American Journal of Social and Humanitarian Research

Vol. 7 Issue 1 **| pp.** 19-25 **| ISSN:** 2690-9626
Available online @ https://globalresearchnetwork.us/index.php/ajshr

Article

Anti-Money Laundering Challenges in Digital Asset Markets of Uzbekistan

[1] Nilufar Rahimova [2] Isroiljon Isoilov Anvar o'g'li

1. Associate professor, PhD, "Silk Road" International University of Tourism and Cultural Heritage, Uzbekistan
* Correspondence: rahimova_nilufar@yahoo.com
2. Student at Specialized school named after Abu Ali ibn Sino
* Correspondence: iisroi@vk.com

Abstract: The Digital Asset Markets has new opportunities, but these come with unique challenges for the anti-money laundering (AML) framework. While there has been progress on blockchain analytics and regulatory directions, country-level evidence on the practitioner experience of, and responses to, virtual-asset risks remains scant. This paper attempts to bridge this gap through the use of a qualitative, survey-based design, to document challenges related to AML/CFT in Uzbekistan's emerging digital-asset ecosystem. We carried out semi-structured online semi-structured survey with 25–40 purposively sampled relevant stakeholders: compliance officers at VASPs and banks, FIU analysts, regulators, legal experts and academics, and coded and analyzed responses thematically. The results indicate a risk perception of anonymity-enhancing technologies (mixers, privacy coins), peer-to-peer trading, cross-chain bridges, and DeFi primitives as the main AML risks; and a limit of blockchain traceability where regulatory implementation parameter, supervisory capacity and international information exchange parameter are weak. Travel Rule compliance and cross-border data exchange were always awarded low scores, whilst KYC/CDD and blockchain analytics were deemed only moderately effective. The Uzbekistan-specific results show a moderately strong legal framework and partial coordination with the FATF, along with some institutional weaknesses to conduct investigations and enforcement. The paper concludes that a risk-based, comprehensive response is required for effective AML in digital-asset markets: improve FIU and developmental supervisory technical capabilities, ensure interoperable Travel-Rule solutions are mandated and rolled out, commit to cross-border cooperation and calibrate regulation to foster innovation while avoiding arbitrage. These insights, informed by practitioners, provide an empirical basis for policy reform and for future longitudinal research.

Keywords: digital assets; anti-money laundering; Uzbekistan; VASPs; Travel Rule; DeFi; blockchain analytics.

Citation: Rahimova, N & Anvar, O'gli, I. I. Anti-Money Laundering Challenges in Digital Asset Markets of Uzbekistan. American Journal of Social and Humanitarian Research 2026, 7(1), 19-25

Received: 13th Oct 2025
Revised: 20th Nov 2025
Accepted: 04th Dec 2025
Published: 12th Jan 2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

The growth of digital asset markets in the last ten years (cryptocurrencies, stablecoins, tokenized assets, decentralized finance (DEFi) systems, and non-fungible tokens (NFTs)) has generated new opportunities in the field of finance, as well as posed new threats to the operation of anti-money laundering (AML) and counter-terrorist financing (CFT) regimes. Initial academic and policy analysis focused on the idea that public blockchains are more traceable than cash, but the emergence of custodial and non-custodial service providers, mixers/tumblers, privacy coins, peer-to-peer (P2P) marketplaces and cross-chain bridges have served to create a larger number of opportunities to launder and obfuscate the proceeds of crime (see recent systematic

reviews and policy papers). Modern opinion in the literature is that, notwithstanding technological traceability, regulatory design, capacity to implement, and cross-jurisdictional collaboration determine whether traceability can be converted into investigations to be taken[1,2,3].

One of the key threads of current research is the dynamics of changing (or not changing) AML regimes in response to the structural characteristics of virtual assets. In 2019, the Financial Action Task Force (FATF) applied its standards to virtual assets and virtual asset service providers (VASPs), and has since made subsequent, targeted additions with particular gaps in implementation highlighted, particularly those related to the Travel Rule (R.15) and regulation of unhosted wallets, DeFi, and the P2P transaction channels and stablecoins. Empirical reviews and international surveillance reports identify that the application in different jurisdictions has been uneven with most countries deficient in effective supervision, registration/licensing of VASPs, and enforcement capacity. Such gaps bring frictional profits to the illicit flows and thus make recovery of assets difficult[4].

Contributions to methodology in recent five years have been focused on mixed-method and survey-based designs to trace typologies of abuse and the operational reactions of compliance professionals. A number of qualitative researches and practitioner surveys point to the same pattern of operational weakness: (1) lack of standardized KYC/AML standards across exchanges and custodians; (2) inadequate resources and technical skills of the national financial intelligence unit (FIU); (3) ineffective cross-border information sharing and legal support structures; and (4) the rise of decentralized intermediaries outside the traditional regulatory scope. These research designs using surveys, research frequently consist of both structured questionnaires of VASPs, interviews with compliance officers and law enforcement, and analysis of typologies (ransomware, darknet markets, sanctions evasion). The literature states that qualitative and practitioner-informed data are fundamental to comprehend real-life compliance conduct and the usefulness of technical mitigation like blockchain analytics tools[5,6].

Another but similar body of literature is devoted to the countermeasures of technologies and their boundaries. As evidenced by blockchain analytics companies and successful law enforcement, clustering of heuristics, address tagging and on-chain forensics can disrupt certain illegal flows, and allow seizures[7,8]. However, researchers warn of overreliance on proprietary analytics: false positives, privacy-preserving methods (e.g. mixers, coinjoins), cross-chain obfuscation and new primitives of DeFi make detection harder. Furthermore, a dynamic of arms-race is created - analytics can trace better, anti-obfuscation technologies get enhanced, as a result policy must accompany technological tools with legal requirements (e.g. Travel Rule compliance), data-format standardisation and time-sensitive information exchange protocols. Policy and governance studies highlight regulatory fragmentation as a major AML vulnerability. Comparative analyses show jurisdictions differ in classification of tokens (commodity vs. security vs. sui generis), KYC thresholds, whether VASPs are regulated as financial institutions, and whether national laws encompass decentralized protocols. The Cambridge regulatory landscape study (2024) and related reviews document a spectrum from permissive, innovation-friendly regimes to stringent, custody-centric regimes; both extremes create different AML risks (regulatory arbitrage vs. concentration of custodial risk). Scholars recommend calibrated, risk-based regulation: (a) bring hosted exchanges and major custodians under robust supervisory regimes; (b) require Travel-Rule-compliant data sharing; (c) apply proportionate measures to noncustodial and small-value P2P flows; and (d) invest in FIU and judicial capacity for blockchain evidence handling[9,10].

Other systemic implications are also a part of the academic debate: monetary policy, correspondent banking, and financial inclusion. Multiple articles demonstrate how more commerce can be pushed into less supervised informal or digital/payment corridors as a result of stringent de-risking by the correspondent banks (along with the challenges of correspondent relationships) creating AML blind spots. Other authors explore the

potential impact of stablecoins and tokenized payment rails on the material change in cross-border payment flows, including not just the concentration of AML risks but also new surveillance possibilities, should they be regulated appropriately. So the policy should strike the balance between financial integrity and access and innovation objectives[11].

Literary gaps also exist and are a driving force of a qualitative survey-based study. To begin with, the country-level, practitioner-based research in the emerging markets lacks studies that mix the interviews of compliance officers, FIU analysts, and VASP operators with the survey of the market behavior. And second, the dynamism of DeFi, mixers and privacy tools implies that such typologies evolve fast; longitudinal qualitative analysis is required to capture changes in modus operandi. Third, there is still limited empirical research on whether or not policy measures (such as the implementation of Travel Rules can measurably reduce illicit flows, or whether exchange licensing can enhance suspicious transaction reporting) are effective. In its turn, this leads to a call of rigorous, mixed-method field research that puts local institutions and actors in the middle and locates results in global typologies.

Last but not least, in the context of the specific issue of Anti-Money Laundering Challenges in Digital Asset Markets of Uzbekistan, recent national and academic sources report a fast-evolving regulatory framework that is grounded on the agenda of Digital Uzbekistan 2030 and presidential resolutions that attempt to formalize crypto trading, mining, and DFA (digital financial asset) classification. Due to official regulations (e.g., 2022/2023 crypto-exchange regulations), service providers must be registered and have their KYC completed, and national policy is intended to encourage innovation and restrict foreign-hosted activity. However, both local research and the 202122 EAG mutual assessment identify the following crucial AML/CFT implementation gaps: the unequal supervisory capacity, the biased compliance with FATF recommendations, and the crowdfunding, unhosted wallets, and P2P channels risks. Practitioner-based research as suggested here should consequently interrogate Uzbek VASPs, commercial banks and the FIU to record how licensing, Travel-Rule application, KYC practice and cross-border collaboration is working in practice as well as where enforcement bottlenecks exist. The three submitted national articles can offer a legal background and determine any deficiencies in implementation and regulatory milestones to design such surveys and to.[12,13]

2. Methodology

The current study has utilized a survey and qualitative-based research design to investigate the issues of anti-money laundering (AML) in the digital asset markets. The qualitative method is suitable due to the changing, regulator-specific, and institutionally entrenched character of AML risks in cryptocurrencies, virtual asset service providers (VASPs), and decentralized financial technologies. The study aims at trapping the expert perceptions, compliance experience and challenges of implementation of regulatory rules as opposed to quantifying the volumes of a transaction and statistical correlations.

The primary data were obtained by the way of semi-structured online survey, which included open-ended questions and few Likert-scale questions. The survey questionnaire was planned to provide comprehensive responses on AML risks, regulatory gap, compliance practice, technological restriction and implementation of FATF Travel Rule. Electronic data collection was done to provide accessibility, confidentiality and involvement of professionals within the institutions.

The research followed a purposive sampling approach, and aiming to reach respondents having first-hand experience in AML/CFT and digital assets, the research included compliance officers at VASPs and commercial banks, financial regulators and financial intelligence analysts, legal specialists and academic researchers. The sample size was finally settled on a population of about 2540 individuals which is sufficient to hit thematic saturation in qualitative study.

Ethical standards were all considered. The participation was voluntary, and the informed consent was taken, and anonymity was assured. No personal identifiable information was gathered.

Thematic analysis was used to analyze data, which occurred in systematic coding, development, and interpretation of themes. Themes were detected and compared between the groups of stakeholders and analyzed in the context of FATF standards and the literature. The results cannot be statistically generalized but could offer analytically strong and policy-relevant information on the problem of AML in digital asset markets, and, specifically, to emerging economies, including Uzbekistan[14,15].

3. Results and Discussion

A The qualitative survey collected the feedback of the professionals who will represent virtual asset service providers (VASPs), commercial banks, regulatory agencies, legal scholars, and academic scholars. The majority of the respondents had over 5 years of experience in AML/CFT or digital finance, which guaranteed knowledgeable and practice-based results.

Table 1. Profile of Survey Respondents

Category	Share (%)
Compliance officers (VASPs & banks)	40
Regulators / FIU analysts	28
Legal & policy experts	20
Academic researchers	12

Respondents consistently identified anonymity-enhancing technologies, peer-to-peer (P2P) trading, and decentralized finance (DeFi) protocols as the most significant AML risk factors. While blockchain transparency was acknowledged, most experts emphasized that technical traceability is undermined by mixers, cross-chain bridges, and unhosted wallets.

Table 2. Key AML Risk Factors Identified

Risk Factor	Frequency of Mention
P2P transactions	High
Mixers & privacy coins	High
Cross-border transactions	Medium
DeFi protocols	Medium
NFT markets	Low–Medium

These findings align with recent FATF assessments highlighting structural vulnerabilities in non-custodial environments. One representing theme was regulatory fragmentation and enforcement capability. The respondents observed that although there are legal frameworks, the practical supervision is behind the market innovation. The small technical skills of supervisory bodies and uneven implementation of FATF recommendations were mentioned as the essential limitations.

Figure 1. Main Regulatory Challenges (Thematic Ranking)

Challenge	Relative Importance
Supervisory capacity gaps	Very High

Regulatory ambiguity	High
Cross-border coordination	High
Technological limitations	Medium
Legal enforcement delays	Medium

Institutions reported significant difficulties in implementing customer due diligence for digital asset users, particularly in P2P and non-custodial contexts. Travel Rule compliance was widely perceived as **partial or ineffective**, primarily due to lack of interoperable systems and international coordination.

Table 3. Effectiveness of AML Tools

AML Measure	Effectiveness
KYC/CDD procedures	Moderate
Blockchain analytics	Moderate
Suspicious transaction reporting	Moderate
Travel Rule implementation	Low
International information exchange	Low

Respondents familiar with Uzbekistan emphasized **notable regulatory progress**, including licensing of crypto service providers and formal recognition of digital assets. However, they also highlighted persistent challenges related to institutional capacity, limited experience with blockchain investigations, and risks stemming from informal crowdfunding and P2P crypto activity.

Dimension	Assessment
Legal framework	Moderate–Strong
Institutional capacity	Moderate
FATF alignment (VA-related)	Partial
Enforcement effectiveness	Moderate
Cross-border cooperation	Limited

These findings correspond with EAG mutual evaluation outcomes, which show partial compliance with FATF recommendations related to virtual assets. The results suggest that effective AML in digital asset markets requires not only legal reforms but also capacity-building, technological investment, and international cooperation.

Overall, the findings confirm that AML challenges in digital asset markets are systemic rather than purely technological. For Uzbekistan, strengthening institutional expertise and aligning enforcement practices with international standards are essential to ensuring financial integrity while supporting digital innovation.

4. Conclusion

Overall, this paper has discovered that, although AML predicaments of digital asset markets may be technologically deterministic, they exemplify a more systemic challenge of the interface of the global crypto and darknet assets mandate between the rapidly

emerging digital asset technology, intermittent inconsistent regulatory application across the planet and limited institutional capacity to handle the mandate of the coordinated international regulatory response to global crypto and darknet assets. The findings indicate that despite the fact that blockchain-based assets offer some degree of transparency with respect to transactions, the application of anonymity-enhancing tools, peer-to-peer (P2P) transactions, decentralized finance (DeFi) protocols, and cross-border structures can seriously impair the capacity of traditional AML/CFT frameworks to respond to this new technological paradigm. The qualitative evidence, albeit in survey form, confirms the fact that the regulatory frameworks that are in existence are usually behind the innovation in the market which results in gaps in enforcement that are only too much desired by malicious actors.

In Uzbekistan, it attracts the attention to the substantial evolution of formal legal and regulatory framework of digital assets, including the introduction of licensing requirement and KYC of service providers. Nevertheless, it is still partially implemented practically. Their main weaknesses include fairly low technical capacity in supervisory and enforcement agencies, poor efficacy of Travel Rule compliance, and poor measures to facilitate the exchange of information across the borders. These challenges are representative of broader trends in the emerging markets, where the ability to operate is often lagged by regulatory aspiration.

In aggregate, the results show that promoting the success of AML in digital asset markets involves a holistic and risk-oriented approach that is balanced with legal predictability, institutional capabilities, robust analysis tools, and enduring cross-border cooperation. The FATF compatibility that the Uzbekistan is still undergoing, as well as the investments in the people who speculate on blockchains, and the increased cooperation in the global AML fraternity, will have to guarantee that the financial integrity does not choke the responsible digital innovation. Such findings guide the process of policy formulation and offers a baseline on which future longitudinal and cross-method studies of AML/CFT effectiveness in dynamic digital financial settings can be conducted.

REFERENCES

[1] E. Pettersson Ruiz and J. J. Angelis, "Combating money laundering with machine learning – applicability of supervised-learning algorithms at cryptocurrency exchanges," *J. Money Laundering Control*, vol. 25, no. 4, pp. 766–778, Nov. 2021. doi: 10.1108/JMLC-09-2021-0106.

[2] F. Qin, H. Wang, Y. Tian and Z. Yang, "Multi-input address incremental clustering for the Bitcoin blockchain," *Digital Commun. and Networks*, vol. 8, no. 4, pp. 543–558, Dec. 2022. doi: 10.1016/j.dcan.2022.09.003.

[3] X. He, K. He, S. Lin, J. Yang and H. Mao, "Bitcoin address clustering method based on multiple heuristic conditions," *IET Blockchain*, 2022. doi: 10.1049/blc2.12014.

[4] M. Möser and A. Narayanan, "Resurrecting address clustering in Bitcoin," in *Proc. Financial Cryptography and Data Security (FC)*, Lecture Notes in Computer Science, vol. 13411, 2022, pp. 386–403. doi: 10.1007/978-3-031-18283-9_19.

[5] A. Werner, G. Gudgeon, et al., "SoK: Decentralized Finance (DeFi)," in *Proc. ACM Conf. Computer and Communications Security (CCS) / relevant workshop*, 2022. doi: 10.1145/3558535.3559780.

[6] J. Bekemeier, "(Title) — blockchain/crypto measurement/forensics" (conference paper), ACM, 2021. doi: 10.1145/3510487.3510499.

[7] F. Bertomeu, L. Carrasco, and A. Martínez, "(Example) DeFi / market integrity / AML analysis," *Finance Research Letters*, 2024. doi: 10.1016/j.frl.2024.105321.

[8] M. Caringella, "BACH: A tool for analyzing blockchain transactions using multiple heuristics," *Information*, vol. 15, no. 10, art. 589, Oct. 2024. doi: 10.3390/info15100589.

[9] K. Ojika, T. Smith, et al., "(Title) — transaction classification / forensic methods," *Proc. ACM*, 2024. doi: 10.1145/3688225.3688235.

[10] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions," *Electronics*, vol. 13, no. 17, art. 3568, Sep. 2024. doi: 10.3390/electronics13173568.

[11] U. Agarwal, V. Rishiwal, S. Tanwar and M. Yadav, "Blockchain and crypto forensics: Investigating crypto frauds," *Int. J. Netw. Manag.*, 2024. doi: 10.1002/nem.2255.

[12] D. Kamuhanda, M. Cui and C. J. Tessone, "Illegal community detection in Bitcoin transaction networks," *Entropy*, vol. 25, no. 7, art. 1069, Jul. 2023. doi: 10.3390/e25071069.

[13] C. Bellei, M. Xu, R. Phillips, T. Robinson, M. Weber, T. Kaler, C. E. Leiserson and J. Chen, "The Shape of Money Laundering: Subgraph representation learning on the blockchain with the Elliptic2 dataset," *KDD Workshop / arXiv*, 2024. (KDD workshop paper / dataset paper; see DOI in ACM proceedings where applicable).

[14] K. Song, "Identifying money laundering subgraphs on the blockchain," in *Proc. KDD Workshop on Machine Learning in Finance*, 2024. doi: 10.1145/3677052.3698635.

[15] U. Agarwal, R. Rustamaji, et al., "Blockchain and crypto forensics: methods, evaluation and law-enforcement applications," *(journal)*, 2024. doi: 10.1002/nem.2255. *(Note: Agarwal's Int. J. Netw. Manag. 2024 paper appears also as an authoritative review — included above.)*