DOI: 10.55643/fcaptp.2.67.2026.5061

Bekzhan Mukhanbetali
Doctoral Student, Institute of Management, Academy of Public Administration under the President of the Republic of Kazakhstan, Astana, Kazakhstan;
ORCID: 0009-0000-3610-9049

Solomiya Hanushchyn
D.Sc. in Public Administration, Associate Professor of the Department of Governance and Administration, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies of Lviv, Lviv, Ukraine;
ORCID: 0000-0002-6328-9978

Tetiana Khalimon
D.Sc. in Economics, Associate Professor of the Department of Management, State University of Information and Communication Technologies, Kyiv, Ukraine;
ORCID: 0000-0002-9194-4108

Serhii Khalimon
PhD Student, Department of Management, State University of Information and Communication Technologies, Kyiv, Ukraine;
ORCID: 0009-0003-1145-1720

Liudmyla Akimova
D.Sc. in Public Administration, Professor of the Department of Human Resources and Entrepreneurship, National University of Water and Environmental Engineering, Rivne, Ukraine; Cyprus University of Technology, Limassol, Cyprus;
ORCID: 0000-0002-2747-2775

Oleksandr Akimov
D.Sc. in Public Administration, Professor of the Department of Public Administration, Interregional Academy of Personnel Management; Scientific and Methodological Center for Personnel Policy of the Ministry of Defense of Ukraine, Kyiv, Ukraine;
e-mail: 1970aaa@ukr.net
ORCID: 0000-0002-9557-2276
(Corresponding author)

Received: 07/11/2025
Accepted: 05/04/2026
Published: 30/04/2026

BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE IN FINANCIAL CONTROL SYSTEMS: SYNERGY OF INNOVATIONS FOR ECONOMIC SECURITY

ABSTRACT

The increasing complexity of global financial systems has necessitated the adoption of more efficient and transparent mechanisms for combating money laundering (AML). Blockchain technology, with its decentralized, immutable, and transparent characteristics, presents a promising solution to address the limitations of traditional AML systems. This paper represents a review, exploring the potential applications of AI and blockchain in enhancing financial control systems, in particular, within AML compliance, focusing on key areas such as transaction monitoring, cross-institutional data sharing, and regulatory reporting. The integration of blockchain can streamline AML processes, reduce operational costs, and increase the effectiveness of detecting illicit financial activity. The combination of blockchain technologies and artificial intelligence algorithms in financial control is considered. It is shown how automation of transaction analysis can strengthen the stability of the banking system and prevent financial crimes. It is demonstrated that the convergence of Artificial Intelligence and blockchain technologies presents a transformative opportunity to strengthen AML frameworks, particularly in the face of rising crypto-enabled financial crimes. This research offers several important contributions to the academic literature. First, it presents a synthesis of the current status of artificial intelligence approaches used for compliance in detecting fraud in Bitcoin transactions. This review discusses the essential methodologies and tactics in a particular area that intersects finance and compliance but falls under the broader disciplines of AI-driven finance and decentralized finance (DeFi). The incorporation of AI into financial control marks a tremendous technological revolution that is affecting industries across the board. Second, the study assesses the current state of the publications, major trends, and research gaps, emphasizing areas that deserve additional investigation.

Keywords: banking system, blockchain, management, innovations, economic security, financial control, financial monitoring

JEL Classification: G15, G18, G19, E61

INTRODUCTION

Many nations rank combating money laundering and terrorism financing as their top national security priorities. According to statistical data, the amount of illegal financial flows associated with financial crime, such as money laundering, financing of terrorism and proliferation, and fraud, is a matter of increasing concern. Digital scams cost individual customers in Asia USD 700 billion in 2024 (Rogers, 2024). Making sure that advances in the financial sector don't turn into tools for financial crime is crucial as Fintech continues to revolutionize financial services. For instance, the growing use of technology-enabled real-time payment solutions has made it easier for users to settle their accounts almost instantly, but it has also given criminals new ways to avoid detection by transferring money quickly between several accounts (Hunter et al., 2025).

Economic security today is one of the most critical components of national security. Money laundering and terrorist financing are major threats to economic security, undermining financial system integrity, fostering corruption, and funding crime by disguising illicit funds as legitimate. Today, financial crime is widespread, and every year, almost USD 2 trillion is laundered. This is significantly more than the USD 275 billion the banking industry spends on stopping this crime (Armstrong et al., 2023). It makes it

easier to hide money obtained illegally from operations, including drug trafficking, financing terrorism, human trafficking, corruption, tax evasion, and cybercrime. As a result, over the past forty years, international efforts to stop money laundering have increased dramatically, leading to the creation of a sophisticated, multilateral regulatory framework. These frameworks seek to advance financial responsibility, transparency, and economic stability in addition to detecting and discouraging illicit financial flows.

Financial crimes continue to be transnational in character, taking advantage of technical blind spots, regulatory discrepancies, and jurisdictional fragmentation despite advancements in financial control. Complex layering across offshore corporations, digital assets, shell firms, and proxy ownership structures is a common feature of sophisticated money laundering schemes, making detection and enforcement extremely challenging. Data privacy regulations, political restrictions, and restricted access to real-time intelligence can make it difficult for law enforcement authorities to coordinate across borders.

Moreover, additional difficulties in tracking financial movements have been brought about by the development of digital financial instruments, including cryptocurrencies, privacy coins, and decentralized finance (DeFi) protocols. These technologies undermine the efficacy of conventional AML procedures that rely on transaction monitoring and customer verification by enabling actors to conduct under false pretenses with little oversight. The need for more flexible, open, and interoperable compliance solutions is growing as criminal networks get better at utilizing technology advancements.

One should note that in recent years, cryptocurrencies have undergone significant change, evolving into a variety of formats and sorts. Specifically, anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralized platforms and exchanges, privacy wallets, etc., that facilitate or permit lesser transparency and greater obfuscation of financial flows have become more prevalent in the virtual asset ecosystem. Other virtual asset business models or activities, such as initial coin offerings (ICOs), which pose hazards of fraud, market manipulation, and money laundering and terrorist financing (ML/TF), also arise as a result. The Financial Action Task Force (FATF) acknowledged the need for additional clarity on the application of the FATF Standards to new technologies and providers in light of the emergence of new types of providers and the development of additional products and services in this arena. In addition to ensuring that virtual asset technologies and businesses can continue to expand and innovate responsibly, the effective global application of these standards by all nations will level the playing field. It will stop terrorists or criminals from looking for and taking advantage of areas with little to no oversight (Jo et al., 2025).

However, given the rise of new provider types and the creation of new products and services in this space, the Financial Action Task Force (FATF) recognized the need for more clarification on how the FATF Standards should be applied to new technologies and providers. Effective international implementation of these standards by all countries would level the playing field and guarantee that virtual asset technologies and enterprises may keep growing and innovating responsibly. It will prevent criminals or terrorists from seeking and exploiting places with little to no supervision (Jo et al., 2025).

There are numerous causes for the gap that exists. The main reason for this is that a lot of AML programs put regulatory and technical requirements ahead of the program's ability to effectively stop criminal activity. The sluggish adoption of new technology by many financial institutions is the other important factor. Monitoring gaps result from their legacy systems' incompatibility with contemporary compliance technologies.

Other significant weaknesses in consumer due diligence include inherent blind spots. The efficacy of AML policies is further compromised by inadequate personnel training. However, the continuous arms race between criminals and the financial sector is the biggest deterrent (Bondarenko et al., 2022). These scammers take advantage of emerging technologies and change more quickly than laws can be put in place. It is challenging for conventional AML systems to keep up with them because they employ sophisticated techniques to get around regulations.

In turn, the changing dangers accelerated the development of RegTech and forced academics and regulators to look for fresh methods of financial management within the larger framework of economic security. By offering instruments for transparency, traceability, and risk management in cryptocurrency transactions, blockchain is specifically utilized for financial surveillance and the fight against financial crimes. To guarantee adherence to anti-money laundering laws, specialized blockchain monitoring systems examine on-chain data to spot suspect trends like fraud and money laundering, find connections between wallet addresses, and issue warnings for high-risk activity.

Thus, this landscape of emerging new threats to economic security as part of national security determines the urgent necessity of scientific analysis aimed at evaluating the role of blockchain and AI in enhancing financial control systems, in particular, due to the potential synergetic effect of these technologies.

DOI: 10.55643/fcaptp.2.67.2026.5061

LITERATURE REVIEW

One of the main forces behind the modernization of international financial systemsis digital transformation. Digitalization has improved accountability and transparency in reporting, increased public access to financial products, and improved service efficiency. Artificial intelligence (AI), the Internet of Things (IoT), and cloud computing have revolutionized the way financial institutions, from banks and cooperatives to microfinance organizations, provide client service (Desi et al., 2023). But these advancements are accompanied by significant obstacles, namely risks to system and data security, such as the crime of skimming. For instance, Indonesia's Financial Services Authority (Otoritas Jasa Keuangan, 2022) noted that the rise in mobile banking and cashless transactions during and after the COVID-19 pandemic has led to a notable increase in instances of skimming and other types of digital fraud. There are still serious security flaws in digital banking systems, as evidenced by the growing number of skimming cases. These problems are frequently caused by antiquated security procedures, inadequate internal controls, and a lack of cybersecurity knowledge among finance managers (Hilal et al., 2022). A forensic accounting method for early skimming identification and prevention in digital financial systems is examined by Idris et al. (2025). Their study's conclusions are consistent with the Fraud Triangle and Fraud Diamond theoretical frameworks, which describe how pressure, opportunity, rationalization, and capability all contribute to fraud. Skimming develops mostly owing to poor internal controls (opportunity) and the technical skills of perpetrators (capacity) (Choi & Lee, 2018). Furthermore, fraudulent conduct has been successfully identified using the Digital Forensic Framework, which includes identification, digital evidence collection, analysis, and reporting (Quick & Choo, 2018).

In 2015, Han looked into how blockchain technology and artificial intelligence could work together in financial institutions, with a focus on operational efficiency, security, and transparency. The study examines how AI anomaly detection algorithms with blockchain's decentralized ledger architecture might improve fraud prevention and regulatory compliance. It looks at how these technologies are used in high-frequency trading (HFT) and cross-border payments, showing how they affect market execution accuracy, transaction cost reduction, and settlement time reduction. Examples include how AI optimization is used in algorithmic trading tactics and how Ripple and Stellar function in decentralized remittance networks. The study also highlights implementation issues in financial infrastructures by addressing constraints such as cybersecurity vulnerabilities, model risk, technology interoperability, and regulatory divergence (Han, 2015).

Experts emphasize that blockchain provides a fresh and creative approach to AML that can solve the problems compliance teams encounter and increase the process's overall effectiveness (Pocher et al., 2022). AML monitoring on the blockchain has the ability to completely transform how financial institutions fight money laundering by utilizing the built-in advantages of blockchain technology, such as increased automation, security, and transparency.

Blockchain enhances financial monitoring for AML within various domains, in particular (Nita, 2025):

1. Improved traceability and transparency: Public blockchains offer an unchangeable, publicly accessible record of transactions, making it easier to track the origins of assets and money movements, which helps to spot illegal behavior.
2. Automated, real-time surveillance that adjusts to changing criminal typologies is made possible by the combination of blockchain technology, artificial intelligence (AI), and smart contracts.
3. Simplified KYC/CDD: Blockchain-based decentralized identification (DID) systems can enable safe, reusable digital IDs, boosting data privacy and Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures.
4. Cross-chain compliance: By developing frameworks to track transactions across several blockchains, blockchain-based solutions can eliminate regulatory blind spots
5. Enhanced efficiency: Smart contract automation can cut down on operational inefficiencies, delays, and human error that come with traditional, centralized solutions.

Along with blockchain, diverse AI-based solutions are entering the RegTech landscape. Meanwhile, there is still a lack of systematization in this field, and the synergetic paradigm rarely becomes a platform for both scholarly research and practical solutions design in the field.

The impact of developing technologies on financial crimes and their incorporation into financial institutions is examined by Ghose et al. (2025). The study aims to classify and identify cyber breaches, financial crimes, and the function of digital evidence in financial technologies. The report draws attention to the growing worry about how new technologies are being used to enable financial crimes like cyber fraud, tax evasion, and money laundering. It also looks at how technological developments have changed the nature of financial crimes and the difficulties in identifying and bringing these crimes to justice.

A comprehensive analysis of AI used for compliance was carried out by Rodríguez Valencia et al. in 2025. The authors' main concern was detecting fraud in cryptocurrency transactions. Between 2014 and 2025, they looked at how AI was incorporated into compliance for bitcoin fraud detection, examining its methods, development, and new trends. The use of ML, deep learning, natural language processing, and technologies of generative AI to increase fraud detection's effectiveness and inventiveness are some of the major developments that have been identified. However, the report emphasizes that difficulties still exist, such as inadequate openness in AI models, regulatory fragmentation, and restricted access to quality data, all of which impede effective fraud detection (Hrytsenko et al., 2024). The long-term usefulness of AI tools in the real world is mostly unknown. This paper discusses the evolution of AI in compliance, identifies opportunities for future research, and stresses linking theory and practice to improve fraud detection in Bitcoin transactions.

Aidoo et al. (2025) underline that, while today's AML compliance efforts are substantial, they lack efficiency and efficacy. Fragmented systems and human processes struggle to manage large-scale data analysis; basic rule-based monitoring generates far too many false alarms; and criminals exploit technological development more quickly than regulators can respond. As a result, experts have assessed the existing quo poorly; for example, in 2020, the FATF's previous executive secretary stated that "everyone is doing it badly" in terms of global AML outcomes. This blunt judgment, along with the reality that illicit flows persist on a massive scale (trillions globally, according to some estimates), creates a tremendous motivation to investigate new technology tools and approaches.

According to some academics, using distributed ledger technology and blockchain to modernize and improve AML compliance is one viable technological path. By enhancing transparency, facilitating safe data sharing, and automating compliance logic, blockchain technology, a secure, network-maintained ledger, could help with a number of the issues mentioned above (Von Hafe et al., 2025).

The literature highlights the use of AI techniques by regulatory bodies and financial institutions to monitor and examine bitcoin transactions for indications of sanctions evasion. These tools can reveal concealed transactions and link illegal payments to organizations or people that are subject to sanctions by utilizing blockchain forensics and advanced analytics (Gupta et al., 2023):

1. AI for blockchain analysis: to trace the movement of cryptocurrency transactions throughout the decentralized network, AI systems employ blockchain analytics. AI can follow the flow of money and flag questionable transactions in real time by recognizing wallet addresses connected to sanctioned people or organizations.
2. Machine learning for crypto risk scoring: similar to conventional banking, AI models employ machine learning to rate the risk of cryptocurrency transactions according to variables such as transaction size, velocity, and wallet address history. These tools are essential for spotting intricate transactions or stacking strategies that point to the evasion of penalties.

AI is becoming increasingly more important in changing AML compliance processes in various sectors. AI's capacity to evaluate enormous datasets, identify irregularities, and adjust to new threats makes it a vital instrument in the continuous battle against financial crime, from large banks and FinTech startups to government partnerships and crypto monitoring (Jain, 2024).

The use of blockchain technology in financial control systems is a topic that is becoming more and more discussed in academic circles and in the creation of actual policies. Transparency, traceability, security, and automation, all of which are intrinsic to blockchain technology, - are highlighted as being very compatible with AML compliance requirements (Konstantinidis & Gegov, 2024). A transparent ledger makes all transfers traceable, but a successful launderer aims to hide the trail of illicit funds. An unchangeable shared ledger would maintain a coherent trail of activity, but a successful launderer takes advantage of shoddy record-keeping and compartmentalized systems (Bashtannyk et al., 2025). From a conceptual standpoint, blockchain presents an exciting idea: what if all financial transactions, or at the very least, all data pertinent to compliance, - were documented on a ledger that authorized parties could view in real time? In addition to lowering some compliance expenses, it might significantly improve the speed and precision of financial crime investigations.

A survey of traditional KYC/AML practices is presented by Moreno et al. (2021), who highlight a subset of current issues in these practices while taking into account the innovation of cryptocurrency transactions and related innovations, such as digital identity and the financial inclusion of unbanked individuals without identity documents. The authors address current approaches to these problems, including the use of cutting-edge technology and the adoption of new KYC/AML procedures. They noted that the new KYC/AML rules are attempting to preserve the fundamentals of conventional financial systems. The study highlights that, regrettably, there are a lot of factors to take into account while working with cryptocurrencies. Creating new solutions that employ non-official personal documents for KYC is one of the suggested recommendations. For instance, a new approach would allow an individual or organization trustee to vouch for the application as a form of

DOI: 10.55643/fcaptp.2.67.2026.5061

identity evidence rather than requiring a document to confirm the address. An alternative strategy would be for the applicant to reveal their location on a regular basis.

According to Kumar (2025), traditional centralized systems frequently fall short in preventing fraud and guaranteeing data integrity, particularly as cyber threats become more sophisticated. To overcome these constraints, the author suggests an artificial intelligence-enhanced blockchain-based platform. Ethereum smart contracts and machine learning models are used in the system's construction, and frontend, backend, and AI components are connected via a modular design. Evaluation reveals dependable audit trails, quick reaction times, and fraud detection accuracy of above 92%. The method offers a safe, clever, and decentralized solution for contemporary data protection and is scalable and appropriate for delicate industries like healthcare and banking.

The number of studies that give a fresh, thorough synthesis of blockchain and AI applications in financial services is growing, and they provide practitioners and scholars with insightful information. In the financial services sector, researchers emphasize that the combination of blockchain technology and artificial intelligence has become a game-changer, spurring innovation in fields like risk management, fraud detection, regulatory compliance, and operational efficiency (Rane et al., 2023; Shi & Wang, 2025). Such studies offer a distinctive viewpoint on these technologies' revolutionary potential in FinTech by rigorously analyzing their difficulties and synergies. However, given how quickly blockchain and AI technologies are developing, it's possible that some conclusions won't be applicable in the long run. This issue needs to be addressed immediately.

AIMS AND OBJECTIVES

Bearing in mind the above-mentioned trends and concerns, the objective of this paper is to:

- systematizing the features of today's landscape of AI- and blockchain-based solutions applicable for financial control systems;
- outlining existing concerns in this field (in particular, within the national security domain) and formulating vectors for making efforts to achieve synergetic effects.

METHODS

The study uses a qualitative approach. The integrative literature review is the research instrument. An integrative review is a special type of review technique that offers a more thorough understanding of a given topic by summarizing previous empirical or theoretical material. It offers knowledge synthesis and practical application of important study findings (Oermann & Knaff, 2021).

A sampling of literature sources for review was carried out based on the standard PRISMA methodology.

In order to facilitate clear and thorough reporting, this investigation follows the standard procedure described by Page et al. (2021) under the PRISMA methodology (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). To encourage thoroughness, repeatability, and clarity in review reporting, PRISMA provides an organized checklist and flow diagram.

Identification, screening, eligibility, and inclusion are the four main stages of the data collection procedure, which was organized using the PRISMA methodology that was modified for the study setting (Figure 1). The search query (and its combinations) was created during the identification step using the Population, Intervention, Comparison, Outcomes, and Context (PICOC) framework: "AML" or "Financial Control" or "RegTech" and "Blockchain" and "Artificial Intelligence" and "Compliance" and "Cryptocurrency" and ("machine learning" or "deep learning" OR "natural language processing" or "Machine Learning"), which was used across keywords, titles, and abstracts.

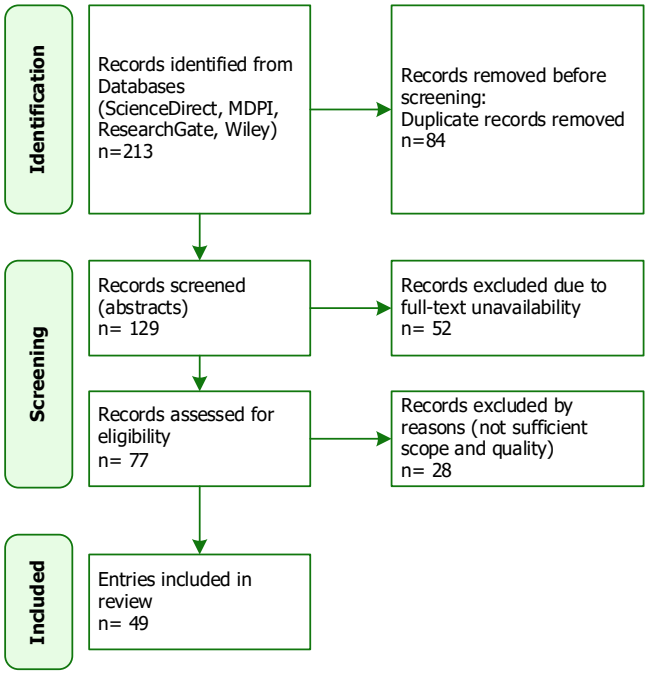

Figure 1. PRISMA flow diagram.

RESULTS

After reviewing the compiled sample of literature sources, it was discovered that blockchain and AI improve economic security by combining blockchain's immutable and transparent ledger with AI's advanced analytical and predictive skills. The synergy between AI and blockchain amplifies the strengths of both technologies:

1. Data integrity and trust. Blockchain provides a secure, decentralized structure that protects data integrity and prevents tampering. AI models, in turn, rely on high-integrity data to produce more accurate and unbiased choices.
2. Enhanced security AI algorithms may evaluate transaction patterns in real time to detect and flag unusual activity, enhancing blockchain's inherent security against fraud and identity theft.
3. Operational efficiency AI can optimize blockchain operations by increasing consensus mechanisms and scalability, allowing networks to process more transactions per second. Smart contracts, a feature of blockchain, can be combined with AI to automate and enforce complicated agreements, reducing human error and the need for middlemen.

The combined technologies are revolutionizing several sectors. The appropriate implications are summarized in Table 1.

Table 1. Key applications of blockchain and AI in economic security.

Benefits
Financial Transactions and Services The integration enhances financial security by boosting Know Your Customer (KYC) and AML processes. AI analyzes massive datasets to identify dangers, whereas blockchain securely maintains immutable client records, which speeds up onboarding and reduces fraud.
Management of Supply Chains: Real-time monitoring, data sharing, and risk management throughout intricate supply chains are made possible by this combination. Blockchain guarantees end-to-end product traceability and transparency, and AI helps forecast market trends and optimize resource allo-cation, strengthening the supply chain's security and resilience.
Cybersecurity Blockchain removes single points of failure that are typical of centralized systems by distributing data throughout a network. AI improves overall network resilience by providing sophisticated analytics for attack identification and quick containment actions.
Risk Control and Adherence to Regulations Large volumes of regulatory data can be analyzed by AI-powered solutions to verify compliance and spot possible problems. This improves oversight, transparency, and auditability for financial institutions and regulators when paired with blockchain-based reporting platforms.
Challenges
system interoperability, scaling concerns, and the requirement for an adaptable regulatory framework. To fully realize the potential of blockchain and AI to promote a safer and more stable global economy, these issues must be resolved.

DOI: 10.55643/fcaptp.2.67.2026.5061

Moreover, the results of the conducted integrative review show that although conventional AML systems have proven successful in identifying simple types of money laundering, they are unable to keep up with new threats. Trade-based money laundering (TBML) and cryptocurrency laundering are two well-known instances of illegal activity that pose serious problems for conventional AML frameworks. Regarding crypto laundering, it should be mentioned that new channels for money laundering have been made possible by the growth of cryptocurrencies. Criminals can more easily move illegal funds across borders undetected thanks to the anonymity and pseudonymity provided by digital currencies like Bitcoin, Ethereum, and others. Since bitcoin operates outside of the conventional banking infrastructure, standard AML systems are frequently ill-equipped to trace cryptocurrency transactions. Although blockchain technology makes cryptocurrency transactions more transparent, it is particularly challenging to identify and stop crypto laundering because many jurisdictions lack thorough regulatory frameworks (Cassara & Poncy, 2015). In turn, TBML entails disguising the transfer of illegal funds through commercial activities. Criminals fabricate trade invoices, over- or under-invoice items, or send things to nonexistent destinations in order to conceal the true source of illegal finances behind a web of trade data that appears legitimate. It is challenging to distinguish TBML from conventional rule-based systems due to the intricacy of international trade and the enormous amount of global trade transactions. To identify TBML, sophisticated methods like artificial intelligence and machine learning are required to evaluate shipping data, invoice inconsistencies, and trade trends in real-time (Spyra et al., 2025).

It is obvious that as new types of financial crime develop, rule-based systems must be supplemented with cutting-edge technologies that can adapt to meet these new risks. This makes a strong case for the creation and uptake of AI-driven AML systems that are capable of analyzing large, complicated data sets, responding to emerging threats, and giving law enforcement organizations real-time knowledge.

Currently, regulated financial intermediaries, - particularly the banking industry, - are essential to the enforcement of anti-money laundering regulations. A payment in an intermediary-based monetary system is made by crediting the recipient's account and debiting the senders. The middleman is responsible for doing customer checks, which can be done during account changes. This idea holds true for payments made both domestically and abroad via the correspondent banking network.

The intermediary-based AML compliance principles are being applied to the crypto sector through the current international guidelines for AML compliance for cryptoassets. But there are unmistakable restrictions on this strategy. Decentralized consensus procedures supported by a distributed group of self-interested "validators" that collaboratively keep track of transactions between addresses on the blockchain in a decentralized manner are the foundation of permissionless public blockchains. The account modification cannot be attributed to any one intermediary.

The possibility of blockchain technology, a subset of distributed ledger technology (DLT), to address these AML issues is being investigated more and more. A decentralized, immutable, and cryptographically secure database that logs transactions over a peer-to-peer network is the fundamental component of a blockchain. An irreversible and transparent chain of records is created by storing each transaction in a block that is time-stamped and connected to the block before it.

Key concepts within blockchain include (Aidoo et al., 2025):

- a consensus-based data structure that is managed by numerous people without the requirement for a centralized authority is known as distributed ledger technology, or DLT;
- smart contracts: blockchain-based self-executing code that, when certain criteria are satisfied, automatically enforces an agreement's terms;
- tokens and digital assets: these include utility tokens, security tokens, and central bank digital currencies (CBDCs), which are native representations of value or rights on blockchain networks.

Blockchain is an interesting option for improving AML systems because of its transparency and traceability, cryptographic security, and programmable compliance requirements. While permissioned blockchains, like Hyperledger Fabric and Quorum, offer regulated access appropriate for institutional collaboration, public blockchains, like Bitcoin and Ethereum, offer open auditability.

Blockchain technology is being investigated by AML systems because it can facilitate information exchange between institutions and jurisdictions, identity verification, and real-time monitoring. Blockchain, for instance, can be used to produce unchangeable KYC data records, cutting down on fraud and redundancy. Without the need for human intervention, smart contracts can immediately embed compliance standards into financial workflows, guaranteeing conformity to regulatory obligations.

ISSN: 2306-4994 | eISSN: 2310-8770 | Том 2 (67), 2026

Blockchain-based AML solutions are being piloted by financial institutions, fintech companies, and regulators in domains such as cross-border payments, digital identity verification, and regulatory reporting. The increased interest in balancing technical innovation with compliance duties is demonstrated by initiatives like ING's Zero-Knowledge Proofs, the Basel Committee's debates on digital assets, and OECD-led frameworks on blockchain standards (Bolton & Mintrom, 2023).

AML has undergone a revolution thanks to machine learning (ML), which has produced systems that can learn from enormous datasets and identify suspicious activity patterns with previously unheard-of accuracy. Behavioral pattern identification is one of the main uses of machine learning in AML compliance. In order to anticipate and identify unusual activity that might point to money laundering, machine learning algorithms are made to examine vast amounts of transaction data.

Financial institutions use static, rule-based detection techniques that depend on hardcoded criteria in traditional AML systems (e.g., a transaction above a specific monetary value). However, because these techniques are unable to take into consideration the subtleties of valid transactions, they frequently produce a significant percentage of false positives. In contrast, machine learning enables computers to recognize intricate and ever-changing patterns in human behavior. For instance, under normal circumstances, a customer's spending habits could seem completely normal, but machine learning algorithms are able to spot anomalies, like an abrupt spike in international transfers or a number of small-value transactions to high-risk locations.

Another effective machine learning tool for AML compliance is risk scoring. ML models may determine a risk score for every transaction or customer by taking into account a number of variables, including transaction history, geography, and known risk factors of the parties involved. By concentrating on higher-risk people or activities for additional research, this scoring system assists financial institutions in allocating resources. The predictive power of the system can be increased over time by retraining it to take into account fresh data. Machine learning is a vital technique for adjusting to changing money laundering strategies because of this dynamic learning process (Aidoo et al., 2025).

Apart from machine learning, deep learning models have demonstrated remarkable efficacy in detecting unusual patterns within extensive datasets. Deep learning is a kind of machine learning that models intricate correlations in data using multi-layered neural networks. This method helps systems identify more subtle irregularities in big datasets, which is especially helpful for handling the vast number and complexity of contemporary financial transactions. One strategy that includes finding uncommon patterns or outliers that vary from accepted standards is anomaly detection. Even with high financial transaction volumes, where conventional rule-based techniques could miss suspicious activity, deep learning algorithms are able to spot these outliers (Karolyi et al., 2025). A sudden increase in foreign wire transfers or odd activity in dormant accounts is an example of large-volume transactions that can be tracked and flagged in real-time using deep learning models if they diverge from the regular trends for a particular customer or account (Ruiz & Angelis, 2022). Additionally, by continuously learning from fresh transaction data, deep learning models can gradually enhance their detection capabilities. For example, previous money laundering patterns may cause a model to initially flag a high-value transaction as suspicious, but the model can be trained to modify its criteria over time to prevent false positives without compromising accuracy (Oyedokun et al., 2024). Deep learning is very helpful for identifying financial crime in intricate financial systems where high transaction volumes are typical because of its capacity to process and evaluate enormous volumes of data in real-time. Its capacity to spot concealed irregularities greatly enhances the efficacy and efficiency of AML compliance plans.

One strategy that includes finding uncommon patterns or outliers that vary from accepted standards is anomaly detection. Even with high financial transaction volumes, where conventional rule-based techniques could miss suspicious activity, deep learning algorithms are able to spot these outliers. Real-time monitoring and flagging of large-volume transactions that diverge from the usual trends for a particular customer or account, like an abrupt increase in foreign wire transfers or odd activity in dormant accounts, is possible with deep learning models.

The processing and analysis of financial intelligence is being completely transformed by large language models (LLMs) such as GPT-4 and BERT. These AI models are extremely beneficial in the context of financial crime detection and AML reporting because of their unparalleled capacity to comprehend, produce, and analyze human language. Large volumes of unstructured data are a major barrier in the AML domain, but LLMs are becoming more adept at processing them thanks to advanced Natural Language Processing (NLP). In order to detect suspicious activities, uncover hidden relationships, and identify emerging risks that traditional rule-based systems might miss, financial institutions and regulators are using LLMs to analyze sources like news articles, legal documents, social media feeds, and ultimate beneficial ownership (UBO) registries.

Several financial institutions and regulatory authorities have successfully used AI models to uncover Trade-Based Money Laundering (TBML) networks, a complicated type of money laundering that involves concealing illicit financial flows by

DOI: 10.55643/fcaptp.2.67.2026.5061

manipulating international trade transactions. AI technologies examine massive volumes of trade data, such as invoices, shipping documents, and customs declarations, for inconsistencies or patterns that may indicate money laundering activity. AI solutions are capable of detecting anomalies in trade documents. AI models trained on past trade data can detect irregularities such as over- or under-invoicing, misstatements of quantities, and fraudulent product descriptions—all of which are prevalent TBML methods. To detect suspect links, the algorithm compares this information to established trade routes, entities, and financial data (Kussainov et al., 2023). Furthermore, AI systems use predictive modeling to foresee potential TBML operations by identifying patterns in genuine trade and comparing them to previous instances of fraudulent transactions. This allows financial institutions to detect TBML in its early phases, preventing larger-scale criminal activity.

FinTech businesses and government agencies are already using advanced AI technology to improve AML compliance and combat financial fraud. This section presents relevant case studies and industry examples to demonstrate how AI is transforming the AML landscape across a variety of sectors, including large banks and FinTechs, government-private partnerships, and emergent concerns such as cryptocurrency transactions. Leading financial institutions, including HSBC and JPMorgan Chase, are using AI-powered AML systems to strengthen compliance operations, detect risks, and ensure real-time surveillance of financial activities. These applications demonstrate the considerable benefits that AI provides to traditional banking operations, allowing institutions to meet ever-increasing regulatory standards and manage risks more effectively.

HSBC, one of the world's top banking and financial services firms, has used powerful AI algorithms for real-time transaction monitoring and risk detection. The bank uses ML models to evaluate vast amounts of financial data, detecting suspicious activity and flagging transactions for further investigation. This method is intended to eliminate false positives, a common problem in traditional rule-based systems, while also improving the overall accuracy and efficiency of anti-money laundering activities. HSBC employs artificial intelligence to calculate risk rankings for transactions based on variables such as transaction size, region, and account holder behavior. These risk scores are linked to real-time warnings, allowing compliance officials to prioritize suspicious behaviors that may be related to money laundering or terrorist financing. HSBC's solution uses machine learning to drastically reduce false positives compared to rule-based systems, reducing the operational strain on compliance teams. As a result, the bank has improved detection accuracy while adhering to regulatory requirements (Gupta et al., 2023).

JPMorgan Chase, another global financial powerhouse, has also integrated AI into its AML framework. The bank's AI system combines real-time monitoring and behavioral analysis to detect abnormal transaction patterns that could signal money laundering. The use of deep learning and NLP also allows the bank to examine both structured and unstructured data (e.g., social media, news sources) for signals of illegal financial activity (Gupta et al., 2023). JPMorgan's AI-powered solution detects suspected money laundering operations by analyzing transaction data from many channels. It employs artificial intelligence to detect abnormalities or departures from expected transaction patterns, which may indicate fraudulent or criminal activity (Maidaniuk et al., 2025). The solution enables JPMorgan to comply with AML requirements while optimizing resource allocation and boosting detection capabilities. JPMorgan Chase also employs AI to generate SARs (Suspicious Activity Reports), which automates and improves regulatory compliance operations. The bank's solution is designed to adapt to changing compliance requirements and detect developing financial crime typologies that standard systems may miss.

One of the most promising applications is for Know Your Customer (KYC) and identity verification. Currently, each financial institution invests significant time and resources in KYC for each new customer, frequently duplicating efforts for the same individuals across institutions. Blockchain technology can offer a "KYC utility" in which customer identification information is confirmed once and securely shared or transferable to other institutions with the customer's permission. For example, a customer's self-sovereign digital identity could be documented on a blockchain (using Hyperledger Indy or Ethereum-based identity protocols). When they need to create a bank account, instead of submitting fresh paperwork, they allow the bank to access their digital identity record on the blockchain, which has verified qualities (Melnyk et al., 2022). The bank trusts the attestation on the ledger (which might be provided by a government agency or another trustworthy party) and onboards the customer more efficiently. This not only saves money, but it also has the potential to improve KYC because modifications (such as address or status changes) can be propagated to all permissioned institutions in real time.

The AnaMeen eKYC platform in Jordan, which is built on the Hyperledger Fabric-based Oracle Blockchain, serves as a practical example. AnaMeen offers KYC-as-a-Service to banks and telcos, allowing customer identities to be confirmed once and then shared. It allegedly lowered a 10-day account opening process to near-instant verification by utilizing an immutable ledger of identities. Customers can restrict access to their data via the blockchain's consent procedures, and each identity record is safe and time-stamped on the ledger. The end result is a more seamless customer experience and reduced duplication of compliance processes, all while protecting privacy through permissioned access (Shehadeh, 2025).

Similarly, in the UAE, regulators established the UAE KYC Blockchain Platform, a consortium that connects banks and government registries. When a corporate customer's license and KYC information are changed in the register, all member banks on the network observe the changes on the blockchain. This has accelerated corporate account opening and enhanced compliance because banks now have access to the most up-to-date verified data (such as beneficial ownership).

Individuals can also possess verifiable credentials (e.g., a digital passport, proof of funds source) and offer selective proofs of information utilizing blockchain self-sovereign identity (SSI) frameworks (such as those based on Hyperledger Indy or Ethereum's ERC-725 identity standard). For example, a zero-knowledge proof could allow a user to verify they are over 18 and not on any penalty list without disclosing their whole identity, balancing privacy and compliance. Thus, blockchain can update KYC by improving data integrity (a single tamper-proof customer record) and increasing privacy (customers contribute only what is necessary via cryptographic proofs). Many financial institutions and startups are testing such solutions, viewing KYC utilities as low-hanging fruit in which a shared ledger obviously outperforms each bank functioning independently (Rafiq & Sohail, 2025).

Traditional AML systems face significant challenges because they rely heavily on structured data such as transaction records or consumer account information. However, in modern financial systems, unstructured data, such as news articles, social media posts, public documents, and Ultimate Beneficial Ownership (UBO) registries, includes a large quantity of information. Traditional systems frequently struggle to extract significant insights from unstructured data, which can conceal key indicators of criminal activity. This is where Natural Language Processing (NLP) shows clear advantages. NLP allows machines to absorb and comprehend human language, which is critical when evaluating massive amounts of unstructured material. NLP algorithms can be used to search news sources, regulatory reports, and even social media platforms for mentions of possible money laundering operations or connections to criminal organizations (Mykolaichuk et al., 2025). For example, NLP can detect linguistic patterns associated with fraud, corruption, or terrorism, alerting compliance officers to the need for additional investigation.

Furthermore, NLP can be used to parse UBO registrations, which list the individuals who eventually own or control a corporation. By examining these registers alongside other data sources, NLP can assist in identifying concealed ownership structures and revealing the genuine controllers of shell businesses. The capacity to associate a UBO with several corporations or flagged entities improves the financial institution's ability to detect problematic networks (Aidoo et al., 2025).

One of the most important benefits of AI in AML compliance is its capacity to map complicated criminal networks using graph analytics and connection analysis. Money launderers frequently use sophisticated networks of transactions, shell businesses, and intermediaries to conceal the origin and destination of illicit payments. Traditional AML systems face a hurdle in detecting these businesses' concealed linkages.

Graph analytics solves this issue by representing entities (e.g., individuals, accounts, and businesses) as nodes and their relationships (e.g., transactions, ownership links) as edges within a graph structure. AI-powered graph algorithms examine these interactions to uncover complex networks of related entities, even if they appear unrelated in a linear transaction history. This allows investigators to find hidden links, such as those involving politically exposed individuals (PEPs), shell firms, and international criminal organizations, that would be difficult to detect using regular transaction monitoring alone. For example, a customer may seem to be conducting routine business, but graph analysis may show that they are sending money to a shell company that is registered in a high-risk jurisdiction or are connected to a network of people involved in a trade-based money laundering scheme (Ortina et al., 2023). Link analysis can also reveal odd trends in activity, including money flowing via several middlemen or circular transactions, which are popular methods for money laundering.

It should be mentioned that the implications of various blockchain designs for AML vary. Anyone can examine the chain's complete history thanks to "open auditability" offered by public blockchains like Ethereum. Law enforcement has previously taken advantage of this; for instance, in order to retrieve ransom payments from the 2021 Colonial Pipeline hack, investigators tracked down Bitcoin transactions, demonstrating that Bitcoin is "traceable by design" to those with the appropriate analytics. On Ethereum, companies such as Chainalysis or Elliptic support crypto AML efforts (e.g., detecting stolen assets traveling through DeFi) by using large-scale analytics to cluster addresses and identify possible illegal actors. On the other hand, public chains permit anonymity until users are deanonymized, which is typically accomplished through blockchain forensic research or exchanges that connect addresses to real-world identities. On the other hand, permissioned blockchains begin with known, verified participants (Piatnychuk et al., 2025). For example, a group of banks can create a Hyperledger Fabric network to exchange KYC information. These methods provide controlled privacy and performance at the expense of a public network's decentralization. Because permissioned networks may limit data access to approved compliance teams and adhere to privacy regulations while maintaining a single source of truth, they are appealing for interbank cooperation on compliance duties for AML purposes. In actuality, one might observe a hybrid strategy in which

DOI: 10.55643/fcaptp.2.67.2026.5061

public blockchain data (from Bitcoin, Ethereum, etc.) is regularly tracked and included into AML analytics, while private blockchain networks are utilized by regulated businesses to exchange information.

The characteristics of blockchain make it suitable for a wide range of applications in the fields of financial crime prevention and compliance. Here, we list a number of important application domains where blockchain (public and private) has the potential to improve or revolutionize AML/CFT initiatives, emphasizing the possible uses of Ethereum, Hyperledger Fabric, and other platforms.

Government-private collaborations are essential to the development of AI-powered AML compliance systems, in addition to private sector initiatives. The Financial Crimes Enforcement Network (FinCEN), which works with digital firms and financial institutions to promote innovation in AML detection and compliance, is one well-known example. In order to protect the financial system against illegal behavior, particularly money laundering and terrorist funding, the Financial Crimes Enforcement Network (FinCEN), a division of the U.S. Department of the Treasury, has implemented a number of programs and strategic initiatives known as the FinCEN initiative. The Bank Secrecy Act (BSA) and associated financial crime legislation are intended to be administered and enforced by these initiatives. In order to use cutting-edge technologies, such as artificial intelligence, to fight financial crime, FinCEN has been aggressively working with both FinTech businesses and traditional financial institutions (Kini et al., 2018). To promote the use of AI-based AML systems and solutions, the agency has started a number of innovation projects, such as sandbox programs for testing machine learning and artificial intelligence technologies. FinCEN collaborates with financial institutions to test innovative artificial intelligence (AI) tools that can enhance the identification of financial crime types and questionable transactions. These initiatives include establishing sandboxes in which organizations can test AI products in a controlled setting prior to full-scale implementation. FinCEN has collaborated with various AI-focused startups and technology companies to further the research and implementation of AI in financial crime detection (Global Financial Integrity, 2021). These collaborations seek to investigate how AI can be used to improve data analysis, transaction monitoring, and information sharing in order to detect illegal activity faster and more effectively.

DISCUSSION

Many researchers (Maleh et al., 2021; Mkhize et al., 2022; Gusrion et al., 2025) correctly point out that the convergence of artificial intelligence and blockchain technology is paving the way for improved security and predictive analytics capabilities. As blockchain networks evolve, they become more vulnerable, making AI integration a critical step in protecting these decentralized systems. AI's capacity to analyze massive amounts of data in real time enables proactive detection of risks and anomalies, hence improving blockchain security.

Meanwhile, two domains, purely 'corporate-nature' cybersecurity (that is, combating fraud and data leaks) and economic security as a crucial sub-system of national security, are usually considered in parallel, as two separate areas. This, to a large extent, prevents integral, synergetic use of advances in both areas and limits the scope of analysis. One of the bright examples is a monographic publication by Press (2024). The author claims that the various uses of AI illustrate its versatility and efficiency in safeguarding blockchain networks:

1. Financial organizations utilize AI to detect and prevent fraudulent transactions.
2. AI improves supply chain management by confirming product authenticity.
3. Healthcare businesses use AI for secure patient data management.
4. AI can monitor smart contracts to detect compliance and security issues.
5. Gaming platforms use AI to combat cheating and safeguard in-game transactions.

As it is evident from the above summary of the mentioned publication, no economic security domain elements are included in the scope.

There are also some industry-specific studies; for example, Talla (2022) considers integrating blockchain and AI to enhance supply chain transparency in the energy sector. Wang and Yu (2023) propose that the combination of artificial intelligence (AI) and blockchain technology (BT) can enable information sharing, risk sharing, data interaction, and other tasks in the logistics industry. The authors underline that smart contracts manage the distribution of duties across all roles in the supply chain, making it safer and more efficient.

ISSN: 2306-4994 | eISSN: 2310-8770 | Том 2 (67), 2026

On the other side, scholars investigate the role of AI and blockchain in cybersecurity from a 'macro'-perspective, that is, in AML and combating terrorism financing. In particular, Japinye (2025, p. 305) investigates "the integration of cybersecurity, artificial intelligence (AI), and blockchain technologies in mitigating money laundering and terrorism financing risks. [His] online survey was targeting 400 LinkedIn users with certifications or job roles in cybersecurity, compliance, AML, or counter- terrorist financing (CTF)."

In contrast, we suggest an integrative approach, combining these two domains, which would allow us to employ their findings and achievements within one ecosystem of AI and blockchain synergy for enhancing economic security through better financial control systems, from individual and corporate levels to the AML-CTF landscape.

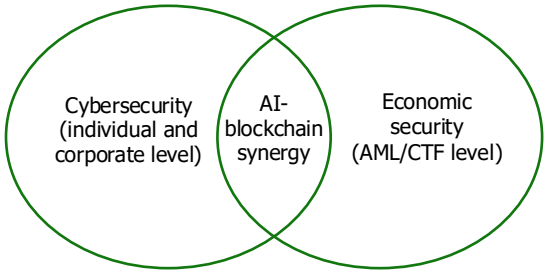

Figure 2. A two-domain ecosystem of AI and blockchain technologies in synergy for enhancing the financial control landscape.

Researchers currently highlight a specific observed trend: the blurring of lines between money laundering and financial fraud (Bartulovic et al., 2023). Criminals accomplish this by devising methods in which fraudulent activities generate money that is then laundered through intricate financial channels. They take advantage of the silos in financial ecosystems. A common example is that compliance teams focus solely on AML, whereas risk teams focus solely on fraud. Criminals have invented means for moving money that avoid discovery by either group alone. For example, stolen payments from phishing assaults may be routed through mule accounts or shell corporations to conceal their origin. It is more difficult to identify and stop fraud and money laundering when there is a lack of integrated monitoring and intelligence sharing, which lets suspicious transactions get through the cracks. Therefore, in financial institutions, the convergence of these two roles is essential. Although regulatory technology (RegTech) automates compliance chores and changes protocols dynamically as regulations change, a coordinated strategy can yield truly substantial benefits and "outperform" criminals' technological achievements in the financial domain.

In keeping with this, Shi and Wang's systematic review from 2025 should be included. The authors examine the advantages, difficulties, and potential paths of blockchain-AI applications in financial services in their study of more than 100 peer-reviewed publications that were published between 2020 and 2024. The results show that AI powers predictive analytics, automation, and decision-making effectiveness, while blockchain improves data quality, security, and transparency. These clauses align with our suggested methodology.

Transparency, accountability, and traceability are some of the fundamental tenets of national security and economic integrity that blockchain supports. Its use within AML frameworks could reduce compliance costs while improving the speed, precision, and scope of financial investigations. Additionally, by facilitating anomaly identification and predictive analytics using integrated, high-quality data sets, blockchain could assist in moving AML operations from reactive to proactive.

From a geopolitical perspective, counterterrorism, the enforcement of sanctions, and the protection of democratic institutions are all becoming more and more linked to the capacity to track down illegal financial flows. Sophisticated money laundering networks are used by terrorist organizations, rogue nations, and transnational criminal organizations to finance operations that jeopardize international security (Stoliarenko et al., 2025). Blockchain has the potential to be a key instrument in thwarting these dangers by improving data exchange between financial institutions and governments and producing tamper-proof ledgers.

Simultaneously, FinTech and RegTech discourse is frequently described as having a shallow perspective. For instance, according to Samuel (2025), the fintech industry is undergoing a transformation as a result of the combination of blockchain technology and artificial intelligence, ushering in a new era characterized by increased security, efficiency, and innovation. The article highlights how blockchain's decentralized ledger ensures transactions are transparent and unchangeable, reducing fraud and fostering user confidence. Simultaneously, AI provides advanced automation, machine learning, and data analysis that improve decision-making, customize financial services, and give predictive capabilities. The study claims that when taken as a whole, these solutions address significant fintech issues such as transaction management complexity,

DOI: 10.55643/fcaptp.2.67.2026.5061

cybersecurity threats, and regulatory compliance (Sydorchuk et al., 2024). For example, blockchain guarantees a secure framework for AI applications with trustworthy data, and AI may examine blockchain data to spot fraud in real time.

In line with this view, Paul and Ogburie (2025) claim that AI-driven automation reduces operational costs for financial institutions while improving strategies of risk management. The authors emphasize that, in spite of its advantages, using AI to combat financial fraud has drawbacks, including potential biases in algorithmic decision-making, ethical issues, and data privacy issues.

Yet, there is emerging concern among the scientific and regulatory community that a deeper and more multifaceted approach is needed to successfully combat ever-emerging and sophisticated threats. Specifically, Moura et al. (2025) found that three key themes surfaced: big data analytics, blockchain and fintech integration, and AI-based fraud detection models. The yearly distribution of publications is shown in Figure 3, which shows an average growth rate of 23.11%. The results show that since 2021, there has been a notable increase in research on the use of AI and ML in financial fraud prevention. This is consistent with recent research highlighting the quickening pace of AI applications in finance during the digital shift following the pandemic. The authors correctly point out that there is still a lack of international cooperation and attention to organizational, ethical, and regulatory concerns despite increasing output.

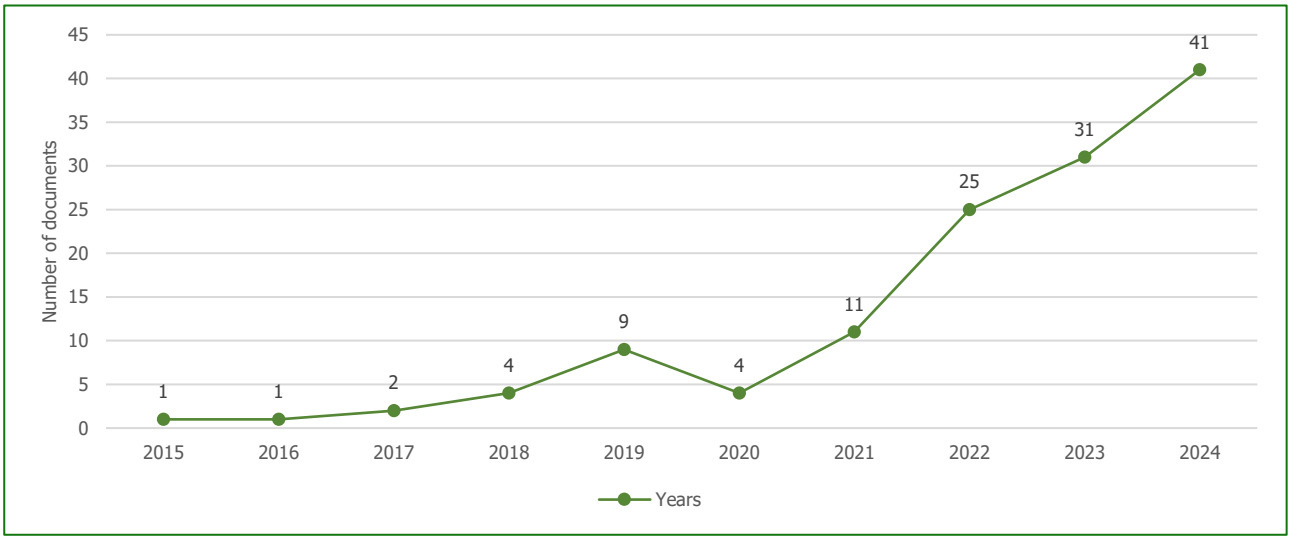

Figure 3. Financial Fraud, AI, and ML in literature growth. *(Source: Moura et al. (2025))*

To better demonstrate blockchain's importance, let us see how features of its potential in the field of economic security through enhancing financial control systems correspond to the challenges:

1. Data silos and inconsistencies: A blockchain can serve as a common data layer that many stakeholders (banks, regulators, and auditors) can access. Instead of each institution keeping separate records that must be reconciled, a consortium blockchain may house a shared KYC registry or a real-time ledger of member transactions. This assures that all participants receive the same information (a single source of truth), which improves consistency. It also reduces redundancy; for example, if one bank completes KYC for a customer and registers it on-chain, another bank can use that record (with the required permissions) instead of duplicating the process. In other words, blockchain can improve the interoperability of compliance data across organizations and countries.
2. Record integrity and auditability: Immutability ensures that an auditable trail is produced automatically. All modifications are documented and time-stamped. This might make compliance audits simpler for regulators because some necessary documents might be on a tamper-proof ledger that examiners can access rather than having to sift through a bank's internal records. If an alarm was examined or a judgment was made, the supporting documentation and reasoning might be hashed onto a blockchain for future use, guaranteeing responsibility in terms of internal compliance. If, for example, lists of sanctioned addresses and the blocks of transactions affecting them are preserved immutably, authorities may feel more confident in the integrity of the data in crucial areas like sanctions compliance.

3. Efficiency through automation: Regular compliance checks can be automated with smart contracts. For instance, a smart contract might be set up to prevent token transfers unless the sender and recipient addresses have been added to a whitelist via a KYC procedure. This is comparable to incorporating a KYC rule into the transaction layer. In a similar vein, a smart contract might, when specific conditions are satisfied, automatically divide a big transaction into a report (such as creating a CTR or SAR) and transmit it to regulators instantly. Human analysts may be relieved of monotonous work by such automation. Once configured, smart contracts can manage functions like transaction monitoring, client due diligence, and reporting automatically, reducing the need for manual intervention and minimizing human errors. This speeds up the process and may identify problems that a manual approach may overlook or postpone.
4. Reducing false positives with better data: By offering deeper context, blockchain's transparency and data-sharing can also aid in lowering false positives in monitoring. A more comprehensive risk assessment would be possible in a blockchain-based network if several institutions shared data about a customer's behavior (within the law). Instead of each bank treating a customer separately, for instance, if one bank has bad information about them (such as a fraud red flag), other banks may be able to use that knowledge to adjust their monitoring criteria. Furthermore, warnings can be more focused because of blockchain's capacity to capture extra metadata and even analytical insights on transactions. In contrast to discrete rule triggers, advanced analytics implemented on top of a rich, shared dataset can more successfully discover truly suspicious patterns (behavioral abnormalities, relationship networks). Essentially, a shared ledger improves data completeness and quality, which can increase the accuracy of detection algorithms and, ideally, result in fewer false positives and more true alarms.
5. Real-time response and monitoring: Conventional AML systems typically process transactions in daily batches, reviewing them after the fact. Because blockchain transactions spread immediately throughout the network and can instantaneously initiate intelligent compliance checks, it can facilitate real-time monitoring. This implies that possible questionable activities could be immediately identified and perhaps halted. For example, a compliance-integrated blockchain system may immediately halt or isolate transactions from a known blacklisted address (for example, linked to ransomware payments or sanctioned businesses). Experts point to blockchain's "real-time monitoring and rapid detection" capabilities as a plus, pointing out that ongoing examination of an unchangeable stream of transactions can "flag any suspicious behavior for further investigation" considerably more quickly. Additionally, regulators could get real-time updates or even act as a node to monitor behavior in real time (with the proper privacy protections in place).
6. Improved cooperation: An ecology of cooperative compliance can be fostered via blockchain networks. Permissioned blockchain consortia for AML might be formed by banks, payment businesses, fintechs, and regulators, who would then contribute and use the shared intelligence. Participants build a collective defense by safely exchanging information on verified harmful individuals, typologies, or illegal addresses. As a collaborative network enables several institutions to collaboratively detect patterns that any one institution might not perceive, this collaboration is frequently recognized as one of the most potent benefits. It breaks down silos and enables a more comprehensive view of potential hazards. In essence, blockchain might serve as the technological foundation for AML services (such as transaction monitoring or KYC services) that governments and business associations have long aimed to develop.

Predominantly, stakeholders' perspectives are not covered in studies devoted to AI and blockchain integration within RegTech. Meanwhile, successful ethical, legal, and governance frameworks necessitate clearly defined roles among stakeholder groups:

1. Regulators must develop adaptable, technology-informed policies that protect privacy and rights while allowing AML objectives, as well as providing guidance on the use of AI and blockchain.
2. Developers are responsible for creating systems that incorporate privacy, security, fairness, and transparency from the start, as well as for ongoing model validation and risk mitigation efforts.
3. Financial institutions and VASPs must establish strong compliance controls, provide staff training, and actively participate in information exchange and public-private partnerships.
4. Users are responsible for understanding the privacy consequences, adhering to AML regulations, and reporting suspicious activity.

These parties' cooperation would support reliable and efficient AI-blockchain AML environments. Furthermore, design thinking is an essential paradigm in RegTech since it offers an iterative, human-centered approach to creating compliance solutions that are efficient, effective, and easy to use (Ononiwu et al., 2025). This assertion is consistent with our findings.

DOI: 10.55643/fcaptp.2.67.2026.5061

Design thinking aids in bridging the gap between intricate legal requirements and useful, adoptable technology by giving priority to user experience (UX) and real-world pain points. "RegTech is the new FinTech", as Deloitte experts correctly noted in 2015 (Deloitte, 2015). According to IMARC Group research, RegTech-as-a-Service (RaaS) is a game-changer as regulatory complexity increases. The global RegTech market is predicted to grow at an 18% CAGR from USD 15.8 billion to USD 70.8 billion by 2033 (*Is RegTech-as-a-Service the future of agile compliance?* 2025). This paradigm redefines the future of agile compliance by leveraging AI, cloud computing, and automation to provide scalable, real-time compliance solutions that reduce costs and increase agility for financial institutions.

Meanwhile, major technical obstacles prevent widespread deployment of blockchain and AI integration for AML, despite the technology's potential. Scalability is still a major issue since blockchain networks, particularly public ones, frequently have throughput restrictions that limit the number of transactions that can be processed and examined in real time. For AI models, especially deep learning architectures, to remain accurate and responsive at scale, significant processing power and high-quality data inputs are required.

The fragmented nature of blockchain protocols, different data formats, and disparate AML systems across organizations and jurisdictions provide interoperability issues. Smooth data interchange and cooperative AML monitoring are still unattainable without standardized interfaces and communication protocols.

Development and implementation are made more difficult by the lack of generally recognized guidelines for combining blockchain technology and artificial intelligence in AML compliance. To guarantee system compatibility, lower integration costs, and foster stakeholder trust, industry-wide agreement on best practices, data schemas, and compliance benchmarks is crucial.

Furthermore, implementing AI-blockchain AML solutions may present significant organizational challenges for institutions. These technologies are highly specialized, requiring individuals with expertise in blockchain development, machine learning, cryptography, and regulatory compliance - skills that are in great demand and hard to come by. Building capacity through hiring and training is crucial, but it takes a lot of resources (Yermachenko et al., 2023). Additionally, change management is extremely difficult; old systems and established compliance routines need to be modified or redesigned, which frequently encounters internal resistance from employees who are apprehensive about new technologies or worried about their job security. To promote corporate buy-in and seamless transitions, leadership must encourage a culture of innovation and ongoing learning while highlighting the strategic benefit of AI-blockchain convergence for AML effectiveness.

Nevertheless, in conclusion, blockchain technology offers the means to rethink AML compliance in a more automated, transparent, and integrated manner, provided that significant efforts are made to overcome the aforementioned issues. But it's important to keep in mind that it's not "a magic bullet." Blockchain implementation presents a unique set of difficulties in the highly regulated and delicate world of financial compliance (Zaporozhets et al., 2024). However, the effects of AML breakthroughs driven by AI go much beyond financial institutions. The expanded implementation of these technologies benefits numerous industries, each contributing to the national interest (Table 2).

Table 2. Systemic benefits of blockchain and AI solution in financial control and AML: synergy points. *(Source: Gupta et al., 2023)*

Domain	Implication
Financial Sector	The stability and security of financial markets are ensured by AI-driven AML systems, which give the financial industry strong instruments to identify and stop financial crimes. Financial institutions can increase their effectiveness in avoiding financial system abuse by enhancing adherence to AML requirements and cutting operating expenses related to manual investigations and false positives. AI has a significant impact on the financial sector because it creates a system that is more reliable, transparent, and safe.
Defense and National Security	By monitoring illegal financial flows connected to organized crime, terrorism, and arms trafficking, AI-powered AML systems improve national security. AI gives law enforcement and intelligence organizations the ability to follow, intercept, and stop financial transactions that are frequently used to finance disruptive activities. The military industry is directly and permanently impacted by the ability to track down funding for terrorist groups, cyberattacks, or criminal syndicates. AI in AML is a vital weapon for military and intelligence organizations by stopping the funding of attacks or destabilizing operations.
Cybersecurity	Cybersecurity has grown to be a major worry as financial systems become more linked and dependent on digital platforms. AI-powered AML solutions assist in detecting the flow of illegal funds through digital wallets and cryptocurrencies, as well as identifying cyberthreats directed at financial institutions. Artificial intelligence (AI) tools can defend financial systems against cybercrime by offering real-time monitoring and sophisticated anomaly detection, protecting everything from individual accounts to vital financial infrastructure.
Regulatory Agencies	Artificial intelligence tools facilitate the quicker and more precise detection of possible financial crimes at the regulatory level, increasing the effectiveness of government oversight organizations such as OFAC and FinCEN. Regulatory agencies can take prompt action to stop fraud, money laundering, and other unlawful acts thanks to the real-time

	detection of suspicious activity. Additionally, AI fosters greater economic stability by relieving financial institutions of the burden of compliance, which benefits the entire country.

Although there is a lot of promise in the combination of blockchain and AI technology, there are also substantial obstacles to overcome, including those pertaining to interoperability, scalability, ethical AI governance, and regulatory compliance. There are currently several important research gaps, such as the absence of established regulatory frameworks, a dearth of real-world case studies, and technical integration hurdles. A thorough theoretical framework that connects technology developments to ethical and regulatory issues is required to close these gaps.

Legislative matters are also quite important. Data protection legislation, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the EU, places stringent requirements on the gathering, handling, and archiving of personal information. These rules place a strong emphasis on concepts like user permission, purpose limitation, data minimization, and the right to be forgotten (Zayats et al., 2025). Because blockchain's immutability naturally clashes with data deletion regulations, AML solutions that include AI and blockchain must carefully manage these requirements. Adopting privacy-by-design principles, making sure that only pertinent data is stored on-chain, and utilizing off-chain storage for personal data that is subject to change or deletion are all important when designing AML solutions that adhere to the CCPA and GDPR. Furthermore, because blockchain networks are decentralized and worldwide, adherence to cross-border data transfer regulations is essential.

CONCLUSIONS

The conducted integrative review demonstrated that for now, scholarly investigations within the field of AI and blockchain potential for financial control systems are carried out in parallel in two actually separate domains – purely cybersecurity' one (mostly cybersecurity at the corporate level) and AML\CTF one (that is, national security). Meanwhile, economic security in its essence represents indivisible unity of these two domains, and, thus, application of AI and blockchain, with the appropriate experience, practices, challenges, and prospects should be considered within the single ecosystem combining "corporate" and national security levels.

A complex strategy that strikes a compromise between strict AML/CFT compliance and the need for broader financial inclusion is needed to counter the growing threat of financial crime. The current issues, which range from antiquated risk assessment frameworks and manual compliance procedures to the abuse of cutting-edge technologies like artificial intelligence and cryptocurrency, highlight the need for thorough and situation-specific solutions. Cutting-edge technologies like FinTech, RegTech, and SupTech are giving regulators and financial institutions new ways to reduce compliance expenses without unintentionally leaving out disadvantaged groups. Additionally, it is imperative that international guidelines , especially those issued by the FATF, be improved in order to better link inclusive growth with financial integrity by offering more proportionate measures and clearer risk-based methods. The region can guarantee that the digital transformation of financial services becomes a potent tool for financial inclusion while protecting against the changing landscape of financial crime by encouraging closer cooperation between regulators, technologists, and financial institutions and directing a concentrated effort towards clear policy direction.

To overcome the barriers described in the paper, regulatory sandboxes offer controlled environments where fintech firms, financial institutions, and regulators can collaboratively test AI-blockchain AML innovations under relaxed compliance conditions. Such sandboxes enable real-world experimentation, risk assessment, and iterative refinement without compromising financial system integrity. Pilot projects involving public-private partnerships further support technology validation and stakeholder alignment. Cross-sector collaboration among regulators, technology providers, financial institutions, and academia is crucial to share knowledge, develop standards, and accelerate best practice adoption.

Our review, in contrast to previous studies, combines and integrates 'micro' (individual and corporate) and 'macro' (AML-CFT and economic national security) perspectives of AI and blockchain use in financial control systems (RegTech). It is expedient to continue these vectors of research in further studies.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

DOI: 10.55643/fcaptp.2.67.2026.5061

FUNDING

The Authors received no funding for this research.

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Aidoo, S., Venditi, A., Dohner, H., Liang, W., Peterson, B., & Hamzah, F. (2025). The Role of Blockchain in AML Compliance: Potential Applications and Limitations. *The Journal of Anti Money Laundering and Countering the Financing of Terrorism*. https://www.researchgate.net/publication/393091361_The_Role_of_Blockchain_in_AML_Compliance_Potential_Applications_and_Limitations
2. Armstrong, D., Hyde, D., & Thomas, S. (2023). *Blockchain and Cryptocurrency: International Legal and Regulatory Challenges*. Bloomsbury Professional.
3. Bartulovic, M., Aljinovic, N., & Piplica, D. (2023). Determining the Relationship Between Corruption and Money Laundering. *Montenegrin Journal of Economics, 19*(2), 109-118. https://doi.org/10.14254/1800-5845/2023.19-2.9
4. Bashtannyk, O., Zayats, D., & Hudenko, B. (2025). Innovative Human Capital Management Practices In The Security And Defense Sector: Challenges For Public Management. *TPM - Testing, Psychometrics, Methodology in Applied Psychology, 32*(S1), 556 – 566. https://doi.org/10.5281/zenodo.16914238
5. Bolton, M., & Mintrom, M. (2023). RegTech and creating public value: opportunities and challenges. *Policy Design and Practice, 6*(3), 1-17. https://doi.org/10.1080/25741292.2023.2213059?urlappend=%3Futm_source%3Dresearchgate
6. Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. *Journal of Information Technology Management*, *14*, 1-24. https://doi.org/10.22059/jitm.2022.88861
7. Cassara, J., & Poncy, Ch. (2015). *Trade-Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*. Wiley.
8. Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks*, *2018*(1), 5483472. https://doi.org/10.1155/2018/5483472
9. Deloitte (2015). *RegTech is The New FinTech How Agile Regulatory Technology Is Helping Firms Better Understand and Manage Their Risks*. https://www.gaco.gi/images/pdf/2017-june/ie-regtech-pdf.pdf
10. Desi, A., Akintoye, R. I., & Aguguom, T. A. (2023). Forensic accounting, a veritable financial tool for qualitative financial reporting systems in the 21st century. *International Journal of Professional Business Review, 8*(6), 1-30. https://doi.org/10.26668/businessreview/2023.v8i6.2342
11. Ghose, P., Parvin, M., Akter, S., Rakib, Sh., & Bhuiyan, M. (2025). Gravitating towards technology-based emerging financial crime: A PRISMA-based systematic review. *International Journal of Innovative Research and Scientific Studies, 8*(2), 3387-3402. https://doi.org/10.53894/ijirss.v8i2.6014
12. Global Financial Integrity (2021). *Enhancing National Security by Re-imagining FinCEN*. Global Financial Integrity. https://gfintegrity.org/wp-content/uploads/2021/02/FinCEN-Paper.pdf
13. Gupta, A., Dwivedi, D., & Shah, J. (2023). *Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance (Future of Business and Finance).* Springer.
14. Gusrion, D., Firdalius, F., & Rahmawati, E. (2025). Exploring the Synergy Between Artificial Intelligence and Blockchain in Enhancing Cybersecurity Solutions. *Journal of Engineering, Electrical and Informatics, 5*(3), 20–28. https://doi.org/10.55606/jeei.v5i3.5567
15. Han, L. (2015). Integrating blockchain and AI in financial systems: A case study on cross-border payments and high-frequency trading synergies. *Journal of Latex Class Files, 14*(8), 1-4. https://doi.org/10.31219/osf.io/2mn3f_v1
16. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, *193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429
17. Hrytsenko, L., Zakharkin, O., Zakharkina, L., Hedegaard, M., Kuznyetsova, A., & Novikova, L. (2024). Assessment Of The Level Of Information Transparency Of Banks. *Financial and Credit Activity Problems of Theory and Practice*, *6*(59), 60–75. https://doi.org/10.55643/fcaptp.6.59.2024.4619
18. Hunter, Sh., Johnson, Th., Chai, A., & de Koker, L. (2025). Navigating the nexus of financial crime prevention and financial inclusion in the age of technology and Fintech. *Asian Development Bank Institute, Policy Brief, 11.* https://www.adb.org/sites/default/files/publication/1054521/adbi-navigating-nexus-financial-crime-prevention-and-financial-inclusion-age-technology-and-fintech.pdf
19. Idris, F., Latif, Y., & Purnamasari, P. (2025). Early detection and prevention of skimming in digital financial systems: A forensic accounting approach in the era of technological transformation. *Inovasi: Jurnal Sosial Humaniora dan Pendidikan, 4*(3), 539-547. https://doi.org/10.55606/inovasi.v4i2.4530

20. Is RegTech-as-a-Service the future of agile compliance? (2025, September 4). Global RegTech Summit. https://fintech.global/globalregtechsummit/is-regtech-as-a-service-the-future-of-agile-compliance/

21. Jain, D. (2024). *AI for AML*. Grin Verlag.

22. Japinye, A. (2025). The Inter-Role of Cybersecurity, AI and Blockchain in Preventing Money Laundering and Terrorism Financing. *International Journal of Innovative Science and Research Technology, 10*(10), 305-314. https://doi.org/10.38124/ijisrt/25oct127

23. Jo, H., Bui, H., & Moreland, D. (2025). The Role of AI in Fraud Detection: Are financial institutions using the most effective systems? *Journal of Finance Issues, 23*(2). https://doi.org/10.58886/jfi.v23i2.10086

24. Karolyi, H., Mishchuk, H. Y., & Karpa, M. I. (2025). Military Migration and Demographic Transformations in Ukraine: Military Consequences for Territorial Communities. *Ukrainian Geographical Journal*, *3*(131), 75–86. https://doi.org/10.15407/ugz2025.03.075

25. Kini, S., Dura, R., & Acosta-Grimes, Z. (2018). FinCEN issues long-awaited guidance on the customer due diligence rule. *Journal of Investment Compliance, 19*(4). https://doi.org/10.1108/JOIC-06-2018-0044?urlappend=%3Futm_source%3Dresearchgate

26. Konstantinidis, G., & Gegov, A. (2024). Deep Neural Networks for Anti Money Laundering using Explainable Artificial Intelligence. In *Proceedings of 2024 IEEE 12th International Conference on Intelligent Systems (IS).* https://doi.org/10.1109/IS61756.2024.10705194

27. Kumar, G. (2025). Blockchain-Based Fraud Detection and Prevention System Enhanced with AI. *International Journal for Research in Applied Science and Engineering Technology, 13*(9), 538-544. https://doi.org/10.22214/ijraset.2025.73998

28. Kussainov, K., Goncharuk, N., Prokopenko, L., Pershko, L., & Vyshnivska, B. (2023). Anti-corruption management mechanisms and the construction of a security landscape in the financial sector of the EU economic system against the background of challenges to european integration: Implications for artificial intelligence technologies. *Economic Affairs (New Delhi)*, *68*(1), 509-521. https://doi.org/10.46852/0424-2513.1.2023.20

29. Maidaniuk, S., Petrukha, N., & Makarevych, O. (2025). Circular Economic Concept: Contribution to Macroeconomic Growth. *International Journal of Ecosystems and Ecology Science, 15*(3), 127-136. https://doi.org/10.31407/ijees15.317

30. Melnyk, D. S., Parfylo, O. A., Butenko, O. V., Tykhonova, O. V., & Zarosylo, V. O. (2022). Practice of the member states of the european union in the field of anti-corruption regulation. *Journal of Financial Crime*, *29*(3), 853-863. https://doi.org/10.1108/JFC-03-2021-0050

31. Mkhize, S., Nkosii, A., Dlamini, Th., Motsoeneng, L., Smith, A., & Thulare, K. (2022). Integrating Blockchain and Artificial Intelligence for Enhanced Transparency, Security, and Efficiency in E-Commerce Supply Chains: Applications, Challenges, and Future Directions. *Journal of Empirical Social Science Studies*. https://www.researchgate.net/publication/386907924_Integrating_Blockchain_and_Artificial_Intelligence_for_Enhanced_Transparency_Security_and_Efficiency_in_E-Commerce_Supply_Chains_Applications_Challenges_and_Future_Directions

32. Moreno, S., Seigneur, J.-M., & Gotzev, G. (2021). A Survey of KYC/AML for Cryptocurrencies Transactions. In: Cruz-Cunha, M.M., ed. *Handbook of research on cyber crime and information privacy*. Hershey: Information Sci Refer IGI.

33. Moura, L., Barcaui, A., & Payer, R. (2025). AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens. *Journal of Risk and Financial Management, 18*(6), 323. https://doi.org/10.3390/jrfm18060323

34. Mykolaichuk, M., Pozniakovska, N., & Hudenko, B. (2025). Conceptual principles of analysis and forecasting threats to national security in modern conditions. *Sapienza: International Journal of Interdisciplinary Studies,* 6(2), e25029. https://doi.org/10.51798/sijis.v6i2.985

35. Nita, B. (2025). Blockchain Technology in Anti-Money Laundering: Challenges and Opportunities in the V4 Countries and Ukraine. In: M. Balytska, H. Bohušová, & P. Luty (Eds.), *The V4 and Ukraine. Fight with Tax Fraud and Money Laundering* (pp. 29-48). Publishing House of Wroclaw University of Economics and Business. https://doi.org/10.15611/2025.32.0.03

36. Oermann, M., & Knaff, K. (2021). Strategies for completing a successful integrative review. *Nurse Author & Editor, 31*(3-4), 65-68. https://doi.org/10.1111/nae2.30

37. Ononiwu, M., Azonuche, T., Enyejo, E., & Onum, F. (2025). Integrating Agile and Design Thinking with Secure Devsecops for Innovation Acceleration in Fintech Api-Driven Startups. *Malaysian E Commerce Journal, 9*(2), 53-62. https://doi.org/10.26480/mecj.02.2025.53.62

38. Ortina, G., Zayats, D., & Karpa, M. (2023). Economic Efficiency of Public Administration in the Field of Digital Development. *Economic Affairs (New Delhi), 68*(3), 1543-1553. https://doi.org/10.46852/0424-2513.3.2023.21

39. Otoritas Jasa Keuangan. (2022). Annual Report of the Financial Services Authority (OJK) 2022. Jakarta: OJK. https://www.ojk.go.id/id/data-dan-statistik/laporan-ta-hunan/Documents/Laporan%20Ta-hunan%20OJK%202022.pdf

40. Oyedokun, O., Ewim, S., & Peter, O. (2024). A Comprehensive Review of Machine Learning Applications in AML Transaction Monitoring. *International Journal Of Engineering Research And Development, 20*(11), 730-743. https://www.researchgate.net/publication/388277251_A_Comprehensive_Review_of_Machine_Learning_Applications_in_AML_Transaction_Monitoring

41. Page, M. J., McKenzie, J. E., Bossuyt, P. M. et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*. https://doi.org/10.1136/bmj.n71

DOI: 10.55643/fcaptp.2.67.2026.5061

42. Paul, A., & Ogburie, Ch. (2025). The Role of AI in preventing financial fraud and enhancing compliance. *GSC Advanced Research and Reviews, 22*(03), 269-282. https://doi.org/10.30574/gscarr.2025.22.3.0086

43. Piatnychuk, I., Serhieiev, V., Bashynskyi, I., & Radchenko, R. (2025). Competences Of Public Administration Leaders In The Face Of Threats To National Security: Strategic Development Guidelines. *TPM - Testing, Psychometrics, Methodology in Applied Psychology, 32*(S1), 340 – 349. https://doi.org/10.5281/zenodo.17295047

44. Pocher, N., Zichich, M., & Ferretti, S. (2022). AML/CFT/CPF Endeavors in the Crypto-space: From Blockchain Analytics to Machine Learning. In *Proceedings of Artificial Intelligence Governance Ethics and Law (AIGEL),* Reviewed, Selected Papers. November 02 - December 19, 2022, Barcelona, Spain, pp. 140-149. https://ceur-ws.org/Vol-3531/SPaper_11.pdf

45. Press, R. (2024). *Securing the future: AI and blockchain technology for enhanced data security and privacy*. Grin Verlag.

46. Quick, D., & Choo, K.-K. (2018). *Big Digital Forensic Data: Volume 1: Data Reduction Framework and Selective Imaging*. Springer.

47. Rafiq, M., & Sohail, M. (2025). Adopting regulatory technology for anti-money laundering in banking: Key enablers and barriers in a RegTech model. *Sustainable Futures, 10*, 101377. https://doi.org/10.1016/j.sftr.2025.101377

48. Rane, N., Choudhary, S., & Rane, J. (2023). Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. *SSRN*. https://dx.doi.org/10.2139/ssrn.4644253

49. Rodríguez Valencia, L., Ochoa Arellano, M. J., Gutiérrez Figueroa, S. A., Mur Nuño, C., Monsalve Piqueras, B., Corrales Paredes, A. d. V., Bemposta Rosende, S., López López, J. M., Puertas Sanz, E., & Levi Alfaroviz, A. (2025). A systematic review of artificial intelligence applied to compliance: Fraud detection in cryptocurrency transactions. *Journal of Risk and Financial Management, 18*(11), 612. https://doi.org/10.3390/jrfm18110612

50. Rogers, S. (2024, October 27). New GASA report estimates $688 billion in scam losses across Asia amid rising cyber-threat worldwide. *Global Anti-Scam Alliance*. https://www.gasa.org/post/2024-asia-scam-report-688-billion-lost

51. Ruiz, E., & Angelis, J. (2022). Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges. *Journal of Money Laundering Control, 25*(4), 766-778. http://dx.doi.org/10.1108/JMLC-09-2021-0106

52. Samuel, K. (2025). Block chain and AI Convergence in Financial Technology: A WASPAS-Based Analysis. *International Journal of Cloud Computing and Supply Chain Management, 1*(3), 1-6. https://doi.org/10.55124/ijccscm.v1i3.247

53. Shehadeh, M. (2025). Disclosures on digital transformation strategy and financial technology in Jordanian banks: innovations, challenges and opportunities. *Journal of Financial Reporting and Accounting*. https://doi.org/10.1108/JFRA-12-2024-0972

54. Shi, J., & Wang, Y. (2025). Academic exploration of blockchain and AI in financial services. *Journal of Electronic Business & Digital Economics*. https://doi.org/10.1108/JEBDE-08-2024-0023

55. Spyra, M., Balina, R., Idasz-Balina, M., Zając, A., & Różyński, F. (2025). Cryptocurrencies as a Tool for Money Laundering: Risk Assessment and Perception of Threats Based on Empirical Research. *Risks, 13*(10), 189. https://doi.org/10.3390/risks13100189

56. Stoliarenko, O., Ortina, G., Stuzhuk, R. Plakhotnii, D. (2025). Natural Resources and Financial Security: The Synergy of Sustainable Development Economics and Artificial Intelligence. *Grassroots Journal of Natural Resources, 8*(2), 775-795. https://doi.org/10.33002/nr2581.6853.080236

57. Sydorchuk, O., Kharechko, D., Kozarevych, N., & Khomenko, H. (2024). Competencies for sustainable financial and economic management: Their impact on human capital development and national security. *Edelweiss Applied Science and Technology, 8*(6), 1445–1454. https://doi.org/10.55214/25768484.v8i6.2261

58. Talla, R. (2022). Integrating Blockchain and AI to Enhance Supply Chain Transparency in Energy Sectors. *Asia Pacific Journal of Energy and Environment, 9*(2), 109-118. https://doi.org/10.18034/apjee.v9i2.782

59. Von Hafe, F., Wagle, Y., Guede-Fernández, F., Giordano, A.P., Silva, L., & Azevedo, S. (2025). Legal frameworks for blockchain applications: A comparative study with implications for innovation in Europe*. Frontiers in Blockchain, 8,* 1655230. https://doi.org/10.3389/fbloc.2025.1655230

60. Wang, D., & Yu, A. (2023). *Supply Chain Resources and Economic Security Based on Artificial Intelligence and Blockchain Multi-Channel Technology*. IGI Global.

61. Yermachenko, V., Bondarenko, D., Karpa, M., & Kalashnyk, N. (2023). Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects. *Economic Affairs (New Delhi), 68*(1), 617-633. https://doi.org/10.46852/0424-2513.1.2023.29

62. Zaporozhets, T., Khomiuk, N., Niema, O., Domsha, O., & Serhieiev, V. (2024). Innovative competences in public administration: The path to sustainable development, financial efficiency and strengthening of national security. *Edelweiss Applied Science and Technology*, *8*(6), 1421–1429. https://doi.org/10.55214/25768484.v8i6.2258

63. Zayats, D., Akimova, L., & Bashtannyk, O. (2025). Innovative Human Capital Management Practices In The Srcurity And Defense Sector: Challenges For Public Management. *TPM – Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S1 (2025): Posted 12 May), 556–567. https://doi.org/10.5281/zenodo.16914238

Муханбеталі Б., Ганущин С., Халімон Т., Халімон С., Акімова Л., Акімов О.

БЛОКЧЕЙН І ШТУЧНИЙ ІНТЕЛЕКТ У СИСТЕМАХ ФІНАНСОВОГО КОНТРОЛЮ: СИНЕРГІЯ ІННОВАЦІЙ ДЛЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Зростання складності глобальних фінансових систем зумовило необхідність упровадження більш ефективних і прозорих механізмів боротьби з відмиванням грошей (AML). Технологія блокчейн із її децентралізованими, незмінними та прозорими характеристиками є перспективним рішенням для подолання обмежень традиційних систем AML. У цій роботі досліджено потенційні застосування блокчейну для покращення функціонування систем фінансового контролю, зокрема в рамках дотримання вимог AML, із зосередженням на ключових галузях, таких як моніторинг транзакцій, міжінституційний обмін даними та регуляторна звітність. Інтеграція блокчейну може оптимізувати процеси AML, знизити операційні витрати та підвищити ефективність виявлення незаконної фінансової діяльності. Автори розглядають поєднання технологій блокчейну та алгоритмів штучного інтелекту у фінансовому моніторингу. Показано, як автоматизація аналізу транзакцій може зміцнити стабільність банківської системи та запобігти фінансовим злочинам. Продемонстровано, що конвергенція штучного інтелекту й технологій блокчейну надає трансформаційну можливість для зміцнення систем AML, особливо в умовах зростання фінансових злочинів, пов'язаних із криптовалютою. Це дослідження пропонує кілька важливих внесків в академічну літературу. По-перше, у ньому представлено синтез поточного стану підходів штучного інтелекту, які використовують для дотримання вимог у виявленні шахрайства в біткоїн-транзакціях. У цьому огляді обговорені основні методології й тактики в певній галузі, яка перетинається з фінансами та дотриманням вимог, але підпадає під ширші дисципліни фінансів на основі штучного інтелекту й децентралізованих фінансів (DeFi). Упровадження штучного інтелекту у фінансовий контроль знаменує собою величезну технологічну революцію, яка впливає на всі галузі промисловості. По-друге, ця робота оцінює поточний стан публікацій, основні тенденції та прогалини в дослідженнях, підкреслюючи, які царини потребують додаткового вивчення.

Ключові слова: банківська система, блокчейн, управління, інновації, економічна безпека, фінансовий контроль, фінансовий моніторинг

JEL Класифікація: G15, G18, G19, E61

DOI: 10.55643/fcaptp.2.67.2026.5061