LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

O'ZBEKISTONDA KRIPTO-AKTIVLAR YORDAMIDA MOLIYAVIY JINOYATLARGA QARSHI KURASHDA KYC TIZIMI

Raxmonova Charos
Toshkent davlat yuridik universiteti magistranti

Annotatsiya: *ushbu maqolada O'zbekiston Respublikasida kripto-aktivlar bilan bog'liq moliyaviy jinoyatlarga qarshi kurashning asosiy huquqiy mexanizmi sifatida «Mijozni bil» (KYC) tizimi tahlil qilinadi. Ichki nazorat qoidalari (рег. № 3309, 2021) va Prezidentning PP-3832-sonli Farmoni (2018) asosida mijozni identifikatsiya qilish, tegishli tekshiruv, shubhali operatsiyalarni aniqlash va aktivlarni muzlatish bo'yicha majburiyatlar ko'rib chiqiladi. Maqolada KYC tekshiruv jarayoni batafsil tahlil qilinib, amaldagi tartibga solishning uchta tizimli kamchiligi aniqlanadi va FATF standartlariga asoslangan huquqiy takliflar ilgari suriladi.*

Kalit so'zlar: *KYC, kripto-aktivlar, AML/CFT, pul yuvish, terrorizm moliyalashtirish, рег. № 3309, tegishli tekshiruv, shubhali operatsiyalar, FATF, O'zbekiston, blokcheyn-analitika, ichki nazorat.*

СИСТЕМА KYC КАК ИНСТРУМЕНТ ПРОТИВОДЕЙСТВИЯ ФИНАНСОВЫМ ПРЕСТУПЛЕНИЯМ С ИСПОЛЬЗОВАНИЕМ КРИПТО-АКТИВОВ В УЗБЕКИСТАНЕ

Рахмонова Чарос

Магистрант Ташкентского государственного юридического университета

Аннотация: в данной статье анализируется система «Знай своего клиента» (KYC) как основной правовой механизм противодействия финансовым преступлениям с использованием крипто-активов в Республике

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Узбекистан. На основе Правил внутреннего контроля (рег. № 3309, 2021) и Постановления Президента № ПП-3832 (2018) исследуются нормы об идентификации клиентов, надлежащей проверке, выявлении подозрительных операций и заморозке активов. Выявлены три ключевых пробела в действующем регулировании и предложены конкретные правовые меры по их устранению.

Ключевые слова: *KYC, крипто-активы, AML/CFT, отмывание денег, финансирование терроризма, рег. № 3309, надлежащая проверка, подозрительные операции, FATF, Узбекистан, блокчейн-аналитика, внутренний контроль.*

THE KYC SYSTEM AS A TOOL FOR COMBATING CRYPTO-ASSET FINANCIAL CRIME IN UZBEKISTAN

Charos Rakhmonova

Master's Student of Tashkent State Law University

Abstract: this article examines the Know Your Customer (KYC) system as the primary legal mechanism for combating financial crimes involving crypto-assets in the Republic of Uzbekistan. Drawing on the Internal Control Rules (Registration No. 3309, 2021) and Presidential Decree No. PP-3832 (2018), the study analyses the specific obligations governing client identification, customer due diligence, suspicious transaction reporting, and asset freezing. The article traces the complete KYC verification flow and identifies three structural gaps in the current framework, proposing concrete legal reforms grounded in FATF standards.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Keywords: *KYC, crypto-assets, AML/CFT, money laundering, terrorism financing, Reg. No. 3309, customer due diligence, suspicious transactions, FATF, Uzbekistan, blockchain analytics, internal control.*

INTRODUCTION

When Uzbekistan legalised crypto-asset trading in 2018, the regulatory challenge was clear: how do you prevent a pseudonymous, borderless financial system from being used to move illicit funds? The answer embedded in Presidential Decree No. PP-3832 was to place responsibility on the service provider - requiring it to know exactly who its clients are before any transaction takes place. That obligation, the Know Your Customer (KYC) system, sits at the core of the Internal Control Rules adopted in 2021 (Registration No. 3309).[1]

Gulommamatova (2025) shows that crypto-asset laundering - disguising illegally obtained digital assets through mixing services, chain-hopping, and privacy coins - reproduces every structural element of classical fraud: misrepresentation, concealment of ownership, and deceptive intent. KYC disrupts this by breaking anonymity at the regulated point of entry. A transaction that cannot be attributed to an identified person cannot be investigated, reported, or frozen. The entire AML/CFT system depends on the KYC layer being sound.[2]

[1]Decree of the President of the Republic of Uzbekistan No. PP-3832 of 3 July 2018 "On Measures for the Development of the Digital Economy and the Sphere of Crypto-Asset Circulation in the Republic of Uzbekistan". Available at: https://lex.uz/docs/3806048
[2]Gulommamatova, P. (2025). Crypto-Asset Laundering is a Fraud Crime. Uzbek Journal of Law and Digital Policy, 3(2), 34–44. https://doi.org/10.59022/ujldp.315

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

This article proceeds in four parts: the legal text of Reg. No. 3309 provision by provision; the KYC verification flow in practice (Figure 1); three gaps in the current framework; and targeted legal reforms to close them.

RESEARCH RESULTS

The Legal Framework: Reg. No. 3309 (2021)

Article 1 defines 'internal control' as a continuous four-element obligation: customer due diligence; risk management for money laundering, terrorism financing, and WMD proliferation financing; identification of suspicious transactions; and screening for operations involving persons on the terrorism list. The definition is significant - KYC is not a one-time onboarding step but a permanent obligation running throughout the entire business relationship.[3]

For client identification, Article 1 requires establishing data based on documents provided by the client. For natural persons: full name, identity document, address, and taxpayer number. For legal entities, the provider must also identify the beneficial owner - the natural person who ultimately controls the entity - by examining ownership structures through founding documents. Chapter 3 mandates enhanced due diligence for politically exposed persons and clients from non-cooperative jurisdictions.[4]

[3]Reg. No. 3309, Art. 1: definitions of 'internal control', 'client identification', and 'customer due diligence'. https://lex.uz/docs/5450936
[4]Reg. No. 3309, Chapter 3: customer due diligence, including enhanced CDD for politically exposed persons and clients from non-cooperative jurisdictions. https://lex.uz/docs/5450936

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Chapter 5 defines a suspicious transaction as any operation where the provider has formed a suspicion of money laundering or terrorism financing. The indicators cover: transfers to persons in offshore zones; repeated crypto-asset exchanges followed by withdrawal to private wallets; persistent use of anonymisation tools or IP-masking; transaction volumes inconsistent with the client's stated business purpose; and counterparties in FATF-identified non-cooperative jurisdictions. These indicators map directly onto the laundering techniques documented by Gulommamatova (2025) - mixing, chain-hopping, and privacy coins.[5]

Chapter 6 requires that when a client matches the terrorism and WMD list (the Perchen'), the provider must immediately freeze assets and notify the DCEC - without informing the client. This obligation is continuous, not limited to onboarding. Article 36 mandates blockchain analytics software capable of assessing wallet risk profiles and tracing transaction flows. Chapter 8, Article 47 requires all KYC records to be retained for a minimum of five years.[6]

The KYC Verification Flow in Practice

Figure 1 shows how the obligations above connect in a single verification process — a cascading gate system where each stage depends on the one before it.

[5]Reg. No. 3309, Art. 1 and Chapter 5: definition and indicators of suspicious transactions. https://lex.uz/docs/5450936
[6]Reg. No. 3309, Art. 36: blockchain analytics software obligation; Chapter 8, Art. 47: five-year record retention. https://lex.uz/docs/5450936

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

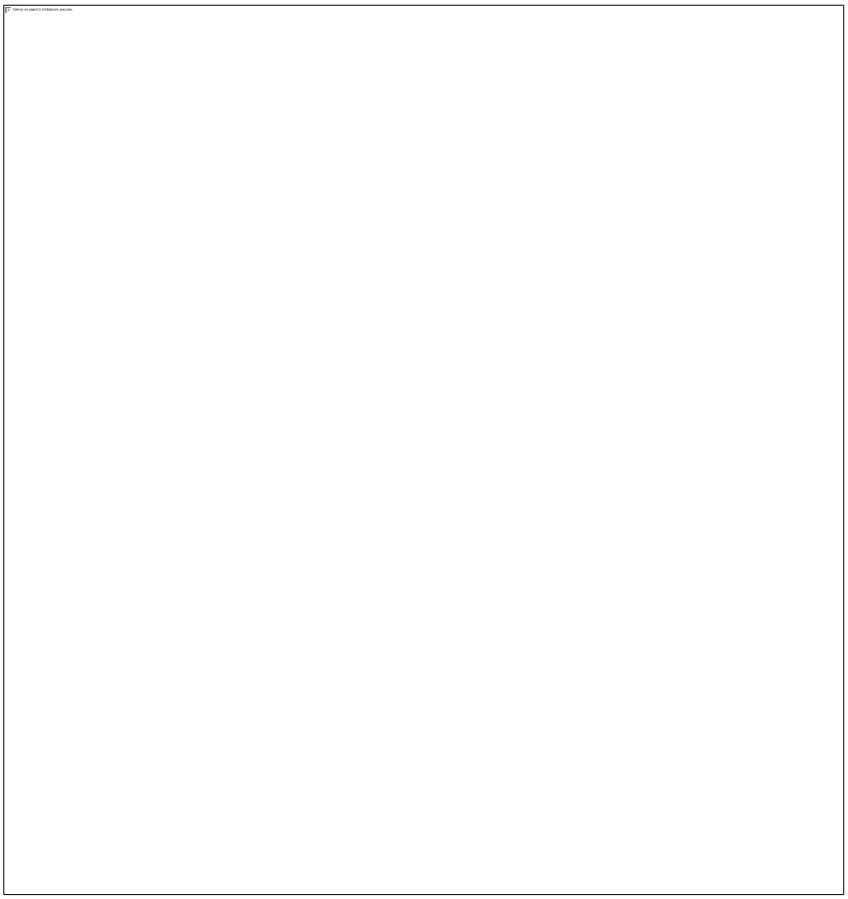

Figure 1. KYC and AML verification flow under Registration No. 3309 (2021) — lex.uz/docs/5450936

The process begins at client registration. Before any transaction, the provider completes identity verification and beneficial ownership identification (Art. 1, Ch. 3). Perchen' screening under Chapter 6 follows immediately: a match triggers an automatic freeze and DCEC notification. Clients who clear screening proceed to risk scoring under Chapter 4, which determines the intensity of subsequent monitoring. Transaction monitoring under Chapter 5 and Article 36 runs continuously: each flagged transaction is assessed at the second decision point, and

confirmed suspicion leads to suspension and reporting to the DCEC. Clients who generate no suspicion remain under ongoing monitoring - the loop never closes.[7]

Three Gaps in the Current Framework

First, the Travel Rule is absent. FATF Recommendation 16 requires that when a crypto-asset transfer moves between two service providers, the sending provider must transmit originator and beneficiary identification data to the receiving provider in real time. Reg. No. 3309 does not implement this rule. A Uzbek provider sending assets to a foreign platform today is not legally required to attach any identification data to that transfer. The receiving institution gets the funds and nothing else.[8]

Second, foreign platforms are not required to hold licences. The Crypto-Magazine Operation Rules (Reg. No. 3395, 2022) permit Uzbek providers to transact through foreign platforms, but neither Reg. No. 3309 nor Reg. No. 3395 requires those platforms to be regulated in their home jurisdictions. A domestic provider can legally route transactions through an unregulated offshore platform - precisely the kind of gap that chain-hopping exploits.[9]

Third, no minimum technical standards govern blockchain analytics. Article 36 requires providers to use analytics software but specifies no minimum capabilities. Two providers can both be formally compliant - one using a

[7]Resolution of the NAPU No. 3 (8 June 2021) and DCEC No. 16 (7 June 2021). Internal Control Rules (Registration No. 3309). Available at: https://lex.uz/docs/5450936
[8]Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. Paris: FATF. https://www.fatf-gafi.org
[9]Order of the Director of NAPP No. 43 of 29 September 2022. Rules for the Operation of a Crypto-Magazine (Registration No. 3395). Available at: https://lex.uz/docs/7790236

sophisticated cross-chain tracing tool, the other using a basic free service that cannot trace assets beyond a single blockchain. The legal obligation is satisfied in both cases; the enforcement outcomes are entirely different.[10]

PROPOSED LEGAL REFORMS

1. Implement the FATF Travel Rule. The NAPP should amend Reg. No. 3309 to require all licensed providers to transmit originator and beneficiary identification data alongside every cross-border transfer above the UZS equivalent of USD 1,000. Mandatory data fields should include full name, wallet address, and transaction reference number (for legal persons: registration number and address). Transmission must occur through a standardised protocol such as OpenVASP or TRISA. For transfers to non-FATF-compliant jurisdictions, pre-transaction enhanced due diligence should be required.

2. Condition foreign platform access on regulatory status. Reg. No. 3395 should be amended so that transactions through a foreign platform are only permissible where that platform holds a valid regulatory authorisation in its home jurisdiction. Where the platform is unregulated, the transaction must receive board-level approval within the Uzbek provider and be supported by a documented AML/CFT risk assessment. The NAPP should maintain a public registry of pre-assessed foreign platforms.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

3. Set minimum standards for blockchain analytics. The NAPP and DCEC should publish minimum capability requirements for the software mandated by Article 36: the ability to trace assets across at least two blockchain networks; integration with an internationally recognised risk database; and real-time alert generation for transactions matching Chapter 5 indicators. Compliance should be assessed as a mandatory component of the licence renewal examination.

CONCLUSION

Registration No. 3309 builds a coherent KYC system. The definitions in Article 1, the due diligence requirements in Chapter 3, the suspicious transaction indicators in Chapter 5, the asset-freezing obligations in Chapter 6, the blockchain analytics mandate in Article 36, and the five-year retention requirement in Article 47 together create a framework that, if properly implemented, makes it significantly harder to use Uzbekistan's crypto platforms for money laundering or terrorism financing.[11]

Three targeted reforms would make it stronger: a Travel Rule amendment to close the information gap in cross-border transfers; a licensing requirement to prevent unregulated foreign platforms from becoming a back door into the Uzbek market; and minimum blockchain analytics standards to ensure every provider's monitoring capability is genuinely adequate. Each reform is a focused amendment - not a reconstruction - of a system that is already largely sound.[12]

[12]Hamilton, R., & Leuprecht, C. (2024). The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions (pp. 15–42). https://doi.org/10.1007/978-3-031-59543-1_2

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 5(2026) / ISSN 3030-3052 Available at www.uznauka.uz

The KYC obligation is not paperwork. It is the mechanism by which an anonymous string of characters on a blockchain becomes attributable to a real person. That attributability is what makes investigation, reporting, and asset recovery possible. Every gap in the KYC system is a gap through which a transaction can pass undetected. The three reforms proposed here would substantially narrow those gaps and bring Uzbekistan's regulatory framework into full alignment with FATF standards.

BIBLIOGRAPHY:

1. Decree of the President of the Republic of Uzbekistan No. PP-3832 of 3 July 2018. Lex.uz. https://lex.uz/docs/3806048
2. Decree of the President of the Republic of Uzbekistan No. PP-3926 of 2 September 2018. Lex.uz. https://lex.uz/docs/3891610
3. Resolution of the NAPU No. 3 and DCEC No. 16, June 2021. Internal Control Rules (Registration No. 3309). Lex.uz. https://lex.uz/docs/5450936
4. Order of the Director of NAPP No. 43 of 29 September 2022. Rules for the Operation of a Crypto-Magazine (Registration No. 3395). Lex.uz. https://lex.uz/docs/7790236
5. Law of the Republic of Uzbekistan on Counteracting the Legalisation of Proceeds from Criminal Activity, the Financing of Terrorism and the Financing of WMD Proliferation. Lex.uz. https://lex.uz/docs/284542
6. Gulommamatova, P. (2025). Crypto-Asset Laundering is a Fraud Crime. Uzbek Journal of Law and Digital Policy, 3(2), 34–44. https://doi.org/10.59022/ujldp.315

7. Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. Paris: FATF. https://www.fatf-gafi.org
8. Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and VASPs. Paris: FATF.
9. Chainalysis. (2024). Crypto Crime Report 2024. New York: Chainalysis Inc. https://go.chainalysis.com/crypto-crime-report.html
10. Hamilton, R., & Leuprecht, C. (2024). The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions (pp. 15–42). https://doi.org/10.1007/978-3-031-59543-1_2
11. Kou, G., & Lu, Y. (2025). FinTech: a literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1. https://doi.org/10.1186/s40854-024-00668-6
12. Europol. (2022). Cryptocurrencies: Tracing the Evolution of Criminal Finances. European Union Agency for Law Enforcement Cooperation.
13. Kholbazarov, T. (2025). Cryptocurrency Regulation in the Republic of Uzbekistan. SSRN Working Paper.