www.rusi.org

Conference Report

Public–Private Partnerships and Virtual Assets in Ukraine

Taskforce Report

Oksana Ihnatenko
and Greta Barkauskienė

Conference Report

194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

RUSI Conference Report, August 2025

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Public–Private Partnerships and Virtual Assets in Ukraine

Taskforce Report

Overview

On 8 July 2025, RUSI's Centre for Finance and Security and the Center for Financial Integrity[1] convened the latest meeting of the Taskforce on Public–Private Partnership (PPP) in Fighting Financial Crime in Ukraine. Fifty representatives, including those from the public and private sectors in Ukraine, and international experts, gathered for an in-person meeting in Warsaw. The discussion focused on virtual assets (VAs)[2] in Ukraine. It included assessments of the related regulatory framework, risks and illicit activities, and international experience. Participants explored several recommendations to support the regulation and development of a safe VA market in Ukraine.

This report summarises the main findings of the meeting. None of the discussions at the meeting are attributable to any specific individual or organisation.

Introduction

As part of the EU accession process, Ukraine is expected to implement 69 reforms under the Ukraine Facility Plan, the EU's assistance programme.[3] One of these includes aligning legislation on VAs with the EU acquis – a step that is expected to be completed by the final quarter of 2025. This forms part of broader anti-money laundering (AML) measures.

1. Center for Financial Integrity, <https://cfi-ua.org/>, accessed 16 July 2025.
2. Virtual assets (VAs) or crypto assets refer to any digital representation of value that can be digitally traded, transferred or used for payment. To learn more, see Financial Action Task Force (FATF), 'Virtual Assets', <https://www.fatf-gafi.org/en/topics/virtual-assets.html>, accessed 16 July 2025. For the purpose of this paper, the terms 'VA' and 'crypto asset' are used interchangeably.
3. Ukraine Facility, <https://www.ukrainefacility.me.gov.ua/en/>, accessed 18 July 2025.

At the same time, Ukraine must ensure proper implementation of Financial Action Task Force (FATF) Recommendation 15,[4] which requires countries to assess and mitigate the money laundering and terrorist financing (ML/TF) risks related to VAs and virtual asset service providers (VASPs).[5] The country was rated as partially compliant in the last FATF follow-up assessment in 2020.[6] However, many experts fear that this rating could be downgraded in the upcoming MONEYVAL evaluation.[7] This could happen as soon as 2027.

Assessment of the Regulatory Framework of VAs in Ukraine

Attempts to regulate the VA market in Ukraine date back to 2018. The initial approach focused on developing regulations in collaboration with market participants. On 17 February 2022, the Law on Virtual Assets No. 2074-IX was adopted in Ukraine, but it has not yet come into force.[8] The key condition for its enactment was the resolution of taxation issues and the introduction of amendments to the Tax Code.

Efforts to amend and overhaul Ukraine's VA legislation led to the development of two draft laws between 2022 and 2023. One was prepared by the National Securities and Stock Market Commission (NSSMC), incorporating EU Markets in Crypto Assets Regulation (MiCA)[9] standards, while the other was proposed by the Ministry of Digital Transformation, combining existing legislation with

4. FATF is an intergovernmental body that sets global standards to combat money laundering, terrorist financing and other financial crimes through its 40 Recommendations. See FATF, 'What We Do', <https://www.fatf-gafi.org/en/the-fatf/what-we-do.html>, accessed 23 July 2025.
5. FATF defines virtual asset service providers (VASPs) as businesses that conduct activities such as exchanging, transferring, safekeeping, or providing financial services related to VAs on behalf of others. See FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', October 2021, p. 22, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>, accessed 21 July 2025.
6. MONEYVAL, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: Ukraine, 2nd Enhanced Follow-Up Report & Technical Compliance Re-Rating', June 2020, <https://rm.coe.int/moneyval-2020-9-sr-2nd-enhanced-fur-ua/1680a01d6a>, accessed 18 July 2025.
7. The MONEYVAL evaluation is a Council of Europe process that assesses countries' compliance with international anti-money laundering and counterterrorism financing standards, and the effectiveness of their implementation. See Council of Europe, 'Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism', <https://www.coe.int/en/web/moneyval/home>, accessed 21 July 2025.
8. « Закон України 'Про віртуальні активи' No. 2074-IX від 17 лютого 2022 » ['Law of Ukraine on Virtual Assets No. 2074-IX Dated 17 February 2022'], 2022, <https://zakon.rada.gov.ua/laws/show/2074-20>, accessed 16 July 2025.
9. European Securities and Markets Authority, 'Markets in Crypto-Assets Regulation (MiCA)', <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>, accessed 21 July 2025.

MiCA provisions.[10] The drafts sparked debate around taxation and market strategy but remain unadopted, leaving the sector unregulated.

On 24 April 2025, the Ukrainian parliament received Draft Law No. 10225-d 'On Amendments to the Tax Code of Ukraine and Certain Other Legislative Acts of Ukraine on the Regulation of the Circulation of Virtual Assets in Ukraine'.[11] This draft law consolidates previous proposals and has been revised to introduce key changes necessary for regulating the creation of a VA market in alignment with international standards. It introduces licensing requirements for platforms – including capital, transparency and know your customer (KYC) standards – and outlines reporting procedures for VA transactions.

The draft law provides clear classifications and definitions of VA types – such as crypto assets, e-money tokens (EMTs) and asset-referenced tokens (ARTs).[12] These fully align with MiCA standards. However, experts at the workshop expressed continued uncertainty about the proposed classifications.

Appointment of the Regulators

The designation of the responsible regulator is a key issue that remains unaddressed. Currently, there is no authority clearly tasked with overseeing the VA market in Ukraine. This creates uncertainty for both market participants and policymakers. The legislative proposals suggest using two separate regulators – in effect, a dual-regulator model. This would not be based on the type of activity, but on the type of entity that is being supervised. Under this model:

- The National Bank of Ukraine (NBU) would oversee banks involved in VA transactions. Banks would need a separate licence to work with VAs, making them active market participants. In this case, the bank would hold its core licence plus another one that allows it to operate in the trading space. The NBU would also regulate EMTs. Some experts pointed out that, in this case, crypto exchanges could also then fall under NBU supervision.

10. Kinga Redlowska and Oksana Ihnatenko, 'Strengthening Ukraine's Fight Against Financial Crime by Building Resilience', Center for Financial Integrity and RUSI Centre for Financial Security, March 2025, <https://cfi-ua.org/strengthening-ukraines-fight-against-financial-crime/>, accessed 21 July 2025.
11. « Проект Закону 'Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні' No.10225-д від 24 квітня 2025 » ['Draft Law on Amendments to the Tax Code of Ukraine and Some Other Legislative Acts of Ukraine on the Regulation of the Circulation of Virtual Assets in Ukraine No.10225-d Dated 24.04.2025'], 2025, <https://itd.rada.gov.ua/billinfo/Bills/Card/56271>, accessed 16 July 2025.
12. E-money tokens (EMTs) are crypto assets backed by a single fiat currency and used primarily for payments, such as USDT or USDC stablecoins. Asset-reference tokens are backed by a mix of assets to maintain stable value, making them more diversified than EMTs.

- Another regulator would oversee crypto exchanges. This regulator has not yet been specified, although Ukrainian experts anticipate that it would probably be the NSSMC. The NSSMC would supervise all other VASPs.

Several international experts at the workshop warned that traditional banking regulations cannot always be effectively applied to the rapidly evolving and distinct crypto sector. In particular, there is a risk of firms exploiting gaps or inconsistencies between the two regulators – regulatory arbitrage.

One expert cited France as a leader in EU crypto regulation, using a dual-regulator model and a phased approach requiring basic AML/counterterrorist financing registration for VASPs, with an optional MiCA-aligned licence. While over 100 VASPs registered by 2023, few pursued full licensing due to MiCA's complexity.[13]

The Ukrainian parliament will determine the regulator when it adopts the draft law. Ensuring coherence, clarity and functional alignment in regulatory oversight will be critical for market development.

Current Challenges to VA Regulation

As Ukraine moves to establish a clear legal framework for VAs, several challenges remain.

Experts raised the question of tax amnesty. Many politicians now argue that VA legislation cannot be adopted without first implementing a tax amnesty, allowing individuals to declare previously unreported assets.[14] While there were proposals for a simplified amnesty procedure in Ukraine, that push was ultimately halted. Ukraine's National Risk Assessment (NRA) identified crypto as a high ML/TF risk,[15] triggering FATF Recommendation 10 on customer due diligence (CDD).[16] In this context, a simplified tax amnesty is not feasible.

Meanwhile, courts are increasingly handling VA-related cases, but legal uncertainty remains due to inconsistent rulings and unclear procedures.[17] A

13. Financial Stability Board, 'Peer Review of France', Review report, 11 December 2024, p. 10, <https://www.fsb.org/uploads/p101224.pdf>, accessed 25 July 2025.
14. FATF, 'Managing The Anti-Money Laundering and Counter-Terrorist Financing Policy Implications of Voluntary Tax Compliance Programmes', October 2012, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Bestpracticesmanagingtheanti-moneylaunderingandcounter-terrorirstfinancingpolicyimplicationsofvoluntarytaxcomplianceprogrammes.html>, accessed 21 July 2025.
15. State Financial Monitoring Service of Ukraine, 'National Risk Assessment Report on Preventing and Countering Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism', 2022, p. 414.
16. FATF Recommendation 10 requires financial institutions to verify customer identity, identify beneficial owners, and monitor transactions. See FATF, 'FATF Recommendations', updated June 2025, page 14, <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf>, accessed 20 August 2025.
17. Dmitry Nikiforov and Victoria Balatskaya, 'Cryptocurrency, Police and Account Blocking: A Review of Court Decisions', Bargen, 1 February 2022, <https://bargen.com.ua/en/2022/02/01/kriptovalyuta-

private sector representative stressed the need to raise awareness and build capacity among judges and enforcement officers. The draft law would not create a separate crypto court – and Ukraine does not need one – but judges and enforcement officers need targeted education and training to ensure consistent, informed decision-making in cases involving VAs.

Despite some momentum, therefore, political will remains fragmented. Experts emphasised that sustained political support and clear interagency coordination will be crucial to moving forward.

Compliance with MiCA

The MiCA regulation entered into force across the EU in June 2023, introducing unified rules for the crypto-asset market.[18] While it offers legal clarity, experts caution that its complexity could stifle innovation and burden smaller firms. Since Ukraine is not yet an EU member, it has the opportunity to adopt a more gradual, tailored approach.

To develop a robust VA market, participants suggested that Ukraine should grant legal status to activities such as lending, borrowing and derivatives trading – all of which fall outside MiCA's current scope. Supporting these activities could help Ukraine to develop more efficient systems for transactions of cash-like assets – its liquidity infrastructure – and generate new revenue streams. Such streams are vital given the country's current economic challenges. For example, the regulation of stablecoins – digital tokens pegged to a stable value[19] – could be simplified by merging EMTs and ARTs into a single category. Issuance could be limited to regulated financial institutions, with the NBU serving as the custodian of reserves. Moreover, stablecoin payouts could be permitted to support usability and liquidity.

Ukraine's current economic needs often contradict the logic of EU legal acts. For now, the country must prioritise stability – even if it means a temporary deviation from MiCA.

What Should the Legislation Look Like?

Countries with the most developed VA markets often offer market flexibility. Since VAs continually change, the legislators cannot practically keep up. Therefore,

pravookhraniteli-i-blokirovka-schetov/>, accessed 19 July 2025.

18. European Securities and Markets Authority, 'Markets in Crypto-Assets Regulation (MiCA)'.
19. A stablecoin is a type of digital asset designed to maintain a stable value relative to a reference asset, such as a fiat currency or a basket of assets. It aims to overcome the price volatility issues often associated with many VAs. For example, a stablecoin such as USDT or USDC aims to keep its value at 1 USD. See FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', p. 17.

one expert suggested a reasonable policy: adopting a very high-level framework law that is sufficiently flexible to encompass future developments. The UAE offers a successful example, with a dedicated regulator and regulatory sandboxes[20] that support innovation while maintaining oversight.[21]

While flexible regulation models such as the UAE's support innovation, some countries have chosen more restrictive approaches. Moldova, for instance, banned VASPs following a FATF downgrade, while still permitting VA use.[22] Enforcement proved difficult, and concerns about election interference and illicit financing persisted.[23] By 2024, Moldova began shifting toward regulation.

To avoid enabling corruption or organised crime, Ukraine's VA legislation must balance effective control with practical implementation. Experts agreed that this includes creating a transparent licensing process and clear enforcement guidelines for law enforcement agencies (LEAs). To demonstrate the effectiveness of VA market regulation to MONEYVAL (the FATF regional body to which Ukraine belongs), Ukraine should register its first VASP. This would send a strong signal of regulatory readiness and help to reverse a growing trend of Ukrainian VASPs relocating abroad to seek clearer legal environments.

In sum, many participants remain hopeful that the long-overdue VA law in Ukraine will be passed by the end of 2025. This legislation could align the country with international standards, provide opportunities for VASPs to legally operate in Ukraine and help to attract investment for recovery.[24] With all this in mind, the desire to combat illicit finance and support global security should be the core driver for the introduction of the law.

20. A regulatory sandbox is a tool allowing businesses to explore and experiment with new and innovative products, services or businesses under a regulator's supervision. See Tambiama Madiega and Anne Louise Van De Pol, 'Artificial Intelligence Act and Regulatory Sandboxes', European Parliamentary Research Service Briefing, June 2022, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf>, accessed 16 July 2025.
21. Virtual Assets Regulatory Authority, <https://www.vara.ae/en/>, accessed 19 July 2025.
22. Parliament of the Republic of Moldova, 'Law on Prevention of Combating Money Laundering and Terrorism Financing No. 308 of 22.12.2017', 22 December 2017, <https://spcsb.gov.md/storage/legislation/National/AML_CFT%20Law%20308_2017.pdf>, accessed 19 July 2025.
23. Tom Keatinge, 'Episode 20: Moldova's Elections: Fighting Financial Interference', RUSI Suspicious Transaction Report Podcast, 6 June 2025, <https://www.rusi.org/podcasts/suspicious-transaction-report/episode-20-moldovas-elections-fighting-financial-interference>, accessed 28 July 2025.
24. Oksana Ihnatenko, 'Shaping Tomorrow: A Roadmap for Ukraine's Reconstruction Using Virtual Assets', RUSI Policy Brief, July 2024, <https://www.rusi.org/explore-our-research/publications/policy-briefs/shaping-tomorrow-roadmap-ukraines-reconstruction-using-virtual-assets>, accessed 21 July 2025.

Risks and Illicit Activities

VAs offer potential for financial innovation but pose regulatory challenges due to their rapid growth, global reach and pseudonymity. In Ukraine – amid war, recovery and EU alignment – a risk-based regulatory approach is essential. Such risks fall into two categories: universal risks experienced by all states; and risks specific to Ukraine.

General Risks

VAs present global risks related to their acceptance, storage and transfer due to limited traceability, inconsistent oversight, and weak consumer protections. A key concern is the difficulty of verifying the source of funds, particularly when transactions involve multiple platforms. Transfers are often irreversible, and interactions with unregulated services increase exposure to illicit finance. Poor wallet management practices can trigger regulatory scrutiny, while the lack of safeguards for storage increases the risk of asset loss and theft.

Ukraine-Specific Risks

The experts noted that Ukraine-specific risks are primarily connected with the over-the-counter (OTC) activities in the country,[25] its role as a threat hub and the role of crypto in funding procurement of sanctioned components for the Russian military, money mules and others.

OTC Activities and Russia's Influence

The FATF does not explicitly define OTC services, but they would fall under the definition of VASPs when facilitating VA transfers or exchanges as a business. Although exact figures are unavailable, OTC desks are reportedly active in nearly every major Ukrainian city and abroad.

Participants discussed how the growth of OTC activity has introduced serious national security and financial crime risks. These services are increasingly used to circumvent international sanctions, including the procurement of dual-use components for the Russian armed forces. Russian actors are actively exploiting OTC platforms as part of hybrid warfare efforts. Experts have noted that Russian actors are using social media platforms – particularly Telegram – to promote

25. An over-the-counter (OTC) desk is a specialised trading service that facilitates large cryptocurrency transactions directly between two parties, without disclosing trade details to the public. However, their confidentiality and often weak know your customer procedures can be exploited by criminals and sanctioned entities to evade financial regulations and launder money.

and facilitate the sale of synthetic drugs, with payments made via crypto wallets. This tactic is reportedly aimed at fostering drug addiction among Ukrainian military personnel, thereby weakening operational readiness and morale.

A targeted enforcement strategy – supported by PPPs and private sector tools – should include dedicated investigative personnel and local oversight. The potential benefits are substantial: one expert estimated that with improved oversight, Ukraine could recover up to $10 billion – a significant contribution to the national budget. Failure to regulate OTC desks may weaken Ukraine's standing with international partners.

The Role of Ukraine as a Threat Hub

By exploiting weak donor verification and outdated electoral finance laws to launder funds into politics, VAs are enabling foreign actors to influence Western democracies.[26] Ukraine, while not the origin, is seen as an emerging hub for laundering crypto funds due to its strategic location, wartime vulnerabilities and evolving regulations.

According to expert assessments by those attending the workshop, Russian intelligence services are leveraging Ukraine as a platform for political ML operations, exploiting its institutional gaps and conflict-related distractions. These networks may rely on corrupt facilitators within Ukraine, while simultaneously positioning Ukraine as the centre for the illicit flows – undermining its international credibility and democratic alliances.

It is therefore essential to strengthen Ukraine's capacity to monitor and regulate the activity of VAs. This supports domestic financial security and preserves the integrity of international political systems. Ukraine must prioritise the development of investigative and compliance capacities to prevent the country from becoming a permissive environment for illicit crypto-financial flows.

Crypto and Money Mules

Following Russia's full-scale invasion, the NBU imposed a temporary restriction on international wire transfers. This was aimed at preventing large-scale capital flight and to stabilise the national economy.[27] As VA use surged in response, new

26. Neil Barnett and Alastair Sloan, 'Democracy In The Crosshairs: How Political Money Laundering Threatens the Democratic Process', Atlantic Council, 2 October 2018, <https://www.atlanticcouncil.org/in-depth-research-reports/report/democracy-in-the-crosshairs-how-political-money-laundering-threatens-the-democratic-process/>, accessed 24 July 2025.
27. National Bank of Ukraine, « Постанова Правління НБУ 'Про роботу банківської системи в період запровадження воєнного стану' No. 18 від 24.02.2022 » ['Resolution of the Board, On the Operation of the Banking System During the Period of Martial Law, No. 18 Dated 24.02.2022'], 24 February 2022, <https://zakon.rada.gov.ua/laws/show/v0018500-22#top>, accessed 24 July 2025.

opportunities emerged for illicit financial activities – most notably through money mules, commonly known in Ukraine as 'drops' schemes.[28]

For a fee, the drops transfer the details and data of their card accounts for use by third parties.[29] One expert noted that crypto drops schemes are increasingly organised and decentralised, using social media and encrypted apps. Expert estimates suggest that the Ukrainian state budget may be losing approximately UAH 1 billion (about $24 million) per month due to crypto-related drops operations.

Several working groups within the Ukrainian parliament are currently reviewing legislative options to address these schemes, including enhanced due diligence requirements, the creation of a drops register,[30] and public awareness campaigns. To effectively counter this growing threat, Ukraine should invest in blockchain investigations, improve coordination between financial institutions and LEAs and engage international partners to trace cross-border flows.

Risk Mitigation and Blockchain Analytics Tools

Representatives from VASPs emphasised that collaborative regulation can yield positive outcomes, but global companies must navigate multiple regulatory frameworks. To manage ML/TF risks, VASPs use blockchain analytics and commercial tools for CDD and ongoing monitoring – although the quality and interoperability of these tools vary. Experts at the workshop noted that these tools often lack compatibility and are not yet fully reliable as court-admissible evidence, prompting efforts to develop standards for minimum requirements.

Participants noted that VASPs often mirror traditional financial institutions in their transaction monitoring but frequently need to build in-house tools for integrated oversight of fiat and crypto transactions. These systems support CDD and can detect risks through pattern analysis, even when external providers do not. However, data protection laws restrict private–private information sharing, limiting timely reporting – particularly in cases involving OTC brokers and peer-to-peer merchants.

VASP representatives also pointed out that, due to the lack of comprehensive legislation, there are challenges in providing cross-border assistance to the

28. On the growing prevalence of money mules, see Kinga Redlowska and Oksana Ihnatenko, 'Strengthening Ukraine's Fight Against Financial Crime by Building Resilience'.
29. Viktor Volokita, « У НБУ розповіли про майбутні проблеми «дропів» » ['The NBU Spoke about the Future Problems of "Drops"'], Українська Правда, 24 May 2024, <https://epravda.com.ua/news/2024/05/24/714190/>, accessed 20 July 2025.
30. FinAP, « НБУ планує створити реєстр «дропів» з обмеженим доступом до переказів » ['NBU Plans to Create a Registry of "Drops" with Limited Access to Transfers'], 8 May 2025, <https://finap.com.ua/nbu-planuye-stvoryty-reyestr-dropiv-z-obmezhenym-dostupom-do-perekaziv/>, accessed 24 July 2025.

public sector and, especially, LEAs. Therefore, broader cooperation initiatives that facilitate this cooperation and assistance are needed.

Role of the Traditional Financial Sector in Mitigating Risks Associated with VAs

During the discussion, it was pointed out that some financial institutions have adopted blockchain analytics and crypto-related KYC practices, although standardisation remains under discussion. Nonetheless, knowledge and capabilities vary widely, with many lacking the tools and expertise to effectively manage associated risks.

Despite efforts by some organisations to better understand sources of funds and indirect exposure, traditional institutions often avoid engaging with the crypto sector – potentially exposing themselves to unknown risks. One solution proposed by participants is to develop best-practice tools, such as KYC and CDD questionnaires, based on models such as the Wolfsberg Group's Correspondent Banking KYC Questionnaire.[31] The Wolfsberg Group Digital Assets Working Group is said to be developing such a questionnaire for crypto-related activity for use in the near future.

As pointed out by one participant, standard CDD questionnaire practices seem lacking – clients of a traditional financial institution may characterise their business as software development or programming services, when, in fact, they may be operating as active VASPs unknown to their financial service provider.

PPPs and VA Risk Assessment

The joint development of risk assessments is one promising area for enhancing the effectiveness of PPPs in Ukraine. A well-designed risk assessment provides an overview of current vulnerabilities and also serves as a strategic planning tool. For Ukraine, this means going beyond compliance checklists and building a forward-looking, evidence-based approach that is tailored to local realities.

Ukraine's 2022 National Risk Assessment included VA-related risks, but experts note it lacked depth and did not reflect sector-specific threats. A major gap is the absence of a clearly designated regulator for VAs. Moreover, LEAs and other key stakeholders were not fully involved in the process, reducing its effectiveness.

31. Wolfsberg Group, 'Correspondent Banking Due Diligence Questionnaire – New Version Publication', 17 April 2020, <https://wolfsberg-group.org/news/correspondent-banking-due-diligence-questionnaire-new-version-publication/>, accessed 16 July 2025.

Access to high-quality data remains a major barrier. While Ukrainian authorities receive summary reports from blockchain analytics providers, these are insufficient. Regulators need direct access to raw data and a wider range of sources, including open-source intelligence and exchange platform data. Tools that provide insights into liquidity, asset types and market behaviour could greatly enhance the state's analytical capacity.

To be meaningful, the process must be tailored to local realities, involve the right stakeholders, promote cross-sector awareness and apply innovative approaches to data collection and analysis.[32]

International Experience and Recommendations

Leveraging PPPs to Address Emerging Threats in the VAs Space

PPPs enable rapid, collaborative responses to financial crime by aligning public and private sector resources.[33] One example is the Europol Financial Intelligence Public Private Partnership (EFIPPP),[34] which was set up in 2017 as a cooperative mechanism between private sector stakeholders, financial intelligence units (FIUs) and investigative authorities to develop and share structured threat information (for example, financial crime typologies) among members.[35] Some FIUs have added greatly to these efforts.

One of the EFIPPP's initiatives is specifically focused on cryptoassets and involves over 100 participants. This initiative facilitates regular, confidential sharing of financial intelligence between public and private sector representatives, raising awareness of emerging risks, promoting mutual understanding, and serving as a key platform for ongoing knowledge exchange.

32. Noémi També and Allison Owen, 'Institutional Virtual Asset Service Providers and Virtual Assets Risk Assessment Guide', RUSI, 7 August 2023, <https://www.rusi.org/explore-our-research/publications/special-resources/institutional-virtual-asset-service-providers-and-virtual-assets-risk-assessment-guide>, accessed 16 July 2025.
33. Ian Mynot and Oksana Ihnatenko, 'First Taskforce Report: PPPs and Fighting Financial Crime in Ukraine', RUSI Conference Report, 10 January 2025, <https://www.rusi.org/explore-our-research/publications/conference-reports/first-taskforce-report-ppps-and-fighting-financial-crime-ukraine>, accessed 18 July 2025.
34. Europol Financial Intelligence Public Private Partnership, <https://efippp.eu/>, accessed 16 July 2025.
35. Europol, 'EFIPPP Practical Guide for Operational Cooperation Between Investigative Authorities and Financial Institutions', 30 January 2025, <https://www.europol.europa.eu/cms/sites/default/files/documents/EFIPPP_Practical_Guide.pdf>, accessed 15 July 2025.

It also provides a platform for discussing pressing matters that need solutions or require clarification. For example, the Travel Rule (TR) requirements[36] under FATF Recommendation 16 are implemented unevenly across jurisdictions.[37] This complicates efforts to establish a universally accepted, one-size-fits-all standard, even though blockchain technology is known to be borderless. Located in various jurisdictions, many VASPs still need to comply with the TR requirements. PPPs, such as EFIPPP, can bridge these gaps by facing challenges from the perspectives of FATF, regulators and VASPs.

Building a network of trusted experts is another way to leverage PPPs for finding solutions. While financial institutions, VASPs and regulators encounter similar challenges – particularly when it comes to a risk-based approach for monitoring and screening solutions – the key question is how to approach this issue, maintain flexibility and attain clarity on regulatory expectations.

PPPs and Challenges: Tackling Illicit Activity While Building Trust

Notably, national PPPs can complement these efforts through their own active international presence. For example, since its inception in 2021,[38] the Lithuanian PPP, the Center of Excellence in Anti-Money Laundering (AML Center), has been an active member of EFIPPP[39] and other international initiatives. To further ensure effective cooperation, it started a gradual expansion process in March 2024. Participants noted that the AML Center is now accepting vetted fintech members licensed by the Bank of Lithuania.

A representative of the AML Center noted that, of Lithuania's 370 registered VASPs, only 120[40] appear active; just 30 had sought licences by mid-2025. This indicates that the rest may potentially move their activities to other jurisdictions. These statistics illustrate that the crypto sector cannot be ignored, and therefore should be included in PPP activities even before full membership.

36. The Travel Rule, under FATF Recommendation 16, requires VASPs to collect and share originator and beneficiary information for VA transfers to detect suspicious activity and enforce sanctions. See FATF, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers', October 2021, para. 281, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>, accessed 13 August 2025.
37. FATF, 'Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers', June 2025, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>, accessed 17 July 2025.
38. Center of Excellence in Anti-Money Laundering, <https://amlcenter.lt/en/about-us/>, accessed 17 July 2025.
39. Europol Financial Intelligence Public Private Partnership, 'A Growing Community', <https://efippp.eu/#community>, accessed 17 July 2025.
40. *Ibid.*

Lithuania's proactive integration of VASPs offers a model for Ukraine, where unregistered activity persists and clarity is lacking. Participants agreed that legal certainty is needed across jurisdictions. However, extensive regulation may overwhelm limited institutional capacity. Instead, Ukraine and similar countries should adopt a focused compliance strategy – starting with essential requirements and gradually expanding – while engaging international partners to better understand and manage emerging risks.

Expert Recommendations

The meeting participants articulated a series of recommendations to enhance coordination and information sharing related to VAs in Ukraine. In addition, they identified legislative and regulatory measures that could reinforce public–private collaboration within the VA sector. Recommendations included the following:

Regulatory

- **Narrow the focus**: Concentrating on the specific assets that the country seeks to attract, such as stablecoins, may serve as an effective starting point. It also showcases the link between the regulatory framework and ensuring market attractiveness.
- **Recognise cybersecurity as interconnected**: There is substantial evidence that illicit activities, cyber threats and VAs are interconnected.
- **Establish clear rules and guidance**: There should be a clear understanding of the regulatory expectations of the minimum standard requirements to ensure satisfactory monitoring and risk mitigation measures, and related tools/solutions.

Supervision and Enforcement

- **Use existing solutions**: While building a regulatory framework takes time, illicit activity continues. LEAs should leverage established tools and expertise without delays.
- **Inspect a broader range of operations**: VA operations are not limited to online or fiat exchanges. Conducting both remote and onsite supervision of unregulated crypto exchanges and licensed currency exchanges is crucial to understanding the full landscape.
- **Adequately equip institutions**: VAs are currently the primary method for cross-border value transfers, yet many institutions lack the tools to trace

them effectively. Commercial solutions remain the most effective way to strengthen their capabilities.

Knowledge and Capacity-Building

- **Double-check the data**: Blockchain analytics tools aid VA tracing and risk mitigation, but are costly and lack interoperability. It is essential to verify their outputs rather than rely on them blindly.
- **Facilitate knowledge sharing**: Public–private knowledge exchange is evolving and often uneven. Sharing information fosters collaboration and reveals who is proactive versus those waiting for legal mandates.
- **Emphasise quality over quantity**: Available information is vast but often low quality. To detect illicit activity effectively, high-quality data must be structured and integrated with risk rules, blockchain analytics, behavioural patterns, and open source intelligence.

Effective Collaboration and Cooperation

- **Build a stakeholder map**: PPPs rely on trust and collaboration, making it essential to identify key stakeholders and understand their needs to support effective information sharing.
- **Foster synergy**: Frequently, business cases are interconnected: VASPs may lack full KYC data, while traditional finance often struggles with crypto risks. Bridging these gaps is key to stronger risk mitigation.

Outcomes

The Taskforce meeting concluded with two key outcomes that encapsulated the overall needs of the VA sector.

First, legislation is not a prerequisite for action. Instead, focused, practical efforts – especially through public–private collaboration – are essential to identifying and mitigating illicit activity. Such partnerships help ensure both sectors understand their roles and are equipped to respond effectively.

Second, Ukraine needs targeted and well-designed legislation. While certain measures – such as improving cybersecurity and disrupting illicit financial flows – can begin without delay, a precise legal framework, tailored to Ukraine's context, is needed.

Participants agreed Ukraine must avoid regulatory stagnation. Many countries have advanced with fewer resources by adopting simple, flexible approaches, which Ukraine must now prioritise to ensure timely progress.

About the Authors

Oksana Ihnatenko is the Managing Director of the Center for Financial Integrity in Ukraine. She is also a Researcher for the Supervising and Monitoring Ukraine's Reconstruction Funds project in RUSI's Centre for Finance and Security. Her research examines the resilience and integrity of Ukraine's financial system. Oksana is a Certified Anti-Money Laundering Specialist.

Greta Barkauskienė is a member of the Certified Financial Crime Specialists Association. She is an expert in financial crimes, specialising in AML/CFT topics, with a strong focus on crypto assets. With previous experience working at law enforcement agencies and the Financial Intelligence Unit Lithuania, she currently serves as an expert at the Center of Excellence in Anti-Money Laundering and is a member of the Digital Assets Task Force within the Global Coalition to Fight Financial Crime.