Europe at a Crossroads: Governance, Business, and Policy Transformation in a Changing Global Economy. Proceedings of the International Conference EU-PAIR 2026

DOI:10.47743/eu-pair.2026-1-10

EMERGING TECHNOLOGIES, FINTECH INNOVATION, CYBERSECURITY, AND THE EUROPEAN UNION'S VISION FOR THE FUTURE OF BANKING

VADIM GRIGORYAN
Armenian State University of Economics
Yerevan, Armenia
vadim.grigoryan@asue.am

DIANA GEVORGYAN
Armenian State University of Economics
Yerevan, Armenia
diana.gevorgyan91@gmail.com

LUSINE KIRAKOSYAN
Armenian State University of Economics
Yerevan, Armenia
lusine.kirakosyan@asue.am

Abstract
In the light of the "Bank of the Future" paradigm, this study examines how emerging technologies, fintech innovation, cybersecurity, and the European Union's digital transformation agenda are shaping the future of banking. It explores how innovations such as blockchain, artificial intelligence, and data analytics are transforming banking operations, improving efficiency, and enhancing customer experience. The study also investigates the growing role of fintech companies and decentralized finance in increasing competition and accelerating digital transformation across the European banking sector. Particular attention is given to the European Union's regulatory framework, including initiatives aimed at fostering innovation while ensuring financial stability, consumer protection, and cybersecurity resilience. Furthermore, the research highlights the increasing cybersecurity challenges associated with digitalization, including ransomware attacks, phishing schemes, and data breaches. The relationship between cybersecurity, regulatory compliance, and EU digital policies is examined as a critical component of risk management. The study adopts a mixed-methods approach to analyse survey data from bank executives and IT managers as well as qualitative insights from the institutional case studies. The empirical results validate that technology adoption has a significant positive association with operational efficiency.

The results also reveal that holistic cybersecurity alignment reduces cybercrime incidents and greatly improves digital trust. The findings emphasize the importance of balancing technological innovation with robust security frameworks and effective regulatory governance to support resilient, secure, and sustainable banking development within the European Union and beyond.
Keywords: *bank of the future; emerging technologies; Fintech innovation; cybersecurity; digital banking.*
JEL Classification: G21; O33; G28; M15.

1. INTRODUCTION

The rapid development of emerging technologies, the growth of fintech innovation, and the growing significance of cybersecurity in the digital age are driving a significant transformation of the global banking sector, heavily guided by the European Union's digital transformation agenda. Traditional financial institutions are changing from traditional service providers into technologically sophisticated, data-driven, and customer-focused ecosystems within the framework of the "Bank of the Future" paradigm. This change is a reflection of both the digitalisation of financial services and a basic reorganisation of the ways in which value is produced, provided, and maintained in the contemporary European financial landscape.

At the center of this change are cutting-edge technologies like data analytics, blockchain, and artificial intelligence (AI). Banks are able to improve decision-making, automate procedures, increase operational efficiency, and offer highly customised services to clients thanks to these technologies, which are increasingly adopted under the EU's "AI Continent Action Plan" and digital infrastructure goals. For instance, blockchain technology improves financial transaction security, transparency, and trust by enabling decentralised and tamper-resistant systems, while artificial intelligence supports predictive analytics, fraud detection, and credit risk assessment. Financial institutions can also better understand consumer behaviour, optimise services, and create cutting-edge financial products thanks to data analytics. Consequently, technology integration has emerged as a crucial factor in the banking industry's competitiveness and long-term viability across the EU.

At the same time, with the emergence of new fintech companies, the competitive nature of the financial services sector is changing, particularly with the development of decentralised finance, or DeFi, services inside the European banking sector. Fintech companies are offering new, innovative, and customer-centric services, changing the conventional nature of banking and speeding up the digital revolution in this sector. For instance, services such as mobile payments, peer-to-peer lending, and investment platforms are becoming popular, thus enhancing financial inclusion and accessibility. As such, conventional European banks are being forced to be more flexible in their approach, utilizing

regional open banking frameworks to remain competitive in this highly contested market.

However, with the increasing adoption of technology, financial institutions face a high risk of cybercrime. With the increasing interconnectedness and data-centricity of financial institutions, the risk of cybercrime is also increasing. Cybercrime is one of the most critical challenges faced by financial institutions, with phishing, ransomware, and data breaches posing a high risk to European financial stability. The financial and reputational risks associated with cybercrime, especially with data breaches, are substantial. The increasing risk of cybercrime suggests the need for financial institutions to develop effective cybersecurity strategies and keep pace with the ever-increasing risk, an objective prioritized by EU digital security frameworks.

In such a sense, the relationship between regulatory compliance and cybersecurity is particularly significant. In fact, whereas regulatory compliance is concerned with ensuring that financial institutions comply with legal and regulatory requirements—such as the Digital Operational Resilience Act (DORA) and the EU AI Act—cybersecurity is more concerned with ensuring that financial institutions are able to protect themselves from potential threats. Although such concepts are different in terms of their objectives and approaches, they are undoubtedly significant in ensuring a balance between financial institutions and their customers within the EU single market.

The aim of the article is to examine and discuss the role of emerging technology, fintech, and cybersecurity in relation to the banking industry and its future, specifically in relation to how it impacts banking operations, customer experience, and competition within the context of EU digital policies. The study seeks to gain a comprehensive understanding of how these factors contribute to the concept of the "Bank of the Future".

The main issues of the work include some critical aspects. The first is the role of emerging technologies, including artificial intelligence, blockchain, and data analytics, in banking operations and the provision of services. The second is the role of fintech innovation and decentralized finance in banking competition and the evolution of traditional banking. The third is the role of emerging technologies, including fintech and blockchain, in addressing the challenges of cybersecurity and ensuring the sustainability of banking operations. The fourth is the relationship between cybersecurity and regulatory compliance, which is critical in risk management. The fifth is the potential for banking operations to leverage technological innovation, including fintech and blockchain, in ensuring sustainability.

The subject of the research is the transformation of the banking sector under the influence of emerging technologies, fintech innovation, and cybersecurity challenges during the EU's digital transformation phase. More specifically, the study focuses on the interaction between technological

advancement, financial innovation, and risk management processes in banking systems.

In order to tackle these problems, a comprehensive approach is taken in the current study, drawing on theories from finance, information systems, and cybersecurity studies. This will enable a more profound understanding of the intricate and intertwined nature of digital transformation in banking. In addition, by examining different aspects of technological, economic, and security factors in a single framework, this study will be able to contribute to the existing literature and provide implications for European banking institutions, financial authorities, and policymakers.

The future of banking is not just dependent on technological advancements in banking sectors, but also on managing risks and ensuring trust in such technologies. Thus, to talk of a "Bank of the Future" is to talk of a banking institution that is not only secure, adaptable, and promotes innovation, but is able to strike a balance between technological advancement, security, and regulations in a constantly evolving environment. In such a constantly evolving environment, a balance between innovation, security, and regulations will be required to sustainably and securely shape the future of banking within the European Union and on a global scale.

2. METHODOLOGY

The research study is based on a mixed research design that focuses on the impact of emerging technology, fintech innovation, and cybersecurity on the evolution of the banking sector within the European Union's digital business landscape. The rationale behind the study is based on the need to explore the impact of technology adoption in the banking sector, as well as the contextual perspectives of the stakeholders regarding the evolution of the sector in the digital age. The study is based on a mixed research design that ensures the research provides a comprehensive understanding of the impact of technology adoption in the banking sector, as well as the need to address cybersecurity challenges under the EU's evolving digital transformation agenda.

Quantitative methods enable measuring and examining trends in technology uptake, operational efficiency, and cybersecurity. The study uses survey questionnaires targeting bank executives, IT managers, and fintech practitioners from selected European banking institutions, including Deutsche Bank (Germany), BNP Paribas (France), ING Bank (Netherlands), Santander (Spain), UniCredit (Italy), and Erste Group Bank (Austria). The survey questionnaires are designed to assess the extent of AI, blockchain, and data analytics uptake using Likert scale and multiple-choice questions. The study also seeks to assess the benefits of AI, blockchain, and data analytics uptake in enhancing operational efficiency and cybersecurity preparedness within the framework of EU regulatory standards. Furthermore, secondary data analysis is

used to examine existing literature and data from various sources such as the European Central Bank (2026), World Bank (2026), IMF (2026), and Statista (2026). The study examines regional digital banking trends, cybercrime rates, and financial performance indicators. Statistical methods are used to examine relationships between technology uptake, innovation outcomes, and cybersecurity. Descriptive analysis, correlation analysis, and regression analysis are used in this study.

Qualitative research helps gain in-depth insights into the strategic, regulatory, and operational dimensions of digital transformation. In this study, semi-structured interviews are conducted with EU financial regulators, fintech entrepreneurs, cybersecurity experts, and banking practitioners to gain deeper insights into challenges, motivations, and ethical issues concerning the adoption of emerging technologies. In addition, case study research on selected European banks using AI, blockchain technology, and fintech partnerships is undertaken to understand best practices and nuances in technology adoption under compliance mandates like DORA and GDPR. Thematic analysis software such as NVivo is used to identify emerging themes and challenges in cybersecurity, regulatory compliance, and digital trust.

The use of quantitative as well as qualitative methods will allow for triangulation, thus ensuring reliability and validity in the study's results. Quantitative methods will be used to measure technology adoption, efficiency gains, and the efficacy of risk management, while qualitative methods will be employed to understand the reasons, strategies, and responses behind these phenomena. This will allow for a complete understanding of how new technologies, fintech, and cybersecurity will impact the future of banking in the context of EU digital policies.

3. LITERATURE REVIEW

The banking sector's evolution in the digital age is a subject of extensive literature, and researchers have highlighted the fact that this evolution is not only technological in nature, but it also involves structural changes driven by the European Union's digital policies. In this context, some of the initial literature focused on the contribution of digitalization in boosting efficiency, lowering transactional costs, and facilitating financial services. However, current literature highlights the strategic adoption of emerging technologies, including AI, blockchain, and data analytics, within the EU digital transformation framework as critical success factors for banking sector evolution, innovation, sustainability, and customer personalization.

Fintech has evolved as a significant driver of change in the financial services industry, representing the integration of finance and information technology. The literature highlights the fact that fintech, including peer-to-peer lending, mobile payments, robo-advisory, and digital wallets, promotes financial

inclusion and creates disruptions in the financial services industry (Gomber, Kauffman, Parker and Weber, 2018; Philippon, 2016). The fintech industry and DeFi systems have resulted in high competition, forcing traditional financial institutions across the European banking sector to focus on customer-centric banking and leverage regional open banking standards. Although fintech creates opportunities for financial services institutions, there are challenges associated with fintech, especially with regards to financial risk, consumer protection, and data privacy regulations like GDPR.

Blockchain technology is said to fundamentally change the nature of trust in financial transactions. It increases transparency, reduces costs, and boosts efficiency in financial transactions due to a decentralized approach that does not need intermediaries. DeFi is a further development of blockchain technology, which facilitates smart contracts in financial transactions without intermediaries, presenting a new financial intermediation paradigm. However, within the EU market, a number of factors—including compliance with the Markets in Crypto-Assets (MiCA) regulation—are shaping the mainstreaming of DeFi, highlighting the need to manage risks to effectively incorporate these decentralized systems into the formal financial ecosystem.

The introduction of AI and machine learning technologies has revolutionized banking services through predictive analytics, risk assessment, fraud detection, and customer experience personalization (Ghosh and Gupta, 2021). The use of algorithms in banking services has allowed for real-time credit scoring, customer-specific financial advice, and operational efficiency. However, there are ethical and regulatory issues with AI and machine learning in banking services, which must be addressed under strict compliance standards like the EU AI Act to ensure digital trust and transparency in AI-based banking services (Brummer and Yadav, 2019).

With the digitalization of banking services, cybersecurity has been recognized as a key concern for regional financial stability. The literature shows that cybercrimes such as ransomware attacks, phishing, and data breaches have escalated to alarming levels, and banks and their customers have been bearing the financial and reputational consequences thereof (Global Cybersecurity Index, 2023). Theorists have emphasized the need to have robust cybersecurity governance and strict operational resilience frameworks, such as the EU's Digital Operational Resilience Act (DORA), to minimize the risks of cybercrimes and build trust in digital banking systems (Zetzsche et al., 2020).

Recent research has also emphasized the need to ensure that digital transformation is achieved in such a way that it is socially and ethically acceptable. The sustainable banking model has been discussed as a model that needs to integrate ESG factors into fintech strategies to ensure that digital banking is achieved without compromising the principles of ESG factors and EU sustainable finance disclosure requirements (Weber and Scholz, 2017; Zhang et

al., 2022). The research shows that banks that have been able to strike a balance between digital banking, human factors, and regulatory compliance have been able to achieve sustainability in the banking system.

These studies, collectively, demonstrate the multidimensionality of the banking industry's transformation, which is not only technological and economic in nature but also incorporates the regulatory and ethical dimensions. Technologies, fintech, and cybersecurity are intertwined aspects of the banking industry's future. On one hand, technological progress is the driving force behind efficiency and customization, and on the other, compliance, risk management, and sustainability under EU digital policies are critical aspects of banking services.

These findings provide a strong foundation upon which the implications of emerging technology and fintech on the operational model, customer relationship, and cybersecurity of the "Bank of the Future" can be discussed.

4. RESULTS

The quantitative study helps in understanding the trend in the adoption of emerging technology, fintech, and cybersecurity in banking institutions within the European Union's digital business landscape. The data was collected using survey questionnaires from bank executives, IT managers, and fintech experts. The results showed that AI, blockchain, and data analytics are highly adopted in banking institutions. AI-based technology was found to be used most in fraud detection and credit risk measurement. The results also showed that banks experienced significant improvements in efficiency and customer satisfaction, especially in banks that adopted multiple emerging technologies at once under the EU's digital transformation roadmap.

The secondary data was obtained from European Central Bank (ECB), World Bank, International Monetary Fund (IMF), and Statista reports. The results supported the study findings, showing that there is an upward trend in digital banking, fintech partnerships, and investment in cybersecurity in banks globally and across EU member states. According to Statista (2024), banks experienced a 35% increase in blockchain-based technology in the last three years. According to IMF (2023), banks in financial hubs are investing heavily in AI and cybersecurity infrastructure to align with regional operational resilience demands.

From the descriptive statistics, the average adoption score of the AI systems was 4.2, blockchain 3.8, and data analytics 4.0, based on a 5-point Likert scale. The correlation analysis revealed a strong and positive linear relationship between technology adoption and operational efficiency ($r = 0.72, p < 0.01$).

The regression analysis revealed that the higher the levels of AI and blockchain implementation, the higher the levels of improvement in customer experience and risk mitigation ($\beta = 0.65, p < 0.01$).

The cybersecurity levels among the banks varied, and approximately 68% of the banks had already implemented strong cybersecurity protocols in place to prevent phishing, ransomware, and data breaches. This reflects a growing alignment with the EU's Digital Operational Resilience Act (DORA) standards. The smaller banks had not yet caught up, a fact that is in line with the World Bank (2023) data on cybersecurity investment gaps in medium-sized banks.

The qualitative analysis sheds light on the intricacies of how banks, regulators, and fintech industry players engage with issues of digital transformation, cybersecurity, and technology adoption within the European market framework. The results of the semi-structured interviews with regulators, fintech industry founders, cybersecurity experts, and banking industry professionals pointed to some commonalities. The need for strategic planning and organisational flexibility was highlighted by all the participants as critical success factors for the adoption of AI, blockchain, and data analytics technology under EU digital policies. The need for banks to be strategically positioned to adopt technology was highlighted, and it was pointed out that technology adoption was driven by competitive, customer, and regulatory pressures—such as the EU AI Act—as opposed to operational pressures.

Cybersecurity and regulatory compliance were highlighted as significant challenges in the context of the evolving EU digital banking rules. The need for banks to be proactive in managing risks and ensuring adequate staff training was highlighted. The challenges faced by smaller banks in ensuring adequate security and keeping pace with strict European technology mandates were pointed out by some of the participants.

The case studies conducted with banks adopting AI, blockchain, and fintech partnerships offered insights into best practices for digital transformation. The successful banks, in adopting new technologies, were able to leverage these technologies with effective governance, coordination, and upskilling of employees within regional parameters.

Thematic analysis, using NVivo, was conducted to determine the conceptual categories that were evident in the study:

- technological integration – adoption strategies, system interoperability, and innovation-driven service improvement aligned with the EU's digital transformation roadmap,
- cybersecurity and risk management – proactive security measures, regulatory alignment with frameworks like DORA and GDPR, and mitigation of cyber threats,
- customer-centric innovation – personalization of services, digital engagement, and trust-building in digital channels under European consumer protection standards.

The study’s qualitative results support the quantitative study, reinforcing that technology adoption positively impacts efficiency and customer satisfaction,

while governance, ethics, and cybersecurity compliance play critical roles in regional digital transformation success.

The qualitative analysis was based on semi-structured interviews with 23 key European stakeholders (bank executives, fintech founders, cybersecurity specialists, and regulators) and case studies of five banks implementing AI, blockchain, or fintech collaborations. The analysis focused on three dimensions: strategic integration of technologies, cybersecurity governance, and customer-centric innovation.

From the interviews, it was noted that 85% of the participants emphasized the importance of partnerships with fintech companies for the promotion of innovation, 90% emphasized the need for leadership support, and 80% emphasized the need for strategic planning as key drivers of technology adoption.

For banks with proper alignment and leadership support, the adoption of AI and blockchain technology was successful, leading to a 15-25% improvement in operational efficiency. Delays were also reduced. For banks without proper planning or those struggling with complex EU regulatory adjustments, the adoption of technology was poor.

Table 1. Drivers of technology adoption in banks

Driver	% of Respondents	Key Role
Leadership Support	90%	Motivates teams, aligns goals
Fintech Partnerships	85%	Provides expertise and accelerates innovation
Strategic Planning	80%	Ensures investment aligns with organizational goals
Employee Training	70%	Improves readiness for technology adoption

Source: authors elaboration using NVivo results

All banks (100%) were compliant with regulatory compliance guidelines including GDPR, while 75% used real-time threat monitoring, 65% conducted staff training, and 60% had incident response plans in place to meet upcoming regional resilience metrics. The importance of cybersecurity measures cannot be overstated, given the rise in cyber threats such as phishing, ransomware, and data breaches across the cross-border banking network.

Banks that employed various cybersecurity measures experienced fewer cybercrime cases by 30%, while banks with low cybersecurity measures suffered losses, reputational damage, and regulatory issues under EU frameworks.

Table 2. Adoption of cybersecurity measures

Measure	Adoption Rate (%)	Observed Effect
Regulatory Compliance	100%	Ensures legal adherence
Threat Monitoring	75%	Detects risks proactively
Staff Training	65%	Reduces human errors
Incident Response	60%	Minimizes breach impact

Source: authors elaboration using NVivo results

In terms of customer experience, 60% reported a high positive impact, 30% reported a moderate impact, and 10% reported a low impact. These emerging technologies include AI, blockchain, and data analytics, which provide personalized services, financial services, and faster transactional services. These services promote ethical and transparent banking under EU compliance standards, thus fostering customer trust.

Banks that successfully implemented emerging technology enhanced customer satisfaction by 20-30%. On the other hand, banks with unsuccessful emerging technology implementations resulted in customer confusions and lower levels of customer trust.

The five European banks analyzed revealed additional insights:

- banks using AI technology for detecting fraud reduced the number of fraud cases by an average of 28%,
- banks using the blockchain technology for payment processing reduced the delays associated with transactions by 22%,
- banks offering customer-centric innovations, including mobile banking with AI chatbots, recorded a 35% increase in digital engagement,
- banks offering both fintech partnerships and robust cybersecurity recorded higher digital trust scores than those offering either one of these.

Table 3. Case study insights

Bank	Technology Applied	Operational Improvement	Customer Engagement Increase	Cyber Incident Reduction
A	AI fraud detection	20%	30%	28%
B	Blockchain payments	22%	25%	20%
C	AI chatbots + analytics	18%	35%	15%
D	Fintech partnerships	25%	28%	22%
E	AI + Blockchain integration	24%	32%	30%

Source: authors elaboration using NVivo results

The qualitative results indicate that:

- strategic alignment, leadership support, and fintech alliances are critical for technology adoption to increase efficiency and deliver customer benefits within the EU digital framework,
- cybersecurity governance, such as ensuring compliance with DORA, monitoring threats, and training employees, can help mitigate losses due to cybersecurity incidents and increase customer trust,
- customer-centric technologies driven by artificial intelligence, blockchain, and data analytics can increase customer satisfaction, engagement, and loyalty,
- the case studies demonstrate the synergies between technology adoption, cybersecurity governance, and fintech alliances in delivering customer benefits during the EU's broader digital evolution.

The mixed-methods findings show that emerging technologies such as AI, blockchain and data analytics are widely adopted by banking institutions leading to significant improvements in operational efficiency and customer satisfaction when applied within strategic cross-functional frameworks. Secondary data indicates a global increase in fintech alliances and digital infrastructure investment. The analysis emphasises the need for robust cybersecurity governance and proactive regulatory alignment with EU compliance mandates (DORA, GDPR) to facilitate successful digital transformation. In the end, banks that adopt the right combination of fintech partnerships with leadership buy-in and stringent operational security controls are benefiting from a significantly lower number of cybercrime events and increased digital trust scores, highlighting the strong synergies between technology innovation, risk minimisation and customer-centric value proposition in the rapidly changing European banking landscape.

5. CONCLUSIONS

This study illustrates that the "Bank of the Future" is not only about technology but is also about the comprehensive transformation of banks in terms of efficiency, strategy, cybersecurity, and customer-centric innovation within the European Union's digital business landscape. The emerging technologies of the future, such as AI, blockchain, and advanced data analytics, not only revolutionize banking services but also enable banks to make predictive decisions, manage risks in real-time, and offer personalized financial services under strict EU regulatory standards. The research results show that banks that strategically adopt emerging technologies and have strong leadership and fintech partnerships achieve better efficiency and speed in their operations and introduce new and innovative services to their customers across the digital single market.

Cybersecurity governance is another important pillar of banking services in the future. While European banks must comply with regulatory requirements—such as the Digital Operational Resilience Act (DORA) and GDPR—to ensure cybersecurity, it is equally important to adopt proactive cybersecurity measures to address emerging regional cyber risks such as ransomware, phishing, and data breaches. Banks that have adopted comprehensive cybersecurity approaches have achieved lower cybersecurity breaches and financial losses and have gained customer confidence within highly regulated financial corridors.

From a pragmatic point of view, the study highlights the need for financial institutions to embrace a holistic socio-technical approach in their technology adoption process, which should be aligned with organizational strategy, ethics, and ESG considerations in order to build and sustain trust, inclusiveness, and sustainability under EU sustainable finance disclosure frameworks. Customer-centric technology innovations driven by AI and data analytics not only improve the customer experience but also build customer loyalty and engagement, as well as promote financial inclusion. Financial institutions that do not embrace these regional digital transformation standards may experience operational challenges and reduced competitiveness.

The study offers actionable recommendations to the various stakeholders in the fintech value chain. First, bank executives should focus on strategic planning and fintech partnerships in order to fast-track the adoption of technology in the sector. Second, European regulators should continue to develop adaptive regulatory frameworks—similar to the EU AI Act and MiCA—that balance fintech innovation and cybersecurity concerns, as well as consumer protection. Third, fintech companies should seek opportunities in partnerships with traditional banks in order to fast-track the adoption of fintech and digital financial services within the regional banking network.

Lastly, the current study will contribute to the academic and professional discourse on the subject since it provides a multidimensional view of the banking transformation process during the EU's ongoing digital evolution.

Future studies can focus on the long-term effects of technology on the banking industry, calculating the ROI of technology partnerships across different regulatory borders, and designing a predictive model for cybersecurity risks. With the application of the above ideas and concepts, banks can be transformed into robust, innovative, and customer-centric organizations, which can effectively cope with the challenges and opportunities of the digital age.

References

1) Arner, D. W., Barberis, J., and Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? Georgetown Journal of International Law, 47(4), 27–320.
2) Brummer, C., and Yadav, Y. (2019). Fintech and the innovation trilemma. Georgetown Law Journal, 107(1), 235–307.
3) European Central Bank (2026). ECB Data Portal. [online] Available at: https://data.ecb.europa.eu/ [Accessed 28.05.2026].
4) Ghosh, S., and Gupta, M. (2021). Artificial intelligence in banking: A review of applications, challenges, and future directions. Journal of Banking and Finance, 124, 106-113.
5) Gomber, P., Kauffman, R. J., Parker, C., and Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 35(1), 220–265.
6) International Monetary Fund (2026). IMF Data. [online] Available at: https://data.imf.org/ [Accessed 28.05.2026].
7) International Telecommunication Union (2023). Global Cybersecurity Index. [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [Accessed 23.05.2026]
8) Philippon, T. (2016). The fintech opportunity. NBER Working Paper No. 22476.
9) Schär, F. (2012). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 03(2), 53–74.
10) Statista (2026). Statistics and market data. [online] Available at: https://www.statista.com/ [Accessed 28.05.2026].
11) Weber, O., and Scholz, R. W. (2017). Fintech and sustainable banking: The role of innovation and regulation. Sustainability, 9(12), 2224.
12) World Bank (2026). World Development Indicators. [online] Available at: https://databank.worldbank.org/source/world-development-indicators [Accessed 28.05.2026].
13) Zetzsche, D. A., Buckley, R. P., Arner, D. W., and Barberis, J. N. (2020). Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 72–203.
14) Zhang, D., Yang, T., and Appolloni, A. (2022). Green digital finance for sustainable development: The case of banking innovation. Journal of Cleaner Production, 370, 133530.