Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.352:004.42(574+519.5)

Article's History:
Received: 31.07.2025; Revised: 17.11.2025; Accepted: 16.12.2025

Digital forensics in combating cryptocurrency-related crimes in Kazakhstan and South Korea

Andrejs Vilks*
PhD, Professor
Riga Stradins University
LV-1007, 16 Dzirciema Str., Riga, Latvia
https://orcid.org/0000-0002-5161-0760

Aldona Kipane
PhD, Associate Professor
Riga Stradins University
LV-1007, 16 Dzirciema Str., Riga, Latvia
https://orcid.org/0000-0001-6408-3456

Anatolijs Krivins
PhD, Associate Professor
Daugavpils University
LV-5401, 13 Vienibas Str., Daugavpils, Latvia
https://orcid.org/0000-0003-1764-4091

Abstract. The purpose of this study was to identify the specific features of national approaches to the use of digital forensics in the investigation of cryptocurrency-related crimes in the Republic of Kazakhstan and the Republic of Korea. The methodological basis was a comparative analysis of regulatory and legal acts, practical approaches and the outcomes of law enforcement activities in both jurisdictions in the context of the transnational nature of cryptocurrency crime. The study revealed fundamental differences between the regulatory approaches: the Kazakhstani model is oriented towards the legalisation of the crypto industry through licensing and the creation of special regimes within the Astana International Financial Centre, whereas the Korean approach is characterised by strict financial supervision and preventive monitoring through specialised legislation on the protection of virtual asset users. An analysis of practical results for 2024 showed a significant asymmetry in the scale of law enforcement activity: Kazakhstan achieved initial success through the dismantling of 36 illegal cryptocurrency exchanges with a turnover of more than 110 million US dollars, the freesing of 4.8 million stablecoins and the return of 545 thousand stablecoins to victims, while in 2024 Korean law enforcement agencies continued to receive an increasing number of reports of suspicious cryptocurrency transactions, indicating the intensification of the financial monitoring system. The findings conceptualise two trajectories in the development of national digital forensics systems and confirm the critical role of the regulatory and legal framework in creating an effective evidentiary trail in cross-border investigations of cryptocurrency-related crimes. The practical significance of the study lies in identifying the preconditions for the successful functioning of digital forensics and the potential for mutual learning between jurisdictions with differing experience in regulating cryptocurrency markets, which may be used by regulatory and law enforcement bodies to improve national systems for countering cryptocurrency-related crime

Keywords: blockchain analysis; virtual assets; law enforcement agencies; international cooperation; regulatory mechanisms; law enforcement practice

Suggest Citation:
Vilks, A., Kipane, A., & Krivins, A. (2025). Digital forensics in combating cryptocurrency-related crimes in Kazakhstan and South Korea. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 75-89.

*Corresponding author

Introduction

With the increase in the volume of cryptocurrency transactions globally, the number of crimes involving digital assets is also growing. The challenges of investigating such crimes are becoming increasingly relevant for law enforcement agencies, as cryptocurrencies are used for money laundering, terrorist financing and fraud. Countries that are actively developing digital technologies and financial innovations, such as the Republic of Korea and Kazakhstan, are faced with the need to improve legal mechanisms and technical tools to combat cryptocurrency crime. This requires the development of specialised approaches to the collection and analysis of digital evidence, as well as the improvement of international cooperation in the field of cryptocurrency investigations.

The technological aspects of digital forensics have undergone significant development thanks to the research of N. Apsimet *et al.* (2024), who found a 40-60% increase in the accuracy of processing digital traces when using artificial intelligence compared with traditional methods. Their results confirmed the critical role of automated analysis of network traffic in identifying the sources of cyber-attacks and reducing human error in processing large data sets. A practical contribution to the development of cryptocurrency forensics was made by A. Park *et al.* (2023), who developed the first systematised three-phase methodology for examining cryptocurrency wallets, capable of ensuring effective investigation even in the absence of prior information on addresses or private keys. Experimental testing demonstrated a 35-50% reduction in the time required to identify cryptocurrency assets and an increase in the reliability of analytical results. Advances in automated fraud detection were demonstrated by U. Agarwal *et al.* (2023), whose system achieved the highest accuracy among existing solutions, at 97.5% when using a random forest algorithm, processing more than 10,000 transactions per minute with minimal false positives.

Structural problems in the sector were identified in the studies of S. Dudani *et al.* (2023), who found that 87% of academic works focus exclusively on Bitcoin, while the analysis of alternative cryptocurrencies remains underdeveloped. A review of 156 publications revealed critical gaps in inter-agency coordination and a lag of 3-5 years in the technological provision of forensic units compared with the pace of development of cryptocurrency technologies. The forensic features of specific categories of crime were examined by S. Choi *et al.* (2024), who identified eleven key scenarios of criminal activity in cryptocurrency Ponzi schemes and established that 73% of victims are persons over the age of 55 with limited knowledge of digital technologies. The results of their study showed that early detection of indicators of Ponzi schemes can prevent losses of up to 2.3 billion US dollars annually on a global scale. The issue of online fraud in the context of national security was addressed by A. Kaliyev (2024), who identified a critical correlation between the level of digital literacy in the population and the effectiveness of countering cybercrime, establishing that 65% of victims do not possess basic cyber security skills. The author demonstrated that a systemic approach to personnel training can increase the clearance rate of online crimes by 40-50% within five years.

The national context of the development of digital forensics in Kazakhstan has been studied by several research groups from different methodological standpoints. The legal foundations of coordination between public and private actors engaged in forensic activity were substantiated by Y. Alimkulov *et al.* (2023), whose findings formed the basis for the draft Law "On Private Detective Activity in the Republic of Kazakhstan". The state of development of the sector was assessed by Y. Saniyazova *et al.* (2024), who recorded a 15-fold increase in the number of cybercrimes over the past five years alongside a decline in clearance rates to 23%, due to a critical shortage of qualified experts and technical equipment. The prospects for technological modernisation of the criminal justice system were analysed by A. Abuova *et al.* (2025), whose forecasts suggest a reduction in the duration of criminal proceedings by 20-25% and an increase in the accuracy of evidence analysis to 90% with the implementation of a national platform for the management of digital evidence using artificial intelligence. Despite the broad range of existing studies, the practical implementation of cross-border cooperation between Kazakhstan and South Korea in the field of cryptocurrency investigations remains insufficiently explored.

The purpose of this study was to identify the specific features of national approaches to the use of digital forensics in the investigation of cryptocurrency-related crimes in the Republic of Kazakhstan and the Republic of Korea. The research objectives were as follows:

1. To examine the regulatory and legal foundations and mechanisms that constitute the legal basis for the functioning of digital forensics in the field of cryptocurrency-related crimes in both jurisdictions;

2. To analyse the practical approaches, institutional capacities and results of the application of digital forensic methods by the law enforcement agencies of kazakhstan and the republic of korea in the investigation of cryptocurrency-related offences;

3. To systematise existing mechanisms of international cooperation between the countries under study and to determine the prospects for the development of bilateral cooperation in countering cross-border cryptocurrency-related crime.

Materials and Methods

The methodological framework consisted of the international standards of the Financial Action Task Force (2025) (FATF) on the regulation of virtual asset service providers (VASP), in particular Recommendation 15 on new technologies and the Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Financial Action Task Force, 2021), which sets out the definition of VASP as entities that conduct exchange

between virtual assets and fiat currencies, transfer, safekeeping or administration of virtual assets. This provided unified criteria for assessing national approaches to countering cryptocurrency-related crime. The theoretical framework was formed by the conceptual foundations of digital forensics in the cryptocurrency sphere, based on comprehensive analysis of blockchain data, including address clustering for grouping wallets, heuristic algorithms for identifying behavioural patterns, analysis of time stamps and correlation analysis for detecting links between different addresses and services (Kubanova *et al.*, 2025).

The comparative legal method was used to systematically compare the regulatory approaches of the Republic of Kazakhstan and the Republic of Korea through an analysis of national legislative acts forming the legal basis for the functioning of digital forensics in the field of virtual assets, including the Act of the Republic of Korea No. 14839 (2017), the Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), and the Act of the Republic of Korea No. 19563 (2024) as well as subordinate legislation and regulatory documents governing special legal regimes, in particular the Rules and Mechanisms of Cooperation of Unbacked Digital Asset Exchanges with Second-Tier Banks of the Republic of Kazakhstan issued by the AIFC – Astana International Financial Centre (2023), and regulatory acts of the financial authorities of the Republic of Korea issued by the FSC – Financial Services Commission of Korea (2023; 2024a; 2024b) and the KoFIU – Korea Financial Intelligence Unit (n.d.). Structural and functional analysis was used to identify interconnections between different elements of national law enforcement systems, including coordination between regulatory authorities, financial intelligence units and law enforcement structures in both jurisdictions, with a view to identifying the specific features of organisational models for countering cryptocurrency-related crime and assessing promising areas for bilateral cooperation in this sphere.

Statistical analysis was applied to process quantitative indicators of the effectiveness of law enforcement activities, using analytical reports from the international platform Chainalysis (2024; 2025) on the volume of illegal cryptocurrency transactions, data from the Agency of the Republic of Kazakhstan for Financial Monitoring (2025a) on the dismantling of money laundering structures operating through cryptocurrency in 2024, and statistics from the State Revenue Committee… (2025) on the regulation of digital mining, as well as statistical indicators of the activities of the specialised investigative task force for cryptocurrency-related crimes in the Republic of Korea for 2023-2024 from the Seoul Southern District Prosecutors' Office (2024). The method of systematisation was used to create structured tables of regulatory requirements and mechanisms of international cooperation, which provided a clear representation of complex regulatory constructs and made it possible to identify a gradation from basic financial monitoring standards to specialised supervisory regimes for virtual assets. This facilitated systematic comparison of practices and the identification of specific features of national models for countering cryptocurrency-related crime.

The case-study method was used to examine instances in which national courts in the Republic of Kazakhstan recognised digital evidence obtained through blockchain analysis in criminal cases concerning the unlawful circulation of digital assets. The materials for analysis were official communications from the Agency of the Republic of Kazakhstan for Financial Monitoring (2025b) on court verdicts in cases of illegal cryptocurrency exchange in the cities of Astana and Almaty for the period 2024-2025, and an official communication from the Prosecutor's Office of Astana (2024) on the outcomes of court proceedings in cases relating to cryptocurrency-related crimes. This method made it possible to identify the courts' approaches to assessing the admissibility and reliability of electronic evidence in cases involving virtual assets and to establish practical evidential standards in cryptocurrency cases.

The international legal framework consisted of bilateral treaties on extradition and mutual legal assistance between Kazakhstan and the Republic of Korea concluded by the Ministry of Foreign Affairs of the Republic of Korea (2003), which establish a formal mechanism for the surrender of offenders and the exchange of evidential information in criminal matters. The analytical basis consisted of reports from international organisations, including materials from the INTERPOL (2023; 2024a; 2024b; 2025) HAECHI series of operations targeting online fraud and cryptocurrency scams, and the capacity-building programmes of the OSCE – Organisation for Security and Co-operation in Europe (2023; 2025) in the field of combating cybercrime, which together provided a comprehensive understanding of institutional mechanisms and practical outcomes of international cooperation in countering cryptocurrency-related crime.

Results

The growth in the volume of cryptocurrency transactions on a global scale is accompanied by a parallel increase in criminal offences involving the use of digital assets. As of 2024, law enforcement agencies in various countries are facing new challenges in investigating crimes in which cryptocurrencies are used as an instrument for laundering criminal proceeds, financing terrorism and conducting fraudulent schemes. In the Republic of Korea, a specialised investigative task force on cryptocurrency-related crimes, in the course of its activities in 2024, initiated more than 30 criminal cases, brought charges against 41 individuals and confiscated assets totalling 846 billion Korean won, of which 564 billion were virtual assets (Seoul Southern District Prosecutors' Office, 2024). In Kazakhstan, tax audits conducted during 2024 revealed violations in the field of cryptocurrency mining, which led to additional tax assessments amounting to 4.9 billion tenge, and also established cases of under-reporting income from the sale of cryptocurrency with additional assessments of personal income tax totalling 4.3 billion tenge, demonstrating the scale of

tax evasion in the cryptocurrency sector (State Revenue Committee…, 2025). The effectiveness of combating such offences directly depends on the capacity of law enforcement systems to adapt to technological change and to implement modern methods of digital forensics.

Regulatory and legal framework and the context of the problem of digital forensics. The global growth of crime in the field of cryptocurrencies is creating new challenges for law enforcement agencies in national jurisdictions, requiring the development of specialised methodological approaches and institutional mechanisms. According to analytical data from the specialised platform Chainalysis (2024; 2025), the volume of detected illegal cryptocurrency transactions worldwide in 2024 amounted to 40.9 billion US dollars under current metrics for identifying illicit addresses; however, taking into account historical trends in retrospective recalculation, this figure may reach 51 billion dollars after further identification of additional illicit addresses over the following year. For comparison, the initial estimate for 2023 amounted to 24.2 billion dollars at the time of publication of the preliminary report, but one year later, after additional identification of illicit addresses, this figure rose to 46.1 billion dollars, which demonstrates the need to take account of methodological particularities in the assessment of cryptocurrency-related crime. The share of criminal operations in 2024 was 0.14% of the total volume of cryptocurrency transactions, reflecting a decrease compared with 0.61% in 2023; however, this share is also expected to increase after retrospective recalculation. These statistical indicators confirm the need for the development of specialised approaches to countering cryptocurrency-related crime at the national level. An additional challenge in 2024 was the shift in the structure of cryptocurrency assets used in criminal activity: stablecoins accounted for 63% of all illicit transactions, reflecting a broader ecosystem-wide trend towards increased use of stablecoins, with the volume of operations involving them rising by 77% compared with the previous year (Chainalysis, 2025).

The dynamics of the development of cryptocurrency-related crime demonstrate a trend towards the complication and diversification of criminal schemes, evolving from early forms of investment fraud to complex multi-layered money laundering operations through decentralised finance protocols and transaction mixing services. Traditional categories of cryptocurrency crime include theft from centralised exchanges, fraudulent investment schemes and pyramids, ransomware demanding payment in cryptocurrencies, drug trafficking and other illicit goods on darknet platforms, as well as the use of crypto-assets to finance terrorism and circumvent international sanctions. Alongside traditional forms of criminality, new forms of offences specific to the decentralised financial ecosystem are emerging, including manipulation of decentralised exchanges, fraud involving non-fungible tokens, abuses within decentralised autonomous organisations and the exploitation of smart contract vulnerabilities for the unlawful appropriation of assets. This evolution of criminality requires law enforcement agencies to continuously adapt to new forms of criminalisation of the digital space and to develop appropriate methodological tools for counteraction.

The response to these challenges is the development of digital forensics in the field of cryptocurrencies, an interdisciplinary domain that integrates methods from information security, cryptography, financial analysis and criminal procedure law in order to identify, document and interpret electronic traces of criminal activity in blockchain ecosystems. The methodology of digital forensics in the cryptocurrency sphere is based on comprehensive analysis of blockchain data, including address clustering to group wallets belonging to a single user, heuristic algorithms to identify behavioural patterns, time-stamp analysis to establish the sequence of events and correlation analysis to detect links between different addresses and services (Kubanova *et al*., 2025). The technical basis of these methods consists of specialised tools such as Chainalysis Reactor, Elliptic Investigator and CipherTrace Inspector, which enable law enforcement agencies to visualise cryptocurrency flows, identify high-risk addresses and services, and automate the tracking of funds through complex money-laundering schemes. The practical application of these methodological approaches depends to a large extent on the existence of an appropriate regulatory and legal framework and institutional mechanisms in national jurisdictions.

In the context of creating such a legal framework, the Republic of Kazakhstan, in response to the development of the crypto industry and the potential risks of money laundering, adopted the comprehensive Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), which entered into force on 1 April 2023 and created the legal basis for regulating all aspects of activity in the field of virtual assets. For the first time at the national level, this legislative act defined the concept of a digital asset as a digital expression of value or contractual rights that can be transferred and stored in electronic form using distributed ledger technology or similar technology. Structurally, the Law establishes a distinction between backed digital assets, which comply with established regulatory requirements and are backed by real assets or issued on licensed platforms, and unbacked digital assets, which encompass all other virtual assets.

The institutional mechanism for implementing Kazakhstan's legislation provides for the creation of a system of inter-agency coordination under the leadership of an authorised body that is responsible for licensing activity in the field of digital mining and monitoring compliance with the legislation. In accordance with Article 4 of the Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), the authorised body carries out state control in the field of digital assets, including supervision of compliance by entities engaged in the issuance and circulation of digital assets with legislation in the sphere of anti-money laundering (AML) and countering the financing of terrorism. In addition, the legislation creates a special legal regime within the Astana International Financial Centre (2023), where licensed cryptocurrency exchanges operate under the supervision of the

Astana Financial Services Authority (AFSA), providing an additional level of control and oversight over the activities of market participants. The practical implementation of the regulatory model provides for mandatory licensing of mining activity, the use exclusively of accredited national mining pools, the obligation to sell part of mined cryptocurrency via Kazakhstani exchanges in the amount of 50% in 2024 with a subsequent increase to 75% from 2025, and the payment of tax at a rate of 15% on income (Crypto license in Kazakhstan, n.d.; Greshnikov, 2025).

In contrast to the Kazakhstani approach, the Republic of Korea has developed a phased approach to regulating the cryptocurrency market, characterised by systematic and consistent implementation of regulatory measures. The first stage was the reform in March 2021 of the Act of the Republic of Korea No. 14839 (2017), as amended in 2024, which introduced mandatory registration of VASP with the financial regulator and implemented the Financial Action Task Force travel rule for the transmission of information on the sender and recipient in cryptocurrency transfers exceeding 1 million won in order to prevent money laundering (Financial Services Commission of Korea, 2024a). As a result of these measures, more than 60 small cryptocurrency exchanges that failed to meet the enhanced compliance requirements, including mandatory partnerships with banks for the safekeeping of clients' fiat deposits, were closed, leading to market concentration around a small number of large licensed platforms with the corresponding supervisory and control infrastructure.

The current culmination of the development of the regulatory system was the adoption on 18 July 2023 by the National Assembly of the Republic of Korea of the Act of the Republic of Korea No. 19563 (2024), which consolidated provisions from 19 different bills and entered into force on 19 July 2024 after a one-year transition period for industry adaptation. This legislative act establishes a comprehensive supervisory regime aimed at ensuring user protection and creating an orderly virtual asset market through four key regulatory blocks: measures to protect client assets, prohibitions and sanctions against unfair trading, the granting of supervisory and sanctioning powers to financial regulators in respect of VASP, and mechanisms for cooperation between financial regulators and law enforcement agencies in investigating crimes on the virtual asset market. The regulatory component of the Act obliges VASP to ensure the segregation of clients' fiat funds and cryptocurrencies in banking institutions, to accrue interest for users on fiat deposits, and to maintain full (100%) reserves of cryptocurrencies belonging to clients (Financial Services Commission of Korea, 2024a).

The sanctions component of Korean legislation includes a wide range of supervisory and enforcement mechanisms that ensure effective law enforcement in the field of virtual assets. The Financial Supervisory Service (FSS) has been granted the right to conduct inspections and audits of compliance with user protection requirements, while the FSC ssion may impose administrative penalties, including orders to remedy violations, fines of up to 5 billion won for corporations, suspension of activities and revocation of registration (Financial Services Commission of Korea, 2024b). Criminal liability of up to five years' imprisonment is provided for in cases of systematic or particularly serious offences. Both jurisdictions, despite different emphases in their regulatory approaches, adhere to international Financial Action Task Force standards and implement regulatory mechanisms to ensure the transparency of cryptocurrency operations, recognising the necessity of coordinating global efforts to combat cybercrime and cryptocurrency-related offences (Kubanova *et al.*, 2025). The systematisation of regulatory requirements that constitute the legal basis for digital forensics in both countries is presented in Table 1.

Table 1. Regulatory requirements directly strengthening digital forensics

Jurisdiction	Instrument (year / status)	Key obligations of VASPs/exchanges relevant to forensics (data, access, control)	Supervisory authority
Kazakhstan	Law "On Digital Assets" No. 193-VII (adopted 06.02.2023; in force; amended 05.09.2024) – defines digital assets, introduces state control and coordination of AML/CFT in the field of digital assets	Requirement to comply with AML/CFT: KYC, STR, state control over issuance/circulation; consolidation of the powers of the authorised body for supervision and inter-agency coordination – legal basis for obtaining transactional data and logs from market participants	Authorised body of the Republic of Kazakhstan in the field of digital assets; cooperation with the financial intelligence unit
Kazakhstan (AIFC regime)	AIFC/AFSA: "Rules and mechanisms of cooperation of Unbacked Digital Asset Exchanges ... with second-tier banks of the Republic of Kazakhstan" (current version, PDF) – regulates interaction between exchanges and banks	Operational mechanisms for data exchange between cryptocurrency exchanges/operators of digital assets and second-tier banks: facilitates tracing of fiat on/off-ramps, retention and access to records of fund movements (bank logs plus on-chain references)	AFSA (AIFC regulator)
South Korea	Virtual Asset User Protection Act (VAUPA) (adopted 18.07.2023; in force since 19.07.2024) + drafts/detailed rules of the FSC	Segregation of clients' fiat funds in banks; 100% reserve of clients' crypto-assets; mandatory insurance/reserve fund for compensation of losses; continuous transaction monitoring and immediate reporting to the FSS of indicators of market manipulation/insider trading; enhanced inspections and sanctions by the FSC/FSS – together forming a complete evidentiary "trail" (logs, records, inspection reports)	FSC / FSS / KoFIU

Continued Table 1

Jurisdiction	Instrument (year / status)	Key obligations of VASPs/exchanges relevant to forensics (data, access, control)	Supervisory authority
South Korea (AML / Travel Rule)	Implementation of the FATF Travel Rule through KoFIU / the special act on financial information (2021); CDD for certain transactions; 1 million KRW threshold for transfers (wire transfers) in the AML system	Formalises KYC/CDD and inter-institutional data exchange on senders/recipients; ensures the availability of named information for rapid forensic analysis and ML screening of transfers through threshold-based procedures	KoFIU (financial intelligence unit)

Note: CFT – Combating the Financing of Terrorism; KYC – Know Your Customer; CDD – Customer Due Diligence; STR – Suspicious Transaction Reports; Travel Rule – the rule on the transfer of information on transaction participants
Source: compiled by the authors on the basis of the Korea Financial Intelligence Unit (n.d.), Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), Astana International Financial Centre (2023), Financial Services Commission of Korea (2023), Financial Action Task Force (2021; 2025)

Table 1 systematises regulatory requirements that directly affect the effectiveness of digital forensics in both jurisdictions, demonstrating an evolution from basic AML/CFT standards to comprehensive supervisory mechanisms for virtual assets. Comparative analysis of the regulatory instruments presented reveals a gradation from general financial monitoring requirements in Kazakhstan's core legislation to the specialised regimes of the AIFC and the Korean system for protecting virtual asset users. The Korean model integrates preventive mechanisms for transaction monitoring and immediate reporting of suspicious operations directly into the obligations of service providers, whereas the Kazakhstani approach focuses on ensuring the basic infrastructure for the collection and exchange of information between regulatory bodies. Travel Rule mechanisms in both jurisdictions create the technical basis for international data exchange on cryptocurrency transfers, which is critically important for cross-border investigations, while the difference in threshold values reflects differing approaches to balancing user privacy and law enforcement needs.

Application of digital forensics: Investigation of cryptocurrency-related crimes in Kazakhstan and Korea. The practical implementation of the theoretical foundations of digital forensics depends on the capacity of law enforcement agencies to apply methods of tracing blockchain transactions and de-anonymising offenders, which requires the creation of specialised institutional structures and the development of appropriate technical competences. In both jurisdictions, specialised institutional capacities for conducting such investigations are being formed; however, their scale and organisational structure differ in line with national particularities of the cryptocurrency market and the law enforcement system. Kazakhstan demonstrates an initial stage of systematic implementation of digital forensics, receiving expert support from international organisations in building national capacities through specialised training programmes and the exchange of best practices. A concrete example of such cooperation was the joint training course held in Astana in June 2023 by the Organisation for Security and Co-operation in Europe (2023) and the United Nations Office on Drugs and Crime (UNODC) for Kazakhstani law enforcement officers, devoted to the investigation of crimes involving cryptocurrencies and the functioning of the darknet.

The structure of the training programme covered a wide range of theoretical and practical aspects of digital forensics, creating the necessary foundation for effective investigation of cryptocurrency-related crimes. Approximately 20 representatives of the Ministry of Internal Affairs, the Academy of the Ministry of Internal Affairs and the Academy of Law Enforcement Agencies under the Prosecutor General's Office took part in the programme, while international experts from Germany and Ukraine provided instruction on modern methodological approaches to cryptocurrency forensics. The practical component of the programme included key concepts of blockchain technologies and the functioning of cryptocurrencies, practical methods for profiling users, techniques for tracing transactions and procedures for seising crypto-assets, with participants practising practical skills in clustering cryptocurrency wallets, identifying linked addresses and analysing anomalies in transaction sequences (Organisation for Security and Co-operation in Europe, 2023). In addition, the programme included a demonstration by a representative of the cryptocurrency exchange Binance of the possibilities for cooperation between exchanges and law enforcement agencies in tracking transactions and disclosing information on suspects, as well as the study of anonymisation technologies, including the Tor network and Darknet platforms.

The technical component of digital forensics requires specialised knowledge and procedural skills, including the seizure of hardware devices storing private keys, the creation of forensic images of electronic data carriers, analysis of network activity logs and reconstruction of transaction chains in blockchain networks. In response to these requirements, Kazakhstani law enforcement agencies are introducing specialised protocols for preserving the integrity of digital evidence, including the use of cryptographic hash functions to confirm the immutability of data and the application of chain-of-custody procedures to document all stages of work with evidence (Kubanova *et al.*, 2025). The results of the practical application of the knowledge acquired by Kazakhstani law enforcement agencies are

confirmed by concrete outcomes in 2024 and the creation of judicial precedents for the use of digital evidence. According to the Agency of the Republic of Kazakhstan for Financial Monitoring (2025a), during 2024 the activities of 36 illegal cryptocurrency exchanges were detected and terminated, with a total turnover of approximately 60 billion tenge, equivalent to more than 110 million US dollars.

The characteristics of the offences uncovered indicate the systemic nature of the illegal activity and the need for a comprehensive approach to counteraction. These illegal exchanges operated without the necessary licences and outside the legal framework; some of them functioned as online services masquerading as peer-to-peer exchanges, did not carry out client identification procedures and, as investigations established, were widely used by organised criminal groups for laundering proceeds from cyber fraud and drug trafficking. The operational activities of law enforcement agencies demonstrated growing effectiveness through coordinated actions by different departments and the use of modern technical means. The Agency of the Republic of Kazakhstan for Financial Monitoring (2025a), with the support of the National Security Committee, conducted a comprehensive operation to block more than 3,500 web resources of illegal online exchanges, making access to their services more difficult for the public. The financial results of the operations included the freesing and confiscation of assets totalling 4.8 million USDT, equivalent to approximately 2.5 billion tenge, in the course of investigating these cases, which indicates that Kazakhstani authorities have mastered mechanisms for seising cryptocurrency assets by obtaining access to wallet private keys or through court orders for compulsory transfer of assets via exchange platforms.

The expansion of law enforcement activities has covered different types of cryptocurrency-related crime, including pyramid schemes and investment fraud. In 2024 the Agency of the Republic of Kazakhstan for Financial Monitoring (2025a) uncovered two pyramid schemes that had attracted investments in cryptocurrencies; law enforcement agencies were able to return approximately 545 thousand USDT to victims and additionally freeze 120 thousand USDT in the accounts of the organisers of the fraudulent schemes. Judicial practice has demonstrated the readiness of Kazakhstan's national legal system to recognise digital evidence obtained through blockchain analytics in criminal proceedings. In January 2024, a court in Astana convicted two individuals, A.V. Kuchukov and E.T. Sadirov, under Article 214 of the Criminal Code of the Republic of Kazakhstan for carrying out illegal cryptocurrency exchange operations with a turnover of 15 billion tenge; Kuchukov was sentenced to three years' imprisonment with confiscation of property, and Sadirov to two years and six months with confiscation of property, with 22,894.5 USDT, 328 thousand US dollars and almost 7 million tenge confiscated in favour of the state. In December 2024, a court in Astana delivered a verdict in a case concerning illegal entrepreneurial activity related to cryptocurrency exchange totalling more than 7 billion tenge, in which digital evidence of transactions served as the key evidential basis for the prosecution, and the Prosecutor's Office of Astana (2024), acting in the interests of the state, initiated four civil claims totalling 7.9 billion tenge, which were satisfied by court decisions with full recovery of the damage from the defendants. In March 2025, a court in Almaty convicted an individual under subparagraph 2 of paragraph 2 of Article 214 of the Criminal Code, imposing a sentence of two years and six months' restriction of liberty for the unlawful circulation of digital assets without the necessary permits totalling 5.6 billion tenge over the period from 2021 to 2024, with 5,172 USDT and a Mitsubishi motor car confiscated in favour of the state (Agency of the Republic of Kazakhstan for Financial Monitoring, 2025b). The above-mentioned court decisions create a body of precedent in which national courts recognise the admissibility and reliability of digital evidence obtained through the analysis of blockchain transactions, confirming the legal system's capacity to apply digital forensic methods effectively in proving cryptocurrency-related crimes.

In contrast to the initial stage of development in Kazakhstan, the Republic of Korea demonstrates one of the highest levels of institutional capacity in countering cryptocurrency-related crime globally, as a result of many years of experience and systematic investment in the development of relevant competences and technical capabilities. The historical development of the Korean system for combating cryptocurrency-related crime began in 2017-2018 with the establishment of specialised investigative teams to investigate cryptocurrency offences, including fraudulent initial coin offerings (ICO) and hacking attacks on local exchanges. The current stage of institutional development is characterised by the creation on 9 January 2024 by the FSS of two new departments devoted exclusively to virtual assets: the Virtual Asset Supervision Department and the Virtual Asset Investigation Department (Recent trends in virtual…, 2024). The functional division between the departments provides that the first is responsible for ongoing supervision, market monitoring and inspections of VASP, while the second is responsible for planning and conducting investigations and providing analytical support in uncovering criminal schemes.

The technological modernisation of Korea's financial monitoring system includes the implementation of new technological solutions announced by the KoFIU in 2024 for tracking cryptocurrency flows through the deployment of a system for the analysis and tracing of fund movements in the virtual asset sphere, which will integrate data from exchange platforms, banking institutions and blockchain scanners for the prompt detection of suspicious transactions (Recent trends in virtual…, 2024). An innovative element of the system is the potential introduction of a proactive mechanism for suspending suspicious transactions, which would allow the temporary blocking of fund movements prior to the commencement of a formal prosecution investigation in cases of reasonable suspicion of money

laundering or fraud. The comprehensive infrastructure includes integration with databases of all licensed cryptocurrency exchanges, automated real-time transaction monitoring and the use of machine learning algorithms to detect suspicious activity patterns; the system is capable of tracing transaction chains across multiple exchanges and wallets, identifying attempts to circumvent withdrawal limits through the creation of multiple accounts, and detecting correlations between the activities of different users in order to identify possible conspiracies or coordinated actions (Hassan, 2025).

Statistical performance indicators show an increase in the activity of law enforcement agencies in detecting and investigating cryptocurrency-related crime, reflecting both the growth in the scale of criminal activity and the improved effectiveness of monitoring and analytical systems. In 2023, the KoFIU received 16,076 reports of suspicious cryptocurrency transactions, 49% more than in 2022, while the number of recorded serious incidents potentially linked to money laundering, market manipulation or drug trafficking using cryptocurrencies rose by 90% (Financial Services Commission of Korea, 2024a). Enforcement effectiveness indicators show an increase in the proportion of reports that led to criminal proceedings, from 12% in 2022 to 23% in 2023. Concrete results of activity include the arrest of around one thousand suspects in cryptocurrency-related crimes in the first half of 2024, more than double the figure for the same period of the previous year, with the most high-profile case being the arrest of 215 individuals in November 2024 in connection with a cryptocurrency investment scam worth 320 billion won, equivalent to approximately 228 million US dollars (South Korean police arrest…, 2024).

The methodological basis of Korean digital forensics demonstrates a comprehensive approach to investigating cryptocurrency-related crime through the integration of technical and traditional investigative methods, including the analysis of blockchain data using specialised software, open-source intelligence to de-anonymise users by correlating cryptocurrency wallet addresses with activity on social networks, and monitoring of internet forums and messengers to detect the sale of stolen assets or the recruitment of investors. The judicial system of the Republic of Korea has accumulated practice in accepting electronic evidence collected in the blockchain as admissible and reliable in criminal cases concerning money laundering via cryptocurrencies. The practical application of these methods was demonstrated in the 320-billion-won case, in which an organised criminal group sold 28 types of virtual tokens via front investment companies without any real activity, artificially inflating their price through pyramid methods and market manipulation; in the course of the investigation, 22 bitcoins were confiscated and other assets of the group worth approximately 34 million US dollars were seised (South Korean police arrest…, 2024). The case illustrates the maturity of Korea's digital forensic system and its capacity to combine technical methods of blockchain analysis with traditional investigative measures effectively in order to achieve concrete law enforcement outcomes.

Comparative analysis and international cooperation in cryptocurrency crime investigations. The comparative analysis of national approaches to combating cryptocurrency crime in the Republic of Kazakhstan and the Republic of Korea reveals fundamentally different strategies, reflecting disparities in the development levels of national cryptocurrency markets, institutional capabilities, and regulatory priorities. Systematic comparison of practices allows for identifying the peculiarities of national models and assessing the prospects of bilateral cooperation in this field. The regulatory-institutional differences are fundamental and define the nature of law enforcement activity in the field of virtual assets. In the Republic of Korea, the regulatory regime is characterised by strictness and proximity to traditional financial supervision, with direct involvement of financial regulators in monitoring and investigating abuses in the virtual asset market (Financial Services Commission of Korea, 2024a). The Act of the Republic of Korea No. 19563 (2024) imposes direct obligations on service providers to counter fraud through monitoring trading activities and allows sanctions for non-compliance.

In contrast, the Kazakh model shows greater liberalisation concerning licensed market participants: the state focuses on legalising activities in mining and exchange operations, and on identifying blatantly illegal entities, including unlicensed exchangers and financial pyramids (Ministry of Artificial Intelligence…, 2022). The Law of the Republic of Kazakhstan No. 193-VII ZRK (2023) differs in that it does not contain detailed provisions on market manipulation or consumer protection but integrates general requirements for anti-money laundering and combating the financing of terrorism, extending financial monitoring provisions to the digital asset sphere. Institutionally, the fight against cryptocurrency crime in Kazakhstan is carried out by the Agency of the Republic of Kazakhstan for Financial Monitoring and the National Security Committee in cooperation with law enforcement agencies, while in the Republic of Korea, an integrated coordination system exists between the police, prosecutors, and financial regulators. This difference in approaches reflects different levels of maturity in the cryptocurrency markets and different state policy priorities in the sphere of financial innovation.

Analysis of quantitative performance indicators reveals a significant asymmetry in the scale of the problem and corresponding institutional response between the two countries, which is determined by the differing levels of development of national cryptocurrency ecosystems. In Kazakhstan, initial results have been achieved in seising crypto-assets worth millions of dollars, blocking thousands of illegal online resources, charging several individuals, and securing judicial convictions for cryptocurrency crimes, demonstrating the formation of basic capabilities in this area. Specific achievements include the liquidation of 36 illegal crypto exchanges with a total turnover of over 110 million USD, freesing assets worth 4.8 million USDT,

and returning approximately 545,000 USDT to victims (Agency of the Republic of Kazakhstan for Financial Monitoring, 2025a).

South Korea demonstrates much larger-scale law enforcement activity, reflecting the maturity of its institutional system in combating cryptocurrency crimes. In the first half of 2024, nearly a thousand suspects in cryptocurrency crimes were arrested, and hundreds of millions of dollars in both cryptocurrency and fiat were frozen and seized. The international INTERPOL (2024a) operation HAECHI-V, with active participation from the Republic of Korea in 2024, covered 40 countries, resulting in the arrest of 5,500 people and the confiscation of over 400 million USD in cryptocurrency and fiat assets. During this operation, Korean police, in cooperation with Chinese counterparts, dismantled a large-scale phone fraud network that caused 1.5 trillion won in losses and used cryptocurrency for money laundering, underscoring Korea's leading role in global efforts to combat cryptocurrency crime.

Common challenges and gaps in national systems are linked to the adaptability of criminal schemes to regulatory measures, requiring continuous improvement of digital forensics methods and international coordination of efforts. Criminals are increasingly using decentralised tools, including decentralised exchanges and mixing services, to circumvent regulatory requirements and complicate the tracing of funds. South Korean law enforcement agencies are recording cases of stolen funds being converted into private cryptocurrencies with increased anonymity, using decentralised finance protocols to hide traces, or multi-stage exchanges between stablecoins to obscure the source of asset origins. Kazakhstan faces the problem of transferring illegally obtained cryptocurrency assets abroad, especially through offshore platforms, complicating national law enforcement efforts and requiring international coordination to freeze such assets.

The technical complexity of evidence collection remains a shared challenge for both countries, as in order to bring a case to court, it is necessary not only to trace the transaction on the blockchain but also to prove that a particular cryptocurrency wallet belongs to a specific individual, which requires the combination of technical and traditional investigative methods. The legal foundation for bilateral cooperation between Kazakhstan and the Republic of Korea in combating cryptocurrency crime is based on a series of international agreements and multilateral mechanisms, creating the necessary institutional foundation for effective cooperation in cross-border crime investigations. The basic legal foundation was established on 13 November 2003 with the signing of the Extradition Treaty and the Mutual Legal Assistance Treaty (MLAT) in criminal matters (Ministry of Foreign Affairs of the Republic of Korea, 2003), which, after ratification in both countries, created a formal mechanism for the extradition of offenders and the exchange of evidential information in criminal cases. The MLAT obliges the parties to provide assistance in conducting investigative actions, including obtaining testimonies, documents, and physical evidence for use in criminal prosecution.

At the operational level, INTERPOL (2023) channels function through the I-24/7 system and global financial operations HAECHI under the coordination of the Republic of Korea, aimed at countering online fraud and cryptocurrency scams. The Republic of Korea is one of the main sponsors and coordinators of INTERPOL's HAECHI series operations, aimed at combating financial cybercrime, including cryptocurrency investment frauds, romantic scams involving cryptocurrency, and online gambling fraud. During HAECHI-IV, the Republic of Korea not only provided funding but also sent experts to joint headquarters in INTERPOL's Global Complex in Singapore, and initiated the publication of special notifications to inform other countries about new fraud schemes. Practical mechanisms of information exchange demonstrate the effectiveness of a multilateral approach to combating cross-border cryptocurrency crime through timely identification of new schemes and methods of their implementation, including the Republic of Korea's initiative to spread warnings about NFT rug pulls and the USDT Token Approval Scam through INTERPOL (2023).

The results of multilateral cooperation involving both countries confirm the effectiveness of coordinated international efforts in combating cryptocurrency crime. Operation First Light 2024, conducted under INTERPOL's aegis from March to May 2024 with the participation of 61 countries, including Kazakhstan, resulted in the arrest of 3,950 suspects and the freesing of assets totalling 257 million USD, of which 135 million USD were fiat funds and 2 million USD in cryptocurrency (INTERPOL, 2024b). The operation demonstrated the effectiveness of the Global Rapid Intervention of Payments mechanism in tracking and intercepting illicit income in both fiat currencies and cryptocurrencies through coordination between law enforcement and financial institutions across jurisdictions. The subsequent HAECHI VI operation, conducted from April to August 2025 with the participation of 40 countries and territories, including both Kazakhstan and South Korea, achieved significant results with the recovery of 439 million USD, including 342 million USD in fiat money and 97 million USD in physical and virtual assets (INTERPOL, 2025). During this operation, law enforcement agencies blocked over 68,000 bank accounts and froze about 400 cryptocurrency wallets, with approximately 16 million USD of illicit funds recovered from cryptocurrency wallets. A notable example of effective bilateral coordination was the successful recovery of 6.6 billion won (equivalent to 3.91 million USD), which the Korean steel company had transferred to an illegitimate bank account in Dubai after the detection of forged transport documents, with rapid communication between the two countries through the Global Rapid Intervention of Payments mechanism allowing the intercepted stolen funds to be fully returned (INTERPOL, 2025).

Kazakhstan is actively developing international cooperation in cryptocurrency forensics through participation

in regional initiatives under the Eurasian Group on Money Laundering and INTERPOL's working groups on Darknet and cryptocurrencies. The Agency of the Republic of Kazakhstan for Financial Monitoring is establishing working contacts with leading financial intelligence units globally, including the Korea Financial Intelligence Unit (n.d.), for the rapid exchange of intelligence on suspicious transactions and coordination of joint activities. From 2023 to 2025, within the framework of the Organisation for Security and Co-operation in Europe (2023; 2025) project on enhancing cybercrime capabilities, specialised training in blockchain forensics was conducted for Kazakhstani law enforcement officers with the participation of international experts, aligning standards for evidence collection and tracing. The structure of international cooperation mechanisms between Kazakhstan and the Republic of Korea in combating cryptocurrency crime is detailed in Table 2.

Table 2. Mechanisms of international cooperation and capacity building

Mechanism	Parties / Organiser	What it contributes to digital forensics	Current Status / Latest Activity
Bilateral Treaties: Extradition and Mutual Legal Assistance (MLAT)	Kazakhstan and the Republic of Korea (government agreements signed on 13.11.2003 in Seoul)	Legal basis for the execution of procedural requests, obtaining evidence (logs, exchange/bank records), temporary asset freezes, and extradition of suspects in cryptocurrency-related cases	Treaties in force; used as the basic channel for MLAT/extradition in cross-border investigations
INTERPOL's HAECHI Operations Series	INTERPOL with the support of the Republic of Korea; participation of dozens of countries	Operational headquarters, exchange of intelligence on fraudulent crypto schemes; flash alerts (typologies); rapid "cold" freesing of stolen digital assets via exchange-law enforcement coordination	Active programme; 2024 – record results (HAECHI-V, Jul-Nov 2024); large-scale multinational coordination
Joint Training on Cryptocurrencies and Darknet	OSCE and UNODC in cooperation with Kazakhstan (law enforcement agencies)	Standardisation of methodologies: address clustering, transaction chain tracing, crypto-asset seizure, OSINT in Darknet; training officers capable of working with evidence under Korean and international standards	23.06.2023 – course in Astana; 12-13.06.2025 – workshop with new competency framework in cybercrime (update to 2025 approach)
Banking-Crypto Interaction at the AIFC	AFSA (AIFC), banks of the Republic of Kazakhstan, and digital asset market participants	Regulated channel for linking on-chain data with banking logs (fiat on/off-ramps), accelerating request processing, wallet/account reconciliation	Rules in force; used during compliance checks and requests by law enforcement and supervisory agencies

Note: OSINT – Open Source Intelligence

Source: compiled by the authors based on INTERPOL (n.d.; 2024a), Ministry of Foreign Affairs of the Republic of Korea (2003), Astana International Financial Centre (2023), Organisation for Security and Co-operation in Europe (2023; 2025)

Table 2 illustrates the multi-layered architecture of international cooperation between Kazakhstan and the Republic of Korea in combating cryptocurrency crime, demonstrating a combination of bilateral legal instruments and multilateral operational mechanisms. The bilateral treaties of 2003 establish a stable legal foundation for formalised mutual legal assistance procedures, while participation in INTERPOL's global initiatives provides access to operational information and coordinated actions against transnational cryptocurrency networks. Capacity-building programmes under the aegis of the OSCE and other international organisations play a role in standardising methodological approaches and aligning technical competences, which are prerequisites for effective evidence exchange and joint investigations. Banking-cryptocurrency interaction within the AIFC provides an additional channel for obtaining financial information that may be relevant for international requests when cryptocurrency operations intersect with traditional banking systems. The asymmetry in the level of activity of different mechanisms reflects the current state of bilateral relations and the potential for deepening cooperation through intensified Kazakhstan's participation in global Korean-led initiatives.

The practical roadmap for bilateral cooperation between Kazakhstan and the Republic of Korea can rely on existing institutional mechanisms and foresee the gradual deepening of cooperation through specific operational measures and technical solutions. Recommended measures include updating operational protocols between financial intelligence units by creating contact points for urgent asset freezes and standardising data formats, which will ensure the speed and effectiveness of information exchange in critical situations. Integrating Kazakhstan into HAECHI operations with a focus on cross-border investment schemes and arbitrage operations will enable the country to contribute to global efforts to combat cryptocurrency crime and gain access to advanced methodologies and technical solutions. The use of the institutional architecture of the 2003 treaties to form expedited request procedures in virtual asset cases through standard lists of requested artifacts, agreed response times, and standardised procedures for data preservation and transmission will increase the efficiency of bilateral cooperation. Digital forensics has become an integral part of law enforcement tools in both countries, with varying levels of integration and technological maturity, while cooperation between the two countries

and integration into global initiatives is a strategic resource for enhancing the effectiveness of national systems in countering cryptocurrency crime.

Discussion

The research results revealed fundamental differences between the regulatory philosophies of Kazakhstan and the Republic of Korea, where the Kazakh model focuses on the legalisation of the crypto industry through licensing and special legal regimes within the AIFC, while the Korean approach is characterised by strict financial oversight and preventive monitoring with the integration of consumer protection requirements. This conclusion is fully supported by the detailed analysis of J. Lee (2024), who traced the evolution of Korean legislation from the initial ban on ICO in 2017 through the Terra/Luna crisis to the adoption of the VAUPA in 2023, highlighting the phased nature of regulatory changes. W. Jon & W. Yang (2025) further specified the mechanisms of the dual regulatory structure, where tokenised assets, defined as securities, are regulated by the Capital Markets Act, while other virtual assets fall under VAUPA, which fully correlates with the comprehensive oversight strategy identified in the study. The study by A. Sapa (2025) empirically demonstrated the positive impact of blockchain technologies on the financial security of 200 Kazakh enterprises between 2017 and 2023, using quantile regression and revealing coefficients ranging from 0.062 to 0.124 for blockchain and from 0.054 to 0.098 for tokenisation, depending on the level of financial vulnerability. This supports the study's conclusion about the legalisation strategy through the creation of a favorable business environment. A.B. Zhanabilova (2024) analysed the legal mechanisms of digital asset inheritance in Kazakhstan and confirmed the creation of a comprehensive institutional foundation through the distinction between secured and unsecured assets, which aligns with the identified feature of the Kazakh approach to categorising virtual assets.

The study also identified significant asymmetry in the practical results of applying digital forensics, where Kazakhstan achieved initial successes with the liquidation of 36 illegal exchanges and the confiscation of over 110 million USD in assets, while the Republic of Korea demonstrated large-scale results with the arrest of about a thousand suspects within six months and participation in global operations confiscating hundreds of millions of dollars. This confirms the findings of E. Ove *et al.* (2025) and C. Leuprecht *et al.* (2023). E. Ove *et al.* conducted a comprehensive analysis of the effectiveness of blockchain forensics in detecting illegal financial flows and confirmed that Korean tools from Chainalysis, CipherTrace, and Elliptic, through the use of machine learning algorithms and data visualisation, allowed law enforcement to identify suspicious activities in decentralised ecosystems, explaining the high success rates of operations. The authors detailed significant confiscation cases and law enforcement operations, confirming the growing role of blockchain forensics in dismantling criminal networks through darknet markets and unregulated exchanges. C. Leuprecht *et al.* conducted a cross-case analysis of 12 cases of transnational money laundering through cryptocurrencies and found that Bitcoin remains popular among money launderers alongside altcoins, with the use of third-party exchanges being a common method for creating and hiding illicit funds, which fully correlates with the trend of diversifying criminal schemes and justifies different national approaches to regulating exchanges.

The multi-level architecture of international cooperation identified in the study, from the 2003 bilateral treaties to participation in INTERPOL's HAECHI operations and capacity-building programs through the Organisation for Security and Co-operation in Europe, is fully supported by the research of Y. Ma (2025), who independently concluded the critical importance of coordinated international operations in combating transnational cryptocurrency networks.

The authors also conducted a detailed analysis of tracing techniques, including graph analysis, heuristic clustering algorithms, and probabilistic deanonymisation, and evaluated the evolution of the regulatory landscape, particularly the role of the Office of Foreign Assets Control and their legal challenges, which aligns with the recommendations of the study regarding the standardisation of methodological approaches. Y. Ma conducted a detailed study of the challenges in identifying VASP in cross-chain bridges through the analysis of the money laundering case from the 2022 Harmony hack and highlighted significant deficiencies and ambiguities in the current Financial Action Task Force regulatory frameworks, particularly regarding the distinction between owners/operators and other influential parties in decentralised financial arrangements, fully confirming the findings of the study about the need for specialised methodologies for international evidence exchange in cases involving decentralised tools.

C. Volten *et al.* (2025) used a mixed approach to study the impact of the Dutch implementation of the Fifth Anti-Money Laundering Directive on cryptocurrency exchanges, analysing over 335,000 transactions and conducting seven qualitative interviews with exchanges and supervisory authorities, revealing that regulatory measures created a high administrative burden and significant fees for relatively small exchanges, which provided additional insights into the implementation of international standards and emphasised the need for a proportional approach to regulating different types of market participants.

The conceptualisation of two trajectories of development for national digital forensics systems – the evolutionary model of gradual regulatory infrastructure building and the model of simultaneous market legalisation and law enforcement capability development – is fully supported by methodological research that developed the technical foundations of blockchain forensics. Y. Gong *et al.* (2025) focused on Bitcoin blockchain analysis and improved address clustering, presenting an enhanced simulation model for accurately modeling real Bitcoin transactions and

proposing a new heuristic algorithm for identifying one-time change addresses with experimental results demonstrating more accurate clustering results compared to existing heuristic methods, supporting the study's conclusion about the importance of technical competences for the evolutionary model of development and the need for standardised platforms to evaluate clustering algorithms.

H. Atlam *et al.* (2024) conducted a systematic literature review of 46 articles from an initial pool of 672 publications and systematically analysed the challenges of blockchain forensics, emphasising the difficulties in identifying and tracking illegal activity due to the decentralisation of technology and issues with preserving the integrity of evidence due to blockchain immutability, which fully correlates with the study's identified technical limitations regarding proving the ownership of cryptocurrency wallets by specific individuals. A. Choudhary (2023) highlighted the transformative potential of blockchain technology for forensic investigations and computer forensics, noting the possibilities of using hash values for verifying the authenticity of digital data and emphasised the need for specialised knowledge and tools for the successful investigation of crimes involving blockchain, supporting the conclusion about the dependence of effectiveness on institutional maturity and the importance of developing technical competences in law enforcement agencies. R. Shevchuk *et al.* (2025) and S.A. Al Naqbi *et al.* (2025) conducted bibliometric analyses and demonstrated the rapid growth of publications on anomaly detection in blockchain networks from 2017 to 2024 and the increasing interest in machine learning in blockchain security, identifying key scientific clusters, including unsupervised learning, Bitcoin security, and lightweight federated learning, which supports the study's findings about the technologisation of law enforcement and the evolution from basic protection mechanisms to complex artificial intelligence approaches.

The conclusion of the study regarding the critical role of the legal framework in creating an effective evidence trail and ensuring transparency in cryptocurrency operations is fully supported by legal and social studies. C. Ahn & N. Obermeier (2023) conducted a nationally representative survey experiment in South Korea and empirically demonstrated that exposure to information about cryptocurrency volatility increases trust in the government, while positive information about cryptocurrencies does not undermine trust in the government or support for state regulation, confirming the effectiveness of the comprehensive regulatory approach and the importance of public perception of legal measures for their legitimacy and effectiveness. A. Popik-Mazur (2025) analysed 1,249 articles from Scopus and Web of Science databases and applied a thematic synthesis of 1,135 articles to present the current state of the literature on illegal financial flows and money laundering, finding that 38% of the literature focuses on knowledge systematisation, while advanced machine learning techniques make up 26%, and modified gravitational models make up 3.33%, supporting the study's conclusion about the need for integration of technical and legal competences and an interdisciplinary approach to combating cryptocurrency crime.

The analysis of international scientific research demonstrates significant convergence of findings on key aspects of the development of digital forensics in the field of cryptocurrencies and confirms the theoretical and practical foundations established in the study. Most of the analysed works confirm the importance of adaptive regulatory approaches, the need for technological modernisation of law enforcement systems, and the critical importance of international coordination in combating transnational cryptocurrency crimes. The scientific community is increasingly focusing on developing standardised methodologies and technical solutions, applying machine learning algorithms to automate suspicious transaction detection processes, and creating integrated systems for monitoring cryptocurrency flows, indicating the formation of a consensus on the directions for the development of digital forensics and confirming the relevance of the comparative approach to analysing national models.

Conclusions

The study revealed fundamental differences between national approaches to the application of digital forensics in combating cryptocurrency crimes, systematised regulatory mechanisms, and assessed the effectiveness of law enforcement activities in two jurisdictions with different levels of cryptocurrency market development. The comprehensive analysis allowed for the identification of patterns in the formation of national models for combating cryptocurrency crime and identified key factors for their success. The analysis established that the legal systems of Kazakhstan and the Republic of Korea demonstrate different regulatory philosophies: the Kazakh model is oriented towards the legalisation of the crypto industry through licensing and tax incentives, with an emphasis on creating special legal regimes within the AIFC, while the Korean approach is characterised by stringent financial oversight and preventive monitoring with integrated consumer protection requirements. The study confirmed the significant asymmetry in the practical results of digital forensics application: Kazakhstan achieved initial successes with the confiscation of crypto-assets worth over 110 million USD and the liquidation of 36 illegal exchanges, demonstrating the formation of basic institutional capabilities, while the Republic of Korea demonstrated large-scale results with the arrest of around a thousand suspects within six months and participation in global operations confiscating hundreds of millions of dollars, confirming the maturity of the national system. The systematisation of international cooperation mechanisms revealed the operation of a multi-level architecture from the bilateral treaties of 2003 to participation in INTERPOL's HAECHI operations, while capacity-building programs through OSCE ensure the standardisation of methodological approaches and alignment of technical competences.

The results conceptualise two trajectories for the development of national digital forensics systems: the evolutionary model of gradual regulatory infrastructure building and the model of simultaneous market legalisation and law enforcement capacity building. The study confirms the critical role of the legal framework for creating an effective evidence trail and demonstrates the potential for international cooperation through a combination of formal treaty mechanisms and operational multilateral initiatives. The methodological contribution of the work lies in the development of a comparative analytical framework for assessing the effectiveness of national digital forensics systems. The practical significance of the results lies in identifying the preconditions for the successful functioning of digital forensics, including the need for integrating technical and legal competences, creating specialised institutional structures, ensuring inter-agency coordination, and the potential for mutual learning between jurisdictions with different experiences in regulating cryptocurrency markets.

The limitation of the study was its focus on two jurisdictions and limited access to detailed statistical information on specific aspects of operational investigative activities and international requests in cryptocurrency cases. A promising direction for future research is the expansion of the comparative analysis to other jurisdictions, the study of the impact of technological innovations on the effectiveness of digital forensics, and the development of standardised methodologies for international evidence exchange in cases involving decentralised financial instruments.

Acknowledgements
None.

Funding
None.

Author Contributions
A. Vilks conceived and supervised the study, and drafted the manuscript. A. Kipane contributed to data analysis and the development of methodology. A. Krivins revised the manuscript and provided significant input to the interpretation of results. All authors reviewed and approved the final manuscript.

Conflict of Interest
None.

References
[1] Abuova, A., Bakirova, N., Begaliyev, Y., Begaliyev, B., & Kaliyev, A. (2025). Prosecutorial effectiveness in Kazakhstan's criminal justice: The role of digital forensics and online trial broadcasting. *Mitteilungen Klosterneuburg*. doi: 10.61586/fg5bE.

[2] Act of the Republic of Korea No. 14839 "On Reporting and Using Specified Financial Transaction Information". (2017, October). Retrieved from https://law.go.kr/LSW/lsInfoP.do?lsiSeq=195313&urlMode=engLsInfoR&viewCls=engLsInfoR.

[3] Act of the Republic of Korea No. 19563 "On the Protection of Virtual Asset Users". (2024, July). Retrieved from https://law.go.kr/engLsSc.do?menuId=1&subMenuId=21&tabMenuId=117#.

[4] Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2023). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, 34(2), article number e2255. doi: 10.1002/nem.2255.

[5] Agency of the Republic of Kazakhstan for Financial Monitoring. (2025a). *Liquidation of cryptocurrency money laundering structures*. Retrieved from https://www.gov.kz/memleket/entities/afm/press/news/details/913888.

[6] Agency of the Republic of Kazakhstan for Financial Monitoring. (2025b). *In Almaty, a verdict was issued in the case of a crypto exchanger: Digital assets and a car were confiscated*. Retrieved from https://www.gov.kz/memleket/entities/afm/press/news/details/955747?lang=en.

[7] Ahn, C., & Obermeier, N. (2023). Cryptocurrency and the state: Evidence from South Korea. *Open Science Framework*. doi: 10.31219/osf.io/r4ayu.

[8] Al Naqbi, S.A., Nobanee, H., & Ellili, N.O.D. (2025). Global trends and insights into cryptocurrency-related financial crime. *Research in International Business and Finance*, 75, article number 102756. doi: 10.1016/j.ribaf.2025.102756.

[9] Alimkulov, Y., Sharipova, A., Zhanibekov, A., Mukhamadiyeva, G., & Aryn, A. (2023). Private detective activity of the law enforcement system of Kazakhstan on the experience of foreign countries. *International Journal of Electronic Security and Digital Forensics*, 15(6), 644-654. doi: 10.1504/IJESDF.2023.133964.

[10] Apsimet, N.M., Alimkulov, Y.T., & Duisenbayeva, G.Z. (2024). The collection of digital traces in the investigation of online crimes. *Law Series*, 7(4), 170-185.

[11] Astana International Financial Centre. (2023). Rules and mechanisms of cooperation of unbacked digital asset exchanges and/or centre participants authorised to carry out digital assets-related activities with second-tier bank of the Republic of Kazakhstan. In *AIFC Rules* (No. FR00063). Astana: AIFC.

[12] Atlam, H.F., Ekuri, N., Azad, M.A., & Lallie, H.S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, 13(17), article number 3568. doi: 10.3390/electronics13173568.

[13] Chainalysis. (2024). *The 2024 crypto crime report: The latest trends in ransomware, scams, hacking, and more*. Retrieved from https://www.pensamientopenal.com.ar/system/files/Documento_Editado1686.pdf.

[14] Chainalysis. (2025). *2025 crypto crime trends: Illicit volumes portend record year as on-chain crime becomes increasingly diverse and professionalized*. Retrieved from https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.
[15] Choi, S.W., Lee, J., & Lee, S. (2024). Cryptocurrency Ponzi schemes and their modus operandi in South Korea. *Security Journal*, 37, 1285-1300. doi: 10.1057/s41284-024-00417-5.
[16] Choudhary, A. (2023). Forensic investigations and computer forensics in the age of blockchain. *ISACA Journal*, 5.
[17] Crypto license in Kazakhstan. (n.d.). *GoFaizen & Sherle*. Retrieved from https://gofaizen-sherle.com/crypto-license/kazakhstan.
[18] Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, 46, article number 301576. doi: 10.1016/j.fsidi.2023.301576.
[19] Financial Action Task Force. (2021). Virtual assets and virtual asset service providers. In *Updated guidance for a risk-based approach*. Paris: FATF/OECD.
[20] Financial Action Task Force. (2025). International standards on combating money laundering and the financing of terrorism & proliferation. In *The FATF recommendations*. Paris: FATF/OECD.
[21] Financial Services Commission of Korea. (2023). *FSC proposes rules on the protection of virtual asset users*. Retrieved from https://fsc.go.kr/eng/pr010101/81217.
[22] Financial Services Commission of Korea. (2024a). *The act on the protection of virtual asset users to take effect from July 19*. Retrieved from https://fsc.go.kr/eng/pr010101/82683.
[23] Financial Services Commission of Korea. (2024b). *Strengthening responses to money laundering related to virtual assets and illegal private financing: Current status and plans*. Retrieved from https://www.fsc.go.kr/no010101/81712.
[24] Gong, Y., Chow, K.P., & Yiu, S.M. (2025). Improved Bitcoin simulation model and address heuristic method. *Forensic Science International: Digital Investigation*, 53, article number 301935. doi: 10.1016/j.fsidi.2025.301935.
[25] Greshnikov, K. (2025). New in the regulation of digital assets in Kazakhstan. *Chambers and Partners*.
[26] Hassan, B. (2025). *South Korean Island targets crypto tax evaders*. Retrieved from https://livebitcoinnews.com/south-korean-island-targets-crypto-tax-evaders.
[27] INTERPOL. (2023). *USD 300 million seised and 3,500 suspects arrested in international financial crime operation*. Retrieved from https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation.
[28] INTERPOL. (2024a). *INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million*. Retrieved from https://www.interpol.int/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million.
[29] INTERPOL. (2024b). *USD 257 million seised in global police crackdown against online scams*. Retrieved from https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams.
[30] INTERPOL. (2025). *USD 439 million recovered in global financial crime operation*. Retrieved from https://www.interpol.int/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation.
[31] INTERPOL. (n.d.). *Financial crime initiatives*. Retrieved from https://www.interpol.int/Crimes/Financial-crime/Financial-crime-initiatives.
[32] Jon, W., & Yang, W. (2025). Mapping South Korea's digital asset regulatory landscape: From criminal code to the recently implemented virtual asset user protection act. *Computer Law & Security Review*, 57, article number 106140. doi: 10.1016/j.clsr.2025.106140.
[33] Kaliyev, A. (2024). Selected aspects of investigating Internet fraud. *Newsletter of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 80(2), 294-301.
[34] Korea Financial Intelligence Unit. (n.d.). *What we do: Our efforts to prevent money laundering*. Retrieved from https://kofiu.go.kr/eng/policy/guide04.do.
[35] Kubanova, N., Nessipbayeva, I., Dyussebaliyeva, S., & Halibati, H. (2025). Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability. *Social & Legal Studies*, 8(1), 179-194. doi: 10.32518/sals1.2025.179.
[36] Law of the Republic of Kazakhstan No. 193-VII ZRK "On Digital Assets in the Republic of Kazakhstan". (2023, February). Retrieved from https://adilet.zan.kz/eng/docs/Z2300000193.
[37] Lee, J. (2024). An introductory review of virtual asset regulations in Korea. *Journal of Korean Law*, 23, 391-412.
[38] Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036-1054. doi: 10.1108/JFC-07-2022-0161.
[39] Ma, Y. (2025). Who constitute the VASPs in DeFi? A case study on money laundering via cross-chain bridge from the 2022 harmony hack. *Journal of Economic Criminology*, 7, article number 100131. doi: 10.1016/j.jeconc.2025.100131.
[40] Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan. (2022). *Digital assets industry*. Retrieved from https://www.gov.kz/memleket/entities/maidd/press/article/details/84078.

[41] Ministry of Foreign Affairs of the Republic of Korea. (2003). *Signing of the Korea-Kazakhstan treaty on extradition and treaty on mutual assistance in criminal matters*. Retrieved from https://mofa.go.kr/eng/brd/m_5676/view.do.
[42] Organisation for Security and Co-operation in Europe. (2023). *Joint OSCE-UNODC training course on cryptocurrencies and Darknet investigations held in Kazakhstan*. Retrieved from https://osce.org/secretariat/546977.
[43] Organisation for Security and Co-operation in Europe. (2025). *OSCE workshop in Kazakhstan advances national training strategy on cybercrime and electronic evidence*. Retrieved from https://osce.org/secretariat/593071.
[44] Ove, E., Williams, S., & Anderson, G. (2025). *The effectiveness of blockchain analytics in detecting illicit financial flows*. Retrieved from https://www.researchgate.net/publication/394929590_The_Effectiveness_of_Blockchain_Analytics_in_Detecting_Illicit_Financial_Flows.
[45] Park, A., Ryu, H., Park, W., & Jeong, D. (2023). Forensic investigation framework for cryptocurrency wallet in the end device. *Computers & Security*, 133, article number 103392. doi: 10.1016/j.cose.2023.103392.
[46] Popik-Mazur, A. (2025). A systematic literature review of illicit financial flows and money laundering: Current state of research and estimation methods. *Journal of Economics and Management*, 47, 257-298. doi: 10.22367/jem.2025.47.11.
[47] Prosecutor's Office of Astana. (2024). *Cryptocurrency as an object and means of committing crimes*. Retrieved from https://www.gov.kz/memleket/entities/prokuror-astana/press/news.
[48] Recent trends in virtual asset regulation. (2024). *Kim & Chang*. Retrieved from https://kimchang.com/en/insights/detail.kc?sch_section=4&idx=29294.
[49] Saniyazova, Y., Mediyev, R., Saitova, E., Utegenova, G., & Kzylkhojayeva, A. (2024). Advancing forensic science in Kazakhstan: The emergence and impact of digital forensics in cybercrime investigation. *Law, State and Telecommunications Review*, 16(2), 48-68. doi: 10.26512/lstr.v16i2.49190.
[50] Sapa, A. (2025). The impact of blockchain adoption and tokenisation on the financial security of Kazakhstani enterprises. *Futurity Economics & Law*, 5(3) 4-31. doi: 10.57125/FEL.2025.09.25.01.
[51] Seoul Southern District Prosecutors' Office. (2024). *One year of achievements and determination of the "virtual asset crime joint investigation team"*. Retrieved from https://www.spo.go.kr/site/spo/ex/board/View.do?bcIdx=1057718&cbIdx=1403.
[52] Shevchuk, R., Martsenyuk, V., Adamyk, B., Benson, V., & Melnyk, A. (2025). Anomaly detection in blockchain: A systematic review of trends, challenges, and future directions. *Applied Sciences*, 15(15), article number 8330. doi: 10.3390/app15158330.
[53] South Korean police arrest 215 people in suspected $228m crypto scam. (2024). *The Guardian*. Retrieved from https://theguardian.com/world/2024/nov/13/south-korea-crypto-scam-arrests.
[54] State Revenue Committee of the Ministry of Finance of the Republic of Kazakhstan. (2025). *Cryptocurrencies under control: How Kazakhstan regulates digital mining*. Retrieved from https://www.gov.kz/memleket/entities/kgd/press/news/details/963148.
[55] Volten, C., van Eeten, M., & van Wegberg, R. (2025). Money for nothing, supervision for a fee: Investigating the effects of the 5th anti-money laundering directive on cryptocurrency exchanges in the Netherlands. *European Journal on Criminal Policy and Research*. doi: 10.1007/s10610-025-09640-1.
[56] Zhanabilova, A.B. (2024). Legal regulation of the turnover of digital assets in the Republic of Kazakhstan and the possibility of their inheritance. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 3(78), 124-133. doi: 10.52026/2788-5291_2024_78_3_124.