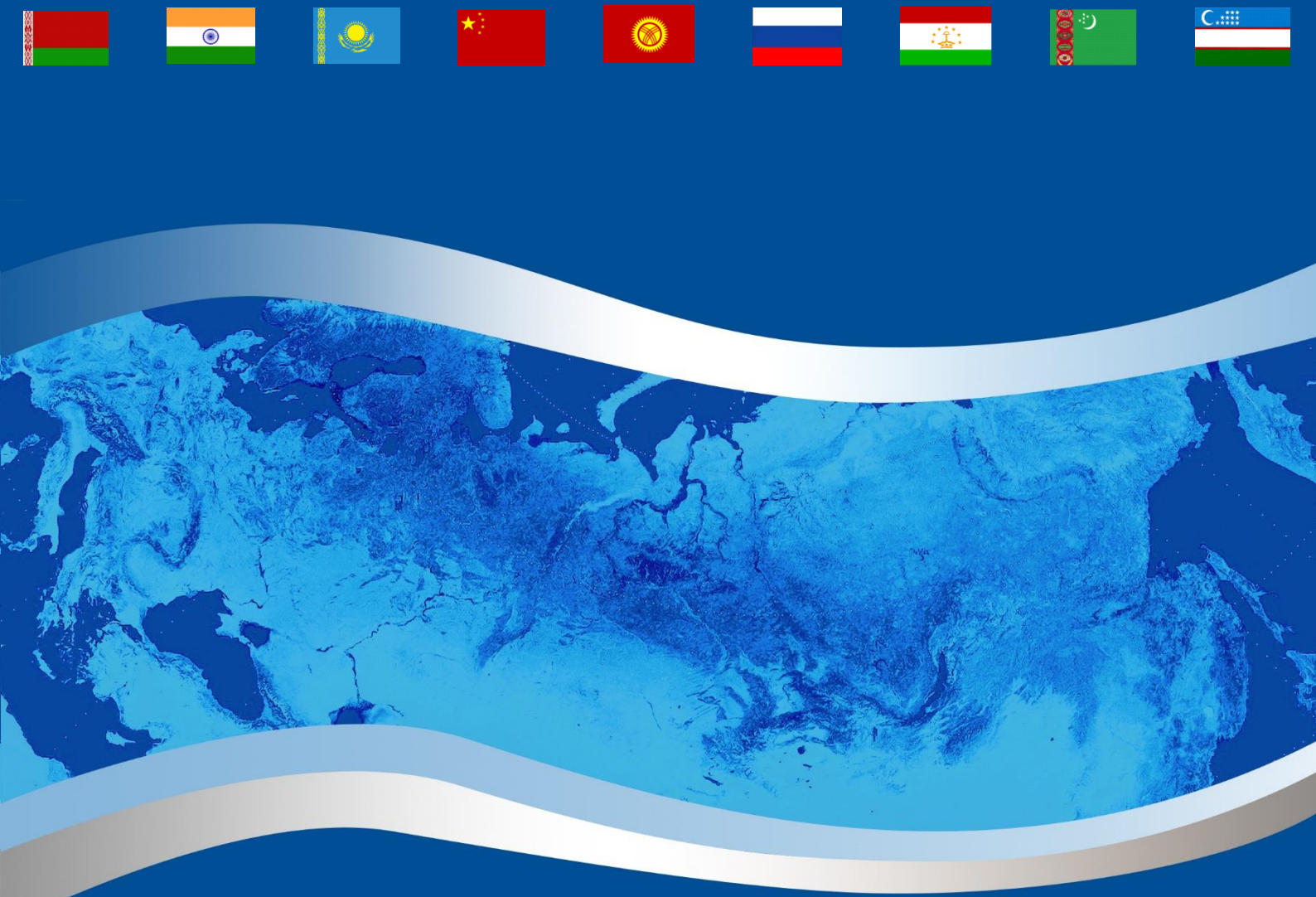
ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism



"Legalization (laundering) of the proceeds of cybercrime, as well as financing of terrorism from the said offence, including through the use of electronic money or virtual assets and the infrastructure of their providers"

EAG TYPOLOGIES PROJECT

2022

CONTENT

Introduction

1. A radical change in the socio-economic situation due to recessionary dynamics in the global economy causes the emergence of new methods of committing crimes. Virtual assets (cryptocurrencies, tokens) and e-money are used as a payment instrument and attract criminal interest increasingly frequently. The dynamics of spreading criminal acts involving virtual assets builds the need of cooperating not only at interagency level but also at supranational level.
2. The legalization of criminal proceeds can be ensured through the use of virtual asset service providers (VASPs), as well as anonymity of transactions in virtual assets. In addition, such assets are being used to finance terrorist groups with increasing frequency.
3. During the project implementation, all the objectives have been achieved:
    - Ensuring effective trilateral cooperation among the state (represented by the regulators), financial institutions and the private sector in order to lower the number of cybercrimes and reduce the ML/TF risk in the use of virtual assets;
    - Collection and analysis of detailed information on virtual asset service providers in the member states;
    - Identification and categorization of characteristic features of cybercrimes and criminal acts involving virtual assets, including cryptocurrencies;
    - Systematization of crimes committed with the use of virtual assets;
    - Categorization of virtual asset service providers in the member states;
    - Collection of detailed information about VASPs that have representative offices or are registered in the jurisdictions of the member states;
    - Analysis of activities of illegal VASPs;
    - Exchange of experience in monitoring and analyzing cryptocurrency transactions and transactions involving e-payment instruments in order to detect, disrupt and investigate crimes committed with the use of virtual assets.
4. We express our gratitude to all the member-states and agencies that took part in the project, and we hope that the results of the typological project will be used by the concerned parties: government institutions, in particular, supervisory, control, law enforcement agencies, financial intelligence units, financial institutions and the private sector representatives.

Special Aspects of Legal Regulation of the Circulation of Virtual Assets and E-Payment Instruments

5. All 8 EAG member states (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, China, Belarus, Russia) and Mongolia (which is an EAG observer) belong to the Romano-Germanic (continental) legal family. The Russian law system is technically similar to the Romano-Germanic legal family, but with its own special features, which makes it possible to classify it as having a mixed form.
6. Circulation of virtual currencies is legislated in Kazakhstan, Kyrgyzstan, Uzbekistan, Belarus, Mongolia and it is not legislated in Turkmenistan, Tajikistan, Russia.
7. The Chairman of the Government of the Russian Federation approved the Concept of Legislative Regulation of the Circulation of Digital Currencies No. D-P13-1613; the Ministry of Finance of Russia submitted a draft federal law "On Digital Currency" to the Government of the Russian Federation. Russia has legislated the use of e-payment instruments and digital financial assets: Federal Law No. 161-FZ dated June 27, 2011 "On the National Payment System", No. 173-FZ dated December 10, 2003 "On Currency Regulation and Currency Control", Federal Law No. 259-FZ dated July 31, 2020 "On Digital Financial Assets, Digital Currency and on Amending Certain Legislative Acts of the Russian Federation". Law enforcement practice generally proceeds from giving virtual currencies the status of property and, if necessary, extends the relevant rules of law to them.
8. China has banned all activities involving virtual currencies. In September 2021, the People's Bank of China, together with the competent authorities, issued a Notice on Further Preventing and Handling the Risk of Speculation in Virtual Currency Transactions.
9. Regulation of e-payment systems operation is under the jurisdiction of the Central Banks in most EAG countries.

Example of Kazakhstan:

10. Digital assets (digital representation of value) can be secured or unsecured (digital tokens received as a reward for participating in maintaining consensus on the blockchain). Subject to Article 1, Clause 55-1 and Article 33-1 (Legal Regime for Digital Assets Circulation) of Law of the Republic of Kazakhstan No. 418-V ZRK dated November 24, 2015 "On Informatization", digital financial assets are recognized as property, but are not recognized as payment instruments.
11. The circulation of decentralized assets is only allowed on the territory of the AIFC (Astana International Financial Centre), where activities with cryptocurrency are permitted in accordance with clear requirements.
12. Activities involving the circulation of cryptocurrency in the AIFC include:
13. Management of a digital asset trading facility ("cryptocurrency exchange");
14. Ensuring of storage and management of digital assets which belong to another person.

E-Payment Systems:

15. Regulation and supervision of payment systems and regulation of their activities is carried out by the National Bank of the Republic of Kazakhstan in accordance with the legislation of the Republic of Kazakhstan on payments and payment systems subject to Article 4 of Law of the Republic of Kazakhstan No. 11-VI ZRK dated July 26, 2016 "On Payments and Payment Systems".
16. As related to regulatory measures, the National Bank of the Republic of Kazakhstan:
    - Determines the rules and procedure for supervising payment systems;
    - Adopts mandatory regulatory legal acts aimed at ensuring the efficiency and reliability of the payment systems operation on the territory of the Republic of Kazakhstan;
    - Defines the importance criteria for payment systems;

- Determines indicators under which the payment system is deemed to be an important system;
- Determines the rules for maintaining the register of systemically important, important and other payment systems of the Republic of Kazakhstan, their inclusion in this register and exclusion from it.

17. An e-money institution can only be a bank, an institution carrying out certain types of banking transactions, or a payment institution which has obtained the relevant license to carry out banking activities or which has been registered as a payment institution.

Example of Kyrgyzstan:

18. Legislative acts in the field of virtual assets issuance, circulation and exchange:
    - Law of the Kyrgyz Republic "On Virtual Assets" (No. 12 dated January 21, 2022, officially published on January 28, 2022, enters into force 6 months after publication);
    - Tax Code of the Kyrgyz Republic (No. 3 dated January 18, 2022).
19. Legislative acts in the field of virtual assets issuance, circulation and exchange:
    - Law of the Kyrgyz Republic "On the Payment System of the Kyrgyz Republic" (No. 21 dated January 21, 2015);
    - Regulation "On E-Money in the Kyrgyz Republic" (approved by Resolution No. 15/6 of the Board of the National Bank of the Kyrgyz Republic dated March 30, 2016).
20. Legally permitted: purchase and sale (exchange) of virtual assets; exchange of one type of virtual currency for another; storage, management of virtual assets; provision of financial services related to initial placement and (or) sale of virtual assets.
21. Banks, non-banking financial and credit institutions and other legal entities supervised by the National Bank are prohibited from carrying out the following transactions: purchase and sale (exchange) of virtual assets; exchange among virtual assets.
22. Groups of participants involved in relations in the sphere of virtual currencies circulation: virtual asset service providers, miners, persons engaged in the issue and initial offer of virtual assets.

E-Payment Systems:

23. Cooperation of the State Financial Intelligence Service of the Kyrgyz Republic with e-payment system operator is carried out in accordance with Law No. 87 of the Kyrgyz Republic dated August 6, 2018 "On Counteracting the Financing of Terrorist Activities and the Legalization (Laundering) of Criminal Proceeds" and the Regulation on the Procedure for Submitting Information and Documents to the Financial Intelligence Unit of the Kyrgyz Republic (approved by Resolution No. 606 of the Government of the Kyrgyz Republic dated December 25, 2018).

Example of Uzbekistan:

24. Law No. ZRU-701 of the Republic of Uzbekistan dated July 14, 2021 "On Licensing, Permitting and Notification Procedures" is in force (a license for carrying out activities involving the circulation of crypto assets, with a subtype of licensed activity "activities of a crypto exchange").
25. Types of transactions with virtual currencies that are legally permitted: sale and purchase of crypto assets for fiat currency, exchange of one crypto asset for another crypto asset, issuance of tokens.
26. Legally prohibited are: transactions with anonymous crypto assets, the use of crypto assets as a means of payment in the territory of the Republic of Uzbekistan.
27. Groups of participants involved in relations in the sphere of virtual currencies circulation of mining and crypto-asset service providers. The types of crypto-asset service providers are crypto-exchange, mining pool, crypto-depository and crypto-store..

E-Payment Systems:

28. A payment system means a set of relations that enable payments through the interaction of the payment system operator, payment system participants and (or) payment institutions by means of application of procedures, infrastructure and payment system rules determined by the payment system operator.
29. A payment system operator is a legal entity that carries out activities enabling operation of the payment system on the territory of the Republic of Uzbekistan, has the relevant license and enables operation of the e-money system.
30. Activities of payment system operators and payment institutions are licensed by the Central Bank of the Republic of Uzbekistan.
31. Separately stand out important payment systems, uninterrupted operation of which contributes to stable operation of the payment services market of the Republic of Uzbekistan, and failures in its operation can lead to risks in the payment services market of the Republic of Uzbekistan.
32. A payment system is deemed to be important if its share of the payment services market exceeds the value determined by the Central Bank for this market, and (or) if amount of payments made through the payment system on the territory of the Republic of Uzbekistan during the year is not less than the values determined by the Central Bank.

Example of Belarus:

33. As related to regulation of activities of the digital economy entities, the issuance, exchange and circulation of digital currencies on the territory of the Republic of Belarus, in the High-Tech Park (HTP) the following instruments are in force: Decree No. 8 of the President of the Republic of Belarus dated December 21, 2017 "On Development of Digital Economy", Decree No. 12 of the President of the Republic Belarus dated September 22, 2005 "On the Hi-Tech Park".
34. Regulated objects: digital signs (tokens); e-money.
35. Individuals have the right to own tokens and carry out the following operations: mining, storage of tokens in virtual wallets, exchange of tokens for other tokens, acquisition/alienation of tokens for Belarusian rubles, foreign currency, e-money, donation and bequest of tokens.
36. Legal entities have the right to own tokens and carry out operations of:
    - Creation/placement of their own tokens in Belarus and abroad via a HTP resident;
    - Storage of tokens in virtual wallets;
    - Acquisition/alienation of tokens through cryptoplatform operators, cryptocurrency exchange operators, other HTP residents.
37. Individual entrepreneurs-HTP residents have the right to:
    - Exercise the above powers;
    - Create/place their own tokens in Belarus and abroad via a HTP resident;
    - Carry out other activities using tokens.
38. Types of transactions involving virtual currencies that are prohibited by law: entrepreneurial activities of individuals and legal entities that are not HTP residents.
39. Groups of participants involved in relations in the sphere of virtual currencies circulation: HTP residents, cryptoplatform operator, cryptocurrency exchange operator.

Example of Mongolia:

40. The Virtual Asset Service Providers Act is in force. Legally permitted:

    Exchange of virtual assets for fiat currencies and vice versa;

    Exchange of virtual currencies of different types between each other;

Transfer of virtual assets;

Storage and management of virtual assets or related instruments;

Provision of financial services related to the public issue of virtual assets or trading in virtual assets.

41. It is prohibited to offer or sell virtual assets to the public without transferring them to a company registered as a provider of the above services.
42. Groups of participants involved in relations in the sphere of virtual currencies circulation: the Financial Intelligence Unit, law enforcement agencies, virtual asset service providers, the Financial Regulatory Commission – as related to registration and monitoring activities.

International Cooperation in Regulating the Circulation of Virtual Assets and E-Money

43. International cooperation in the EAG member states is carried out subject to the ratified international treaties, agreements or on a reciprocal basis. Separate legal acts covering digital currency and digital financial assets at the international level are missing.
44. The internal affairs authorities, state security and financial intelligence units are responsible for cooperation with e-payment system operators.
45. Cooperation of virtual asset service providers with the FIU is carried out as part of complying with the requirements of the AML/CFT legislation in accordance with the following documents:
    - Laws on combating the legalization of proceeds from crime, the financing of terrorist activity and the financing of proliferation of weapons of mass destruction;
    - Laws on the national payment system;
    - Laws on investigative activities;
    - Laws on communications;
    - Laws on information, information technologies and information protection;
    - Internal control rules on combating the legalization of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction for persons engaged in activities involving circulation of crypto assets (Uzbekistan).
46. Cooperation of the FIU and law enforcement agencies in relation to responses to requests sent to virtual asset service providers is carried out subject to the existing legal acts and inter-agency instructions.
47. International cooperation in the investigation of crimes related to the circulation of virtual assets is carried out subject to the criminal procedure legislation of the countries (Belarus, Kazakhstan, Russia, Mongolia). The competent authority sends orders for the provision of legal assistance via the following channels:
    - National Central Bureau (NCB) of Interpol (for law enforcement agencies of Belarus, Russia),
    - International Criminal Police Organization Interpol (for law enforcement agencies of Belarus, Mongolia),
    - Ministry of Justice (China), in the absence of a mutual legal assistance agreement via diplomatic channels (China),

- Egmont network (for the FIUs of Belarus, Kyrgyzstan, Mongolia, Russia, Turkmenistan),
- Information exchange systems of the CIS Council of Heads of Financial Intelligence Units (CIS CHFIU) (Kyrgyzstan).

48. Informally, requests are sent for obtaining information on registration of property, company, stake in legal entities, etc., which do not require court order: to the technical support service or the management of cryptoplatforms via e-mail, via the CARIN network (Belarus), international information exchange networks Karin - Europe and ARIN-AP - Asia Pacific, open sources (Kazakhstan), Arin network (Mongolia). Informal correspondence and negotiations are used (Kyrgyzstan).
49. In conducting financial investigations of crimes involving virtual assets, countries are guided by international treaties and ratified conventions, inter-agency agreements and memoranda, and national legislation.
50. In order to investigate crimes that require time-consuming and complex investigative actions, the investigative agencies can create inter-agency investigative groups (Kyrgyzstan), specialized groups on specific cases (Belarus), inter-agency and international working groups for investigating specific criminal cases (Russia).
51. Joint international investigations in the field of virtual assets are conducted by Tajikistan, China, Russia, Kyrgyzstan.
52. Each employee of the competent agency, in particular, the unit/employee responsible for international cooperation, is responsible for execution and control over the completeness and timeliness of execution of international requests. Also, in Uzbekistan, for example, there is an internal document of the Department that regulates timeliness (priority) of execution of international requests.
53. Requests sent to the FIUs of foreign jurisdictions regarding investigation of crimes related to the circulation of virtual currencies, depending on information availability, include the following data:
    - Information about official investigation or court proceedings in connection with the case;
    - Information about the competent authorities involved in this investigation;
    - Brief plot of the crime, connection with the country whose FIU is to disclose the information;
    - Information about the involved persons (full name, date of birth; mobile phone number; bank card details; e-mail address; person's nickname in VASP; cryptocurrency wallet/address or account number);
    - Name and jurisdiction of the VASPs for which the involved person is a customer, including the name of the exchange and exchange service;
    - Transaction data (date and time of the transaction; transaction hash ID; transaction amount);
    - Information about possible confiscation of assets;
    - Amount and type/essence of the assets in the case.
54. In order to speed up request execution, some jurisdictions allow sending official requests directly to a foreign competent authority that possesses the requested information, without sending a request to the FIU of the foreign jurisdiction. For example:
    - A request can be sent directly to a foreign competent authority, bypassing the FIU: through the Prosecutor General's Office, channels of the National Central Bureau

(NCB) of Interpol, under inter-agency mutual assistance agreements and memoranda, to foreign central banks / other banking supervisory authorities.

- Sending a scanned copy of the official request to email of the VASP.
- Informal appeal to the head of the authority to speed up request execution.
- Sending a request marked URGENT.

55. Formal international cooperation is carried out subject to the criminal procedure legislation and by sending legal assistance requests through the channels of the NCB of Interpol, International Criminal Police Organization Interpol, the Ministry of Justice, diplomatic channels, the Egmont Group, Information Sharing Systems of the CIS CHFIU.
56. Formal international cooperation agencies:
    - Judicial authorities, Ministry of Justice, diplomatic channels, financial intelligence units, law enforcement agencies.

Role of the Private Sector in Countering ML/TF

57. Participation of the private sector in investigations (as a specialist, expert; when financial institutions submit information to the FIU) is allowed in Kyrgyzstan, China, Russia.
58. Information spontaneously sent by the private sector representatives, such as financial institutions, non-financial institutions, in the form of an application of individuals and legal entities (on paper or in the form of an electronic document in a standard form) to the FIU is a reason for conducting financial investigations in Kyrgyzstan, Kazakhstan, Turkmenistan, Russia, Tajikistan, Belarus, Mongolia, China, Uzbekistan. STRs are sent, as well as information about available ML/TF facts. After analysis, the information is sent to the law enforcement authorities.

Example of Russia:

59. Cooperation was built up with Rosseti Northern Caucasus, PJSC to identify the organizers of illegal mining farms in the district. Joint work made it possible to identify two individuals allegedly involved in the financing of international terrorist organisations and cryptocurrency mining. Financial investigation has been carried out, the materials were transferred to the law enforcement authorities for conducting intelligence operations.
60. Problems during cooperation of state agencies with the private sector in the field of investigation of crimes involving virtual currencies:
    - Insufficient legislative regulation;
    - It is difficult for financial institutions to identify transactions with virtual currency;
    - Anonymity of money transfers;
    - Internal controls of credit institutions are not focused on in-depth analysis of transfers between individuals;
    - Most cryptoplatforms operate internationally, but officially are not linked to a specific jurisdiction (this complicates informational cooperation with them);
    - Transactions with virtual assets are usually carried out on special platforms, and not through financial institutions (as a rule, platforms are installed on servers in foreign jurisdictions);
    - Long time to wait for the requested information.

Categorization of VASPs in the EAG Member States

61. VASPs are economic entities in Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, Belarus. They are not economic entities in Turkmenistan, Mongolia, China, Russia.
62. In Kazakhstan, there are activity codes for organizations that issue and maintain records of virtual currencies and ensure their circulation.
63. The specified activity is categorized as entrepreneurial in Kyrgyzstan and as activity in the field of crypto asset circulation – in Uzbekistan.
64. In Belarus, there is a code in the All-Republican Classifier of the Republic of Belarus "Types of economic activity" (OKRB 005-2011): 63111 – Digital Signs (Tokens) Mining.
65. In Kazakhstan, a special activity type is differentiated – issuing digital assets, organizing trading and providing services for exchange of digital assets for fiat money and vice versa. The authorized body in the field of information security – the Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan – determines the procedure for the issuance and circulation of secured digital assets and digital currencies.
66. The requirements for virtual asset service providers in the EAG member states, except for China, where such activities are prohibited, relate to compliance with the AML/CFT legislation and the licensing requirements. Special requirements for VASPs are determined: reliability, compliance with the information confidentiality requirements, existence of a business plan, implementation of internal controls, the legitimate origin of the capital, no arrears in fees, etc., knowledge in economics, IT, law and other.
67. Requirements for e-payment system operators: submission of reports and other information to the Central Bank, business continuity, compliance with the AML/CFT measures, compliance with the license requirements, information confidentiality.
68. Information is shared between virtual currency service providers and supervisory authorities through e-mail, written requests. The transfer of information about cryptocurrency transactions and the persons who performed them at the requests of the competent government authorities is possible in Russia, Uzbekistan, Tajikistan, and Belarus and is not possible in Turkmenistan, China, Mongolia, Kazakhstan.
69. Licensing of VASP activities:
    - Uzbekistan maintains an electronic register of licenses. Licensing requirements cover the size of the authorized capital, organization of the electronic trading system, trading rules, currency quotation and storage of transactions information.
    - In Kazakhstan, licensing is carried out at the site of the Astana International Financial Centre.

Example of Uzbekistan: blocking and revocation of the license of a virtual asset service provider.

70. Subject to Clauses 33-35 of the Regulation on Licensing Activities of Cryptocurrency Exchanges, the license:
    - Shall be suspended in case of detected violations;
    - Shall be terminated on the basis of an application for termination, liquidation or reorganization of the legal entity (except for transformation/merger); as a result of systematic/gross violation of the license requirements; non-elimination by the licensee of the circumstances that resulted in the license suspension;
    - Shall be canceled if the licensee fails to submit a document confirming the payment of the state fee, fails to sign the license agreement, the application for license cancellation within 3 months from the date of receipt of the notice about issued license.

71. Decision on license suspension/termination/cancellation may be appealed in court.
72. Virtual asset service providers are categorized in Kyrgyzstan (if possible, use services of e-payment platforms, upon registration with the tax authorities as a tax entity), in Belarus (by types of activities), in Mongolia.
73. Strict requirements for security and effectiveness of AML/CFT activities are imposed in the EAG countries on e-payment system operators and payment systems themselves.

Example of Kyrgyzstan:

74. The e-payment system operator shall take measures to counter the financing of terrorist activities and money laundering and implement the requirements of the Kyrgyz Republic legislation on countering the financing of terrorist activities and money laundering.
75. The operator shall carry out activities under a license issued by the National Bank in accordance with the Kyrgyz Republic legislation and the requirements of the regulations of the National Bank.
76. The operator shall ensure confidentiality and storage of information on e-money holders and transactions involving e-money.
77. The operator shall develop internal rules and procedures to ensure uninterrupted operation of its information system and security of payments.
78. The operator must set limits for electronic wallets in its information system, comply with the requirements for maintaining records of e-money subject to the terms of the agreement with the bank, the Regulation on E-Money and other regulations of the National Bank.

Typologies of Criminal Proceeds Laundering

79. The countries participating in the typological project follow the FATF Recommendations for assessing the risks of money laundering and terrorist financing involving virtual assets and e-money.
80. The risk of virtual currencies being used for the financing of terrorism is assessed in Kazakhstan, Uzbekistan, Tajikistan, Mongolia, China, Russia and is not assessed in Turkmenistan.
81. The use of virtual currencies in the context of money laundering and terrorist financing risks associated with the coronavirus disease pandemic are assessed in Uzbekistan, China, Russia and are not assessed in Kazakhstan, Turkmenistan, Kyrgyzstan, Tajikistan, Mongolia.
82. Criminal episodes involving virtual currency theft were observed in Belarus, Mongolia, China, Russia and were not observed in Kazakhstan, Turkmenistan, Kyrgyzstan, Uzbekistan, Tajikistan.
83. Criminal episodes involving virtual currency theft by way of violence were observed in China, Russia and were not observed in Kazakhstan, Turkmenistan, Kyrgyzstan, Uzbekistan, Tajikistan, Belarus, Mongolia.
84. The following indicators of virtual currencies being used for legalizing criminal proceeds were listed:

Uzbekistan (Internal Control Rules on Combating the Legalization of Proceeds From Crime, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction for Persons Engaged in Activities Involving Circulation of Crypto Assets (No. 3309 dated June 9, 2021)):

- Crypto wallets were used for criminal purposes;
- Exchange transactions at a deliberately unfavorable exchange rate were identified;
- Crypto asset price manipulation;
- Lack of "White paper";
- A large number of cryptocurrency wallets on one IP address;
- Frequent change of personal data, IP address and domain;

- Lack of knowledge in the field of crypto assets circulation.

Belarus (Instruction on Completion, Submission, Registration and Storage of Special Forms Intended for Registration of Financial Transactions that are Subject to Special Control approved by Resolution No. 367 of the Council of Ministers of the Republic of Belarus dated March 16, 2006):

- The customer refuses to provide information or provides false information;
- The transaction amount is split, and the transaction has no economic sense;
- Virtual wallets are used that are obviously associated with illegal activities, in particular, illicit drug trafficking or mixers and other options for bypassing the identification of counterparties in transactions.

Mongolia (Law on Combating Money Laundering and Terrorist Financing):

- High customer risk has been revealed;
- Significant product and service risk has been identified.

China (Chinese Legislation):

- Several significant-amount transactions have been performed in a short time;
- Separate accounts have been created in different names.

*Example of Russia (*based on procedural guidelines for the internal affairs bodies*):*

85. When studying the Hydra trading platform located in the non-public segment of the Internet ("Darknet"), it was found out that settlements between sellers and buyers were in cryptocurrency Bitcoin, wallets for which were provided directly by the site. For buyers of drugs, counterfeit banknotes and other items prohibited for free circulation, a number of services is arranged that allowed purchasing Bitcoins for the ruble equivalent by crediting them to Qiwi, YuMoney electronic wallets, bank cards or mobile phone account balances. Amounts of money transferred to the services are credited to the user's personal accounts in Bitcoins. The key indicator of money transfer from QIWI Wallet used for settlements to the exchanger's QIWI Wallet is a transaction fee. That is why the transaction amount is not a whole number and is displayed with kopecks. The money is converted into cryptocurrency in the "official" QIWI Wallet of the exchanger.

Involvement of Criminal Syndicates in the Use of Digital Technologies

86. Activities of criminal groups (according to open source data) are analyzed in Russia, Turkmenistan, Kyrgyzstan, Uzbekistan, Belarus, and China.
87. The involvement of criminal syndicates and organized criminal groups in the crimes committed with the use of virtual currencies is assessed in Russia, Kyrgyzstan, Uzbekistan, and China.
88. FATF and Egmont Group reports on cybercrime monitoring have been analyzed in Russia, Turkmenistan, Kyrgyzstan, Uzbekistan, Belarus, and China.
89. The received materials are sent to law enforcement authorities, used in financial investigations and for improving the skills of employees of the financial intelligence units; current and potential risks are assessed; suspiciousness indicators are updated.
90. Cooperation with international criminal police organizations (Interpol, Europol) is carried out in Kyrgyzstan, Uzbekistan, Tajikistan, Belarus.
91. In China, the Ministry of Public Security is the coordinator of cooperation with international criminal police organizations.
92. The impact of transnational criminal groups on the cryptocurrency market is assessed in Russia (based on media reports), Uzbekistan, China and is not assessed in Kyrgyzstan, Tajikistan, Mongolia.

93. In China, the involvement of transnational criminal groups in the crimes committed with the use of virtual assets is revealed based on information from foreign FIUs and the media.

Using OSINT (Open Source Intelligence):

94. To reveal the involvement of transnational criminal groups in the crimes committed with the use of virtual assets, transaction analysis tools are used:
    - Wallet explorer – Bitcoin wallet transaction history,
    - Blockpath.com – viewing Bitcoin wallet transactions presented graphically.
95. Tools for monitoring the Internet and Darknet segments are used in Russia, Uzbekistan, Belarus, China, and Kyrgyzstan.
96. Software analytical resources used to monitor the Internet and Darknet segments in Russia (Rosfinmonitoring and the Ministry of Internal Affairs of Russia) are Yandex, Google, TOR, Transparent Blockchain.

Detection and Investigation of Crimes Involving the Circulation of Virtual Assets and E-Money

97. Analysis of the status, structure and dynamics of the number of crimes involving the circulation of virtual currency is carried out in Kazakhstan, Belarus (the Ministry of Internal Affairs maintains the Unified State Data Bank on Offenses, and the Investigative Committee and other law enforcement authorities provide data for it), in China (the People's Bank of China analyzes evolving ML/TF risks associated with virtual currencies and sends risk warnings and red flags to its branches and reporting entities), in Russia (requests are sent to the law enforcement authorities in order to obtain practice regarding criminal cases; the statistical accounting form of the Main Information and Analytical Centre of the RF Ministry of Internal Affairs is analyzed).
98. Computer and technical expertise to establish the alleged use of malicious software to steal money is in place in Turkmenistan, Belarus, Russia (falls within the competence of the law enforcement authorities).
99. Information about the use of anonymizing resources to hide the IP address by the alleged criminals is collected in Kyrgyzstan, Uzbekistan, China, and Russia.
100. Cooperation of the FIU with virtual currency service providers in order to identify and investigate crimes committed with the use of virtual currencies and e-money is established in Kyrgyzstan, Belarus, Uzbekistan and is not established in Kazakhstan, Turkmenistan, Tajikistan, Mongolia, China, Russia.
101. Traditional for the member states indicators of potential crimes involving the circulation of virtual currencies and e-money:
    - Significant-amount transactions performed in a short time (usually within 24 hours);
    - Transactions involving multiple accounts;
    - Funds received from a wallet associated with the Darknet markets;
    - Money transfers in favor of exchange services for cryptocurrency purchase and sale;
    - Using bank instruments opened in the names of nominees (“drops”);
    - Short term of the bank card;
    - No payments in favor of legal entities, no purchase transactions;
    - Replenishment of bank accounts for non-whole amounts;
    - Establishing a VPN connection when using banking products;

- Systematic cash withdrawals;
- Creation, distribution and use of computer programs for neutralization of computer security features, unauthorized modification, copying, destruction, blocking of computer information;
- Identified hacker attacks on the computer system;
- False exchange offices and crypto exchanges;
- Fake wallets for cryptocurrency storage;
- Fake cloud mining of cryptocurrency - Projects that mimic cloud mining pools without the necessary capacity and infrastructure at their disposal (often fraudulent schemes disguised as venture capital investment projects);
- Transactions with funds or other property of persons included in the list of persons involved or suspected of being involved in terrorist activities or proliferation of weapons of mass destruction;
- Transfer of funds through payment systems and mobile applications to accounts opened for anonymous owners, receipt of funds from abroad from accounts opened for anonymous owners (Kazakhstan).

102. The financial intelligence units of the typological project's member states receive information about allegedly illegal nature of transactions from foreign FIUs, credit institutions, law enforcement authorities, virtual asset service providers, and other sources on paper or in electronic form.

103. Suspicious transaction reports are received from credit institutions (in Kazakhstan – form FM1 requisite 3.14, in Russia – additional code 6001 under code 1190).

104. STRs are not detailed in Turkmenistan, Kyrgyzstan, Tajikistan, China, Mongolia. Tajikistan has no system for prompt reporting of suspicious transactions.

105. In a number of countries inter-agency working groups are created. Participation of experts, specialists, witnesses and other persons, including blockchain experts, is allowed in accordance with criminal procedure legislation and agency-level instructions. Following the results of financial investigations, information is sent to the law enforcement authorities or foreign FIUs in order to get additional information. There are no special deadlines for financial investigations involving virtual assets (according to general rules). To investigate crimes involving virtual currency, joint task forces can be created with the participation of law enforcement authorities and the FIU.

Example of China:

106. The People's Bank of China (PBOC) is conducting administrative investigations. If suspicions of legalization of criminal proceeds cannot be eliminated after an administrative investigation, the PBOC sends information to the law enforcement authorities for additional inspections.

Example of Uzbekistan:

107. The World Wide Web is monitored on an ongoing basis. As a result, 6 facts of operation of payment platforms without a license were revealed for the period 2019-2020. Materials on the revealed facts were sent to the Department under the General Prosecutor's Office and tax authorities, and 4 criminal cases were initiated following the consideration. In one of the criminal cases, 9.5 bitcoins were recovered to government revenue.

108. 6 information resources for illegal purchase and sale of cryptocurrency assets were identified.

Example of Russia:

109. When analyzing bank card/account statements of persons suspected of being involved in criminal activity, it is not always possible to determine that the funds are being spent on cryptocurrency

purchase. Also, it is not always possible to establish to which crypto exchange the address of the involved person belongs or in which jurisdiction this exchange is located. If relevant data (for example, crypto addresses) are available, requests are sent to the relevant FIUs, which can receive from the relevant cryptocurrency exchanges the identification data of the exchange customers, information about bank cards and accounts used to buy and sell cryptocurrencies for fiat money, etc. However, this is only possible if local AML/CFT legislation covers persons providing services of cryptocurrency exchanges.

110. Problems of general (organizational) nature when investigating crimes involving virtual currencies and e-money:

- Lack/insufficiency of the regulatory framework;
- Lack of a unified system and algorithm for international information cooperation with VASPs (with closer cooperation with e-payment system operators);
- Lack of asset seizure/confiscation mechanism, etc.

111. Legal acts and (or) inter-agency instructions governing cooperation between the FIU and the law enforcement authorities in relation to responses to requests sent to VASPs:

- Mutual cooperation agreements, inter-agency agreements;
- Instructions for organizing information cooperation with the law enforcement authorities;
- Notices;
- Resolutions on the seizure, storage and confiscation procedures.

112. Law enforcement authorities send information to the FIU regarding the use of virtual currencies and e-money in illegal activities: a written request containing the plot, details of the criminal case, defendants, wallets.

113. Assets seizure during the investigation of crimes involving virtual currencies is possible in Kazakhstan, Tajikistan, Uzbekistan, China. The seized cryptoassets are transferred for storage to the authorized body in Belarus – by transferring to a special government wallet or by exchanging the seized cryptocurrency for fiat money under the control of the investigator, followed by subsequent transfer to the bank account intended for the seized money.

Examples of Successful Cooperation:

114. Case "PlusToken" (China): pyramid investment scheme. As a result of a criminal case, virtual assets in the amount of 40 billion yuan were confiscated.

115. In the Far Eastern Federal District of Russia, a financial pyramid was disrupted. The company carried out fraudulent operations under the guise of investment activities and raised funds of citizens of the Russian Federation in virtual currencies and e-money.

116. E-payment system operators in Kyrgyzstan are guided by the requirements of the legislation in the field of combating the financing of terrorist activities and the legalization (laundering) of criminal proceeds. Following the results of effective work of the internal control department of an e-payment system, namely, after recognizing the transaction as suspicious and sending the relevant report to the State Financial Intelligence Service (SFIS), a financial investigation has been initiated, summary has been prepared based on the results and sent to the law enforcement authorities.

117. In 2022, the national security authorities provided information about suspicious transactions with a bank card of Subsidiary Bank Sberbank of Russia JSC, which belonged to a citizen of Kazakhstan "T". Analysis of the bank card transactions showed that the card was allegedly used to finance widows of "Da'esh" militants placed in the Syrian Al-Hawl refugee camp. In addition, citizen "T" used the services of the Zolotaya Korona money transfer system when making transfers. The transfers were

made to bank cards of the Republic of Kazakhstan and the Russian Federation. Monitoring of financial transactions revealed a group of persons with external evidences of religiosity, who were possibly involved in the financing of terrorism. Among these persons there were citizens previously convicted of terrorism and extremism and included in the list of entities and persons involved in the financing of terrorism and extremism. The materials were handed over to the law enforcement authorities.

Terrorist Financing Methods Involving Virtual Currencies and E-Money

Example of Russia:

118. Information about raising funds for the needs of international terrorist organizations is published in closed Telegram channels, other instant messengers, social networks, Qiwi wallets. Subsequently, the raised funds are either transferred to cards through several levels of cards or smurfed in small amounts to a number of other wallets, mostly unidentified. Then they are withdrawn as cash in the countries with increased risks of terrorist activity.

119. Terrorism is financed using e-payment systems: Western Union, Webmoney, Qiwi, Golden Crown, Unistream, Yandex.Money. The most frequently used method (up to 95% of cases) is the use of Qiwi wallets.

120. A common method of making money transfers for the purpose of terrorist financing in the Russian Federation – transfers through Sberbank of Russia JSC (a huge number of customers, convenient Internet banking service “Sberbank Online”, linking bank cards to the international payment systems Visa and Mastercard).

Example of Uzbekistan:

121. Citizen A., staying in zones of increased terrorist activity, posted a social media publication with a call for making donations to members of terrorist organizations through his bank card. The received funds were subsequently converted to a currency card using the bank's application and withdrawn in zones of increased terrorist activity.

Example of Kazakhstan:

122. A person acting as a “collector” accumulates funds from various persons by money transfers through e-wallets under the guise of financial aid or charity. In the future, this person himself or through third parties periodically transfers funds through money transfer systems to countries of increased terrorist activity, most often stating financial aid as the reason for the transfer. This helps to avoid attention from the authorized state bodies and internal control departments of financial institutions. Subsequently, the money is spent on the needs of international terrorist organizations.

Example of China:

123. Terrorism is financed through the use of e-payment systems: non-bank payment services, e-wallets and prepaid cards.

Conclusion

124. The results of the study are aimed at their practical application by the countries participating in the project, as well as the entire Eurasian region as a whole.

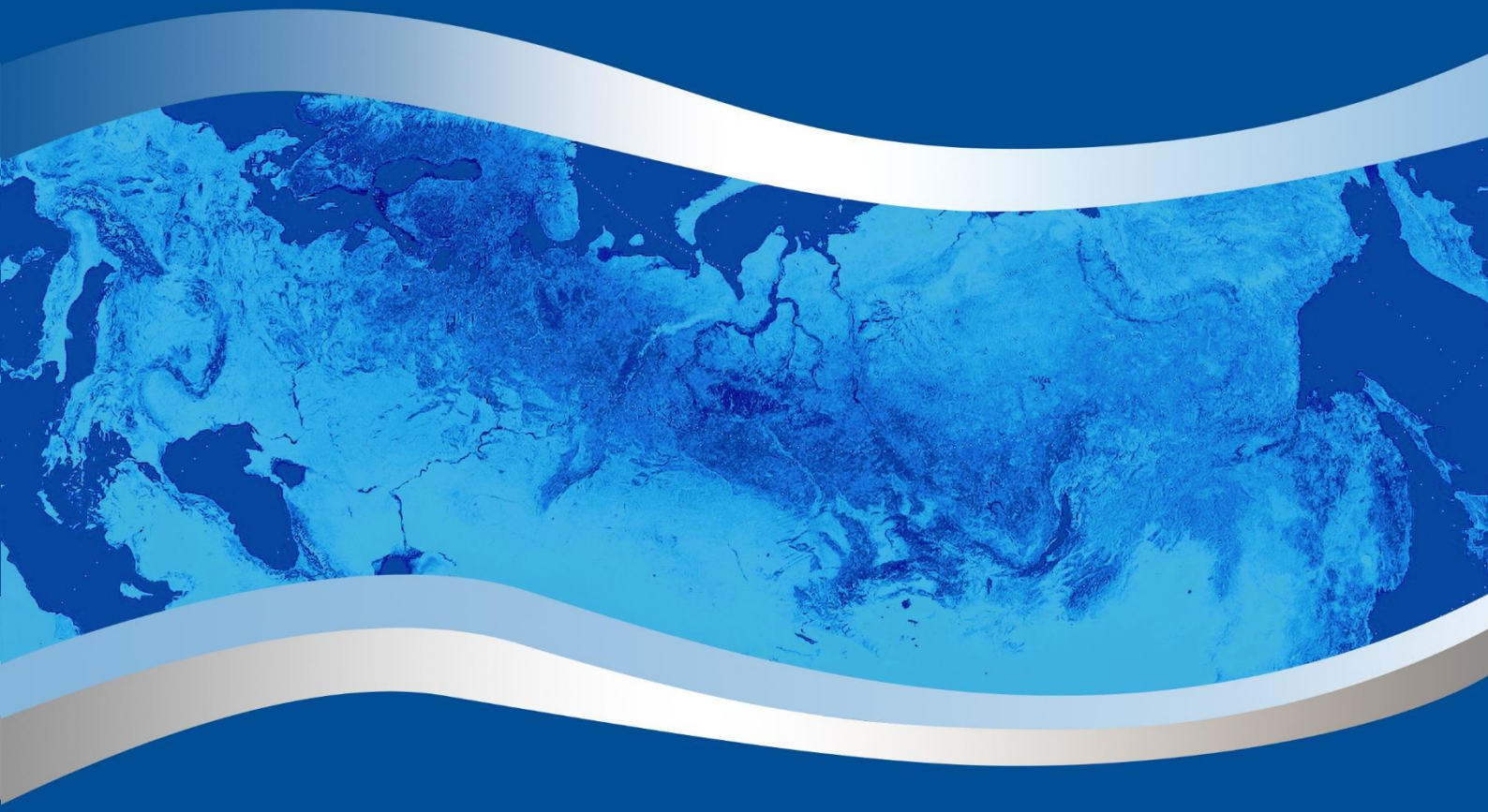
125. During the study, information from the typological project's member states has been received and processed. The information concerned regulatory mechanisms applied to the activities of virtual asset service providers and e-payment system operators in the jurisdictions under consideration.

126. Common features and differences in the countries' legislation in the field of operation of cryptocurrency platforms and e-payment systems have been identified.

127. The principles of inter-agency and international cooperation in terms of improving the efficiency of work of financial intelligence units of the typological project's member states have been studied.

128. The countries have provided examples and typologies of money laundering involving virtual assets and e-money.

129. We express our gratitude to the states and agencies that took part in the project.



www.eurasiangroup.org