The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 08 - 2026

Crypto-Assets as An Object of Forensic Examination: Grounds for Appointment, Limits of Expert Competence and Foreign Experience

Mansurov Oybek Olim ugli

Basic Doctoral Student (PhD Candidate), Forensic Science Research Institute, under the Republican Center of Forensic Expertise, named after Kh. Sulaymonova, Tashkent, Uzbekistan

Received: 26 Mar 2026 | Received Revised Version: 22 April 2026 | Accepted: 04 May 2026 | Published: 31 May 2026

Volume 08 Issue 05 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue05-24

Abstract

The article examines the procedural and forensic aspects of appointing and conducting forensic examinations in criminal cases involving crypto-assets. It substantiates that the absence of a dedicated type of examination, an approved methodology and a corresponding expert specialty in state forensic institutions has become a significant obstacle to the investigation of such crimes, given the introduction of criminal liability under Article 278⁸ of the Criminal Code of the Republic of Uzbekistan, the growing share of crypto-assets in fraud, money laundering and drug trafficking, and the spread of privacy-oriented cryptocurrencies. The specific nature of a crypto-asset as an object of forensic examination is revealed: since it has no physical form, the object of examination is the set of traces reflecting its ownership, movement and value, which are classified into six groups according to their carrier. Drawing on the typology of cryptocurrency-related crimes proposed in international literature, two procedural models for appointing an examination are distinguished, depending on whether the investigation begins with seized devices or with blockchain traces. The limits of expert competence among the computer-technical, blockchain-analytical and economic domains are defined, and a set of sample questions for the expert is proposed. The experience of the Russian Federation, the Republic of Kazakhstan, the Republic of Indonesia and the European Union, as well as the Budapest Convention, the FATF Recommendations and the ISO/IEC 27037, ISO/IEC 27042 and NIST SP 800-86 standards, is analysed. Based on Law No. ZRU-1152 "On Forensic Expert Activity", the article substantiates the introduction of a new type of forensic economic examination - the examination of crypto-asset transactions - at the Republican Center of Forensic Expertise named after Kh. Sulaymonova, and proposes measures for its implementation.

Keywords: Crypto-asset, cryptocurrency, forensic examination, blockchain, on-chain analysis, off-chain analysis, forensic economic examination, computer-technical examination, expert competence, digital evidence, appointment of examination, wallet, private key.

© 2026 Mansurov Oybek Olim ugli. This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0). The authors retain copyright and allow others to share, adapt, or redistribute the work with proper attribution.

Cite This Article: Mansurov Oybek Olim ugli. (2026). Crypto-Assets as An Object of Forensic Examination: Grounds for Appointment, Limits of Expert Competence and Foreign Experience. The American Journal of Political Science Law and Criminology, 8(05), 154–161. https://doi.org/10.37547/tajpslc/Volume08Issue05-24

1. Introduction

The value of money rests not on its material form but on trust among the members of a community. The stone money of the Yap Islands in Micronesia is a telling example: ownership of the stones was recorded in the collective memory of the entire community. According to N. Furneaux, this arrangement mirrors almost exactly the distributed ledger mechanism of the modern blockchain [1, p. 3-5]. The emergence of Bitcoin in 2009

opened the era of cryptocurrencies that operate without a central issuer or intermediaries, while their pseudonymity and cross-border nature paved the way for their extensive use for criminal purposes.

The cryptocurrency market has reached an enormous scale within a short period: its total capitalization reached USD 826 billion in January 2018 [2]. According to Europol, criminals use cryptocurrencies for money laundering, terrorist financing, the purchase of illicit goods on darknet markets, and ransomware and DDoS extortion attacks, while in recent years a shift toward privacy-enhanced cryptocurrencies such as Monero and Zcash has been observed [3]. Chainalysis data indicate that illicit addresses received at least USD 40.9 billion in crypto-assets in 2024 and that, since 2022, stablecoins have accounted for the bulk of illicit on-chain volume [4], [5].

On the Bitcoin network, all transactions are recorded on a public blockchain and can be traced to a specific address. Privacy-oriented cryptocurrencies such as Monero and Verge, however, rely on untraceable addresses, concealed transaction amounts and IP address obfuscation through the Tor and I2P networks, which makes it extremely difficult to link a payment to a specific person or to trace and seize funds [2]. At the same time, most forensic research on cryptocurrencies has been confined to Bitcoin, and models integrating on-chain and off-chain analysis into a single forensic process have only recently begun to appear [2], [4].

In Uzbekistan, the legal regulation of crypto-asset circulation began with Presidential Resolution No. PP-3832 of July 3, 2018 [6]. Law No. ZRU-899 of January 19, 2024, added Article 2788 to the Criminal Code, establishing liability for violating legislation on the circulation of crypto-assets; the provision took effect on April 20, 2024 [7]. The Criminal Code defines a crypto-asset as a property right that represents a set of digital records in a distributed data ledger and has a value and an owner [8]. In practice, the number of criminal cases under this article is steadily growing, and crypto-assets increasingly appear as a means of payment in fraud, money laundering and drug trafficking.

Nevertheless, the procedural and methodological framework for appointing and conducting forensic examinations in such cases has yet to be developed: state forensic institutions have no examination type, approved methodology or expert specialty dedicated to crypto-assets. Meanwhile, Law No. ZRU-1152 “On Forensic Expert Activity” of June 11, 2026 [9], which enters into force on December 13, 2026, creates a favourable legal opportunity to regulate this field anew.

This article aims to reveal the specific features of crypto-assets as an object of forensic examination, to determine the grounds for appointing an examination and the limits of expert competence, and, on the basis of an analysis of foreign experience, to develop proposals for introducing such examinations into the national forensic system. The study employs comparative-legal, systemic-structural and formal-logical methods, as well as the generalization of scientific sources.

Crypto-Assets as an Object of Forensic Examination: A crypto-asset has no physical form and exists solely as a record in a distributed ledger. The expert therefore examines not the crypto-asset itself but the traces reflecting its ownership, transfer and use. The statutory definition, which characterizes a crypto-asset simultaneously as “a set of digital records” and as “a property right”, points to its dual technical and economic nature [8]. This predetermines the need to combine computer-technical and economic expertise in its examination.

As N. Furneaux emphasizes, before transactions on a blockchain can be traced, investigators must locate evidence of cryptocurrency use and identify the addresses or private keys used by the suspect, and this task begins not in the laboratory but at the initial premises search [1, p. 120]. Law No. ZRU-1003 of November 21, 2024, introduced the concept of digital evidence and the procedure for handling it into the Criminal Procedure Code; under the new rules, electronic data collected during a search or seizure without the participation of a specialist is inadmissible as evidence [10]. Consequently, the detection and acquisition of crypto-asset traces require specialized knowledge from the very first stage of the investigation.

The objects of examination can be classified into the following groups according to their carrier.

The first group comprises traces on physical (paper) carriers: public addresses, private keys, mnemonic seed phrases (sequences of unrelated words), QR codes and “paper wallets”. In real cases such records have been found on whiteboards, printed e-mails, sticky notes attached to monitors and cards kept in a suspect’s wallet [1, p. 122]. They are easy to identify by their format: a Bitcoin address begins with “1” or “3” and consists of 34

Base58 characters, a SegWit (Bech32) address begins with “bc1” and consists of 42 characters, and an Ethereum address begins with “0x” and also consists of 42 characters, while a Bitcoin private key is most often stored in the Wallet Import Format (WIF) - 51 characters beginning with the digit “5” [1, p. 122-124]. Once a private key or seed phrase is found, control over the funds can be obtained; such objects are therefore significant not only as evidence but also as objects of confiscation.

The second group comprises traces in the non-volatile memory of computers and mobile devices. The principal object is the wallet file (for example, wallet.dat for Bitcoin Core), which contains private keys, addresses, the transaction history and other metadata [1, p. 131]. Even if the file has been renamed, moved or deleted, it can be located by means of a characteristic internal “magic value” [1, p. 133-134]. Browser artefacts, extended private keys, wallet user profiles and contact labels, client logs (debug.log, peers.dat) and operating system artefacts such as prefetch, iconcache and thumbcache are also important sources of evidence [4]. Such examinations are performed on a forensic image of the drive using tools such as EnCase, FTK, X-**Ways and Magnet AXIOM [1, p. 130-131].**

The third group comprises data in volatile memory (RAM). If the drive is fully encrypted or the wallet is stored in an encrypted container, a memory image may be the only source of evidence; a recovery seed that was never written to the disk may survive only in RAM [1, p. 136]. Experiments by W. Koerhuis and co-authors showed that, even for the privacy-oriented Monero and Verge wallets, mnemonic seed phrases and plaintext passwords remain in volatile memory, while network traffic retains indicators of cryptocurrency use [2].

The fourth group comprises data on a live (running) computer. If wallet software is running, it is possible to obtain the balance, the list of transactions, the IP addresses of connected peers and information on the use of the Tor network - data that are difficult to recover later from a disk image [1, p. 141-143]. However, it is mandatory in such cases to record both the system time and the actual time, to minimize and document any changes made, as otherwise the reliability of the evidence may be challenged in court [1, p. 138].

The fifth group comprises blockchain data (on-chain traces): sender and recipient addresses, amounts, timestamps, transaction frequency, relationships between addresses and interactions with smart contracts [4]. Since these data are stored in a public ledger, they can always be re-verified; by themselves, however, they reveal nothing about the identity of the person behind an address.

The sixth group comprises off-chain data held by third parties: KYC records of centralized exchanges, records of fiat payments (bank transfers, cards) and data held by wallet service providers [4], as well as addresses published on forums, social networks and websites [1, p. 125-127]. It is precisely these traces that make it possible to link a pseudonymous address to a real person.

Thus, the object of a crypto-asset forensic examination is the set of traces reflecting the ownership, movement and value of a crypto-asset that exist on physical, digital and distributed-ledger carriers. This multi-layered nature of the object directly affects both the appointment of the examination and the allocation of expert competence.

Grounds for Appointing a Forensic Examination

Under Article 172 of the Criminal Procedure Code of the Republic of Uzbekistan, an examination is appointed when information on circumstances relevant to the case can be obtained through a special study conducted by a person with knowledge in the field of science, technology, art or a profession, and the possession of such knowledge by the investigator, prosecutor, judge or specialists does not release them from the obligation to appoint an examination [11]. In crypto-asset cases, circumstances such as whether an address belongs to the suspect, the path of movement of funds, the amount of crypto-assets and their value in fiat currency can be established only on the basis of specialized knowledge. Such circumstances should therefore be confirmed by an expert conclusion rather than by data that the investigator has personally retrieved from a blockchain explorer or by a specialist’s reference note.

When choosing a procedural model for appointing an examination, the typology proposed by O. Regina and co-authors is of practical value [4]. They distinguish two types of cryptocurrency-related crime:

- Type A, in which the suspect is known and the investigation starts with seized devices and off-chain evidence before moving on to trace transactions on the blockchain (for example, the conversion of embezzled or corruptly obtained funds into crypto-assets);

- Type B, in which the offender is anonymous and the

investigation starts with blockchain traces and is aimed at identifying the real person through deanonymization techniques (ransomware, darknet markets, funds transferred as a result of fraud).

Adapting this typology to national criminal procedure, two models for appointing an examination can be distinguished. In the first model, a computer-technical examination of the seized devices is appointed first (to identify wallets, keys, seed phrases and addresses), followed by a blockchain-analytical and economic examination of the identified addresses. In the second model, a blockchain-analytical examination of addresses obtained from the victim or other sources is appointed first in order to identify the points at which funds exit to KYC-compliant exchanges; requests are then sent to the providers on the basis of the findings, and once the suspect has been identified, their devices are submitted for computer-technical examination.

On this basis, the following grounds for appointing an examination in crypto-asset cases can be identified:

- the need to establish whether seized devices and media contain crypto-wallets, keys and traces of their use;

- the need to establish links between addresses and the path of movement of funds;

- the need to determine the amount of crypto-assets and their value at the time of the offence, which is decisive for establishing aggravating circumstances under Article 2788 of the Criminal Code, such as commission “on an especially large scale”, and the amount of damage caused [7];

- the need to establish the link between crypto-asset and fiat flows in money laundering cases.

For the results of an examination to be admissible as evidence, objects must be identified, acquired and preserved in accordance with international standards. ISO/IEC 27037:2012 sets out guidelines for the identification, collection, acquisition and preservation of digital evidence, and ISO/IEC 27042:2015 provides guidelines for its analysis and interpretation [12], [13], while NIST SP 800-86 divides a digital forensic investigation into the phases of collection, examination, analysis and reporting [14]. Under these requirements, a cryptographic hash value (for example, SHA-256) of each acquired object and copy is calculated at the moment of acquisition and re-verified at every stage of the examination, and the case number, timestamp, time zone and place of acquisition are documented [4]. M. Fröwis and co-authors identify seven requirements for the forensic processing of cryptocurrencies: lawfulness, authenticity, reliability, qualification, verifiability, chain of evidence and the right to inspect the records [15]. These requirements should also be reflected in the order appointing the examination, in the description of the objects and in the procedure for sending them to the forensic institution.

Another specific feature of crypto-asset cases is urgency. Because a third party may also hold copies of the suspect’s private keys, there is a risk that the funds will be moved to another address before the investigators return to the laboratory [1, p. 137-138]. This calls for procedural regulation of the transfer of crypto-assets, with the participation of a specialist, to a state-controlled wallet at the time of the search.

Limits of Expert Competence: The allocation of expert competence is one of the most debated issues in the examination of crypto-assets. M.M. Vinogradova shows that cryptocurrency differs from traditional objects of forensic examination and distinguishes the questions relating to crypto-asset circulation that fall within the competence of a forensic economist from those that belong to computer-technical examination [16]. Drawing on the practice of the Russian Federal Center of Forensic Science under the Ministry of Justice of Russia, she emphasizes that cryptocurrency has only a market value and identifies the situations in which a comprehensive computer-technical and economic examination is required and those in which an economic examination alone is sufficient [17].

In our view, it is advisable to distinguish three domains in the expert examination of crypto-assets.

The computer-technical domain (off-chain examination) covers the detection, extraction and recovery of wallet files, private and public keys, seed phrases, log files, and browser and system artefacts from devices, storage media and volatile memory [1], [4].

The blockchain-analytical domain (on-chain examination) covers tracing transactions and the movement of funds, clustering addresses and identifying addresses controlled by a common owner. It relies on the multi-input heuristic, according to which all input addresses of a single transaction are controlled by the same entity [18], as well as on change address identification, graph analysis and the tracing of tainted

funds (taint analysis) [4].

The economic domain covers determining the amount of crypto-assets, their value in fiat currency on a given date, the amount of damage caused and income received, and the flows of crypto-assets and fiat funds on the basis of accounting and financial documents [16], [17].

It should be stressed that blockchain-analytical methods often yield probabilistic findings. Clustering heuristics and attribution tags assigned to addresses may be erroneous, and their evidential value in court has not yet been fully established [15]. Moreover, on-chain methods rarely lead to conclusive identification of a person without off-chain evidence [4]. The expert conclusion should therefore state openly the heuristics applied, the data sources used and their degree of reliability, and the conclusion should, where necessary, be formulated in probabilistic terms.

The external boundary of expert competence must also be clearly defined. The expert does not determine the legal owner of a crypto-asset, the lawfulness of a transaction, whether a licence was required or the guilt of a person: these are legal questions that fall within the competence of the investigator and the court. The expert establishes only technical and economic facts, such as the device on which a particular wallet was stored, the amount of crypto-assets transferred between particular addresses and their value.

Where the questions relate to more than one domain, a comprehensive examination is appointed. Sample questions that may be put to the expert are given below.

Computer-technical domain:

- Does the submitted device (medium) contain crypto-wallet software, wallet files, private keys or seed phrases? If so, to which cryptocurrencies do they relate?

- Which crypto-asset addresses are recorded on the device, and when were they used?

- Does the device contain data reflecting access to crypto-exchanges and wallet services?

Blockchain-analytical domain:

- Were transactions carried out between the specified addresses? If so, when and in what amounts?

- To which addresses and services (exchanges, mixers) were the funds transferred from the specified address?

- Are there indications that the specified addresses are controlled by a common owner?

Economic domain:

- What amount of crypto-assets was received at and transferred from the address (wallet) during the specified period?

- What was the value of the crypto-assets in national currency on the specified date?

- To which accounts were the fiat funds obtained from the sale of the crypto-assets transferred, and in what amounts?

Foreign Experience

In the Russian Federation, the examination of crypto-assets is developing mainly within the framework of forensic economic and computer-technical examinations. The economic examination department of the Russian Federal Center of Forensic Science has developed a practice of conducting examinations in criminal cases related to the circulation and theft of cryptocurrency [17]. In addition, the Ministry of Justice of Russia, together with the Central Bank, is developing a forensic examination of digital currency, which specialists regard not as yet another variety of computer-technical examination but as an independent field requiring specialized algorithms, software tools and unified, scientifically grounded methodologies [19].

The Republic of Kazakhstan has achieved notable practical results in this area. According to the Ministry of Justice of Kazakhstan, forensic examination of digital assets is already applied in practice, and a dedicated methodology has been used in criminal cases since October 2025 [20]. This is one of the first examples of the institutional introduction of crypto-asset examination in Central Asia.

In Indonesia, the forensic model developed by O. Regina and co-authors, which integrates on-chain and off-chain analysis into a single process, was validated by experts from the Indonesian Digital Forensics Association, the Cybercrime Directorate of the Indonesian National Police and the National Cyber and Crypto Agency. The model comprises the phases of identification, collection and acquisition, examination and analysis, and reporting, and is aligned with ISO/IEC 27037, ISO/IEC 27042 and NIST SP 800-86. The experts recommended improving the documentation standard for on-chain evidence and extending the model to privacy-oriented

cryptocurrencies [4].

In the European Union, Europol urges law enforcement agencies and private companies not to confine themselves to Bitcoin but to continue developing their knowledge and expertise on emerging cryptocurrencies [3]. Several models for the forensic examination of cryptocurrency wallets have been proposed in academic literature: A. Park and co-authors developed a three-phase model comprising forensic readiness, acquisition and investigation [21]; A. Holmes and W.J. Buchanan proposed a framework for the live triage of Bitcoin wallets on a running host [22]; and S. Taylor and co-authors developed a comprehensive methodology for the forensic preservation of crypto wallets [23]. M. Fröwis and co-authors translated the legal requirements for safeguarding the evidential value of cryptocurrency analysis into a technical data-sharing framework [15]. In Ukraine, too, research on blockchain technologies as an innovative component of forensic support has intensified [24].

At the international level, the main legal basis for collecting electronic evidence and ensuring its admissibility is the Council of Europe Convention on Cybercrime (Budapest, 2001) [25]. The FATF Recommendations establish the regulation of virtual assets and virtual asset service providers, including the requirement to transmit originator and beneficiary information for transfers (the “Travel Rule”) [26]. INTERPOL has developed practical guidelines for first responders on the search and seizure of digital evidence [27].

The analysis of foreign experience reveals three main trends. First, crypto-asset examination is emerging as an independent type of examination or expert specialty. Second, it is interdisciplinary, combining computer-technical, blockchain-analytical and economic knowledge. Third, the admissibility of its results depends on documentation in accordance with international standards. In Uzbekistan, however, a unified approach, an approved methodology and specialized expert personnel in this field have yet to be established.

2. Conclusion

The study leads to the following conclusions. First, since a crypto-asset has no physical form, the object of forensic examination is not the asset itself but the set of traces reflecting its ownership, movement and value. These traces are stored on physical carriers, in the non-volatile and volatile memory of devices, on live systems, in the blockchain ledger and in data held by third parties.

Second, in crypto-asset cases, establishing whether an address belongs to a person, the movement of funds and the value of crypto-assets requires specialized knowledge and therefore necessitates the appointment of an examination under Article 172 of the Criminal Procedure Code. The model for appointing an examination should be chosen according to the starting point of the investigation - seized devices (Type A) or blockchain traces (Type B).

Third, expert competence is distributed among the computer-technical, blockchain-analytical and economic domains, and a comprehensive examination is appointed where they intersect. Determining the value of a crypto-asset at the time of the offence, the amount of damage caused and the amount of criminal proceeds falls precisely within the competence of forensic economic examination.

Fourth, the experience of Russia and Kazakhstan demonstrates a trend toward institutionalizing crypto-asset examination as an independent field, while the experience of Indonesia and Europe demonstrates the need to integrate on-chain and off-chain analysis into a single process based on international standards.

Accordingly, it is proposed to introduce a new type of forensic economic examination - “Examination of Transactions Carried Out with Crypto-Assets” -at the Republican Center of Forensic Expertise named after Kh. Sulaymonova. The legal grounds for this proposal are as follows:

- Law No. ZRU-249 “On Forensic Examination” [28] and Law No. ZRU-1152 “On Forensic Expert Activity”, which replaces it from December 13, 2026 [9], establish the legal framework of forensic expert activity, including the requirement that a forensic expert be trained in a particular expert specialty and certified;

- Presidential Resolution No. PP-4125 of January 17, 2019, “On Measures to Further Improve Forensic Expert Activity” [29] and Presidential Decree No. PF-6256 “On Measures to Improve the Forensic Expert System of the Republic of Uzbekistan” [30] are aimed at improving the forensic system and introducing modern research methods;

- Articles 172-182 of the Criminal Procedure Code [11] and the provisions on digital evidence introduced by Law

No. ZRU-1003 of November 21, 2024 [10] form the procedural basis for appointing examinations and handling digital evidence;

- Article 2788 of the Criminal Code [7] and Resolution No. PP-3832 [6] establish liability for offences in the field of crypto-asset circulation and the framework for regulating this field.

To implement the proposal, the following measures are advisable:

1. Include the specialty "Examination of Transactions Carried Out with Crypto-Assets" within forensic economic examination in the list of types of forensic examination and expert specialties conducted by state forensic institutions, and reflect this in the subordinate regulations to be adopted in connection with the entry into force of Law No. ZRU-1152.

2. Establish a crypto-asset examination sector within the forensic economic examination unit of the Center and define the procedure for conducting comprehensive examinations jointly with the computer-technical examination unit.

3. Develop and approve a "Methodology for the Forensic Economic Examination of Transactions Carried Out with Crypto-Assets" based on the integration of on-chain and off-chain analysis and aligned with ISO/IEC 27037 and ISO/IEC 27042. The methodology should specifically regulate the criteria for selecting exchange-rate sources when determining the value of crypto-assets, the application of heuristics and the formulation of probabilistic conclusions.

4. Develop training, retraining and continuing professional development programmes for experts in this specialty, and establish the exchange of experience with forensic institutions of Russia and Kazakhstan.

5. Equip the Center with blockchain analytics software and tools for the forensic acquisition of wallet data.

6. Establish a mechanism with the National Agency of Perspective Projects and licensed crypto-asset service providers for the provision, in accordance with the established procedure, of data required for examinations.

7. Develop methodological recommendations for investigators on appointing examinations in crypto-asset cases, submitting objects and formulating questions for the expert.

The implementation of these proposals will enhance the scientific validity and evidential value of expert conclusions in the detection and investigation of crypto-asset-related crimes, and will contribute to the accurate calculation of damage and the correct determination of the amount of property subject to confiscation.

References

1. Furneaux N. Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence. - Indianapolis: Wiley, 2018.
2. Koerhuis W., Kechadi T., Le-Khac N.-A. Forensic analysis of privacy-oriented cryptocurrencies // Forensic Science International: Digital Investigation. - 2020. - Vol. 33. - Art. 200891. - DOI: 10.1016/j.fsidi.2019.200891.
3. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2017. - The Hague: Europol, 2017.
4. Regina O., Ramli K., Amarullah A.H. Illicit Cryptocurrency Investigation Digital Forensic Framework: Integrating Off-chain and On-chain Analysis for Two Types of Crime // International Journal of Electrical, Computer and Biomedical Engineering (IJECBE). - 2025. - Vol. 3, No. 2. - P. 411-432. - DOI: 10.62146/ijecbe.v3i2.135.
5. Chainalysis. The 2025 Crypto Crime Report. - New York: Chainalysis, 2025.
6. O‘zbekiston Respublikasi Prezidentining 2018-yil 3-iyuldagi PQ-3832-son "O‘zbekiston Respublikasida raqamli iqtisodiyotni va kripto-aktivlar aylanmasi sohasini rivojlantirish chora-tadbirlari to‘g‘risida"gi qarori // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/-3806053).
7. O‘zbekiston Respublikasining 2024-yil 19-yanvardagi O‘RQ-899-son "O‘zbekiston Respublikasining Jinoyat, Jinoyat-protsessual kodekslariga va Ma’muriy javobgarlik to‘g‘risidagi kodeksiga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida"gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/6763724).
8. O‘zbekiston Respublikasining Jinoyat kodeksi (1994-yil 22-sentabr) // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/111453).
9. O‘zbekiston Respublikasining 2026-yil 11-iyundagi O‘RQ-1152-son "Sud-ekspertlik faoliyati to‘g‘risida"gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/8265035).
10. O‘zbekiston Respublikasining 2024-yil 21-noyabrdagi O‘RQ-1003-son "O‘zbekiston

Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi, 21.11.2024-y., 03/24/1003/0943-son.

11. O‘zbekiston Respublikasining Jinoyat-protsessual kodeksi (1994-yil 22-sentabr) // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/111460).
12. ISO/IEC 27037:2012. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.
13. ISO/IEC 27042:2015. Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence.
14. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response: NIST Special Publication 800-86. - Gaithersburg: NIST, 2006.
15. Fröwis M., Gottschalk T., Haslhofer B., Rückert C., Pesch P. Safeguarding the evidential value of forensic cryptocurrency investigations // Forensic Science International: Digital Investigation. - 2020. - Vol. 33. - Art. 200902. - DOI: 10.1016/j.fsidi.2019.200902.
16. Виноградова М.М. Криптовалюта как новый объект судебной экономической экспертизы // Теория и практика судебной экспертизы. - 2024. - Т. 19, № 2.
17. Виноградова М.М. Возможности судебной экономической экспертизы при расследовании преступлений, связанных с оборотом криптовалюты // Российский следователь. - 2024. - № 8. - С. 2-5. - DOI: 10.18572/1812-3783-2024-8-2-5.
18. Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G.M., Savage S. A fistful of bitcoins: characterizing payments among men with no names // Proceedings of the 2013 ACM Internet Measurement Conference (IMC). - 2013. - P. 127-139. - DOI: 10.1145/2504730.2504747.
19. Судебная экспертиза цифровой валюты: новый этап развития экспертного обеспечения правосудия // Институт судебных экспертиз и криминалистики (sl.ceur.ru).
20. Виртуальное вскрытие и анализ дипфейков: как в Казахстане меняют судебную экспертизу // Bizmedia.kz. - 19.05.2026 (bizmedia.kz).
21. Park A. et al. Forensic investigation framework for cryptocurrency wallet in the end device // Computers & Security. - 2023. - Vol. 133. - Art. 103392. - DOI: 10.1016/j.cose.2023.103392.
22. Holmes A., Buchanan W.J. A framework for live host-based Bitcoin wallet forensics and triage // Forensic Science International: Digital Investigation. - 2023. - Vol. 44. - Art. 301486. - DOI: 10.1016/j.fsidi.2022.301486.
23. Taylor S. et al. A comprehensive forensic preservation methodology for crypto wallets // Forensic Science International: Digital Investigation. - 2022. - Vol. 42-43. - Art. 301477. - DOI: 10.1016/j.fsidi.2022.301477.
24. Шевчук В.М. Використання технологій блокчейн як інноваційна складова криміналістичного забезпечення правозастосовної діяльності в умовах війни // Науковий вісник Ужгородського національного університету. Серія: Право. - 2026. - Вип. 93. - DOI: 10.24144/2307-3322.2026.93.5.30.
25. Council of Europe. Convention on Cybercrime (ETS No. 185). - Budapest, 23.11.2001.
26. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations. - Paris: FATF, 2012 (as updated).
27. INTERPOL. Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence. - Lyon: INTERPOL, 2021.
28. O‘zbekiston Respublikasining 2010-yil 1-iyundagi O‘RQ-249-son “Sud ekspertizasi to‘g‘risida”gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/-1633102).
29. O‘zbekiston Respublikasi Prezidentining 2019-yil 17-yanvardagi PQ-4125-son “Sud-ekspertlik faoliyatini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/docs/-4172023).
30. O‘zbekiston Respublikasi Prezidentining PF-6256-son “O‘zbekiston Respublikasida sud-ekspertlik tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi Farmoni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz/acts/-5491507).