DOI: 10.55643/fcaptp.2.67.2026.5170

BLOCKCHAIN PRINCIPLES' INTEGRATION INTO THE PAYMENT SECURITY ARCHITECTURE OF THE FINANCIAL SYSTEM

Victoria Kovalenko
D.Sc. in Economics, Professor of the Department of Banking, Odesa National Economic University, Odesa, Ukraine;
e-mail: kovalenko-6868@ukr.net
ORCID: 0000-0003-2783-186X
(Corresponding author)

Sergii Sheludko
Candidate of Economic Sciences, Associate Professor, Head of the Analytical and Methodological Support Unit, Pivdenny Bank PJSC, Odesa, Ukraine;
ORCID: 0000-0003-0636-4940

Oleksandr Bezkrovnyi
Candidate of Economic Sciences, Academician, Professor of the Department of Finance, Economic Research and Tourism, Poltava State Agrarian University, Poltava, Ukraine;
ORCID: 0000-0003-1939-8090

Olga Doroshenko
Candidate of Economic Sciences, Associate Professor of the Department of Finance, Banking and Insurance, Poltava State Agrarian University, Poltava, Ukraine;
ORCID: 0000-0003-1163-8635

Andrii Doroshenko
Candidate of Economic Sciences, Associate Professor of the Department of Finance, Banking and Insurance, Poltava State Agrarian University, Poltava, Ukraine;
ORCID: 0000-0002-6314-1586

Vadym Borsa
PhD in Economics, the Department of Finance, Odesa National Economic University, Odesa, Ukraine;
ORCID: 0000-0002-2436-7945

Received: 02/02/2026
Accepted: 01/04/2026
Published: 30/04/2026

ABSTRACT

The relevance of this study is driven by the rapid digitalisation of payment systems and the growing exposure of the financial system to cyber, operational, and AML/CFT-related risks, intensified by the expansion of non-cash transactions, the proliferation of crypto-assets, and the increasing involvement of state and non-state actors in illicit financial activities. These processes exacerbate vulnerabilities in payment security, particularly under conditions of geopolitical instability and hybrid threats. The aim of the study is to theoretically and empirically substantiate the principles of integrating blockchain technology into the architecture of payment security and the AML/CFT framework in order to mitigate emerging risks. The research methodology is based on a combination of systemic and descriptive analysis, systematisation and generalisation, statistical analysis, and economic-mathematical modelling. An autoregressive distributed lag (ARDL) model is employed to assess the impact of regulatory enforcement measures on banks' due diligence in ensuring payment legitimacy, using data from the Ukrainian banking sector. The results demonstrate that payment security is closely dependent on the effectiveness of financial monitoring and regulatory oversight, with enforcement measures exerting a statistically significant short- and long-term effect on the intensity of suspicious transaction reporting. The study establishes that blockchain technology possesses substantial potential to enhance payment security by improving transaction transparency, strengthening AML/CFT controls, and increasing resilience to cyber threats, including those associated with the illicit use of crypto-assets. It is substantiated that the harmonisation of blockchain-based solutions with regulatory principles is a necessary condition for maintaining financial stability in an environment of accelerating digitalisation. Based on the findings, practical recommendations are formulated for integrating blockchain technology into payment security and financial monitoring systems, which may be of relevance for regulators, financial institutions, and policy-makers concerned with strengthening economic and payment security.

Keywords: blockchain, payment security, cryptocurrency, AML/CFT, digital transactions, KYC, RegTech

JEL Classification: G21, O33, E42

INTRODUCTION

The modern financial ecosystem relies on a secure, structured payment system, transforming as digital transactions replace cash. Regulatory support and innovations like open finance and instant payments drive this shift. Rapidly evolving payment systems in the digital economy enhance infrastructure, introduce new instruments, and boost markets, economies, competitiveness, employment, and living standards. However, even top-tier systems face risks from cyberattacks, fraud, and the integration of financial innovations.

It can be stated that the operation of payment systems belongs to a high-risk domain. This is due to the extensive network of connections among participants, the volume and size of transactions processed, the high mobility and speed of settlements, and the rapid advancement of technologies. Additionally, the development of remote banking services further amplifies the potential for disruptions in payment processes, which can immediately trigger severe negative consequences for the entire payment system. Given these

factors, the issue of ensuring payment security within the financial system becomes increasingly urgent. Experts from Asseco South Eastern Europe Group (ASSE) have identified five key trends in payment security within the banking sector for 2025 (ASSE, 2025): acceleration of digital innovation; integration of artificial intelligence (AI) and automation into cybersecurity systems; imperatives of cloud security adaptation to regulatory transformations; and control of third-party risks.

The issue of payment security is further exacerbated by the fact that a comprehensive system of risks associated with payment systems has emerged to date, both at the global and national levels. The identified risks include legal risk, financial risks (credit, investment, and liquidity risks), settlement risk, operational risk, cyber risk, and systemic risk. Additionally, the list encompasses risks related to the laundering of criminal proceeds, the financing of terrorism, and the proliferation of weapons of mass destruction (AML/CFT). The emergence of AML/CFT risks is closely linked to the effectiveness of the financial monitoring system established within a country. The efficiency of financial monitoring has a direct and proportional impact on payment security, as it focuses on tracking financial transactions associated with fraudulent activities.

Mitigating risks that affect payment security and enhancing the effectiveness of existing financial monitoring systems can be achieved through the adoption of blockchain technology. This technology incorporates built-in mechanisms designed to prevent the unauthorised initiation of transactions and to ensure consistency and integrity in the collective recording of transactional data. Blockchain serves as an effective tool for fraud prevention and plays a critical role in strengthening payment security. Consequently, the growing relevance of blockchain technology necessitates a more in-depth examination of its instruments, functions, and practical applications, as a clear understanding of its role and potential is essential for improving payment security within the financial system.

LITERATURE REVIEW

Addressing the aforementioned issues, it is essential to note that the global scientific community dedicates significant attention to ensuring a high level of payment security and addressing its primary challenge – mitigating AML/CFT risks through the application of blockchain technology.

In this context, M. Cologgi (Cologgi, 2023) highlighted the effectiveness of innovations introduced by the Payment Services Directive (PSD2) in mitigating fraud risks associated with remote transactions. Drawing on data provided by Italian banks for supervisory purposes and employing a panel data model, the author found that Strong Customer Authentication (SCA) reduces fraud risk by 60% for remote card payments and by 80% for electronic money payments. Moreover, transactions exempt from SCA requirements were also found to maintain a high level of security.

In the study by Adil O. Y. Mohamed (Adil, 2023), the potential use of blockchain for securing mobile electronic payments is explored. The research depicts that with cryptographic secured distributed ledger systems, validation of transactions can be made in real time without depending on any intermediary institutions, such as banks or clearing organizations. Blockchain can provide fast, secure, decentralized, and cost-effective transactional services. Its inherent transparency and data security streamline money transfers. The paper proposes a blockchain-based framework for secure mobile payments, highlighting the advantages of this technology and how it ensures multi-level authentication to safeguard mobile financial transactions. Furthermore, security challenges associated with blockchain-based payment applications and potential solutions are examined.

Aburbeian and Fernández-Veiga (2024) designed a security architecture integrating multi-factor authentication with machine-learning techniques for the better protection of online financial operations. In their proposed design, the entire system is based on a two-tier architecture. At the first tier, user identity is verified through a two-factor authentication procedure. The second tier is embedded with an intelligent analytical module that can detect suspicious activity, serving as an internal fraud-detection mechanism. At this stage, face recognition is one crucial factor in the authentication process, providing extra security. The primary contribution of this study lies in the methodological integration of machine learning into the authentication architecture as a native component rather than an addition. This kind of structure tries to balance security, usability, and operational efficiency while being responsive to the functional features of different e-commerce environments. Since the financial ecosystem is fast changing, according to the authors, continuous investigation regarding authentication variables and training data is necessary to get better, and also to cope with protective measures continuously.

In the context of identifying effective instruments to counter high-technology fraud, Darwish Saad M. et al. (Saad et al., 2026) substantiate the inadequacy of traditional rule-based systems and standard machine-learning models due to their

DOI: 10.55643/fcaptp.2.67.2026.5170

limited scalability and high incidence of Type II errors (false positives). The authors propose an innovative integrated architecture based on the combination of a lightweight blockchain and deep learning. Within this framework, blockchain technology serves as a guarantor of data immutability and decentralised transparency, while neural networks enable adaptive identification of complex anomalous patterns. The adoption of a lightweight blockchain protocol mitigates excessive computational overhead, thereby rendering the system suitable for real-time transaction monitoring, including in mobile environments and resource-constrained Internet of Things (IoT) devices.

A significant group of researchers focusing on the search for tools to ensure payment security emphasizes the readiness of clients to use electronic payment systems and the development of financial inclusion in this context. For instance, D. Mondego and E. Gidep (Mondego, Gidep, 2023) argue that cloud-based payment systems (CBPS) offer clear advantages, but their perceived acceptance – illustrated by Australian users – remains comparatively lower than that of users from other countries. Ordinary citizens are either dissatisfied with current payment methods or unaware of the benefits of CBPS. The authors, using the Technology Acceptance Model (TAM) to predict perceived ease of use and usefulness, applied a qualitative research approach through semi-structured interviews with 20 Australian users. The findings suggest that the respondents placed a high value on safety mechanisms such as two-factor authentication and other sophisticated security technologies. Although the Australian consumer has a high level of confidence in banking institutions, education level and the fact that they have to pay an extra fee for digital payment services results in a state of ambivalence. In the context of the environment of the CBPS, electronic devices were identified as being user-friendly and having a level of functional benefits. According to the findings, the service provider also has to build on the security infrastructure, ensuring that they have the latest technologies that have the purpose of ensuring the safety of the information of the individual, as well as dealing with cases of fraud. Based on the overall findings of the research, the Australian banking service appears to have a high level of positivity.

Using data from Brunei, H. Susanto et al. (Susanto et al., 2024) analyzed the level of acceptance of a cashless economy. Against the backdrop of the COVID-19 crisis, the authors characterized the factors influencing the willingness to adopt noncash payments among the working population in Brunei. They employed integrated concepts from the Technology Acceptance Model (TAM) and the Technology Readiness Index (TRI). Based on a quantitative approach using an online survey to collect non-random responses from 212 participants, the study revealed that factors such as payment method evaluation, technological development, digital literacy, awareness, regulatory policies, and security concerns significantly impact the readiness of society to embrace a cashless economy.

Regarding the role of financial inclusion in ensuring payment security, the study by S. Tsai et al. (Tsai et al, 2022) is particularly noteworthy. The article identifies factors influencing consumers' willingness to adopt mobile payments. The research demonstrated that consumers' awareness of ease of use and perceived usefulness significantly positively influences their perception of mobile payments. Moreover, empirical research on the mediating effect of transaction security on usage and the intention to adopt mobile payments revealed that secure transactions can positively impact users' behavior regarding the use of mobile payment services. This also explains why the penetration of mobile payments is lower in developed countries compared to developing ones. To encourage users to quickly adopt new mobile payment tools, it is essential to make these tools user-friendly and ensure transaction security (Tsai et al., 2022).

In reviewing the literature, attention should be paid to the use of blockchain technology in financial monitoring systems, which serves as a primary lever for ensuring payment security. The article by A. Thommandru and B. Chakka (Thommandru, Chakka, 2023) focuses on compliance and AML (Anti-Money Laundering) policies in the banking sector through the application of emerging technologies such as blockchain. The study demonstrates that blockchain is an ideal platform for decision-making in user identification and verification, providing a process that is simple, secure, and reliable, while also enhancing the overall user experience and ensuring regulatory compliance. For users who are not yet engaged with blockchain, this can be further developed to create a universal solution within the "Know Your Customer" (KYC) system, which could replace the manual execution of this process.

V. Buterin et al. (Buterin et al., 2024) explored the use of Privacy Pools, an innovative protocol based on smart contracts aimed at enhancing privacy. The protocol allows for the implementation of a system in which the participants will be able to attest to specific characteristics of the transaction while the underlying information in the transaction remains concealed. The fundamental idea behind the protocol is the publication of a zero-knowledge proof in which the linking of the funds controlled by the user to specific illicit sources will be disallowed while remaining anonymous. The paper focuses on the technical system, the incentives, and implications of the protocol, emphasizing the potential for Privacy Pool–type protocols in accommodating the activities in the blockchain while respecting the privacy of the users and adhering to the regulatory environment.

H. Ahmad and G.S. Aujla (Ahmad, Aujla, 2023) highlight in their work that the General Data Protection Regulation (GDPR) aims to give users greater control over their personal data. In the last few years, solutions in the blockchain-oriented technology domain have reportedly emerged with considerable interest in the role they can play in solving the problem of proof of GDPR compliance in multi-functional complex systems. The utilization of smart contracts on distributed ledger platforms reportedly allows for the production of transparent and tamper-proof records of data processing activities in a way that can be automated to verify GDPR compliance. The authors propose a scenario for a cloud-based e-commerce application, focused on a user-oriented blockchain framework for data management in the cloud environment. In this scenario, all data operations related to GDPR are executed on the blockchain through clearly defined smart contracts hosted on the Ethereum network.

A. Miglionico's (Miglionico, 2022) scientific work deserves particular attention, as it emphasizes that the scope of traditional banking functions, such as lending, deposit acceptance, and payment intermediation, is being supplemented by new ones, which encompass virtual currencies, crypto-assets, shadow payments, and quasi-money. The possibilities for technological change in the financial industry can be seen, for instance, in distributed ledger procedures, where blockchain is a particularly prominent technology tied to decisions with automated processes. The author highlights that new developments in financial services, for instance, with respect to cryptographic protection, large data sets, distributed computing, as well as new software-based infrastructure like crowdfunding, cryptocurrencies, or blockchain-based systems, require ongoing communication between financial market players and regulatory agencies with respect to ensuring their sound institutional and technical foundation.

Thus, the future of payment security lies in the plane of hybrid systems that combine structural reliability (blockchain) and intelligent flexibility (AI).

AIMS AND OBJECTIVES

The aim of the study is to provide a theoretical and empirical substantiation of the principles for integrating blockchain technology into the architecture of payment security within the financial system and the AML/CFT framework, with a focus on mitigating emerging cyber, financial, and geopolitical risks under conditions of accelerated digitalisation and hybrid threats. The research objectives consist of analysing key risks to payment security in the context of digitalisation and AML/CFT challenges; assessing the effectiveness of financial monitoring and regulatory enforcement in ensuring payment legitimacy; and substantiating the role of blockchain technology in enhancing payment security and strengthening the AML/CFT framework.

METHODS

This study uses a diverse methodology to explore blockchain integration into payment security, including a review of payment trends and blockchain adoption potential. Economic-mathematical modeling, statistical analysis, and expert evaluations assess the link between payment systems and financial monitoring for effective blockchain use. Systemic and descriptive analyses highlight blockchain's value in security, while specification, systematization, and generalization pinpoint key integration directions.

Based on the most pressing and relevant issues highlighted and episodically addressed in previous publications, the design of this study follows a structured sequence of steps (Figure 1).

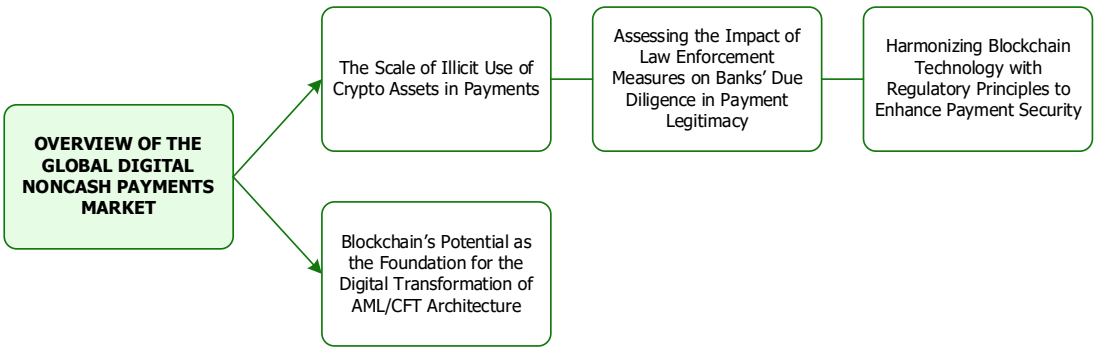


Figure 1. Design of the research on blockchain principles' integration into the payment security architecture of the financial system.

DOI: 10.55643/fcaptp.2.67.2026.5170

In addition to qualitative research methods, such as literature review, descriptive statistics, and legislative-regulatory analysis, this study employs mathematical modeling tools to assess the impact of law enforcement measures on banks' due diligence in payment legitimacy. A review of similar studies indicates that the effectiveness and efficiency of a country's financial monitoring system, AML/CFT measures, and banking payment compliance are typically evaluated using expert-based methods (e.g., surveys, discussion panels, stakeholder interviews). This methodological preference is largely due to the traditional lack of quantitative data on financial monitoring operations – whether due to restricted access to such information or the irregularity and limitations of official statistical reporting. In this study, however, a small yet fully representative dataset of raw information was compiled through manual data collection from non-statistical sections of the official websites of the National Bank of Ukraine and the State Financial Monitoring Service of Ukraine.

The autoregressive distributed lag (ARDL) model is an ordinary least squares-based econometric approach that is particularly advantageous for analyzing both non-stationary time series and datasets with a mixed order of integration. Unlike traditional cointegration methods, the ARDL framework accommodates variables integrated at different levels, making it a robust tool for empirical research. This model employs a sufficiently large number of lags to effectively capture the underlying data-generating process, following a general-to-specific modeling strategy.

To demonstrate the ARDL modeling technique, consider the following simplified equation:

$$y_t = \alpha + \beta x_t + \delta z_t + e_t \quad (1)$$

A key advantage of the ARDL model is that it naturally leads to the derivation of a dynamic error correction model (ECM) through a straightforward linear transformation. The ECM formulation seamlessly integrates short-run dynamics with long-run equilibrium properties, ensuring that valuable long-term relationships within the data are preserved. This transformation also mitigates potential econometric issues, such as spurious regression, which can arise from non-stationary time series. The ECM representation of the ARDL model is expressed as follows:

$$\Delta y_t = \alpha_0 + \sum_{i=1}^{p} \beta_i \Delta y_{t-i} + \sum_{i=1}^{p} \delta_i \Delta x_{t-i} + \sum_{i=1}^{p} \varepsilon_i \Delta z_{t-i} + \lambda_1 y_{t-1} + \lambda_2 x_{t-1} + \lambda_3 z_{t-1} + u_t \quad (2)$$

The equation can be conceptually divided into two distinct components, each representing different aspects of the model's dynamics. The first part, which includes the parameters β, δ, and ε, captures the short-run dynamics by reflecting the immediate effects of changes in the explanatory variables on the dependent variable over a limited time horizon. This section of the equation is crucial for understanding how temporary fluctuations in the independent variables influence the system within the short term.

In contrast, the second part of the equation, characterized by the λ coefficients, represents the long-run equilibrium relationship between the dependent and independent variables. This segment is fundamental for assessing the persistent or equilibrium effects that manifest once short-term adjustments have stabilized. By estimating these long-run parameters, the model identifies whether a stable and statistically significant relationship exists over time.

A central aspect of the model involves testing the presence of a long-run relationship through a formal hypothesis. The null hypothesis (H_0) is defined as $\lambda_1 + \lambda_2 + \lambda_3 = 0$, which implies the absence of a long-run relationship among the variables. If this hypothesis cannot be rejected, it suggests that no stable equilibrium exists, meaning that any observed correlation between the variables may be purely coincidental or reflective of short-term dynamics rather than a genuine long-term association. Conversely, rejecting the null hypothesis indicates the existence of a cointegrating relationship, implying that the variables share a stable long-term connection despite short-run fluctuations.

This hypothesis testing framework is a critical feature of the ARDL model, as it allows researchers to formally evaluate the existence of cointegration while maintaining the flexibility to accommodate variables integrated at different orders.

Additionally, two useful reparameterizations of the ECM allow for a clear distinction between short-run and long-run effects, facilitating an intuitive interpretation of the estimated coefficients. Another significant feature of the ARDL approach is its ability to test for the presence of a long-run equilibrium relationship through the widely used bounds testing procedure, which is available as a post-estimation diagnostic tool. In the case of non-stationary variables, this test essentially serves as a cointegration check, verifying whether a stable long-run relationship exists. Importantly, the ARDL methodology remains flexible, accommodating both stationary and non-stationary variables, thereby broadening its applicability across a range of empirical contexts.

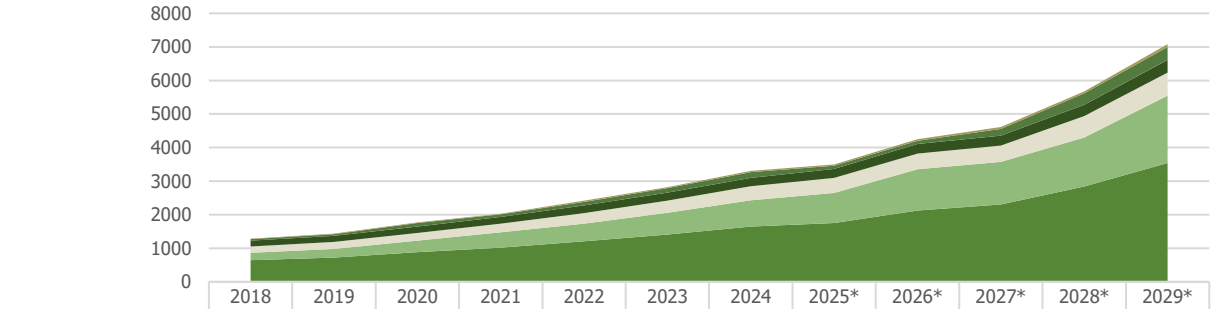
The study draws upon a diverse range of sources, including academic research, books, reports, and other publications related to blockchain technology and payment security. Additionally, information has been sourced from the National Bank

of Ukraine, the State Financial Monitoring Service of Ukraine, the Basel Institute on Governance, and leading industry players such as Capgemini and Chainalysis.

RESULTS

Overview of the Global Digital Noncash Payments Market

The global payment landscape demonstrates an accelerated rate of growth. As evidenced by a retrospective analysis (Figure 2), over the past two decades, the volume of cashless transactions has expanded more than tenfold, confirming the irreversibility of the transition towards digital payment instruments. Notably, during the period 2014–2024, the growth rate of cashless payments exceeded global GDP dynamics by more than 2.5 times, indicating an autonomous digital intensification of the financial sector.



	2018	2019	2020	2021	2022	2023	2024	2025*	2026*	2027*	2028*	2029*
Middle East fnd Africa	16,3	16,3	20,6	24,5	29,8	34,1	39,2	41,1	42,4	56,9	64,5	84,5
Latin America	48,6	48,8	99,8	72,1	109,3	132,9	167,3	95,5	99,3	198,8	340,7	383,1
North America	170,5	180,3	192,4	204,7	227,7	237,4	252,6	260,5	280,8	298,1	338,3	373,4
Europe	187,4	216	226,1	258,6	312,4	361,2	417,3	454,5	468,6	482,2	637,1	692,3
Asia -Pacific	221,8	257,7	346,7	456,4	528,7	645,8	777,5	896,9	1232,3	1269,6	1457,8	2006,9
Global	644,6	719,1	885,6	1016,3	1207,9	1411,4	1652,1	1748,5	2123,4	2305,6	2838,4	3540,3

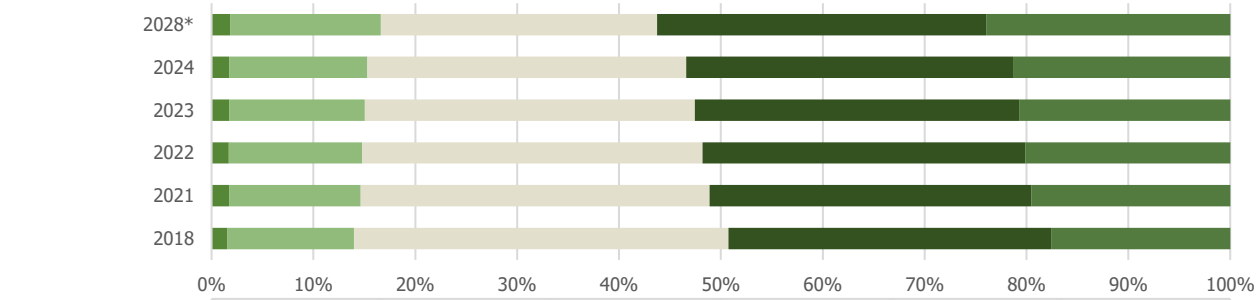
Figure 2. Volume of global non-cash transactions in 2018 – 2029, USD billion. Note: 2025*–2029* represents forecasted. *(Source: prepared on the basis of research by Capgemini (2026))*

According to forecast estimates, the global market for cashless transactions, which reached 1,685 billion transactions in 2024, is expected to demonstrate steady growth by 2029 with a compound annual growth rate (CAGR) of 16%, reaching a volume of 3,540 billion transactions. The regional specificity of this process can be characterised as follows:

- *Asia–Pacific region.* Acts as the global engine of digital transformation, with a projected CAGR of 20.2%. The dominant growth drivers are the scaling of mobile wallet ecosystems and real-time payment solutions.
- *Latin America.* Exhibits high adaptability to mobile financial technologies. The expected growth of 22.4% in 2025 is driven by the active development of digital commerce and the implementation of national real-time payment schemes.
- *Europe.* Despite market maturity, the region maintains positive momentum (CAGR of 10.8% by 2029), stimulated by stringent regulatory pressure and initiatives aimed at implementing open banking standards.
- *North America.* The market is characterised by stable evolutionary development (CAGR of 7.8%). Despite the traditional dominance of card-based products, a systematic displacement of plastic cards by digital wallets and contactless technologies is observed.
- *Middle East and Africa.* The projected growth rate of 13.9% is driven by the active development of government-led digital infrastructure, the integration of digital identity systems, and a high level of mobile penetration among the population.

At the global level, an intensive transformation of B2B payment architectures towards full digitalisation is underway. Business entities, regardless of their scale of operations, are increasingly integrating innovative payment instruments. The key driver of this process is the activity of FinTech and PayTech providers, which offer customised digital services for small and medium-sized enterprises (SMEs), while simultaneously delivering comprehensive solutions for the modernisation of the financial infrastructure of large corporations (Figure 3).

DOI: 10.55643/fcaptp.2.67.2026.5170



	2018	2021	2022	2023	2024	2028*
Middle East fnd Africa	1,7	2,3	2,5	2,8	3,1	5,1
Latin America	13,4	17,3	19,2	21,6	24,4	41,2
North America	39,7	45,8	49	52,5	56,2	75,5
Europe	34,2	42,3	46,5	51,6	57,6	89,9
Asia -Pacific	19	26,1	29,5	33,6	38,3	66,7

Figure 3. B2B volume by global regions, Billion Units. Note: 2028* represents forecasted. *(Source: prepared on the basis of research data by Capgemini (2026))*

The growth dynamics of B2B transactions demonstrate a stable upward trajectory: in 2024, the global volume of payments in this segment increased by 10.8%, while the projected annual growth rate through 2028 is estimated at 11.4%. Regional analysis reveals the following features:

- The Asia–Pacific region demonstrates the highest growth dynamics (projected increase of 14%); however, developing markets (notably India and Viet Nam) continue to retain a significant share of cash settlements and manual transaction processing methods.
- Europe maintains leadership in terms of aggregate transaction volumes due to the deep institutionalisation of digital payment standards.
- North America ranks third in terms of volumes, with the United States exhibiting a specific conservative tendency towards the continued use of paper cheques in corporate transactions, despite the overall trend towards digitalisation.
- Digital pioneers such as Australia and Singapore have effectively completed the transition to paperless and fully automated payment models.

Particular attention should be paid to the phenomenon of "technological conservatism" in North America. Despite its status as a global technological hub, the United States demonstrates considerable inertia in the transition to paperless settlements, retaining a substantial share of paper cheques in the B2B segment. This anomaly is driven by the specific architecture of the US banking system:

1. **Complexity of clearing procedures** – the entrenched nature of Automated Clearing House (ACH) mechanisms and the historical reliance on cheque-based settlements within domestic clearing systems.
2. **Institutional fragmentation** – the presence of thousands of local banks, which complicates the rapid unification of payment standards compared to the more consolidated European market.
3. **Legal habit** – a high level of business trust in paper-based instruments as legally incontrovertible proof of payment.

In contrast, Europe emerges as a leader in the volume of digital transactions, driven by the PSD2 directives and the implementation of instant payment systems (Instant SEPA). Australia and Singapore have already reached the stage of a "paperless ecosystem", whereas the markets of India and Vietnam, despite their digital ambitions, remain dependent on cash liquidity and manual operational support of transactions.

The contemporary transformation of retail (B2C) payments is characterised not only by growing volumes but also by a fundamental shift in consumer paradigms. According to Capgemini Analytics, more than 90% of cashless transactions are concentrated in the retail segment, where traditional card-based products are increasingly displaced by digital wallets and account-to-account (A2A) payment models. The evolutionary trajectory of commerce may be conceptualised as a sequence of stages reflecting the progressive reduction of barriers between purchase intention and transaction execution (Figure 4).

Figure 4. Stages of transformation in digital commerce architecture.

The introduction in 2025 of Intelligent Commerce and Agent Pay platforms by market leaders (Visa, Mastercard, PayPal) marked a transition towards automated consumption. Within this model, an AI assistant independently conducts search, comparison, and transaction finalisation based on user preferences, rendering the payment process "invisible" and continuous.

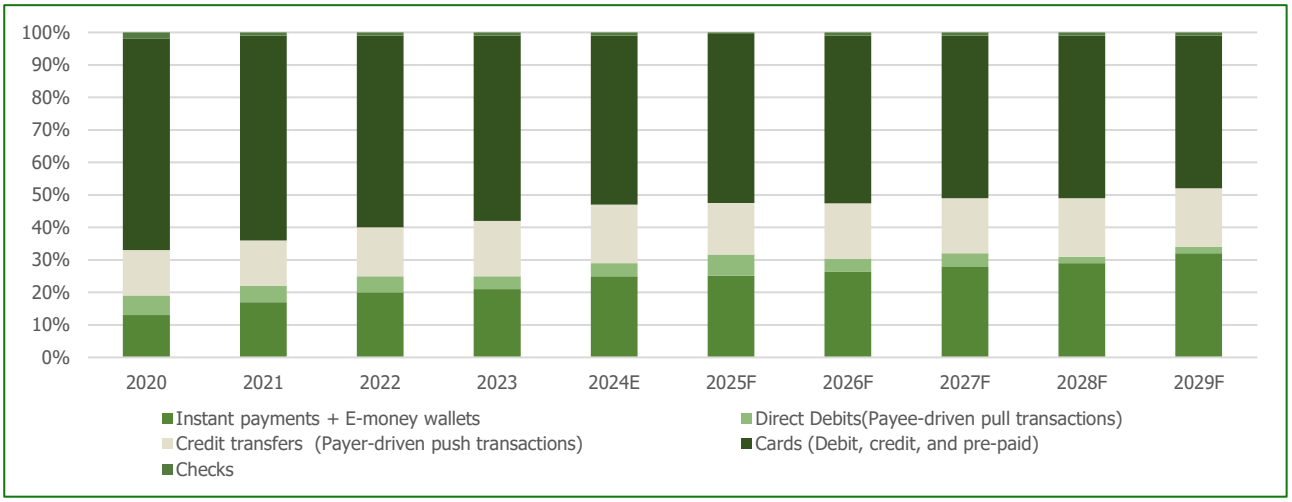


Figure 5. The new payment mix is taking up a bigger global share. Note: E = estimate and F = forecast. *(Source: prepared on the basis of research data by Capgemini (2026))*

The projected growth of e-commerce by 2030 (CAGR of 8%) significantly outpaces the dynamics of physical retail (4%) (Figure 5), thereby reshaping the architecture of payment methods:

1. *Dominance of digital wallets.* Their share in transaction value is expected to increase from 53% in 2024 to 65% in 2030. This creates a risk of the "de-institutionalisation" of banks, as card issuers lose direct customer interaction and a portion of fee-based revenues.
2. *Decline of card-based products.* Direct usage of credit and debit cards demonstrates negative dynamics, with market shares decreasing from 20% to 13% and from 12% to 7%, respectively.
3. *Ascendancy of real-time settlements.* Instant payment systems (UPI, Pix, FedNow), supported by API-based infrastructures, provide higher speed and transparency compared to traditional bank transfers. By 2029, the combined share of instant payments and electronic money is expected to reach 32% of total cashless transaction volumes.

Traditional banking institutions, whose business models have historically relied on acquiring and interchange revenues, are increasingly exposed to the risk of losing both financial flows and valuable data assets. The future competitiveness of banks will depend on their ability to integrate into embedded payment flows (Embedded Finance) and to adapt to the requirements of agent-based commerce.

The Scale of Illicit Use of Crypto Assets in Payments

The transformation of the payment landscape at the present stage is characterised by a marked increase in the involvement of nation-states in the cryptocurrency domain, which has driven the illicit blockchain ecosystem to a new level of operation. In recent years, the landscape of crypto-related crime has undergone profound professionalisation: illicit organisations now operate extensive infrastructures that enable transnational criminal networks to procure goods and services and to launder capital.

A distinctive feature of the period 2024–2025 has been the entry of nation-states into this domain, both through the utilisation of existing professional service providers and through the development of autonomous infrastructures designed

DOI: 10.55643/fcaptp.2.67.2026.5170

for large-scale circumvention of international sanctions. Within the scope of this study, three key milestones in the evolution of crypto-crime (2009–2025) have been identified.

Figure 6. The "Three Waves" evolutionary model of crypto-crime. *(Source: compiled by the authors based on data from Chainalysis and TRM Labs (2025-2026))*

The proposed model demonstrates a transition from the quantitative accumulation of incidents (Waves 1 and 2) to a qualitative transformation in the nature of threats within the Third Wave. The principal distinguishing feature of the current stage lies in a shift in the architecture of obfuscation: rather than concealing the identity of perpetrators (anonymity), state actors focus on masking the origin and destination of capital within ostensibly legitimate blockchain protocols.

According to the analytical findings of the *DNS Threat Landscape Report* (Infoblox, 2025), there is evidence of the rapid adaptation of malicious actors to conventional security mechanisms through the use of DNS queries as covert channels for the delivery of malicious content. The systematisation of the most common scenarios involving newly registered domains has made it possible to identify the following key threat vectors:

1. *Implementation of fraudulent schemes and financial scams*. Domains are utilised to create counterfeit investment platforms, particularly within the crypto-asset ecosystem.
2. *Generation of phishing interfaces*. The development of ostensibly authentic web pages designed to exfiltrate personal identifiers and sensitive payment card details.
3. *Distribution of malicious software (malware).* This vector encompasses the deployment of information stealers (including Lumma Stealer), automated downloaders (such as SocGholish), as well as the expansion of botnet infrastructures and crypto-locker ransomware (e.g., BlackBasta).
4. *Hosting of illegitimate content.* The use of domain names to host prohibited online gambling resources (with pronounced regional concentration, particularly in the Asian region) and other forms of unauthorised content.
5. *Traffic obfuscation via traffic distribution systems (TDS).* The employment of TDS to covertly deliver payloads and to manipulate users into enabling unwanted browser notifications.
6. *Dissemination of potentially unwanted programmes (PUPs).* The coercive installation of dubious browser extensions and scareware applications that destabilise the operation of end-user devices.
7. *Exploitation of electronic communications for spam campaigns.* The use of domain infrastructure to initiate large-scale distributions of malicious email messages.

In one use case scenario, an evaluation of the DL-based worldwide distributed ledger market indicates that the most popular segment within the broader DL framework relates to "Supply Chain Auditing." Projected results highlight that the figure could potentially rise above the USD 103 billion mark by the year 2030, signifying that it will increase by over USD 102 billion from its current position in the year 2020. Other large segments in the DL landscape are tamper-resistant records, digital identity services, smart contract infrastructure, and proof of work systems (Table 1).

Table 1. Global distributed ledger market size (2020 – 2030) by use cases (USD million). *(Source: prepared on the basis of research data by Statista (2026))*

Segment	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Supply Chain Audit	880	1.556	2.91	5.41	9.62	16.57	27	41.17	58.97	79.88	103.4
Immutable Records	180	275	449	744	1.22	2.05	3.15	6.07	10.39	17.18	26.76
Digital Identity	405	569	819	1.17	1.66	2.33	3.25	4.51	6.2	8.42	11.28
Smart Contracts	3	5	7	10	14	19	38	27	53	73	100
Proof-of-Work	1	1	1	2	3	4	7	5	9	17	17

Currently, the rapid expansion of the digital asset market poses a significant threat to payment security. In 2024, the size of the Bitcoin blockchain was approximately 5,450 gigabytes, with the database increasing by nearly one gigabyte every few days. The Bitcoin blockchain contains an ever-growing record of all transactions and entries, expanding continuously while remaining secure from tampering since its initial release in January 2009.

The total value of cryptocurrency received from illicit addresses is presented in Figure 7.

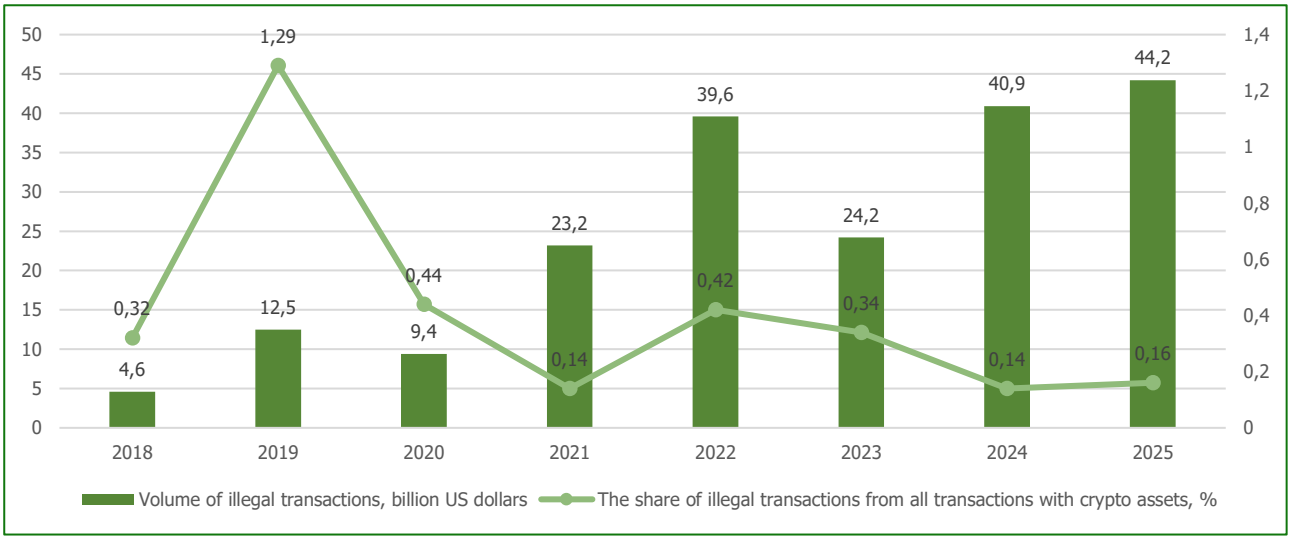


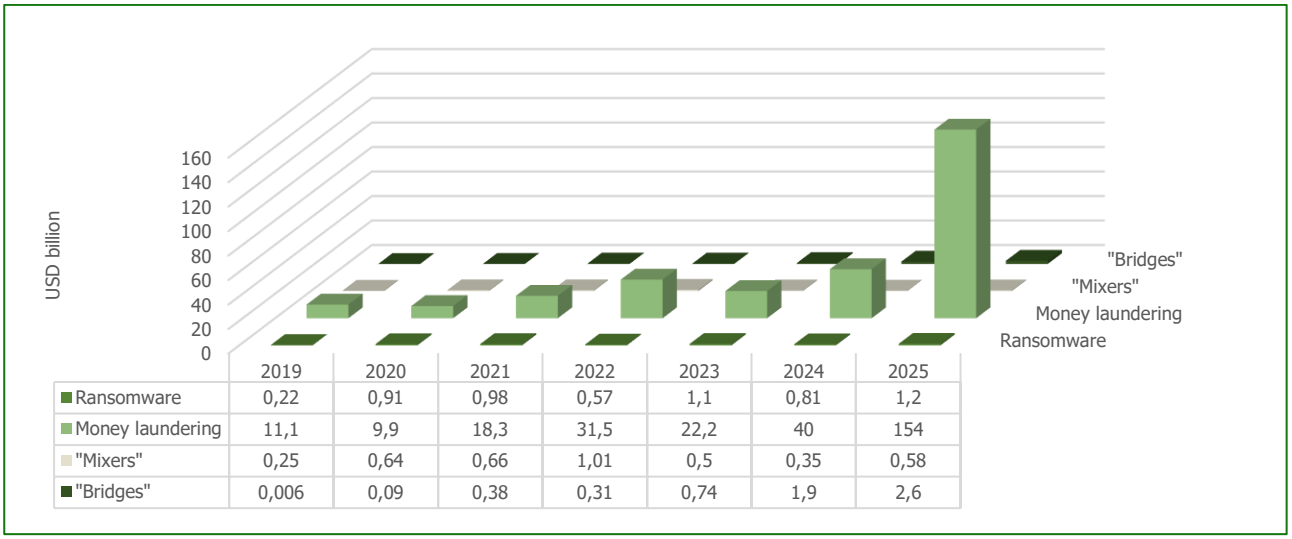
Figure 7. Total cryptocurrency value received by illicit addresses 2018 – 2025. *(Source: compiled by the authors based on data from Chainalysis (2025: 2026))*

Despite the fact that the absolute volume of illicit funds increased to USD 44.2 billion, their share of the overall ecosystem remains marginal (0.16%). This indicates that legitimate uses of cryptocurrencies are expanding at a faster pace than criminal activity. In 2025, the majority of illicit funds (over 60%), driven by the growth of the DeFi sector and stablecoins, once again flowed through stablecoins, which have become the primary instruments for sanctions evasion and money laundering.

The increase to USD 44.2 billion is attributable to a rise in targeted attacks on cross-chain bridges and lending protocols. A significant proportion of the "illicit volume" recorded in 2025 relates to transactions involving addresses subject to sanctions (OFAC and other regulators), rather than solely to direct theft or fraud.

The analysis of the dynamics of illicit crypto-asset circulation during 2024–2025 (Figure 8) points to a fundamental shift in both the objectives and the toolkit of offenders. Traditional forms of cybercrime, such as ransomware, although exhibiting growth to USD 1.2 billion in 2025, account for only a minor share of the total volume of illicit transactions.

DOI: 10.55643/fcaptp.2.67.2026.5170



	2019	2020	2021	2022	2023	2024	2025
Ransomware	0,22	0,91	0,98	0,57	1,1	0,81	1,2
Money laundering	11,1	9,9	18,3	31,5	22,2	40	154
"Mixers"	0,25	0,64	0,66	1,01	0,5	0,35	0,58
"Bridges"	0,006	0,09	0,38	0,31	0,74	1,9	2,6

Figure 8. Structure of illegal cryptocurrency transactions (2019 – 2025). *(Source: compiled by the authors based on data from Chainalysis (2025;2026); TRM (2026))*

The key trend of the reporting period is the dominant role of stablecoins, which accounted for more than 80% of all illicit transaction volumes in 2025. This is explained by their high liquidity and price stability, making them an ideal instrument for integration into global money-laundering schemes and sanctions evasion. A systematic shift away from the use of classical crypto-mixers (whose share declined in 2024) towards cross-chain bridges is observed. The volume of transactions conducted via bridges reached a record USD 2.6 billion in 2025, driven by the following factors:

- Monitoring complexity – cross-chain protocols enable instantaneous switching between blockchain networks, creating "blind spots" for most standard AML analytical tools;
- Sanctions pressure – regulatory restrictions imposed on well-known mixers (e.g., Tornado Cash) have compelled professional actors to seek decentralised alternatives.

The sharp increase in the "money laundering" indicator to USD 154 billion in 2025 reflects a new stage in market evolution – namely, the integration of crypto-assets into state-level mechanisms for circumventing financial restrictions. As noted by Almeida José and Gonçalves Tiago Cruz (José & Tiago Cruz, 2026), this development represents the "professionalisation" of shadow financial flows, in which cryptocurrencies function as a parallel payment infrastructure for sanctioned entities.

Within the framework of the "Third Wave" concept (from 2025 onwards), the structure of crypto-asset offloading through fiat off-ramp services was analysed. The results confirm the hypothesis that the involvement of nation-states and major geopolitical alliances has led to a profound transformation in transaction profiles (Table 2).

Table 2. Structure of withdrawing crypto assets through fiat services (Off-ramps), 2023–2025. Note: * – the sharp jump in the USD 10 million+ category in 2025 is due to the discovery of large sanctioned exchange nodes (OTC desks*). (Source: compiled by the authors based on data from Chainalysis (2025;2026); PwC (2026); Elad Barry & Kinder Kathleen (2025))*

Transaction category	Value 2024 (USD billion)			Trend 2025
	2023	2024	2025	
USD 5 – USD 100	0.0694	0.115	0.142	Growth through AI bots
USD 100 – USD 1 thousand	0.4354	0.580	0.695	Mass phishing
USD 1 thousand – USD 10 thousand	1.4	1.95	2.40	Professional "drops"
USD 10 thousand – USD 1 million	6.0	9.40	14.80	Mainstream channel (OTC)
USD 1 million – USD 10 million	3.3	4.80	7.20	State actors / Hackers
USD 10 million+	3.4	5.10	18.50*	Sanctions operations
Total:	14.6	21.9	43.7	

During 2024–2025, a notable trend emerges: while the total volume of conversions into fiat currency increases, it shifts either towards very small transactions (bot-driven automation) or towards extremely large ones (institutional-scale laundering). The findings demonstrate that the most significant growth is concentrated in the category of transactions exceeding USD 10 million. This serves as a direct indicator that the professional blockchain infrastructure initially developed for cybercriminals is now being scaled by state institutions for the purpose of evading international sanctions.

The key conclusions regarding the institutionalisation of off-ramping, namely the large-scale monetisation of cryptoassets through fiat conversion mechanisms designed to obscure the origin of funds, are as follows:

1. *Geopolitical instrumentality.* The surge in the USD 10 million+ category (from USD 3.4 billion to USD 18.5 billion) indicates the use of cryptocurrencies not as a store of value, but as a "shadow" settlement gateway for financing state procurement and interstate transactions outside the SWIFT system.
2. *Symbiosis of criminal networks and states.* In 2025, nation-states ceased developing isolated proprietary systems and instead integrated into the existing "professionalised" infrastructure of Wave 2 (2020–2024). This enables them to exploit established obfuscation techniques (mixers, bridges) to conceal the state origin of capital.
3. *National security challenges.* As these transactions are embedded within broader illicit fiat outflows, identifying a "state footprint" becomes exceedingly difficult. This raises the stakes for security teams, which are no longer confronting isolated hacker groups but the resources of entire states.

In analysing crypto-to-fiat off-ramping schemes, the geographical specificity of such services must be taken into account. Although precise country-level statistics remain limited, a synthesis of studies by the Basel Institute on Governance (2025), Chainalysis (2026), PwC (2026), and Elliptic (2025), together with traffic and liquidity analysis, allows for the identification of three types of regional hubs where off-ramps are most prevalent:

1. *High-risk jurisdictions and "shadow hubs" (Eastern Europe and South-East Asia).* Regions characterised by a high level of activity of unregulated OTC desks. Transactions in the USD 1 million – USD 10 million and USD 10 million+ categories dominate, with primary flows linked to money laundering and sanctions evasion.
2. *Regions with transitional economies (Latin America and Africa).* P2P platforms and mid-range transactions (USD 100–USD 10 thousand) prevail. Cryptocurrencies are used by the population as a store of value amid fiat inflation, while the same channels are actively exploited to off-ramp illicit proceeds from cybercrime.
3. *Offshore financial centres.* These are utilised for complex schemes to legitimise large sums through shell companies.

The lack of transparent geographical distribution of off-ramp services underscores the problem of regulatory arbitrage. Criminal groups deliberately select jurisdictions with weak oversight of virtual asset service providers (VASPs). The growth of transactions exceeding USD 10 million in 2025 indicates that national AML systems in developed countries are becoming more effective, forcing major actors to migrate towards unregulated digital havens.

Assessing the Impact of Law Enforcement Measures on Banks' Due Diligence in Payment Legitimacy

Since banks are a key component of the financial monitoring system (accounting for over 95% of reports submitted to the State Financial Monitoring Service), it is reasonable to analyze the relationship between enforcement measures and the effectiveness of financial monitoring within the banking system. The dependent variable representing the relative effectiveness of financial monitoring is the reporting load on banks (annual dynamics of the number of reports per active bank – NOTIF). The independent variable, which reflects regulatory enforcement measures for non-compliance with financial monitoring rules, is the penalty burden (the ratio of imposed fines to commission income across the system – FINES). Descriptive statistics for these variables are presented in Table 3.

The indicators presented in Table 3 provide insights into the distribution, dynamics, and integration of the underlying time series. On average, the financial monitoring reporting load per bank increased by 2% year-on-year each quarter. However, the median trend shows a positive growth of almost 22%, which can be attributed to significant fluctuations during certain periods, as evidenced by the high standard deviation (data dispersion reaching 42%). The relative penalty burden averaged below 0.2%, although in Q4 2018, imposed fines amounted to 1% of the quarterly commission income.

Table 3. Descriptive statistics of the time series sample (2018Q1 – 2025Q1). Note: * – t-value is significant at 1% significant level. *(Source: calculated by the authors based on data from the State Financial Monitoring Service of Ukraine (2025) and the National Bank of Ukraine (2025))*

Variables	Mean	Median	Max	Min	Std. Dev.	t-Statistic (ADF)		Integration order
						Level	1st Diff.	
NOTIF	1.0227	1.2160	1.6013	0.1213	0.4233	-1.8945	-4.2146*	I(1)
FINES	0.0015	0.0009	0.0100	0.0000	0.0022	-4.7676*	-5.7532*	I(0)

The stationarity check of the time series using the Dickey-Fuller test revealed that the variables have different orders of integration. Consequently, applying the ordinary least squares method without transforming the series would not yield

DOI: 10.55643/fcaptp.2.67.2026.5170

statistically significant results. In this case, it is advisable to use the ARDL modeling approach, which accounts for differences in integration orders and allows for the identification of long-term effects (provided cointegration of variables is present). To estimate the ARDL model, Eviews software was employed, enabling the automatic selection of the optimal lag lengths for the dependent and independent variables based on the Akaike criterion. The resulting model takes the following form:

$$NOTIF_t = 0.3190^{**} + 1.0178^{*}\ NOTIF_{t-1} - 0.3905^{***}\ NOTIF_{t-2} - 0.8798\ FINES + 38.6715^{***}\ FINES_{t-1}$$

R^2 = 0.6642, DW = 2.0786, AIC = 0.3843, Bounds Test (F-stat) = 4.3265*** (3)

*Note: *, **, *** – t-value is significant at 1%, 5%, 10% significant level.*

Among the 12 automatically evaluated models, the ARD(2, 1) model stands out for its highest quality. This model implies the distribution of the influence of both variables over half of a year (2 quarters). The estimates reveal that the reporting burden exhibits a complex inertia–adjustment dynamic, distributed over approximately two quarters. The positive and statistically significant coefficient on the first lag of NOTIF indicates strong short-term persistence: an increase in the number of reports in the previous quarter leads to an almost proportional rise in the current reporting load. At the same time, the negative and significant coefficient on the second lag of NOTIF reflects a partial self-correction mechanism, whereby excessive reporting intensity is gradually offset through organizational learning, procedural optimization, and internal resource reallocation within banks.

The effect of NBU fines is characterized by a distinctly delayed and systemic impact. The contemporaneous effect of fines is negative and relatively weak, which may capture short-term caution, temporary suspension of operations, or immediate revisions of compliance procedures following the imposition of sanctions. In contrast, the lagged effect of fines is strongly positive and highly significant: an increase in fines in the previous quarter results in a substantial surge in the reporting burden in the subsequent period. This pattern points to the high sensitivity of the entire banking system to regulatory enforcement, as penalties imposed on individual banks trigger a sector-wide tightening of financial monitoring practices. Such behavior is consistent with risk-averse responses under stringent supervision, given that repeated or large fines may ultimately lead to license revocation and bank liquidation.

The identified impact of the penalty burden has both short-term and long-term effects. Since the conducted boundary testing (Pesaran *et al.*, 2001) identified the presence of a cointegrating long-term relationship with statistical significance at the 90% level, the resulting model can be transformed into its long-term form:

$$NOTIF = 0.2747^{*} + 88.3667^{*}\ FINES \quad (4)$$

*Note: * – t-value is significant at 1% significant level.*

The results indicate that, in the long term, penalties imposed on banks for non-compliance with financial monitoring rules have an even more significant impact on enhancing the effectiveness of subsequent anti-money laundering and counter-terrorism financing measures. Specifically, a 1% increase in fines leads to an over 88% rise in the number of reports on suspicious transactions. It is important to note that during the period selected for modeling, there was a tightening of financial monitoring legislation, which resulted in an administrative strengthening of reporting discipline among primary monitoring entities. This finding is consistent with the empirical conclusions regarding the direct and sustained positive impact of regulatory measures on the effectiveness of financial monitoring in Ukrainian banks, both in the short and long term.

DISCUSSION

The results of this study enhance the ongoing academic discourse regarding payment security, the efficacy of AML/CFT measures, and the function of blockchain technologies by advancing current conceptual and empirical frameworks in significant ways.

The ARDL modeling shows that there is a strong link between how well regulatory enforcement works and how well financial monitoring works in the banking sector. Earlier research predominantly examined this relationship indirectly or depended on expert evaluations and survey-derived data (Miglionico, 2022; Thommandru & Chakka, 2023). The current study, on the other hand, offers statistically validated empirical evidence based on the ARDL bounds approach, with its

application being relatively scarce in the empirical analysis of AML/CFT enforcement efficiency owing to the availability of relevant data. With the proposed analysis yielding short- and long-run causal effects, it clearly exceeds other perception-related and/or cross-sectional-based approaches applied by previous researchers. This finding supports the general argument advanced by Tsai et al. (2022) and Susanto et al. (2024) that transaction security and regulatory credibility significantly influence behavioural responses within payment ecosystems. However, unlike these studies, which focus on consumer adoption and perceived security, the current analysis demonstrates that regulatory pressure itself functions as an endogenous driver of payment legitimacy, shaping institutional compliance dynamics rather than merely reacting to them.

The findings partially refine and supplement those of Aburbeian and Fernández-Veiga (2024) and Cologgi (2023), who highlight technological controls like multi-factor verification, strong customer authentication, and machine-learning-based fraud detection. While these studies clearly show the effectiveness of micro-level security tools, the current study shows that, in the absence of proper regulatory enforcement, the systemic efficacy of such micro-level security tools remains structurally limited. In this regard, blockchain-based solutions should be seen as infrastructure mechanisms that increase the disciplining effect of enforcement by improving data immutability, traceability, and auditability across payment chains, rather than as alternatives to regulatory oversight.

The current literature on crypto-crime and AML/CFT risks is expanded by the examination of illicit crypto-asset flows and the suggested "Three Waves" evolutionary model. Blockchain is primarily conceptualized as either a technological risk or as a privacy-enhancing solution that is compliant with regulations in previous research, such as Saad et al. (2026) and Buterin et al. (2024). The entry of state actors and the deliberate use of cross-chain protocols and stablecoins for sanctions evasion are two qualities that define the qualitative change in the nature of blockchain-enabled threats that the current study illustrates. The optimistic view of blockchain transparency presented in previous works (Mohamed, 2023) is nuanced by this finding, which implies that transparency is not enough when adversaries operate at a geopolitical and institutional level. While the prior classifications of crypto-related risks are focused on technology-based vectors or on criminal typologies, the concept of “Three Waves” provides the added benefit of a geopolitical-based approach, which addresses the change from criminal to state exploitation of blockchain technology.

The results partially refute the literature's implicit presumption that an increase in illegal cryptocurrency activity inevitably compromises payment security as a whole. The study demonstrates that while the overall volume of illegal transactions has grown, their relative share is still small, in line with Chainalysis-based data referenced in the Results section. This bolsters the argument made by Ahmad and Aujla (2023) that data protection and privacy requirements can coexist with blockchain architectures that comply with regulations. However, the concentration of illegal activity in high-value off-ramp transactions points to structural flaws at the interface between traditional financial intermediaries and decentralized systems, an area that hasn't gotten much attention in previous empirical research.

By suggesting a hybrid conceptualization of payment security – in which blockchain technology is incorporated into the AML/CFT architecture as a regulatory-aligned infrastructure layer rather than as an independent solution – this study adds to the body of literature. Although previous research has focused on either technological innovation (Mohamed, 2023; Saad et al., 2026) or regulatory adaptation (Miglionico, 2022), the current study shows that the interplay of enforcement rigor, institutional incentives, and technologically enforced transparency leads to sustainable payment security. Given that it functions in an environment of increased geopolitical risk and rapid digitalization, the Ukrainian banking industry offers a particularly instructive example in this respect.

In conclusion, the scientific value of the research lies in the attempt to empirically connect regulatory enforcement, blockchain-based transparency, and institutions in one intellectual picture. Through the use of economics and the structural analysis of the evolution of crypto-crimes, the research presents the role of blockchain systems in supporting, rather than undermining, the regulatory underpinnings of payment systems security. It provides both a conceptual framework and empirical validation for incorporating blockchain into payment security architectures. By going beyond descriptive analyses and showing how blockchain-based infrastructures can strengthen rather than weaken the institutional underpinnings of financial stability, this approach contributes to the existing body of knowledge by empirically reconciling regulatory enforcement with blockchain-based payment infrastructures.

CONCLUSIONS

The evolving financial landscape necessitates a deeper examination of payment security challenges arising from the accelerated digitalisation of payment systems, the expansion of crypto-assets, and the increasing complexity of hybrid financial threats. While payment security has a global dimension, it also exhibits pronounced country-specific characteristics shaped by regulatory frameworks, technological maturity, and geopolitical conditions.

DOI: 10.55643/fcaptp.2.67.2026.5170

The findings of this study confirm that traditional approaches to protecting payment systems are increasingly insufficient under conditions of high transaction velocity, cross-border digitalisation, and the growing involvement of state and non-state actors in illicit financial activities. In this context, blockchain technology emerges as a promising instrument for enhancing transparency, integrity, and trust in payment operations; however, its effective application requires careful alignment with regulatory and supervisory mechanisms. A global assessment of digital non-cash transactions demonstrates that payment security is closely intertwined with the effectiveness of anti-money laundering, counter-terrorist financing, and counter-proliferation measures. The empirical analysis conducted using an autoregressive distributed lag (ARDL) model provides robust evidence that regulatory enforcement measures exert both statistically significant short-term and long-term effects on banks' financial monitoring behaviour. In particular, the existence of a cointegrating relationship confirms that sustained regulatory pressure contributes to a structural strengthening of payment discipline within the banking system.

The study highlights the critical role of banks as the core component of the financial monitoring system, especially under conditions of martial law. The Ukrainian case demonstrates that intensified supervisory and enforcement actions lead to a measurable increase in due diligence and suspicious transaction reporting, thereby reinforcing payment security at the systemic level. This finding substantiates the hypothesis that effective financial monitoring functions not only as a compliance mechanism but also as an instrument of national economic security. A key contribution of the study is the identification of a qualitative transformation in the nature of payment security threats, conceptualised as the "Third Wave" of crypto-related illicit activity, characterised by the growing involvement of state actors and the use of blockchain infrastructure for large-scale sanctions evasion and geopolitical obfuscation. This shift significantly raises the stakes for regulators and financial institutions, as traditional AML tools prove insufficient for detecting and countering such sophisticated schemes.

The analysis confirms that blockchain technology offers substantial benefits for payment security, including tamper-resistant data architecture, enhanced transaction traceability, improved resilience to cyberattacks, and reduced dependence on costly intermediary verification processes. However, the study demonstrates that blockchain should not be viewed as a standalone solution; rather, its effectiveness is maximised when combined with machine learning and artificial intelligence tools capable of predictive anomaly detection and adaptive risk assessment.

Further research should focus on the development of hybrid blockchain–AI security architectures, the extension of financial monitoring mechanisms to non-banking financial institutions and virtual asset service providers, and the harmonisation of blockchain-based solutions with international cybersecurity and regulatory standards, including the NIS2 Directive. Strengthening coordination among financial institutions, regulators, and cybersecurity stakeholders remains a prerequisite for ensuring payment security in an increasingly digital and geopolitically fragmented financial system.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. ASSE. (2025). Top 5 Banking Security Trends in 2025 to Look Out For. https://cybersecurity.asee.io/blog/top-banking-security-trends/
2. Cologgi, M. (2023). The impact of regulation on retail payments security: Evidence from Italian supervisory data. *Finance Research Letters*, *54,* 103799. https://doi.org/10.1016/j.frl.2023.103799
3. Infoblox. (2025). DNS Threat Landscape Report. https://surl.li/jzmngt
4. Basel Institute on Governance. (2025). Basel AML Index 2025: 14th Public Edition Global money laundering and financial crime risk ranking. https://surl.li/ejrugm/
5. State Financial Monitoring Service of Ukraine. (2025). Official website. https://fiu.gov.ua/

6. Adil, O. Y. Mohamed. (2023). Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System. *International Journal of Interactive Mobile Technologies (iJIM)*, *17*(04), 37–46. https://doi.org/10.3991/ijim.v17i04.37671

7. Aburbeian, A. M., & Fernández-Veiga, M. (2024). Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. *AI*, *5*(1), 177-194. https://doi.org/10.3390/ai5010010

8. Darwish, S. M., EL-Naggar, S., & Elkaffas, Saleh M. (2026). Securing financial transactions: exploring the role of lightweight blockchain-enabled deep learning for fraud detection in FinTech systems. *Cybersecurity*, *9*(1). https://doi.org/10.1186/s42400-025-00436-8

9. Mondego, D., & Gide, E. (2023). Cloud-Based Payment Systems in Australia: How Security Affects Consumer Satisfaction. *Engineering Proceedings*, *55*(1), 89. https://doi.org/10.3390/engproc2023055089

10. Susanto, H., Tamtini, N., Ibrahim, F., Susanto, A. K. S., Setiana, D., & Yie, L. F. (2024). Demystification of Readiness, Security, and Technological Enhancements in the Adoption of a Cashless Economy. *Economies*, *12*(11). https://doi.org/10.3390/economies12110285

11. Tsai, S.-C., Chen, C.-H., & Shih, K.-C. (2022). Exploring Transaction Security on Consumers' Willingness to Use Mobile Payment by Using the Technology Acceptance Model. *Applied System Innovation*, *5*(6). https://doi.org/10.3390/asi5060113

12. Thommandru, A., & Chakka, B. (2023). Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks. *Sustainable Futures*, *5*. https://doi.org/10.1016/j.sftr.2023.100107

13. Buterin, V., Illum, J., Nadler, M., Schär, F., & Soleimani, A. (2024). Blockchain privacy and regulatory compliance: Towards a practical equilibrium. Blockchain: *Research and Applications*, *5*(1). https://doi.org/10.1016/j.bcra.2023.100176

14. Ahmad, H., & Aujla, G.S. (2023). GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment. *Computers and Electrical Engineering*, *109*. https://doi.org/10.1016/j.compeleceng.2023.108747

15. Miglionico, A. (2022). Digital payments system and market disruption. *Law and Financial Markets Review*, *16*(3), 181–196. https://doi.org/10.1080/17521440.2023.2215481

16. Capgemini. (2026). World Payments Report 2026. The (not-so) silent takeover: Winning back merchants means playing differently. https://www.capgemini.com/pt-en/insights/research-library/world-payments-report-2023/

17. Statista. (2026). Official website. https://www.statista.com/

18. Chainalysis. (2025). The 2025 crypto crime report. The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation. https://surl.lu/ohyslv

19. Chainalysis. (2026). The 2026 Crypto Crime Report: Trends in illicit activity and the role of stablecoins. https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction//

20. TRM. (2026). 2026 Crypto Crime Report Key Insights: TRM Identifies Record USD 158 Billion in Illicit Crypto Flows in 2025, Reversing a Multi-year Decline. https://surl.li/tsjgcs/

21. Gonçalves, Tiago Cruz, & Almeida, J. (2026). Cryptocurrencies and economic sanctions. *North American Journal of Economics and Finance*, *81,* 102537. https://doi.org/10.1016/j.najef.2025.102537

22. PwC. (2026). Global Crypto Regulation Report. PwC's Global Crypto Regulation Report 2026. https://www.pwc.de/de/unterlagen/pwc-global-crypto-regulation-report-2026.pdf

23. Elad, B., & Kinder, K. (2025). Cryptocurrency Anti Money Laundering (AML) Statistics 2026: Revealing Illicit Flows & Enforcement. https://coinlaw.io/cryptocurrency-anti-money-laundering-statistics/

24. Elliptic. (2025). The state of cross-chain crime 2025. Contemporary risks, trends & best practices to counter them. https://surl.lu/nhpsua

25. National Bank of Ukraine. (2025). Official website. https://bank.gov.ua/

26. Pesaran, M. H., Shin, Y., & Smith, R. J. (2001). Bounds testing approaches to the analysis of level relationships. *Journal of Applied Econometrics*, *16*, 289–326. https://doi.org/10.1002/jae.616

27. Mohamed, A., Abdelqader, K., & Shaalan, K. (2025). Explainable Artificial Intelligence: A systematic Review of Progress and Challenges. Intelligent Systems with Applications, 28. https://doi.org/10.1016/j.iswa.2025.200595

Коваленко В., Шелудько С., Безкровний О., Дорошенко О., Дорошенко А., Борса В.

ІНТЕГРАЦІЯ ПРИНЦИПІВ БЛОКЧЕЙН В АРХІТЕКТУРУ ПЛАТІЖНОЇ БЕЗПЕКИ ФІНАНСОВОЇ СИСТЕМИ

Актуальність дослідження зумовлена стрімкою цифровізацією платіжних систем і зростанням вразливості фінансової системи до кібернетичних, операційних ризиків і ризиків у царині протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму (ПВК/ФТ), що посилюються внаслідок розширення безготівкових розрахунків, поширення криптоактивів і зростання ролі державних і недержавних акторів у незаконній фінансовій діяльності. Зазначені процеси поглиблюють уразливість платіжної безпеки, особливо в умовах геополітичної нестабільності та гібридних загроз. Метою дослідження є теоретичне й емпіричне обґрунтування принципів

DOI: 10.55643/fcaptp.2.67.2026.5170

інтеграції технології блокчейн в архітектуру платіжної безпеки та систему ПВК/ФТ з метою мінімізації новітніх ризиків. Методологічну основу дослідження становить поєднання системного й описового аналізу, методів систематизації та узагальнення, статистичного аналізу й економіко-математичного моделювання. Для оцінювання впливу заходів регуляторного примусу на належну перевірку банками легітимності платіжних операцій застосовано модель авторегресії з розподіленими лагами (ARDL) на основі даних банківського сектора України. Отримані результати свідчать про тісну залежність рівня платіжної безпеки від ефективності фінансового моніторингу та регуляторного нагляду, при цьому заходи примусового впливу мають статистично значущий короткостроковий і тривалий ефект на інтенсивність подання повідомлень про підозрілі фінансові операції. У ході дослідження встановлено, що технологія блокчейн має значний потенціал для посилення платіжної безпеки завдяки підвищенню прозорості транзакцій, зміцненню механізмів ПВК/ФТ й підвищенню стійкості до кіберзагроз, у тому числі пов'язаних із незаконним використанням криптоактивів. Обґрунтовано, що гармонізація блокчейн-рішень із регуляторними принципами є необхідною умовою забезпечення фінансової стабільності в середовищі прискореної цифровізації. За результатами дослідження сформульовано практичні рекомендації щодо інтеграції технології блокчейн у системи платіжної безпеки та фінансового моніторингу, які можуть бути корисні для регуляторів, фінансових установ і суб'єктів формування державної політики в царині економічної та платіжної безпеки.

Ключові слова: блокчейн, платіжна безпека, криптовалюта, ПВК/ФТ, цифрові транзакції, KYC, RegTech

JEL Класифікація: G21, O33, E42