Chapter 3

Blockchain Technology in Anti-Money Laundering: Challenges and Opportunities in the V4 Countries and Ukraine

Bartłomiej Nita

Wroclaw University of Economics and Business

ORCID: 0000-0001-5036-912X

Quote as: 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.

DOI: 10.15611/2025.32.0.03

3.1 Introduction – Blockchain Technology and AML Challenges

Since its inception with Bitcoin in 2008, blockchain technology has revolutionized data storage and transactions in the digital realm. Its fundamental attributes, including decentralization, transparency, and immutability, position it as a key tool in combating money laundering (AML) (Barbereau & Bodó, 2023). AML regulations require financial institutions to monitor transactions, identify suspicious operations, and report them to relevant authorities. Blockchain supports these efforts by enabling the real-time tracking of financial flows and automating anomaly detection (OECD, 2022).

A notable application of blockchain in AML is the use of smart contracts, which can automatically freeze funds associated with suspicious transactions. Additionally, blockchain data analysis assists law enforcement agencies in identifying criminal network 'nodes' by analysing connections between digital addresses. However, blockchain technology also presents limitations. The anonymity and pseudonymity of many blockchain systems, coupled with the growing popularity of decentralized tools such as non-custodial wallets, hinder user identification and source-of-fund verification (FATF, 2021).

Non-custodial wallets, such as MetaMask and MyEtherWallet, are increasingly favoured by users valuing privacy and autonomy over their assets. Unlike traditional custodial wallets, where private keys are managed by financial institutions, non-custodial wallets enable users to independently manage their funds. While this design promotes privacy protection, it also poses significant challenges for regulators who struggle to enforce AML compliance effectively (Barbereau & Bodó, 2023). The case of Tornado Cash, a decentralized cryptocurrency mixer implicated in laundering billions of dollars, highlights the scale of the problem. Regulatory actions,

such as sanctions imposed by the US Treasury Department on Tornado Cash in 2022, highlight the difficulties in regulating decentralized technologies (U.S. Department of Treasury, 2022).

Central and Eastern Europe, encompassing the V4 countries (Poland, the Czech Republic, Hungary, and Slovakia) and Ukraine, offers a compelling context for analysing blockchain applications in AML. These countries vary not only in their levels of technological advancement but also in their regulatory approaches to cryptocurrencies and blockchain technology. Poland and the Czech Republic have implemented comprehensive regulatory frameworks that include AML requirements for cryptocurrency service providers, such as exchanges and custodial wallets. For instance, Polish regulations mandate full compliance with KYC standards and the reporting of suspicious transactions to the General Inspector of Financial Information (FATF, 2021).

Slovakia and Hungary, despite being EU members, face challenges due to financial and technological constraints that hamper the effective implementation of AML regulations. Ukraine, meanwhile, has adopted a more flexible approach, allowing the use of cryptocurrencies for humanitarian support and sanction evasion during wartime. At the same time, Ukraine is introducing measures to enhance the transparency of cryptocurrency transactions, a critical factor in combating corruption (OECD, 2022).

This chapter aimed to analyse the application of blockchain technology in combating money laundering in the V4 countries and Ukraine, addressing their specific regulatory, technological, and operational challenges. It explores how blockchain can support AML systems, identifies the associated risks, and proposes recommendations for regulators and financial institutions.

In the context of a dynamically evolving technological and financial environment, blockchain technology is increasingly regarded as a critical tool in combating money laundering (AML). In Central and Eastern Europe, encompassing the V4 countries (Poland, the Czech Republic, Hungary, Slovakia) and Ukraine, the application of blockchain faces specific challenges arising from diverse legal, technological, and operational conditions. To address the opportunities and limitations of implementing blockchain in AML, it is essential to conduct an analysis at both local and global levels.

The following research questions aim to systematize this analysis and highlight key factors influencing the effectiveness of blockchain applications in combating money laundering.

1. What are the most significant technological advancements and barriers in using blockchain for AML processes in the V4 region and Ukraine?
2. How do differences and similarities in AML regulations across the V4 countries and Ukraine influence the harmonization of blockchain adoption?
3. How can international collaboration, particularly through organizations like FATF (The Financial Action Task Force) and Europol, support the integration of blockchain into AML systems?
4. What trends, investments, and educational initiatives are necessary to enhance the effectiveness of blockchain in AML efforts?

This chapter is structured into four cohesive sections that together provide a comprehensive perspective on the application of blockchain technology in combating money laundering and its significance for the V4 countries and Ukraine. Each section addresses critical technological, regulatory, and international aspects that shape the effectiveness of blockchain implementation in AML activities.

The first section, encompassing the introduction, analyses the fundamental issues related to blockchain's potential in AML, considering the specific context of the V4 region and Ukraine. It

outlines the main challenges associated with using blockchain to combat money laundering and defines the research questions that guide the chapter's narrative.

The second section examines the technological applications and limitations of blockchain in AML. It focuses on mechanisms such as real-time financial monitoring, smart contracts, and financial flow analysis, and also discusses technological barriers, including scalability, interoperability, and resource constraints in countries like Slovakia and Ukraine. Examples of successful blockchain implementations from regions like Singapore offer inspiration and practical benchmarks for the V4 countries and Ukraine.

The third section explores the regulatory landscape in the V4 region and Ukraine. It provides a comparative analysis of AML regulations, highlighting similarities and differences influenced by EU directives such as AMLD5 and AMLD6, as well as the FATF 'travel rule'. A comparative table visualizes these differences, accompanied by commentary on regulatory gaps and opportunities for harmonization within the region.

The fourth section underlines the importance of international cooperation in advancing blockchain technology for AML. It discusses the role of global organizations, such as FATF and Europol, in fostering collaboration and regulatory harmonization. The section also highlights the benefits of initiatives like harmonized VASP reporting systems, blockchain pilot projects, and joint training programmes to address cross-border financial crimes effectively.

The final section focuses on development prospects and recommendations. It analyses key technological and regulatory trends, proposing investments in blockchain analytics, targeted reforms, and educational initiatives. The section also addresses emerging risks in Decentralized Finance (DeFi) and emphasizes the need for compliance-oriented innovations to mitigate these challenges. By implementing these measures, the V4 countries and Ukraine can strengthen their AML systems and enhance international collaboration in combating financial crime.

The chapter is based on an analytical-comparative approach and employs various research methods.

1. Literature review – a review of the latest academic publications and international reports on blockchain technology, AML, and international cooperation.
2. Legal regulation analysis – a comparison of AML regulations in the V4 countries and Ukraine with international standards, such as FATF recommendations. This analysis also considers EU directives and regional initiatives.
3. Review of international initiatives – an analysis of examples of international cooperation in blockchain and AML, such as projects led by FATF, Europol, and KYC platforms in Singapore.
4. Comparative methodology – a comparison of the approaches of V4 countries and Ukraine to blockchain technology, focusing on technological, regulatory, and operational differences.
5. Analysis of best practices – an analysis of practical implementations of blockchain technology in AML, including initiatives such as Ukraine's "Virtual Assets Law" and blockchain platforms in Poland.

The proposed research questions, chapter structure, and modified research methodology enable an in-depth analysis of blockchain applications in AML. The emphasis on international cooperation, regulatory harmonization, and technological prospects allows for the inclusion of both local conditions and global trends.

3.2. The Application of Blockchain Technology in AML

Blockchain technology is transforming the approach to combating money laundering (AML) by offering new opportunities for monitoring and analysing financial transactions. Its unique features, such as transparency, decentralization, and immutability of records, make it an ideal tool for tackling criminal activities in the global financial system. Blockchain not only enhances compliance processes but also introduces new mechanisms that are difficult to achieve with traditional technologies.

In recent years, blockchain has found applications in various aspects of AML, including process automation through smart contracts, financial flow analysis, and improving compliance with "Know Your Customer" (KYC) standards. Each of these applications brings significant innovations to AML systems, offering more efficient and automated solutions. This section discusses the primary mechanisms of blockchain in AML, which form the foundation of its growing role in combating financial crimes.

Smart contracts

Smart contracts, computer programmes operating on blockchain networks can automate AML compliance processes. These contracts are designed to execute predefined instructions automatically, such as freezing funds originating from suspicious sources or instantly reporting detected irregularities to financial regulators (OECD, 2022). For example, systems can be implemented to analyse financial flows in real-time and automatically trigger alerts when transactions exceed specified thresholds or are linked to previously flagged high-risk addresses. Such solutions, as seen on platforms like Ethereum, enable immediate responses to suspicious activities, eliminating the need for manual analysis of transaction data (Barbereau & Bodó, 2023). Moreover, smart contracts can support 'compliance tokenization', where financial institutions tokenize assets that are then automatically monitored for AML compliance. For instance, these systems can be programmed to block the transfer of digital assets if they do not adhere to "Know Your Customer" (KYC) standards (Sun et al., 2022; Zetzsche et al., 2020).

Financial flow analysis

One of the most significant applications of blockchain in AML is its ability to conduct comprehensive financial flow analysis. Every transaction on a blockchain is recorded in a public ledger, enabling end-to-end tracking. Advanced data analysis algorithms and machine learning allow blockchain to detect patterns indicative of criminal activities. For instance, money laundering schemes such as 'smurfing', which involves breaking large sums into multiple smaller transactions to evade detection by traditional monitoring systems, can be identified using blockchain's transparent and real-time tracking capabilities (OECD, 2022).

Examples of financial flow analysis applications include utilizing network analysis technologies to map connections between blockchain addresses. Such analyses help identify central nodes within criminal networks, significantly facilitating investigative efforts (Pocher et al., 2023).

Compliance technologies

Blockchain also plays a critical role in implementing compliance principles, such as KYC. Decentralized systems enable secure and transparent storage of identification data while minimizing the risk of privacy breaches (FATF, 2021). An innovative example of compliance technology is blockchain platforms that allow for one-time identity verification, with the

results stored securely on the blockchain. This enables users to safely share their data only when necessary, eliminating the need for repeated verification across various financial institutions.

Through these advancements, blockchain technology is reshaping AML practices, providing tools for more efficient compliance processes, and enhancing the ability to track and analyse financial transactions in a secure and transparent manner. Blockchain technology is increasingly being utilized in global anti-money laundering (AML) systems, contributing to enhanced efficiency in monitoring and reporting financial transactions. Its transparency and ability to track fund flows in real-time enable the rapid identification of suspicious activities and support collaboration among financial institutions worldwide. The practical implementations of this technology showcase its potential in combating money laundering and adapting to diverse legal and technological challenges. From advanced monitoring platforms in Singapore and FATF's guidelines to Estonia's innovative user identification systems, blockchain is redefining the approach to AML. The following examples illustrate how this technology supports AML efforts on a global scale:

- Project Ubin in Singapore – Singapore has implemented a blockchain-based platform to monitor financial transactions in real time. This project has significantly improved AML processes by eliminating delays in identifying suspicious transactions and reducing operational costs (Menon, 2023)
- FATF's travel rule initiative – FATF has recommended implementing the 'travel rule', requiring financial institutions to share information about the sender and recipient of cryptocurrency transactions. Adopting this rule enhances international cooperation in AML (Chuah, 2023).
- Estonia's e-residency system – Estonia leverages blockchain technology to store and verify user identity data in its e-Residency program. This approach reduces the risk of financial abuse while ensuring full transparency in operations (Sullivan & Burger, 2017).

Despite its vast potential, the application of blockchain in AML systems encounters significant technological, operational, and regulatory limitations. These challenges can impact the effectiveness of AML efforts and their global coordination. The key issues include:

1. Scalability and network performance. Blockchains like Ethereum and Bitcoin are designed with a focus on security and decentralization, often at the expense of performance. High network activity can lead to congestion, resulting in increased transaction fees and longer confirmation times, making blockchain less efficient for large-scale financial operations. Technological solutions, such as "Layer Two" protocols (e.g. Lightning Network for Bitcoin or Polygon for Ethereum), promise increased scalability. However, implementing these solutions requires significant investment, and interoperability among various systems remains a challenge (Benson et al., 2024; OECD, 2022).
2. Implementation and maintenance costs. Implementing blockchain technology involves high initial costs, including the development of technical infrastructure, staff training, and integration with existing financial systems. Operational costs are particularly high for blockchains utilizing consensus algorithms like proof-of-work (PoW), which require substantial energy resources for transaction validation. In the context of financial institutions, smaller entities often lack the necessary resources to adopt blockchain technology, potentially exacerbating technological inequalities within the financial sector. Alternatives like proof-of-stake (PoS) consensus offer reduced energy costs, but their adoption is still in the developmental stage (Ristic, 2023; Shanaev et al., 2020).

3. User privacy and data protection. One of the fundamental challenges of blockchain technology is balancing transaction transparency with user privacy protection. Public blockchains, such as Bitcoin and Ethereum, allow any user to view transaction histories. Although blockchain addresses are pseudonymous, advanced analytical tools can link transaction data to real--world users, potentially leading to privacy violations (Sun et al., 2022).
4. Anonymity and pseudonymity in blockchain. While blockchains provide an immutable ledger of transactions, user anonymity poses significant challenges for combating money laundering. Non-custodial wallets, which allow users full control over their assets without requiring identity verification, are particularly problematic. These tools are often exploited by criminals to obscure the origins of funds. A notable example is Tornado Cash, a decentralized cryptocurrency mixer that was implicated in laundering billions of dollars. Despite sanctions imposed by the US Department of the Treasury, the anonymity provided by such tools makes effective prevention of misuse difficult (OECD, 2022; Pocher et al., 2023).
5. Regulatory discrepanciPPes and lack of international consistency. The diversity of regulatory approaches across countries complicates the global implementation of blockchain-based AML standards. For instance, while EU member states have adopted AML directives aligned with the "Know Your Customer" principle, their implementation and enforcement vary significantly between countries The lack of regulatory harmonization creates legal loopholes that financial criminals can exploit. Initiatives like FATF's guidelines, including the 'travel rule', aim to standardize cryptocurrency transaction reporting requirements, but their implementation remains in the early stages in many countries (FATF, 2021; OECD, 2022; Vandezande, 2017).
6. Interoperability issues. The vast blockchain ecosystem, encompassing numerous protocols and standards, leads to significant challenges in integrating different systems. Interoperability among blockchains and their integration with traditional financial systems remain technological hurdles that require substantial investments in research and development (OECD, 2022; Utkina, 2023).

Although blockchain represents a promising tool in combating money laundering, its implementation requires overcoming numerous technological, operational, and regulatory challenges. Solutions such as proof-of-stake consensus, privacy-enhancing technologies, and regulatory harmonization initiatives can help address these barriers. However, their effectiveness relies on international collaboration and the commitment of both the public and private sectors. Blockchain technology offers significant benefits for anti-money laundering efforts, yet its success depends on overcoming technological, regulatory, and operational barriers. Practical examples of implementation, such as the e-Residency system in Estonia and the Ubin project in Singapore, demonstrate that blockchain can become a central component of global AML strategies, whilst further investments in technology development, international regulatory harmonization, and the education of users and regulators are essential.

3.3. The Regulatory Landscape in the V4 Countries and Ukraine

The anti-money laundering (AML) and blockchain regulations in the V4 countries and Ukraine reflect the diversity of approaches shaped by their specific economic, political, and technological contexts. For EU member states such as the V4 countries, AMLD5 and the upcoming AMLD6 directives form the foundation for harmonizing their regulations with EU standards, especially in light of the growing role of cryptocurrencies. Ukraine, while not a member of the EU, has

introduced its own regulations inspired by international guidelines and is actively aligning its regulatory framework with EU standards as part of its EU candidate status It is particularly evident in Ukraine's 2023 Virtual Assets Law which brings its digital asset regulations closer to European standards.

Blockchain technology, with its transparency, decentralization, and immutability, brings new possibilities to AML systems. However, its full potential can only be realized within effective and well-harmonized regulatory frameworks. The countries in this region face the challenge of aligning their legal systems with the demands of modern technology while ensuring data protection and eliminating legal loopholes. This section examines the key EU directives shaping AML approaches and the diverse regulatory strategies employed by the V4 countries and Ukraine, highlighting both their strengths and areas for improvement.

The EU's anti-money laundering framework has evolved significantly through several key directives. The Fourth AML Directive (AMLD4, Directive (EU) 2015/849…) was adopted on 20 May 2015, establishing the foundational framework for preventing the use of the financial system for money laundering and terrorist financing purposes (OECD, 2022; Tosza, 2024).

AMLD5 (Directive (EU) 2018/843…), adopted on 30 May 2018, amended AMLD4 in response to the rapidly evolving digital asset market and increasing risks of money laundering and terrorism financing. AMLD5 introduced several key changes

1. Mandatory registration of Virtual Asset Service Providers (VASPs). All entities offering cryptocurrency-related services, such as exchanges and custodial wallets, are required to register and comply with "Know Your Customer" (KYC) standards. This enhances market transparency and limits the anonymity of cryptocurrency transactions.
2. Expansion of AML obligations to new entities. The directive extended AML compliance requirements to include cryptocurrency exchanges, custodial wallet providers, and crowdfunding platforms, significantly broadening the scope of regulation to encompass new financial technologies.
3. Enhanced due diligence and reporting requirements. Obligated entities must conduct enhanced customer due diligence and report suspicious transactions to national Financial Intelligence Units (FIUs), particularly for transactions exceeding EUR 15,000. The directive also mandates identifying ultimate beneficial owners in corporate structures.

The Sixth AML Directive (AMLD6, Directive (EU) 2024/1640…) was adopted on 31 May 2024 and published in the Official Journal on 19 June 2024. This directive, which is part of a comprehensive new AML package, introduces significant changes:

1. Harmonization of AML framework. AMLD6 enhances the EU's framework for anti-money laundering and countering terrorist financing by establishing mechanisms for EU Member States to prevent the use of financial systems for illicit purposes. It aims to avoid regulatory divergence between the member states.
2. Enhanced institutional framework. The directive clarifies the role of public authorities in the oversight of self-regulatory bodies and establishes the new Anti-Money Laundering Authority (AMLA), to be based in Frankfurt. AMLA will commence most of its tasks by mid-2025, with direct supervision of selected obligated entities beginning in 2028.
3. Beneficial ownership transparency. The directive emphasizes the importance of identifying and verifying beneficial owners across entities. It provides access to beneficial ownership registers for persons with legitimate interests, such as journalists and civil society organizations.

4. Strengthened supervision and cooperation. AMLD6 enhances the cooperation between Financial Intelligence Units and improves information sharing mechanisms. It establishes a more robust framework for cross-border cooperation and supervision.

These directives represent a progressive evolution of the EU's approach to combating money laundering and terrorist financing. The transition from AMLD4 through AMLD6 shows an increasing focus on technological challenges, institutional cooperation, and transparency requirements. The new framework, particularly with the establishment of AMLA and the enhanced cooperation mechanisms, positions the EU as a leader in developing comprehensive anti-money laundering regulations.

EU Member States are required to transpose AMLD6 into their national legislation, marking another significant step in the EU's efforts to combat financial crime and strengthen the integrity of its financial system.

The directives provide a solid foundation for the V4 countries and Ukraine, highlighting pathways for further AML regulatory development in the context of new financial technologies. The regulatory approaches to blockchain technology and AML in the V4 countries (Poland, the Czech Republic, Hungary, and Slovakia) and Ukraine reflect a diverse range of strategies shaped by their unique economic, political, and technological circumstances.

Poland

Poland has implemented significant changes to its anti-money laundering (AML) framework through the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (AML Act), which transposed the EU's Fourth and Fifth AML Directives (Ustawa z dnia 1 marca 2018…). This legislation marked a substantial shift from previous regulations, introducing more stringent security measures and expanding obligations for regulated entities.

The AML Act requires obligated institutions to conduct thorough customer due diligence, verify beneficial owners, and implement risk-based approaches to monitoring transactions. A key change was the establishment of the Central Register of Beneficial Owners and enhanced requirements for verifying beneficial ownership information beyond just consulting the register.

However, implementation challenges persist. The Supreme Audit Office's inspection from 2013-2015 revealed deficiencies in supervision by the General Inspector of Financial Information (GIIF) over entities required to monitor transactions exceeding EUR 15,000. With estimated money laundering volumes of PLN 18.2 billion in 2014, only PLN 1.2 million in assets were seized and PLN 11.5 million forfeited – representing just 0.07% of estimated illicit funds.

Recent amendments in 2021 further expanded the scope of obligated institutions to include:

- providers of tax, accounting and customs advisory services,
- real estate agents,
- art dealers and auction houses (for transactions over EUR 10,000),
- virtual asset service providers.

While Poland has made progress in aligning with EU standards, practical implementation faces several challenges:

- limited resources and expertise for proper risk assessment, especially among smaller entities,
- difficulties in ongoing monitoring of business relationships,

- complex verification requirements that strain organizational capacity,
- delayed implementation of EU directives.

The effectiveness of the system will depend on addressing these operational challenges while maintaining a robust oversight of the expanding scope of regulated entities. The establishment of the new EU Anti-Money Laundering Authority (AMLA) in Frankfurt may provide additional support for strengthening Poland's AML framework (Piątkowska & Skelnik, 2022).

Czech Republic

The Czech Republic has implemented European AML directives primarily through Act on anti-money laundering and counter-terrorist financing (AML Act), which has undergone multiple amendments to comply with evolving EU requirements (Zákon č. 253/2008…).

The Financial Analytical Office (FAU), established in 2017 as an independent administrative unit, serves as the key supervisory authority for the AML system. As part of AMLD5 implementation in 2020, the Czech Republic introduced significant changes to its legislation, expanding the scope of obligated entities to include virtual asset service providers (VASPs) and implementing more stringent due diligence requirements. Special attention was paid to cryptocurrency-related activities, introducing mandatory registration requirements for service providers in this sector.

The 2021 amendment implementing AMLD6 requirements strengthened the system of penalties and sanctions for AML violations, introducing higher financial penalties and expanding the list of predicate offenses. The Czech Republic stands out in the region for its effective beneficial ownership registration system and well-developed inter-institutional cooperation in information exchange. The Czech Anti-Money Laundering framework distinguishes itself through several significant features, including the systematic adaptation of national law to EU requirements, establishment of a specialized supervisory body (FAU), a comprehensive system of sanctions and penalties, an effective beneficial ownership registration system, and the enhanced cooperation between national institutions (Financial Analytical Office, 2020).

Hungary

Hungary has strengthened its regulatory framework for cryptocurrencies and anti-money laundering (AML), introducing rigorous requirements for Virtual Asset Service Providers (VASPs), including mandatory registration and comprehensive reporting obligations. In 2022, new legislation imposed significant financial penalties for non-compliance with AML standards, further supported by the deployment of blockchain-based monitoring systems to enhance transaction scrutiny and mitigate financial crime risks (OECD, 2022).

Despite these advancements, criticisms remain. The regulatory environment has been marked by a lack of transparency in licensing procedures for VASPs and inefficiencies stemming from fragmented coordination among the numerous governmental agencies tasked with financial oversight. These issues have been indicated as impediments to the system's overall effectiveness (FATF, 2021; MONEYVAL_4HU, 2022).

Slovakia

Slovakia has developed a regulatory framework consistent with AMLD5 and AMLD6 directives, yet implementation is hindered by technical and staffing constraints. The National Bank of Slovakia (NBS) and other oversight bodies report a pressing need for enhanced

investments in blockchain monitoring technologies to combat effectively money laundering and terrorist financing.

However, the regulatory framework faces notable gaps. Similarly to Poland, Slovakia has not established detailed regulations for non-custodial wallets, creating vulnerabilities that can be exploited for financial misuse. Moreover, insufficient awareness and education among cryptocurrency entrepreneurs pose challenges to the comprehensive implementation of AML regulations. Despite efforts in outreaching, the integration of these stakeholders into the compliance framework remains limited (MONEYVAL_3SL, 2023).

Ukraine

Ukraine has made significant strides in aligning its regulatory framework with international anti-money laundering (AML) and counter-terrorist financing (CTF) standards, addressing several deficiencies identified in earlier evaluations. Notable improvements include enhanced sanctions for AML/CFT violations, the introduction of risk-based supervision for virtual asset service providers (VASPs), and the adoption of comprehensive legislative changes through Law No. 361 (Law of Ukraine of December 6, 2019 No 362-IX)

Despite these advancements, challenges persist. The implementation of freezing obligations for terrorism-related assets remains incomplete, particularly concerning natural and legal persons beyond reporting entities. Moreover, while VASPs are now regulated, sector-specific guidelines and enforcement mechanisms are still under development, limiting their effectiveness. Ukraine also faces gaps in supervisory practices, such as the inconsistent application of risk-based approaches for non-financial businesses and professionals (DNFBPs), and limited sanctioning frameworks for management roles within these entities.

Efforts to improve technical compliance have led to upgraded ratings for specific recommendations, such as Recommendation 5 (now largely compliant). However, others, including Recommendations 6, 7, and 28, retain partially compliant statuses due to persistent shortcomings. A continued focus on implementing sector-specific measures and enhancing interagency coordination will be critical for Ukraine to further strengthen its AML/CFT framework (MONEYVAL_5UA, 2020).

Reports conducted by the Council of Europe's Committee of Experts provide comprehensive assessments of countries' compliance with international anti-money laundering and counter-terrorist financing standards, identify gaps, and recommend measures to enhance regulatory effectiveness. The alignment of anti-money laundering (AML) regulations among the V4 countries (Poland, Hungary, Slovakia, Czech Republic) and Ukraine with international standards, such as the FATF guidelines and EU AML directives (AMLD5 and AMLD6), is crucial for ensuring robust defence against money laundering and terrorist financing. Despite substantial progress, these countries face several significant regulatory and operational challenges.

Implementation of the travel rule

The travel rule, which mandates the sharing of sender and receiver information in virtual asset transfers, remains inconsistently adopted. Both Poland and Hungary have introduced customer identification and suspicious transaction reporting mechanisms consistent with FATF principles. Poland has established a VASP registry and lowered the threshold for customer due diligence (CDD) for virtual asset transactions to EUR 1,000. Slovakia and the Czech Republic face slower implementation. Slovakia has not fully addressed regulatory gaps regarding P2P transactions and non-custodial wallets, creating vulnerabilities. The Czech Republic also struggles with

enforcing compliance in decentralized and less-regulated virtual asset ecosystems. Despite adopting the "On Virtual Assets" law in 2020, Ukraine has yet to fully implement mechanisms for enforcing the travel rule, impeding cross-border AML collaboration. There is a lack of technical and legislative infrastructure to support compliance.

Persistent regulatory gaps and challenges

The alignment of AML frameworks across the V4 countries (Poland, Hungary, Slovakia, and the Czech Republic) and Ukraine is critical to strengthening their protection against financial crimes. These nations have made notable strides in adopting international standards, such as FATF guidelines and EU AML directives, but significant challenges remain. Key obstacles include the inconsistent implementation of regulations, limited resources, and gaps in monitoring emerging financial technologies such as virtual assets and non-custodial wallets. Addressing these issues is essential for enhancing regional and international cooperation in combating money laundering and terrorist financing.

- Lack of harmonization. Variations in regulatory frameworks among the V4 countries and Ukraine create opportunities for financial misuse. Differences in rules for non-custodial wallets allow criminals to exploit weaker regulatory environments. For example, while Poland has strict measures for VASPs, Slovakia and Ukraine lag in this regard, undermining regional AML consistency.
- Education and awareness deficiencies. Low awareness and understanding of AML/CFT obligations among key stakeholders hinder effective implementation.

Both Hungary and Slovakia report difficulties in engaging cryptocurrency entrepreneurs and financial institutions. Training programmes and outreach efforts are limited, leading to frequent non-compliance with AML regulations. In Ukraine, the integration of educational initiatives into regulatory strategies remains insufficient, further complicating compliance.

Limited technical and human resources

Slovakia and Ukraine face critical shortages in the technology and expertise needed to combat sophisticated financial crimes:

- blockchain monitoring: Slovakia reports insufficient investment in blockchain analytics tools, a critical gap in modern AML systems. Ukraine similarly struggles with deploying advanced technological solutions;
- specialized staff: resource constraints affect supervisory authorities, delaying implementation of FATF recommendations.

Impact of EU directives and national progress

The AML directives have been pivotal in shaping regulatory practices. These directives emphasize KYC measures, entity registration, and transaction reporting obligations, setting global benchmarks for financial transparency. Poland has implemented many aspects of AMLD5, including stricter CDD measures for VASPs and penalties for non-compliance. Hungary has enhanced its monitoring frameworks but still faces challenges in certain sectors. Slovakia and the Czech Republic are less advanced, with ongoing gaps in P2P oversight and implementation of risk-based approaches for non-financial businesses.

Non-custodial wallets and anonymity

Non-custodial wallets pose a significant regulatory challenge across the region. These wallets allow users to manage their private keys independently, creating anonymity risks:

- regulatory inaction: Slovakia, Ukraine, and the Czech Republic lack specific measures to regulate these wallets, enabling criminals to obscure financial flows;
- risk mitigation strategies: the adoption of blockchain analytics and enhanced transaction monitoring remains limited due to technical constraints, particularly in Slovakia and Ukraine.

Broader challenges and recommendations

The findings underscore several critical issues requiring urgent attention:

- Regional cooperation: greater collaboration among V4 countries and Ukraine is essential to close regulatory gaps and harmonize AML practices.
- Technological investment: enhancing blockchain monitoring capabilities should be a priority, alongside the development of cross-border transaction monitoring systems.
- Capacity building: investing in education and training for financial institutions, regulators, and cryptocurrency businesses will promote compliance and awareness of AML obligations.
- Unified standards: adopting a standardized framework for non-custodial wallets and virtual assets would prevent regulatory arbitrage.

While the V4 countries and Ukraine have made considerable progress, fragmented implementation and resource limitations continue to undermine the effectiveness of AML regulations. A coordinated, technology-driven approach, combined with strong education initiatives, is critical for advancing compliance and addressing the risks posed by emerging financial technologies. This would align the region more closely with FATF guidelines, fostering greater transparency and international cooperation.

These directives provide a robust foundation for the V4 region and Ukraine, offering clear directions for the further development of AML regulations in the context of emerging financial technologies.

Table 1 is based on MONEYVAL reports published by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. These reports assess the compliance of anti-money laundering (AML) and counter-terrorist financing (CFT) frameworks with international standards, such as the FATF recommendations. The table presents the legal foundations, cryptocurrency regulation scope, and key challenges for Poland, Slovakia, Hungary, Czech Republic, and Ukraine.

The table summarizes the key aspects of AML regulations in the V4 countries and Ukraine, highlighting the diverse approaches to blockchain and cryptocurrency technologies:

1. Poland and Hungary – both countries have made significant progress in implementing AMLD5 and AMLD6 directives, positioning themselves as regional leaders in aligning with EU standards. Poland has established a VASP registry but struggles with an incomplete alignment with FATF definitions and limited resources for oversight. Hungary, on the other hand, has enhanced its blockchain monitoring capabilities but faces challenges with transparency in VASP licensing and fragmented enforcement among agencies.

2. Czech Republic – the country adopts a moderate approach to blockchain regulation, allowing for innovation while maintaining oversight. However, gaps in regulations for non-custodial wallets and P2P transactions present vulnerabilities. Additionally, the lack of a unified supervisory framework complicates effective enforcement.
3. Slovakia – the country has aligned its legal framework with EU directives, but its implementation capacity is hindered by technological and staffing limitations. Education and awareness among private-sector stakeholders, particularly in cryptocurrency compliance, remain underdeveloped.
4. Ukraine – despite not being an EU member, Ukraine has modelled its AML framework on EU directives, showcasing regional influence. The law "On Virtual Assets" (Law of Ukraine of February 17, 2022…) was a landmark regulation, but the absence of robust blockchain monitoring tools and incomplete adherence to FATF guidelines limit its efficacy. Ukraine also faces resource constraints, further hindering full implementation.

Table 3.1. Overview of AML frameworks, cryptocurrency regulations, and challenges in the V4 countries and Ukraine

Country	Legal basis for AML	Scope of cryptocurrency regulations	Key challenges
Poland	AML/CFT Act (2021), enhanced through follow-ups (2023).	Virtual Asset Service Provider (VASP) registry established; lacks comprehensive alignment with FATF definitions.	Incomplete alignment with FATF; limited focus on risk assessments for new technologies.
Slovakia	AML Act (2018), further refined in enhanced follow-ups (2022, 2023).	Basic AMLD5 implementation; limited focus on non-custodial wallets.	Technical and staffing limitations; gaps in addressing non-custodial wallets.
Hungary	AML Act (2017), multiple updates including the 2022 follow-up.	Regulations for VASPs established; blockchain monitoring improved but gaps in enforcement remain.	Transparency in VASP licensing; fragmented enforcement across agencies.
Czech Republic	AML/CFT Act (2018), refined through three enhanced follow-ups by 2022.	Moderate cryptocurrency oversight; improvements noted in non-custodial wallet transparency.	Effective coordination between agencies; gaps in blockchain analytics investment.
Ukraine	Law No. 361 (2019), updated in the 2020 follow-up.	Initial VASP requirements introduced; more robust measures pending.	Limited resources for implementation; challenges in harmonizing with FATF standards.

Source: author's own work on the basis of (MONEYVAL_1PL, 2023; MONEYVAL_2CZ, 2022; MONEYVAL_3SL, 2023; MONEYVAL_4HU, 2022; MONEYVAL_5UA, 2020).

This table highlights the varied approaches to AML regulation and enforcement across the region, shaped by each country's legal, technological, and resource capacities. Key challenges, such as the harmonization of regulations, gaps in oversight of innovative technologies like blockchain, and deficiencies in P2P transaction monitoring, emphasise the need for enhanced regional collaboration and investment in advanced analytical tools. This serves as a foundation for examining the effectiveness of these regulations in both regional and global contexts.

3.4. The Importance of International Cooperation in Blockchain Development for AML

Money laundering and terrorist financing are global issues that demand coordinated international actions. In the era of digitalization and the growing popularity of cryptocurrencies, blockchain technology is seen as a tool to enhance AML systems, however the effective implementation of blockchain in AML requires regulatory harmonization, system interoperability, and international collaboration. The V4 countries (Poland, Czech Republic, Hungary, Slovakia) and Ukraine, despite their differing approaches to blockchain, can benefit from coordinated global efforts.

The Financial Action Task Force (FATF) plays a pivotal role in shaping global AML standards, including those related to cryptocurrencies and blockchain. Through its recommendations, such as the "travel rule," FATF requires Virtual Asset Service Providers (VASPs) to collect, store, and share information about the senders and recipients of cryptocurrency transactions (FATF, 2021).

- Travel rule: this rule obligates VASPs to exchange information with each other to identify users, increasing transaction transparency and making it harder to use cryptocurrencies for money laundering, yet implementing this rule faces technical challenges, particularly with transactions conducted via non-custodial wallets (Chuah, 2023).
- Promoting global standards: FATF supports member countries in adapting their legal systems to the challenges posed by cryptocurrencies. Uniform definitions of AML crimes and blockchain-related guidelines are key components of these efforts (Vandezande, 2017).
- EU directives: directives impose obligations on member states, such as registering VASPs, reporting suspicious transactions, and complying with KYC requirements. While countries like Poland and Hungary have aligned their regulations with these directives, differences in their interpretation and implementation persist.
- Role of regional initiatives: initiatives such as the EU's cryptocurrency regulations (MiCA) highlight that regional harmonization can be an effective solution. MiCA establishes legal frameworks for cryptocurrency market participants, serving as a model for other regions.

International collaboration in blockchain-based AML initiatives includes both governmental and international organizational projects:

- Europol: it conducts pilot projects leveraging blockchain to monitor financial flows across EU countries. These platforms enable faster detection of cross-border criminal activities by analysing large datasets in real time (Campbell-Verduyn & Hütten, 2021; Vandezande, 2017).
- Singapore: Singaporean authorities have developed a blockchain-based KYC platform that integrates data between public and private sectors. This system facilitates the rapid identification of suspicious activities and serves as a model for countries, including V4 members (Campbell-Verduyn, 2018).
- G20: G20 summits have repeatedly emphasized the importance of international regulatory frameworks for cryptocurrencies. Collaboration among member states has led to the development of common guidelines for blockchain and AML.

Despite the benefits of international collaboration, implementing blockchain in a cross-border context faces significant challenges:

1. Technology interoperability: the lack of common technical standards complicates the integration of blockchain systems between countries. Solutions developed in one country are often incompatible with systems used in other jurisdictions (Utkina, 2023).

2. Data protection and sovereignty: some countries are concerned that sharing financial data with others could undermine their sovereignty and lead to unintended political consequences (Zetzsche et al., 2020).
3. Implementation costs: developing blockchain systems that comply with international standards requires significant investments, which poses challenges for less affluent nations (Utkina, 2023).

Blockchain technology can play a pivotal role in global AML systems, but its effective implementation requires regulatory harmonization and international cooperation. FATF and regional organizations, such as the EU, should continue to promote global standards, support system interoperability, and encourage countries to invest in modern technologies. Only through coordinated global efforts can the full potential of blockchain in combating money laundering be realized.

3.5. Development Prospects and Recommendations

Blockchain technology holds transformative potential in the fight against money laundering (AML) in the V4 countries (Poland, Czech Republic, Hungary, Slovakia) and Ukraine. Despite advancements in regulatory frameworks, significant challenges remain in aligning technological capabilities, harmonizing legal standards, and fostering effective international cooperation. Drawing on insights from MONEYVAL reports, issued by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism other relevant studies, this section explores key development prospects and offers detailed recommendations to address these challenges.

Technological advancements and investment

The adoption of advanced technological tools is fundamental to modernizing AML frameworks. Blockchain analytics platforms capable of real-time financial flow monitoring enable authorities to detect suspicious transactions more effectively. However, countries such as Slovakia and Ukraine face resource constraints, limiting their access to these tools.

Investment in these technologies should be prioritized, supported by public-private partnerships and funding programmes, such as those offered by the European Union (Vandezande, 2017). Poland has demonstrated progress in implementing blockchain monitoring systems but requires further enhancements to fully leverage their potential. Some examples, e.g. Singapore's integrated financial supervision platforms, can serve as a model for implementing advanced analytics tailored to the unique needs of Central and Eastern Europe. Moreover, targeted training programmes for financial regulators, law enforcement, and compliance officers are essential. By equipping professionals with skills in blockchain analysis and cryptographic methods, countries can strengthen the operational capabilities of their AML frameworks.

Harmonization of international standards

The fragmented approach to AML regulations within the V4 region and Ukraine creates significant vulnerabilities, particularly in cross-border financial oversight. This issue has been highlighted in multiple MONEYVAL reports, which underline the importance of harmonizing regulatory frameworks to close legal loopholes exploited by financial criminals.

Implementing the FATF travel rule across all the countries in the region is a crucial step. This rule mandates that financial institutions share information about cryptocurrency transaction senders and recipients. While Poland, Czech Republic, and Hungary have taken initial steps toward compliance, Slovakia and Ukraine must accelerate their efforts to align with these international standards.

Additionally, Ukraine's virtual assets law (Law of Ukraine of February 17, 2022…) marks significant progress, but further steps are needed to harmonize its regulations with EU directives. Collaborative projects, such as drafting region-specific compliance guidelines or participating in EU-driven initiatives, could streamline the adoption of international AML standards across the region (Karpuntsov & Veresha, 2023).

Strengthening international cooperation

International cooperation is critical in combating the inherently global nature of money laundering. Countries in the region must prioritize collaboration with global organizations such as FATF, Europol, and Interpol. Coordinating joint operations and sharing intelligence can significantly improve the detection and prevention of cross-border financial crimes.

One promising area is the harmonization of VASP (Virtual Asset Service Provider) reporting systems, which would facilitate better information exchange and the oversight of cryptocurrency transactions. Initiatives like Europol's blockchain pilot projects demonstrate the effectiveness of real-time data sharing and could serve as a blueprint for regional cooperation.

Joint training programmes and workshops involving multiple jurisdictions can also enhance the skills of supervisory authorities, fostering a unified approach to tackling financial crime. Regular dialogue between regulatory bodies and private-sector stakeholders is equally important, ensuring that the latest technological and procedural innovations are effectively integrated into AML efforts.

Addressing emerging risks in Decentralized Finance (DeFi)

Decentralized Finance (DeFi) platforms present a double-edged sword in the fight against money laundering. While their transparent and immutable transaction ledgers offer new tools for oversight, their pseudonymity and lack of regulation pose significant challenges.

To mitigate risks, countries should develop targeted regulatory frameworks addressing the unique characteristics of DeFi ecosystems. For example, the enhanced scrutiny of cryptocurrency mixers, which obscure transaction origins, is essential. Such cases as Tornado Cash stress the need for robust international cooperation and innovative legal responses to address these emerging threats. Governments should also explore partnerships with blockchain developers to create DeFi platforms compliant with AML standards. By incorporating built-in compliance mechanisms, such as automated KYC processes and real-time transaction monitoring, DeFi can become a safer environment for legitimate financial activities (Zetzsche et al., 2020).

Education and awareness

Educational initiatives are a cornerstone of effective AML systems. Lack of awareness among financial institutions, VASP operators, and regulators often leads to gaps in compliance, increasing the risk of exploitation (FATF, 2021).

Countries should implement comprehensive education programmes targeting key stakeholders, which could include:

- Training for cryptocurrency service providers: focused on KYC protocols, transaction monitoring, and reporting suspicious activities. Such training ensures compliance with AML obligations and fosters a culture of accountability.
- Workshops for financial institutions: designed to enhance understanding of blockchain technology and its application in financial flow monitoring. These workshops can bridge the knowledge gap between traditional banking practices and emerging digital finance tools.
- Public awareness campaigns: aimed at educating the broader community about the risks of money laundering in the cryptocurrency environment. These campaigns can promote best practices and encourage individuals to support legitimate financial activities.

Moreover, integrating AML education into university curriculums, particularly in law and finance programmes, can build a new generation of professionals equipped to tackle the evolving challenges of financial crime. The integration of blockchain technology into AML systems offers immense opportunities to enhance transparency, efficiency, and cross-border cooperation. However, realizing this potential requires coordinated efforts to address existing challenges. By prioritizing technological investments, harmonizing regulations, fostering international collaboration, and emphasizing education, the V4 countries and Ukraine can establish a robust framework for combating financial crime. These measures will not only strengthen regional AML systems but also position Central and Eastern Europe as a global leader in leveraging blockchain technology for financial integrity. With consistent implementation, this region can set a benchmark for the effective use of innovation in the fight against money laundering.

3.6. Key Findings and Conclusions

The analysis presented in this chapter highlights the transformative potential of blockchain technology in combating money laundering (AML) within the V4 countries (Poland, Czech Republic, Hungary, Slovakia) and Ukraine. By addressing the research questions and the overarching goal of evaluating blockchain's application in AML systems, numerous key findings emerge.

A critical question addressed in this chapter concerns the benefits of international cooperation in implementing blockchain technology for AML. The findings reveal that effective collaboration among countries, supported by organizations like FATF, Europol, and Interpol, significantly enhances cross-border financial crime prevention. Initiatives such as the FATF travel rule and Europol's blockchain pilot projects demonstrate the value of shared intelligence and harmonized regulatory frameworks. These efforts enable consistent oversight, reduce the exploitation of jurisdictional gaps, and improve the ability to track illicit financial flows across borders.

The fragmented nature of AML regulations among the V4 countries and Ukraine creates vulnerabilities that financial criminals can exploit. This chapter highlights the need for harmonized approaches to blockchain regulation. While Poland and Hungary have made significant strides in implementing FATF and EU directives such as AMLD5 and AMLD6, Slovakia and Ukraine lag behind due to technological and regulatory constraints. Harmonizing these frameworks is not just a regional necessity, but also a global imperative to close legal loopholes and ensure consistent compliance mechanisms.

Addressing the question of how regulatory and technological disparities impact the adoption of blockchain in AML, the chapter identified several barriers, in particular:

- Technical infrastructure: Slovakia and Ukraine face resource limitations that hinder the adoption of advanced blockchain analytics platforms. Investments in these technologies are crucial to ensuring that financial flows can be monitored effectively in real-time.
- Non-custodial wallets and DeFi risks: the pseudonymity and lack of regulation in DeFi ecosystems present new challenges for AML compliance. Regulatory frameworks that target cryptocurrency mixers and mandate compliance features in DeFi platforms, such as automated KYC processes, are necessary to mitigate these risks.

A consistent theme throughout the analysis is the importance of educational initiatives to enhance AML compliance. A lack of awareness among cryptocurrency service providers, financial institutions, and regulators continues to hinder the effective implementation of AML standards. This chapter emphasizes the need for:

- training programmes for VASPs focused on KYC and suspicious activity reporting,
- workshops for financial institutions to bridge the gap between traditional finance and blockchain technologies,
- public awareness campaigns to educate users about the risks of money laundering in digital finance.

Integrating AML education into university curricula can also create a future workforce equipped to tackle the evolving complexities of financial crime.

In addressing the technological, regulatory, and operational dimensions of blockchain adoption for AML, the chapter highlighted significant opportunities:

- **Technological advancements**: blockchain enables the real-time monitoring of financial transactions, automated compliance mechanisms through smart contracts, and enhanced transparency in financial systems. The implementation of platforms such as Singapore's Project Ubin provides a model for Central and Eastern Europe.
- **International cooperation**: the region's ability to combat financial crime depends on its capacity to collaborate with global organizations and align with international standards. This includes adopting FATF guidelines and participating in EU-led initiatives such as MiCA to create a cohesive regulatory landscape.

The chapter's primary goal was to analyse the application of blockchain technology in AML within the context of the V4 countries and Ukraine, considering local challenges and global trends. The findings confirm that while blockchain technology offers immense potential for transforming AML systems, its effective implementation requires addressing the following:

- harmonizing AML regulations across the region to close legal loopholes,
- investing in advanced blockchain technologies to enhance oversight capabilities
- strengthening international cooperation to improve cross-border collaboration,
- enhancing education and awareness to foster compliance and reduce misuse.

By focusing on these areas, the V4 countries and Ukraine can build robust AML frameworks that leverage blockchain's unique features while addressing its inherent risks. The insights provided in this analysis serve as a foundation for further research and policy development, contributing to the broader understanding of how blockchain can combat financial crime in diverse regulatory and technological environments.

References

Barbereau, T., & Bodó, B. (2023). Beyond financial regulation of crypto-asset wallet software: In search of secondary liability. *Computer Law and Security Review*, *49*, Article 105829. https://doi.org/10.1016/j.clsr.2023.105829

Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: A call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, *32*(1), 80-97. https://doi.org/10.1108/JFRC-04-2023-0065

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*(2), 283-305. https://doi.org/10.1007/s10611-017-9756-5

Campbell-Verduyn, M., & Hütten, M. (2021). The formal, financial and fraught route to global digital identity governance. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.627641

Chuah, J. C. T. (2023). Money laundering considerations in blockchain-based maritime trade and commerce. *European Journal of Risk Regulation*, *14*(1), 49-64. https://doi.org/10.1017/err.2022.21

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) (OJ L 141, 5.6.2015, pp. 73-117).

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) PE/72/2017/REV/1 (OJ L 156, 19.6.2018, pp. 43-74).

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive(EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Text with EEA relevance) PE/37/2024/INIT (OJ L, 2024/1640, 19.6.2024).

FATF. (2021). *Updated guidance for a risk-based approach to virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Financial Analytical Office. (2020). *Annual report 2020*. https://fau.gov.cz/files/annual-report-2020-financial-analytical-office-of-the-czech-republic.pdf

Karpuntsov, V., & Veresha, R. (2023). Legal Aspects Of Virtual Assets Regulation in Ukraine. *Danube*, *14*(3), 235--252. https://doi.org/10.2478/danb-2023-0014

Law of Ukraine of December 6, 2019 No. 361-IX About prevention and counteraction of legalization (washing) of income gained in the criminal way, to financing of terrorism and financing of distribution of weapons of mass destruction (as amended on 18-12-2024)

Law of Ukraine of February 17, 2022 On virtual assets. https://zakon.rada.gov.ua/laws/show/2074-20#Text

Menon, R. E. (2023). From crime prevention to norm compliance: anti-money laundering (AML) policy adoption in Singapore from 1989-2021. *Journal of Money Laundering Control*, *26*(1), 69-92. https://doi.org/10.1108/JMLC-12-2021-0134

MONEYVAL_1PL. (2023). *Poland. Anti-money laundering and counter-terrorist financing measures. 1st enhanced follow-up report & technical compliance re-rating*. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Poland-MONEYVAL-FUR-2024.pdf.coredownload.inline.pdf

MONEYVAL_2CZ. (2022). *Czech Republic. Anti-money laundering and counter-terrorist financing measures. 3rd enhanced follow-up report & technical compliance re-rating*. https://rm.coe.int/moneyval-2022-15-fur-cz/1680a91c5f

MONEYVAL_3SL. (2023). *Slovak Republic. Anti-money laundering and counter-terrorist financing measures. 2nd enhanced follow-up report & technical compliance re-rating*. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Slovak Republic-MONEYVAL-FUR-2024.pdf.coredownload.pdf

MONEYVAL_4HU. (2022). *Hungary 5th enhanced follow-up report*. https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/Moneyval-FUR-Hungary-2022.pdf.coredownload.inline.pdf

MONEYVAL_5UA. (2020). *Ukraine. Anti-money laundering and counter-terrorist financing measures. 2nd enhanced follow-up report & technical compliance re-rating*. https://rm.coe.int/moneyval-2020-9-sr-2nd-enhanced-fur-ua/1680a01d6a

OECD. (2022). *Why Decentralised Finance (DeFi) matters and the policy implications*. OECD. https://doi.org/10.1787/109084ae-en

Piątkowska, B., & Skelnik, K. (2022). Binding solutions in the penalty system in the related institutions in the context Anti-money laundering directive. *Probacja*, *4*, 181-215. https://doi.org/10.5604/01.3001.0016.1255

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*, *33*(1), Article 33. https://doi.org/10.1007/s12525-023-00654-3

Ristic, P. (2023). Cryptocurrency money laundering: A new challenge for the European anti-money laundering framework. *Zeitschrift für Europarechtliche Studien*, *26*(2), 189-218. https://doi.org/10.5771/1435-439X-2023-2-189

Shanaev, S., Sharma, S., Ghimire, B., & Shuraeva, A. (2020). Taming the blockchain beast? Regulatory implications for the cryptocurrency Market. *Research in International Business and Finance*, *51*, Article 101080. https://doi.org/10.1016/j.ribaf.2019.101080

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*, *33*(4), 470-481. https://doi.org/10.1016/J.CLSR.2017.03.016

Sun, N., Zhang, Y., & Liu, Y. (2022). A privacy-preserving KYC-compliant identity scheme for accounts on all public blockchains. *Sustainability*, *14*(21), Article 14584. https://doi.org/10.3390/su142114584

Tosza, S. (2024). Enforcement of international sanctions as the third pillar of the anti-money laundering framework. An unannounced effect of the AML reform and the Sanctions Directive. *New Journal of European Criminal Law*, *15*(3). https://doi.org/10.1177/20322844241274166

U.S. Department of Treasury. (2022). *National money laundering risk assessment*. https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018 poz. 723).

Utkina, M. (2023). Leveraging blockchain technology for enhancing financial monitoring: Main challenges and opportunities. *European Journal of Interdisciplinary Studies*, *15*(2), 134-151. https://doi.org/10.24818/ejis.2023.21

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law and Security Review*, *33*(3), 341-353. https://doi.org/10.1016/j.clsr.2017.03.011

Zákon č. 253/2008 Sb. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. https://www.zakonyprolidi.cz/cs/2008-253

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, *6*(2), 172-203. https://doi.org/10.1093/jfr/fjaa010