УДК 336.71

Spiridonova Irina Alekseevna, Graduate Student, Federal State-Funded Educational Institution of Higher Education «Financial University under the Government of the Russian Federation» (Financial University), Moscow,

THE EVOLUTION OF AML AND KYC: HOW TECHNOLOGIES COUNTER NEW MONEY LAUNDERING METHODS

Abstract

In the article describes the development of Anti-Money Laundering (AML) and Know Your Customer (KYC) systems, talking about their relevance, purpose, research methods, and key findings. It narrates the global significance of AML/KYC in confronting financial crimes, challenging people who commit them, with an estimated sum of $2 trillion, which are considered to be laundered annually. The main intention of this article, its intent, is to explore precisely how tech advancements or enhancements - such as artificial intelligence (AI), blockchain, and biometrics - are transforming compliance processes to solve modern problems like cryptocurrencies and trade-based laundering. The article uses case studies and analytical frameworks to highlight real-world applications, such as AI uncovering over-invoicing schemes and blockchain analytics tracing illicit funds in decentralized finance (DeFi). It also discusses regulatory responses like GDPR and FATF's «Travel Rule», showcasing the interplay between compliance and data privacy. The main results demonstrate that continuous innovation in AML/KYC technologies is essential to stay ahead of increasingly sophisticated criminal tactics. With its focus on cutting-edge solutions, this article is highly relevant for professionals in finance, compliance, and technology. It is worth reading for those who want to learn the future of AML/KYC systems and their role in safeguarding global financial integrity.

Key words: Anti-Money Laundering (AML), Know Your Customer (KYC), financial crime prevention, Artificial intelligence (AI), regulatory compliance, cryptocurrencies, machine learning, digital identity systems

Introduction

It's important to mention: money laundering constitutes a major global threat, with its extensive complicity and involvement into economic systems, corporate integrity, and, of course, societal stability. Every year, criminals move between $800 billion and $2 trillion illegally. This amount equals about 2–5% of the world's total economy, which shows how serious the problem is [2]. Money laundering allows criminals to hide their illegal profits and use them for activities like terrorism, drug trafficking, and corruption. These crimes do not only harm people but also disrupt economies and weaken trust in financial systems.

The impact of money laundering goes way beyond just financial losses. It damages the reputation of banks and other financial institutions, making people less confident in using their services. Honest businesses also face difficulties and other issues because they have to compete with companies funded by laundered money. For example, criminals can use fake companies or shell corporations to offer products at unfairly low prices. This creates an uneven playing field for legitimate businesses that follow the rules [5].

Governments and private organizations all across the world have been trying for decades to fight money laundering. To resolve this issue, systems like Anti-Money Laundering (AML) and Know Your Customer (KYC) were created and introduced. Initially, these systems operated on a reactive basis, they didn't prevent suspicious activities, but highlighted them post-factum. This approach was not always helpful, rather than slow and often ineffective because criminals continuously developed creative, unconventional methods for concealing illicit doings. Over time, however, AML and KYC systems gained experience, data and became more advanced.

Today, AML and KYC are proactive tools that use modern technologies to detect risks before crimes occur. Technological tools such as artificial intelligence, blockchain analytics, and biometric verification have significantly enhanced the speed, precision, usability, and applicability of compliance mechanisms. For example, AI can analyze large amounts of data to find patterns that might indicate money laundering. Blockchain technology helps track cryptocurrency transactions, which are often used by criminals because of their anonymity [6].

My article will explore how AML and KYC systems have evolved over time. It will look at the problems, which have appeared because of modern money laundering methods, such as cryptocurrency misuse and trade-based laundering schemes involving fake invoices or manipulated prices. It will also try to explain how new technologies are helping financial institutions fight back against these crimes. The main idea is: technology is essential for staying ahead of criminals who constantly adapt their methods to avoid detection.

By understanding how AML/KYC systems work and how they are improving with technology, we can see why innovation is so important in this fight. Malefactors continuously adapt their methodologies to circumvent regulatory mechanisms to use weaknesses in financial systems against us, so governments and businesses must keep improving their tools to stop them quickly and effectively.

1. Historical evolution of AML/KYC

Money laundering has been a sore spot for governments and financial institutions for decades. Over time, the fight against this crime has led to the development of Anti-Money Laundering (AML) laws and Know Your Customer (KYC) procedures. These measures have evolved significantly, shaped and changed by historical events, technological advancements, and regulatory milestones.

The foundation of modern AML laws was laid in the 20th century, primarily to fight and stop organized crime in the financial sphere. In the early 1900s, criminals like Al Capone used laundromats as fronts to mix illegal profits with legitimate business income, giving rise to the term «money laundering»[2]. As organized crime grew, governments realized the need for stricter financial controls [11].

The first major step in combating money laundering came with the Bank Secrecy Act (BSA) of 1970 in the United States. This legislation required financial institutions to report cash transactions exceeding $10,000 to the Financial Crimes Enforcement Network (FinCEN). It also mandated record-keeping and reporting requirements to help authorities trace suspicious activities [11]. The BSA marked the beginning of formal AML regulations, gave an opportunity and set a precedent for other countries to follow.

During this era, KYC processes were manual and paper-based, which was not 100% reliable and fast. Banks relied on basic identity checks, such as verifying government-issued IDs, but had limited tools for calculating customer risk. These methods were slow and prone to errors, making it easier for criminals to find and use loopholes in financial systems [13].

The rise of digital technology in the late 20th century transformed both financial systems and money laundering methods. Online payment platforms like PayPal and Western Union introduced convenience but also created vulnerabilities that criminals could exploit [5]. This digital revolution forced financial institutions to adapt their AML and KYC strategies in a short period of time to catch up with lawbreakers [2].

One major difference and improvement was the move from manual KYC processes to digital KYC systems. Technologies such as Optical Character Recognition (OCR) enabled faster document verification, while databases allowed banks to cross-check customer information against global watchlists [6]. Automated verification reduced errors, eliminated human factor from the process and improved efficiency, making it harder for criminals to bypass checks.

Table 1

Manual vs. automated AML/KYC processing speeds

	Manual processing	Automated processing
Time per transaction	1-2 days	2-10 minutes
Error rate	10-15%	1-2%
Cost per check	$50–$100	$5–$10

Scalability	Limited by human capacity	Handles millions of records

Source: compiled by the author

In addition to technological advancements, regulatory frameworks expanded during this period. The establishment of the Financial Action Task Force (FATF) in 1989 marked a global effort to combat money laundering. FATF issued recommendations encouraging countries to adopt risk-based approaches and enhance international cooperation [2]. These guidelines laid the groundwork for harmonized AML practices worldwide [14].

The 21st century brought significant updates to AML/KYC regulations as governments sought to resolve new issues like cryptocurrency misuse and trade-based laundering. One important milestone was the European Union's 6th Anti-Money Laundering Directive (AMLD6) in 2020 [5]. This directive expanded AML requirements to cover emerging risks such as crypto assets and art markets while harmonizing rules across EU member states [14].

FATF continued to play a central role in changing global standards. Its risk-based approach encouraged financial institutions to allocate resources based on customer risk levels, geographies, and transaction types [14]. This strategy allowed institutions to focus on high-risk areas while maintaining efficiency [1].

Another important development was the introduction of dynamic KYC systems, also known as Perpetual KYC (pKYC). These systems enable continuous monitoring of customer data rather than relying solely on periodic updates [2]. By integrating AI and machine learning into compliance processes, pKYC enhances real-time risk assessment and helps institutions respond quickly to suspicious activities [3].

The historical evolution of AML/KYC demonstrates how laws, technology, and global cooperation have adjusted modern financial crime prevention measures. From manual processes in the pre-digital era to automated systems powered by AI today, these tools have become irreplaceable in fighting increasingly sophisticated and constantly evolving money laundering schemes.

2. Modern money laundering problems

As technology evolves, criminals are finding new ways to launder money, making it harder for governments and financial institutions to keep up. Modern money laundering methods are more sophisticated and difficult to track, they use gaps in regulations and leveraging advanced tools like cryptocurrencies and trade manipulation.

According to Chainalysis (2024), approximately $20 billion in cryptocurrency transactions were linked to illicit activities, representing 0.14% of total crypto volume. However, privacy coins like Monero complicate tracking: only 15% of transactions involving such coins were successfully traced in 2022 [7]. This underscores the need for advanced blockchain analytics - tools like Elliptic identified 85% of suspicious Bitcoin transactions in 2023.

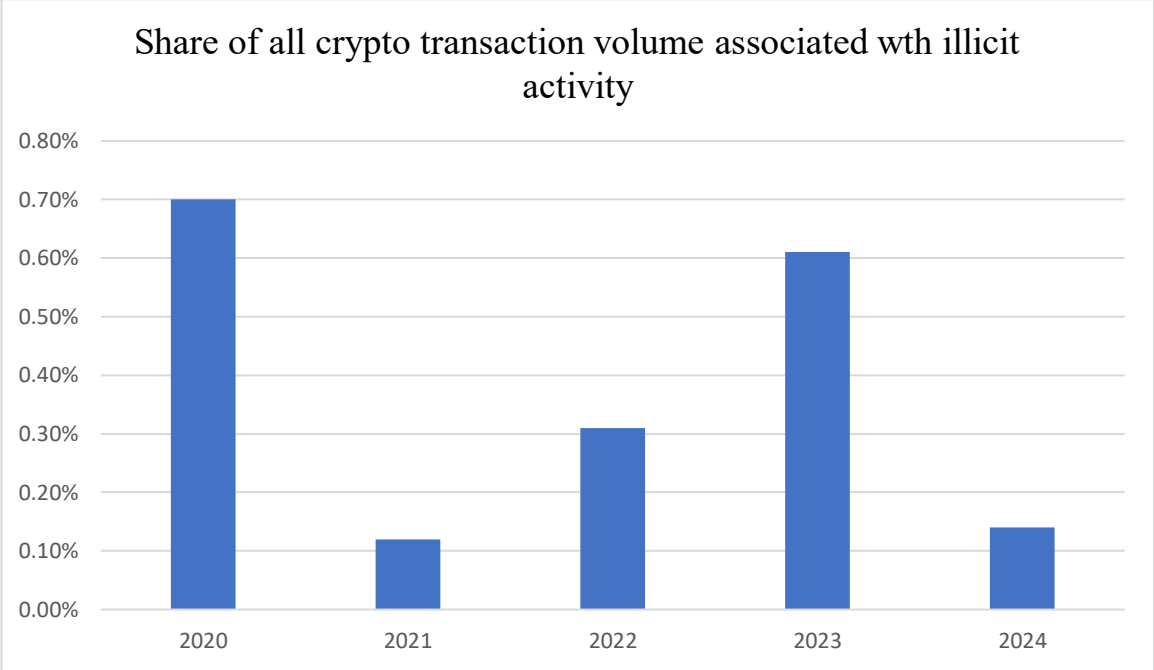

Figure 1. 2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized

Source: 2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized - URL: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ (accessed date 17.04.2025)

Certain illicit actors utilize cryptocurrency mixing services and privacy-centric digital assets, such as Monero and Zcash, to obfuscate transactional origins and beneficiaries. Mixing services combine multiple cryptocurrency transactions and redistribute them, making it nearly impossible to trace the original source of funds [5]. Privacy coins go a step further by using advanced cryptographic techniques to hide transaction details entirely.

For example, a recent case involved the use of Monero in ransomware attacks, where hackers demanded payments in this privacy coin to avoid detection. While blockchain analytics tools are improving, they are still far from perfection in tracing funds [4].

Trade-based money laundering (TBML) is another major complication. Criminals manipulate international trade processes by using fake invoices, overpricing or underpricing goods, and creating shell companies. These tactics allow them to disguise illegal profits as legitimate business transactions.

One common method involves creating false invoices for goods that were never shipped or received. For instance, a criminal might claim to export $1 million worth of goods but actually ship nothing, pocketing the funds while appearing totally honest and compliant with trade regulations. Similarly, overpricing or underpricing goods can be used to transfer value between parties without raising suspicions [15].

Modern technology is helping fight TBML. AI solutions are being developed to analyze trade finance data and detect unusual patterns or inconsistencies in invoices and pricing [13]. These tools use machine learning algorithms to mark suspicious activities that would be difficult for humans to identify manually and report those. For example, AI can compare historical pricing data for similar goods across different regions to spot anomalies that might show laundering [6].

Despite advancements in AML/KYC systems, traditional models are still limited in their functions and abilities. One of the biggest issues is the high rate of false positives in transaction monitoring systems. These systems often mark legitimate transactions as suspicious, leading to wasted resources and delays in compliance processes.

Manual compliance procedures remain in use but are associated with considerable operational inefficiencies and risk exposure. Many financial institutions still rely on human analysts to review flagged transactions and verify customer information [15]. This approach is intensive and time-consuming, making it difficult for organizations to keep up with the volume of transactions in today's globalized economy [3].

Additionally, traditional models struggle with adapting to new laundering methods quickly enough. Criminals constantly innovate their techniques, by exploiting emerging technologies like decentralized finance (DeFi) platforms or finding gaps in regulatory frameworks [11].

Modern money laundering problems highlight the need for continuous innovation in AML/KYC systems. Cryptocurrencies and trade-based schemes show how criminals operate technology and global trade networks, while the limitations of traditional models clearly emphasize the importance of adopting advanced tools like AI and blockchain analytics. By addressing these obstacles, governments and financial institutions can better protect economies from the devastating effects of financial crimes.

Technology has revolutionized the way financial institutions fight money laundering and verify customer identities. With criminals constantly developing new methods to hide illicit funds, tools like artificial intelligence, blockchain, biometrics, and RegTech solutions have become essential in making AML/KYC systems faster, smarter, and more effective. These innovations are changing compliance processes and helping institutions stay ahead of financial crimes.

Artificial intelligence and machine learning are transforming transaction monitoring and risk assessment in financial systems. AI can analyze vast amounts of data in real-time, identifying unusual patterns or behaviors that might indicate money laundering. For example, if a customer suddenly begins transferring large sums of money across multiple accounts without a clear reason, artificial intelligence systems can autonomously identify such anomalies and flag them for subsequent

investigative review [4]. This ability to detect anomalies quickly makes AI a powerful instrument in opposing financial crime.

Machine learning is also useful in using predictive analytics to assess customer risk. It examines behavioral patterns, such as frequent transactions with high-risk countries or unusual spending habits, to assign risk scores to individuals or businesses [14]. These scores help financial institutions focus their resources on higher-risk customers while allowing lower-risk clients to pass through compliance processes more smoothly. Banks that have adopted AI have reported significant improvements, including a reduction in false positives - legitimate transactions flagged as suspicious - by up to 40%. This saves time and resources while improving efficiency [6].

Blockchain technology is widely known for powering cryptocurrencies, but it is also becoming a big deal in AML/KYC processes. One of its best features is the creation of immutable records - every transaction is permanently stored on the blockchain and cannot be altered. This transparency makes it easier for investigators to trace suspicious flows of money, even across decentralized platforms [4].

Despite the anonymity offered by cryptocurrencies like Bitcoin, blockchain analytics tools are improving their ability to track transactions involving privacy coins such as Monero and Zcash. These coins are designed to obscure transaction details, but advanced algorithms are helping regulators follow the trail of illicit funds across exchanges [13].

Smart contracts add another layer of functionality to blockchain technology. These self-executing agreements automate tasks such as sanctions screening or payment blocking for wallets linked to illegal activities [6]. By reducing the need for human intervention, smart contracts enhance the speed and accuracy of compliance processes and decrease the amount of funds needed for manual checking process.

Biometric technology is making identity verification faster and more secure than ever before. Tools like facial recognition and voice biometrics ensure that

customers are real people during onboarding processes, preventing criminals from using stolen photos or recordings to open accounts under fake identities [4].

One example of biometric innovation is liveness detection, which checks whether the person being verified is physically present rather than relying on images or videos. This technology is particularly useful for online banks that need to communicate with customers remotely while maintaining high security standards [3].

Government-backed digital IDs, such as the EU's eIDAS system, simplify identity verification even further by allowing banks to instantly confirm a customer's identity using official databases [13]. This speeds up onboarding while reducing errors and improving overall security.

Regulatory Technology (RegTech) focuses on automating compliance tasks to make them faster and less expensive for financial institutions [4]. Customer Due Diligence (CDD), which used to take days or weeks, can now be completed in minutes using RegTech tools that cross-check customer data against global watchlists [14].

Behavioral biometrics offer an additional layer of security by analyzing how people interact with devices - for example, their typing speed or mouse movements - to detect fraud. If someone's behavior changes significantly during a transaction, the system can block it automatically [13].

RegTech solutions not only save time but also reduce human error in compliance processes. By automating repetitive tasks like document verification and risk scoring, these features allow financial institutions to focus their efforts on higher-risk cases.

Technological innovations are transforming AML/KYC from slow manual processes into dynamic systems capable of keeping up with modern criminal activity. AI enables real-time monitoring and predictive risk assessment, blockchain ensures transparency in cryptocurrency transactions, biometrics improve identity verification security, and RegTech simplifies compliance tasks efficiently [3].

These technological instruments facilitate regulatory compliance while simultaneously enhancing institutional credibility and client confidence who expect safe and seamless services from their banks. As technology continues to evolve, its role in protecting global economies from financial crime will only grow stronger.

3. Regulatory responses and global standards

Governments and organizations around the world are constantly working to improve regulations that fight money laundering. These rules aim to stop criminals while also protecting people's privacy. However, balancing anti-money laundering (AML) checks with data privacy laws, like the General Data Protection Regulation (GDPR), can be tricky. At the same time, global standards like FATF's «Travel Rule» are pushing for better cooperation across borders, even as differences between countries create problems [1].

The GDPR is a law in the European Union designed to protect people's personal data. It requires companies to get clear permission from customers before collecting or using their information. This law has changed how banks handle customer data during onboarding and monitoring processes [1]. For example, banks must explain why they need certain information and make sure they only collect what is absolutely necessary.

AML regulations, on the other hand, require banks to collect detailed data about customers to identify risks and prevent illegal activities. Sometimes these two goals, privacy and compliance, can conflict. To solve this, banks often use a risk-based approach [6]. This means they collect more data for high-risk customers or transactions while keeping things simpler for low-risk clients. By doing this, banks can follow both GDPR rules and AML requirements without overstepping or crossing privacy boundaries [8].

Cryptocurrencies have made it easier for criminals to move money anonymously across borders. To fight this, the Financial Action Task Force (FATF) introduced the «Travel Rule». This rule requires Virtual Asset Service Providers (VASPs), like crypto exchanges, to share information about the sender and receiver of transactions above a certain amount [2]. For example, if someone sends Bitcoin

worth $10,000, both their name and the recipient's name must be recorded and shared with authorities.

The Travel Rule aims to bring more transparency to cryptocurrency transactions and stop criminals from using digital assets to hide their money. It is part of FATF's larger effort to create global standards that all countries can follow [9]. By applying these rules consistently, regulators hope to close loopholes that criminals use when moving funds across borders [1].

One of the biggest problems in fighting money laundering is that different countries have different rules. For example, the European Union has combined its AML laws under directives like 6AMLD (Sixth Anti-Money Laundering Directive) [12]. These rules ensure that all EU countries follow similar standards. However, outside the EU, regulations vary widely [11].

This lack of consistency makes it hard for international businesses to comply with AML laws everywhere they operate. A company might meet the requirements in one country, but face completely different expectations in another. Cryptocurrencies and decentralized finance (DeFi) platforms add even more complexity and issues because they often operate outside traditional financial systems [6].

Regulators are working on solutions, but progress is slow. Global cooperation is essential to create unified rules that focus on new risks while keeping compliance manageable for businesses and individuals.

Regulatory responses are evolving to meet modern requirements and instruments like cryptocurrencies and fragmented global standards. Laws like GDPR focus on protecting privacy, while FATF's Travel Rule aims to bring transparency to crypto transactions. Despite these efforts, differences between countries remain a huge obstacle to creating effective global AML frameworks [8]. Financial institutions must continue adapting their processes as regulations change and new technologies are created.

4. Future trends

The fight against money laundering and financial crime is constantly evolving, and new technologies are shaping the future of AML/KYC systems. Quantum computing, decentralized identity systems, and AI-powered risk prediction are set to transform how financial institutions detect and prevent illegal activities. These innovations promise faster analysis, better security, and more accurate predictions.

Quantum computing is one of the most exciting technologies in financial crime prevention. Unlike classical computers, quantum computers use principles like superposition to process massive amounts of data simultaneously. This allows them to analyze complex transaction networks much faster and uncover hidden connections that traditional systems might miss. Quantum computing could reduce transaction analysis time by 90% by 2030 (IBM Research).

For example, quantum computers can trace concealed transaction chains by exploring multiple paths at the same time [7]. This makes it possible to identify links between accounts that appear unrelated on the surface. Additionally, quantum algorithms can optimize fraud detection systems by balancing false positives and false negatives more effectively than classical methods [11]. While quantum technology improves, its ability to provide real-time risk scoring and anomaly detection will significantly increase the speed and accuracy of AML efforts [10].

Identity verification is a critical part of AML/KYC processes, and decentralized identity systems are becoming a promising solution. These systems use blockchain technology to give individuals control over their own digital identities, known as self-sovereign IDs. Instead of relying on centralized databases, users store their personal information securely on the blockchain.

Self-sovereign IDs improve privacy while ensuring authenticity during financial transactions. For example, a customer could share only the necessary parts of their identity with a bank without exposing sensitive data like full addresses or social security numbers. This reduces the risk of identity theft while maintaining compliance with AML regulations.

Blockchain-based identity systems also simplify cross-border transactions by providing a universal standard for identity verification [7]. As global financial systems become more interconnected, decentralized IDs could play an important role in streamlining compliance processes across jurisdictions.

Artificial intelligence continues to push the boundaries of risk prediction in financial crime prevention. AI-powered systems can analyze customer behavior and transaction patterns to predict potential laundering methods before they occur. By using machine learning models trained on historical data, these systems identify trends that indicate emerging risks [6].

For instance, AI can detect unusual spending habits or sudden changes in transaction volumes that might signal money laundering attempts. Predictive analytics allows institutions to focus their resources on high-risk areas while reducing unnecessary checks for low-risk customers [10].

The combination of AI with quantum computing could further enhance risk prediction capabilities. Quantum-powered AI algorithms would process larger datasets at unprecedented speeds, enabling institutions to respond to threats in real time.

Conclusion

The fight against money laundering has come a long way. From manual checks and paper-based systems to AI-driven, real-time monitoring, the evolution of AML/KYC processes reflects the growing complexity of financial crime. Early efforts like the Bank Secrecy Act (BSA) laid the foundation for tracking suspicious activities, but today's systems leverage advanced technologies such as artificial intelligence, blockchain, and biometrics to stay ahead of criminals. These tools have made compliance faster, more accurate, and better equipped to handle modern challenges like cryptocurrencies and trade-based laundering.

Despite these advancements, the battle is far from over. Criminals are constantly adapting their methods, exploiting new technologies and loopholes in regulations. This makes continuous innovation inevitable. Financial institutions must embrace modern trends such as quantum computing for faster transaction

analysis and decentralized identity systems for secure verification. Governments and regulators must also work together to combine global standards and close gaps between jurisdictions.

The imperative is evident: global financial and regulatory frameworks must continue to evolve in tandem with emerging threats and innovations. By investing in cutting-edge technologies and increasing international cooperation, stronger defenses against money laundering can be built. Only by staying one step ahead can computer science protect economies, businesses, and individuals from the damaging effects of financial crime.

References

1. Anti-money laundering and combating the financing of terrorism (AML/CTF) regulations for banks & DFIs (2016) State Bank of Pakistan URL: https://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf (access date 15.04.2025)

2. Basel Institute on Governance (2020) Anti-Money Laundering Index. URL: https://www.baselgovernance.org/aml-index (access date 15.04.2025)

3. Burak A. (2024) Relevant Software. AML and KYC Solutions Development. URL: https://relevant.software/blog/aml-kyc-solutions-development (access date 15.04.2025)

4. Didit (2024) AI and Biometrics: How They're Revolutionizing KYC and AML Processes URL: https://didit.me/blog/ai-biometrics-how-they-re-revolutionizing-kyc-and-aml-processes (access date 15.04.2025)

5. Financial Action Task Force (FATF) (2020) Guidance on Digital Identity. URL: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity.html (access date 15.04.2025)

6. Global Anti-Money Laundering Survey (2022) Deloitte. 2022.https://www2.deloitte.com/us/en/pages/risk/articles/2022-global-anti-money-laundering-survey.html (access date 15.04.2025)

7. Goliya A. (2024) The Future of KYC/AML. Algoworks. URL: https://www.algoworks.com/blog/future-of-kyc-aml (access date 15.04.2025)

8. Jersey Financial Services Commission (2023) Anti-Money Laundering Regulations URL: https://www.jerseyfsc.org/media/3389/lawsregulations/Anti-MoneyLaunderingRegulations2023Revision_1673895715.PDF (access date 15.04.2025)

9. Kosba A., Miller A., Shi E., Thiruvengadam A., Hawkey, K. (2021) Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. IEEE Security & Privacy. 14(3). 28–39. https://doi.org/10.1109/SP.2016.55 (access date 15.04.2025)

10. Pasquest V. (2025) Perpetual KYC in 2025: Reviewing AI Use Cases and Challenges. Projective Group. URL: https://www.projectivegroup.com/perpetual-kyc-in-2025-reviewing-ai-use-cases-and-challenges (access date 15.04.2025)

11. Segal T. (2025). How Technology is Transforming KYC and AML Processes. LinkedIn. URL: https://www.linkedin.com/pulse/how-technology-transforming-kyc-aml-processes-tal-segal-lk0gf (access date 15.04.2025)

12. Sixth Anti-Money Laundering Directive (AMLD6) (2020) European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020L0849 (access date 15.04.2025)

13. Steinert M., Williams D. (2020) A KYC–AML Utility: Driving Scale, Efficiency, and Effectiveness. McKinsey & Company. URL: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/a-kyc-aml-utility-driving-scale-efficiency-and-effectiveness (access date 15.04.2025)

14. The Future of Anti-Money Laundering: How Technology Can Help (2020) Accenture. URL: https://www.accenture.com/_acnmedia/PDF-82/Accenture-Future-Of-Anti-Money-Laundering.pdf (access date 15.04.2025)

15. Ughade N. (2024) Combat Money Laundering: Using AML & KYC to Prevent Money Laundering. Hyperverge.co. URL:

https://hyperverge.co/blog/using-kyc-aml-to-combat-money-laundering (access date 15.04.2025)