its introduction point to the risk of a "digital bank run" towards central bank liquidity during periods of crisis. However, according to the position of R. Auer and R. Böhme [3], as well as the Bank for International Settlements [12], this risk can be effectively mitigated through prudential constraints: the e-hryvnia should function exclusively as a means of exchange rather than as an instrument for storing large volumes of capital. The imposition of strict quantitative holding limits and the absence of interest accrual make it possible to preserve the key role of commercial banks in credit intermediation.

A primary subject of academic debate is the balance between the fundamental right of users to transaction privacy and the regulator's obligation to conduct effective financial monitoring. Unlike the e-CNY model, which is based on the concept of "managed anonymity" with a high

degree of centralised control, the Ukrainian e-hryvnia project should evolve within the framework of the European legal order.

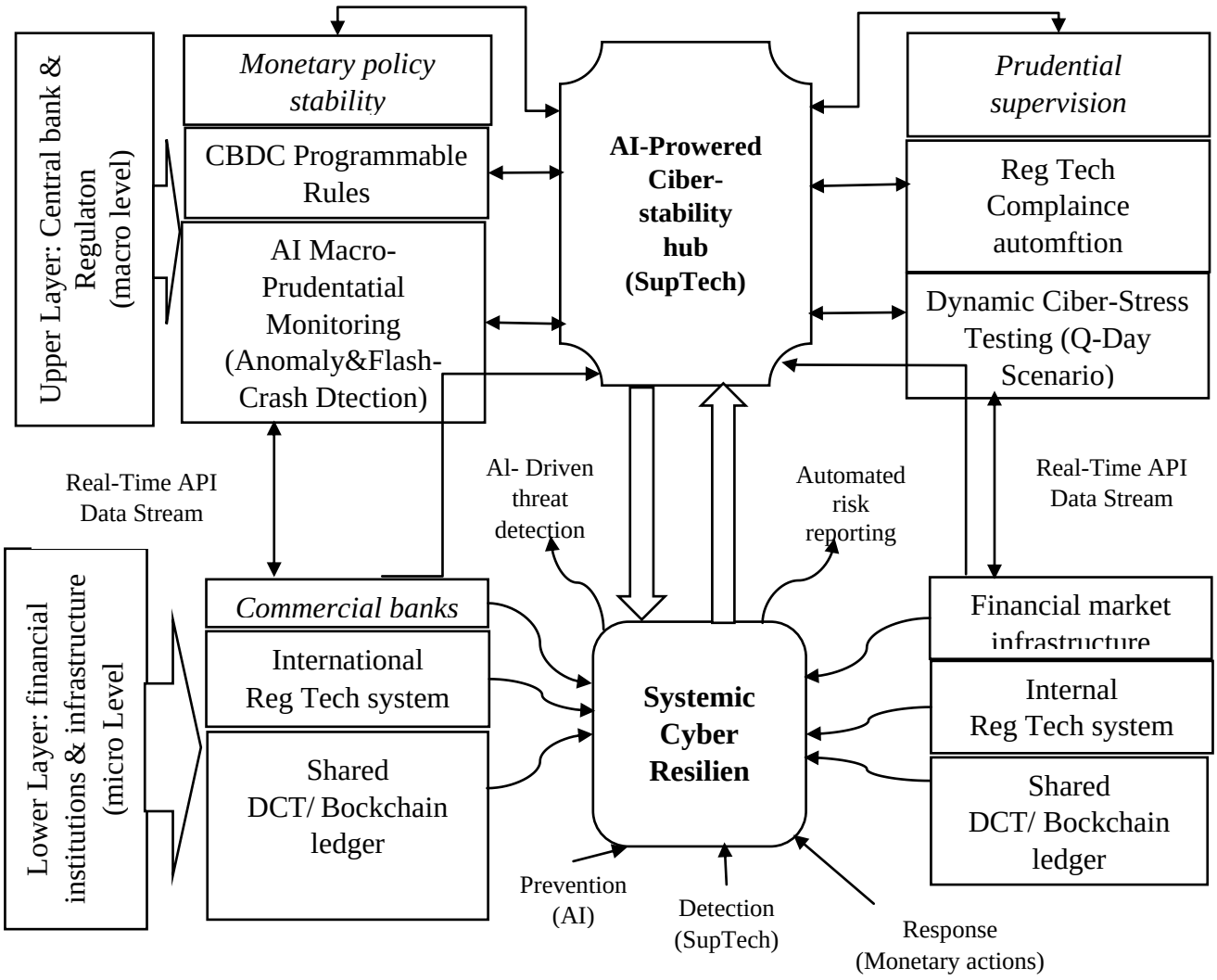

Figure 2. Architecture for the Integration of Digital SupTech, RegTech and Monetary Policy Instruments to Ensure Cyber Resilience
Source: authors' own elaboration.

We argue that the resolution of this contradiction lies in the application of Zero-Knowledge Proofs (ZKP). This approach enables the verification of transaction legitimacy without disclosing the personal data of the wallet holder, thereby complying with the requirements of the GDPR and the standards of DORA. Such an approach transforms the role of the NBU from a passive controller into an active architect of a secure digital environment.

The debate over the choice between a centralised ledger and distributed ledger technology (DLT) acquires particular significance in the context of national security. Although centralised systems traditionally exhibit higher throughput, for jurisdictions facing elevated geopolitical risks, decentralisation becomes a critical necessity. As emphasised in the World Economic Forum report [22], in countries exposed to physical threats to infrastructure, the resilience of DLT nodes outweighs latency costs. Thus, the choice of DLT for the e-hryvnia is not a matter of technological fashion, but a means of ensuring the continuity of financial operations under emergency conditions.

Conclusions. The generalisation of the study's findings allows us to conclude that the digital transformation of the financial sector is driving a fundamental reconfiguration of the instruments of monetary and prudential policy. The paper substantiates that, in the context of

evolving cyber threats, traditional regulatory methods are increasingly being supplanted by algorithmic and predictive supervisory mechanisms.

It is demonstrated that the integration of SupTech technologies and the implementation of CBDCs transform the function of the central bank from passive oversight to active architectural management of financial stability. This enables real-time monitoring of systemic risks, which is critical for preventing "digital panics" and flash crashes.

An architectural model of interaction between the regulator and commercial banks has been developed, in which cybersecurity is embedded directly into the monetary transmission mechanism. It is established that the operational resilience of payment channels becomes a necessary condition for the effectiveness of the policy rate as the primary instrument of monetary policy.

The analysis of the e-hryvnia project confirms its high adaptability to security challenges. The use of distributed ledger technology (DLT) and Zero-Knowledge Proof (ZKP) protocols is identified as an optimal approach to ensuring a balance between transaction privacy and AML/KYC requirements within the European legal framework (DORA, GDPR).

A system of safeguards (holding limits and the absence of interest accrual) is substantiated, enabling the avoidance of disintermediation in the banking sector while preserving the investment capacity of commercial financial institutions.

Given the dynamic nature of the issue under study, further research should focus on the following areas:

1. *Interoperability and cross-border resilience*. Investigation of mechanisms for the seamless integration of the e-hryvnia with other CBDCs (in particular, the Digital Euro) in order to establish a unified secure payment space, which requires the synchronisation of cybersecurity protocols at the international level.

2. *Post-quantum cryptography in the financial sector*. Analysis of the vulnerabilities of blockchain infrastructures to future quantum computing and the development of encryption algorithms for the e-hryvnia which are resilient to quantum-level attacks.

3. *Economic efficiency of "smart money"*. Empirical assessment of the impact of currency programmability on the velocity of money and the targeted use of international financial assistance in the context of Ukraine's post-war recovery.

4. *AI-driven liquidity regulation*. Development of artificial intelligence models for the predictive detection of manipulation in digital asset markets and the prevention of systemic disruptions in real time.

References

1. IMF. (2024). *Cyber Risk and Financial Stability: Growing Threats and Policy Challenges. IMF Global Financial Stability Report*. Retrieved from: https://www.imf.org/en/Publications/GFSR/
2. Bharath, A., Paduraru, A., & Gaidosch, T. (2024). *Cyber Resilience of the Central Bank Digital Currency Ecosystem*. IMF Fintech Notes. Retrieved from: https://surli.cc/vbvwfa
3. Auer, R., & Böhme, R. (2020). The technology of retail central bank digital currency. *BIS Quarterly Review*, March, 85–100. Retrieved from: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf
4. Agur, I., Ari, A., & Dell'Ariccia, G. (2022). Designing central bank digital currencies. *Journal of Monetary Economics*, 125, 62–79. DOI: https://doi.org/10.1016/j.jmoneco.2021.05.002
5. Ferrari, M. M., Mehl, A., & Stracca, L. (2021). *Central Bank Digital Currency in an Open Economy*. ECB Working Paper, No. 20202488. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3733463/
6. Bordo, M. D., & Levin, A. T. (2024). Central bank digital currency and the future of monetary policy. *Journal of Financial Stability*, 70, 101211. Retrieved from: https://surl.lt/ljzdgp
7. Rupeika-Apoga, R. (2025). Editorial-The Future of Money: Central Bank Digital Currencies, Cryptocurrencies and Stablecoins. *Journal of Risk and Financial Management*, 18(9), 469. DOI: https://doi.org/10.3390/jrfm18090469
8. Brühl, V. (2026). The potential impact of a central bank digital currency (CBDC) on the banking sector: the case of a digital euro. *Eurasian Economic Review*. DOI: https://doi.org/10.1007/s40822-025-00359-2
9. Qiaoying, D., & Wensheng, H. (2023). Digital Transformation, Monetary Policy and Risk-taking of Banks. *Finance Research Letters*, 55(3), 103986. DOI: https://doi.org/10.1016/j.frl.2023.103986
10. Stetsko, M. V. (2025). Monetary policy as a tool for ensuring the financial stability of the banking system and economic security of Ukraine. *Innovative Economy*, 3(103), 107-113. DOI: https://doi.org/10.37332/2309-1533.2025.2.13 [in Ukrainian]

11. Ninyuk, I. (2024). Digitalisation of Monetary Policy as a Factor in Ensuring Financial Stability in Ukraine. *Current Issues in Economic Sciences*. DOI: https://doi.org/10.5281/zenodo.14603985 [in Ukrainian]
12. BIS. (2025). *Project Agora: exploring tokenisation of cross-border payments*. Retrieved from: https://surl.li/ckbhvj
13. ESRB. (2024). *Advancing macroprudential tools for cyber resilience – Operational policy tools. A review of national and pan European frameworks*. Retrieved from: https://surl.li/gmonzm
14. Bank of England. (2025). *Financial Stability Report – December 2025*. Retrieved from: https://www.bankofengland.co.uk/financial-stability-report/2025/december-2025
15. Li, Y., Xia, Y., Sun, Z., & Sun, N. (2025). Does digital transformation affect systemic risk? Evidence from the banking sector in China. *International Review of Financial Analysis*, 102. DOI: https://doi.org/10.1016/j.irfa.2025.104137
16. European Parliament. (2025). *Regulation (EU) 2025/2554 on digital operational resilience for the financial sector (DORA) and its Technical Standards*. Retrieved from: https://surl.li/jlkiwi
17. Kovalenko, V. V. (2026). Transformation of policy coordination mechanisms of the National bank of Ukraine under the digitalization of the financial sector. *Scientific Bulletin of the Odesa National Economic University*, 1(388), 51-60. DOI: https://doi.org/10.32680/2409-9260-2026-1-338-51-60 [in Ukrainian]
18. Nijsse, J., & Pinto, A. (2026). Central Bank Digital Currencies: Where is the Privacy, Technology, and Anonymity? *Cryptography and Security*. DOI: https://doi.org/10.48550/arXiv.2602.23659
19. Cipollone, P. (2025). *Digital euro: protecting our freedom, autonomy and security*. Retrieved from: https://surl.li/jervcn
20. Bezpalko, I., & Bezpalko, M. (2025). Digital transformation of the financial sector: Central banks' digital currencies as a global trend and national strategy. *Efficient Economy*, 1. DOI: https://doi.org/10.32702/2307-2105.2025.1.64 [in Ukrainian]
21. NBU. (2023). *Strategy "Financial Fortress of Ukraine"*. Retrieved from: https://bank.gov.ua/ua/news/all/strategiya-natsionalnogo-banku-ukrayini [in Ukrainian]
22. WEF. (2026). *Global Cybersecurity Outlook: Resilience of Financial Infrastructures under Geopolitical Threats*. Geneva: WEF White Papers. Retrieved from: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Received: 22.12.2025 *Accepted: 03.05.2026*
Received after review: 12.04.2026 *Published: 30.06.2026*

Authors Contribution: *All authors have contributed equally to this work*
Conflict of Interest: *The authors declare no conflict of interest*

Коваленко Вікторія
доктор економічних наук, професор,
професор кафедри банківської справи,
Одеський національний економічний університет
вул. Преображенська,8, 65082, м. Одеса, Україна
e-mail: kovalenko-6868@ukr.net
ORCID ID: 0000-0003-2783-186X
Шелудько Сергій
кандидат економічних наук, доцент,
начальник відділу аналітичної та методологічної підтримки,
ПАТ Акціонерний банк «Південний»
вул. Краснова, 6/1, 65059, м. Одеса, Україна
e-mail: s.szeludko@gmail.com
ORCID ID: 0000-0003-0636-4940
Сергєєва Олена
кандидат економічних наук, доцент,
доцент кафедри банківської справи
Одеський національний економічний університет,
вул. Преображенська,8, 65082, м. Одеса, Україна
e-mail: lenasergeeva2007@ukr.net
ORCID ID: 0000-0002-5523-3894

Цифрові інструменти монетарної та пруденційної політики у забезпеченні кібербезпеки фінансового простору

Анотація. В умовах безпрецедентної швидкості цифрової трансформації та зростання геополітичних ризиків, традиційні методи монетарного регулювання потребують фундаментального перегляду.

Постановка проблеми. Еволюція кіберзагроз від фінансового шахрайства до складних операцій із застосуванням ШІ створює ризики для макроекономічної стабільності. Побудова інтегрованої системи захисту на базі цифрових активів центральних банків (CBDC) та SupTech-інструментів є критичною умовою збереження фінансового суверенітету, особливо для України в контексті євроінтеграції та воєнного стану.

Невирішені аспекти проблеми. Теоретичне обґрунтування та розробка практичних рекомендацій щодо інтеграції передових цифрових інструментів (CBDC, штучний інтелект, технологія розподіленого реєстру (DLT) та SupTech) у механізми монетарної та пруденційної політики з метою формування комплексної системи кібербезпеки для фінансового сектору залишаються недостатньо розглянутими.

Мета статті. Метою цієї статті є теоретичне обґрунтування та розробка практичних рекомендацій щодо інтеграції сучасних цифрових інструментів (таких як штучний інтелект, блокчейн-технології та SupTech) у механізми монетарної та пруденційної політики з метою створення комплексної системи кібербезпеки для фінансового сектору.

Дослідження базується на системному підході до аналізу координації політик регулятора. Використано порівняльно-правовий аналіз (зіставлення моделей е-гривні та Digital Euro), структурно-функціональне моделювання (архітектура дворівневої CBDC) та сценарний аналіз для ідентифікації кіберризиків (DDoS, вразливості смарт-контрактів) та методів їх нівелювання.

Основний матеріал. Розроблено модель гібридної координації, де кібербезпека інтегрована безпосередньо в механізм монетарної трансмісії. Доведено, що програмованість е-гривні та використання технологій Zero-Knowledge Proofs (ZKP) дозволяють автоматизувати пруденційний нагляд, зберігаючи приватність користувачів. Проаналізовано світові кейси (Китай, ЄС, Багами) та виокремлено особливості українського проєкту е-гривні як інструменту прозорості та кіберрезильєнтності.

Вперше запропоновано розглядати цифрову валюту центрального банку не лише як платіжний засіб, а як активний елемент системи кіберпруденційності, що дозволяє динамічно корегувати ліквідність та ліміти в умовах реальних кібератак. Дістала подальшого розвитку концепція конвергенції SupTech та RegTech систем на базі єдиних розподілених реєстрів.

Запропонована архітектурна модель та матриця кіберризиків можуть бути використані НБУ при фіналізації проєкту е-гривні та розробці нормативів цифрової операційної стійкості згідно з регламентом DORA.

Висновки. Було продемонстровано, що цифровізація перетворює регулятора на архітектора безпечного фінансового середовища. Подальші дослідження будуть зосереджені на взаємодії центральних банків цифрових валют (CBDC) між країнами та ролі ШІ у запобіганні маніпуляціям на ринках цифрових активів.

Ключові слова*: е-гривня, монетарна політика, пруденційний нагляд, кібербезпека, CBDC, SupTech, смарт-контракти, фінансова стабільність*

Формули: 0; рис.: 2; табл.: 4; бібл.: 22

Для цитування: Kovalenko Victoria, Sheludko Sergii, Serhieieva Olena. Digital instruments of monetary and prudential policy in ensuring the cybersecurity of the financial space. Фінансово-кредитні системи: перспективи розвитку. №2(21) 2026. С. 154-166. https://doi.org/10.26565/2786-4995-2026-2-12

Список літератури

1. IMF. Cyber Risk and Financial Stability: Growing Threats and Policy Challenges. IMF Global Financial Stability Report. 2024. URL: https://www.imf.org/en/Publications/GFSR/
2. Bharath, A., Paduraru, A., Gaidosch, T. Cyber Resilience of the Central Bank Digital Currency Ecosystem. *IMF Fintech Notes*. 2024. 53 p. URL: https://surli.cc/vbvwfa
3. Auer, R. Böhme, R. The technology of retail central bank digital currency. *BIS Quarterly Review*. 2020. March. P. 85–100. URL: https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf
4. Agur, I., Ari, A., Dell'Ariccia, G. Designing central bank digital currencies. *Journal of Monetary Economics*. 2022. № 125. P. 62–79. . URL: https://doi.org/10.1016/j.jmoneco.2021.05.002.
5. Ferrari, M.M., Mehl, A., Stracca, L. Central Bank Digital Currency in an Open Economy. *ECB Working Paper*. 2021. No. 20202488. 69 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3733463/
6. Bordo, M. D., Levin , A. T. Central bank digital currency and the future of monetary policy. *Journal of Financial Stability*. 2024. № 70. 101211, URL: https://surl.lt/ljzdgp.
7. Rupeika-Apoga, R. Editorial-The Future of Money: Central Bank Digital Currencies, Cryptocurrencies and Stablecoins. *Journal of Risk and Financial Management*. 2025. № 18(9). 469. URL: https://doi.org/10.3390/ jrfm18090469.
8. Brühl, V. The potential impact of a central bank digital currency (CBDC) on the banking sector: the case of a digital euro. *Eurasian Economic Review*. 2026. URL: https://doi.org/10.1007/s40822-025-00359-2.
9. Qiaoying, D., Wensheng, He. Digital Transformation, Monetary Policy and Risk-taking of Banks. *Finance Research Letters*. 2023. № 55(3). 103986. URL: https://doi.org/10.1016/j.frl.2023.103986/
10. Стецько, М.В. Грошово-кредитна політика як інструмент забезпечення фінансової стабільності банківської системи та економічної безпеки України. Інноваційна економіка.2025. № 3 (103). С. 107-113. URL: https://doi.org/10.37332/2309-1533.2025.2.13.
11. Нінюк, І. Цифровізація монетарної політики як фактор забезпечення фінансової стабільності в Україні. *Актуальні питання економічних наук.* 2024. URL: https://doi.org/10.5281/zenodo.14603985.
12. BIS. Project Agora: exploring tokenisation of cross-border payments. 2025. URL: https://surl.li/ckbhvj.
13. ESRB. Advancing macroprudential tools for cyber resilience – Operational policy tools. A review of national and pan European frameworks, 2024. 44 p. URL: https://surl.li/gmonzm.
14. Bank of England Financial Stability Report – December 2025. URL: https://www.bankofengland.co.uk/financial-stability-report/2025/december-2025.
15. Yawen, Li, Yufei, Xia, Zongting, Sun, Naili, Sun (2025). Does digital transformation affect systemic risk? Evidence from the banking sector in China. *International Review of Financial Analysis*. Elsevier. 2025. 102. URL: https://doi.org/10.1016/j.irfa.2025.104137.
16. European Parliament. Regulation (EU) 2025/2554 on digital operational resilience for the financial sector (DORA) and its Technical Standards.2025. URL: https://surl.li/jlkiwi.
17. Коваленко В.В. Трансформація механізмів координації політики Національного банку України в умовах цифровізації фінансового сектору. *Науковий вісник Одеського національного економічного університету*. 2026. № 1 (388). С. 51-60. https://doi.org/10.32680/2409-9260-2026-1-338-51-60.
18. Nijsse, J. Pinto, A. Central Bank Digital Currencies: Where is the Privacy, Technology, and Anonymity? *Cryptography and Security*. 2026. 21 p. URL: https://doi.org/10.48550/arXiv.2602.23659.
19. Cipollone, P. Digital euro: protecting our freedom, autonomy and security. 2025. URL: https://surl.li/jervcn.
20. Безпалько, І., Безпалько, М. Цифрова трансформація фінансового сектору: цифрові валюти центральних банків як глобальний тренд та національна стратегія. Ефективна економіка. 2025. Вип. 1. URL: http://doi.org/10.32702/2307-2105.2025.1.64.
21. НБУ. Стратегія «Фінансова фортеця України». Strategy "Financial Fortress of Ukraine". 2023. URL: https://bank.gov.ua/ua/news/all/strategiya-natsionalnogo-banku-ukrayini.
22. WEF. Global Cybersecurity Outlook: Resilience of Financial Infrastructures under Geopolitical Threats. *Geneva: WEF White Papers*. 2026. 64 p. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.

Стаття надійшла до редакції 22.12.2025 *Статтю рекомендовано до друку 03.05.2026*
Стаття надійшла після рецензування 12.04.2026 *Статтю опубліковано 30.06.2026*

Внесок авторів: *всі автори зробили рівний внесок у цю роботу*
Конфлікт інтересів: *автори повідомляють про відсутність конфлікту інтересів*