INTERNATIONAL JOURNAL OF TECHNOLOGY AND ACADEMIC RESEARCH

ISSN: 2224-6878 | Pakistan Volume 6, No. 10.

IF: 14.91 | 2026 http://waerasia.org/index.php/ijtar

Theoretical and practical issues of legal regulation of crypto-assets in criminal proceedings

Sardorbek Odilbekovich Urozbaev,
Head of the Research Institute of Digital Forensics,
Law Enforcement Academy, Candidate of Legal Sciences, Associate Professor
doi:https://doi.org/10.5281/zenodo.23360891

Abstract. The article provides a scientific analysis comprehensive legal and doctrinal analysisof the criminal-law and criminal-procedural nature of crypto-assets. It substantiates treating crypto-assets as procedural property based on their recognition as property rights in the Criminal Code of the Republic of Uzbekistan. It also examines practical challenges in investigating crypto-related crimes, collecting and evaluating digital evidence, and confiscating assets.

Keywords: crypto-asset, criminal law, criminal procedure, property right, procedural property, digital evidence, investigation, confiscation, blockchain, crypto-related crime

The rapid global development advancement of digital technologies is transforming almost every sphere of society. Crypto-assets, virtual assets, and new blockchain-based settlement instruments are increasingly used in integrated into financial and economic relations. They can improve efficiency, promote financial inclusion, and simplify cross-border operations, but their criminal use is also increasing. Europol reports that criminal use of cryptocurrencies now extends beyond cybercrime to many offenses requiring the transfer of funds.

FATF analyses record document the use of virtual assets for money laundering, trafficking in controlled substances, fraud, extortion, and terrorist financing. Traditional procedural mechanisms are therefore proving insufficient for detecting, investigating, and proving such offenses. The pseudonymous, decentralized, and cross-border nature of crypto-assets creates particular challenges for criminal proceedings.

Correct Accurate legal characterization of crypto-asset relations, recognition of relevant information as evidence, and proper procedural documentation are consequently important. Scientifically grounded approaches to collecting, preserving, examining, and evaluating digital evidence, especially blockchain data, are urgently required. increasingly necessary.

Legal and economic literature defines crypto-assets in different ways. In general, they are digitally represented objects of value created using cryptographic methods, existing in a digital environment, and transferred through blockchain or another distributed-ledger technology. They include cryptocurrencies, tokens, stablecoins, and other virtual assets.

Under the concept advanced by approach proposed by S. P. Kushnirenko and A. G. Kharatishvili, procedural measures applicable to property in criminal proceedings may also be applied to crypto-assets.

In Uzbekistan, the concept of a crypto-asset was first addressed in Presidential Resolution No. PP-3832 of 3 July 2018 “On Measures to Develop the Digital Economy and the Sphere of Crypto-Asset Turnover in the Republic of Uzbekistan.”

Under the Criminal Code of the Republic of Uzbekistan, a crypto-asset is a property right having value and an owner and represented by a set of digital records in a distributed data ledger. This definition establishes crypto-assets as independent objects of property in criminal-law relations.

ISSN: 2224-6878 | Pakistan Volume 6, No. 10.

IF: 14.91 | 2026 http://waerasia.org/index.php/ijtar

A similar definition appears in the Regulation on Licensing Service Providers in the Sphere of Crypto-Asset Turnover, approved by Order No. 32 of the Director of the National Agency for Perspective Projects dated 14 July 2022.

From a criminal-procedural perspective, a crypto-asset may simultaneously constitute an object of property rights, the subject matter of an offense, or property obtained through crime. It may also serve as an instrument of crime, as when proceeds of unlawful activity are laundered through cryptocurrency.

The Instruction approved by Joint Decision No. 3591 of the Prosecutor General's Office, the Ministry of Internal Affairs, and the National Agency for Perspective Projects of dated 25 December 2024 regulates seizure, attachment, storage, and transfer of crypto-assets discovered during pre-investigation checks and criminal investigations. Under article 329 of the Criminal Procedure Code, such assets may be seized during a personal search or inspection of the scene.

Determining whether a crypto-asset should be treated as physical or digital evidence is particularly important. Unlike traditional physical evidence, a crypto-asset has no material form, and control is exercised through cryptographic keys. Identification, seizure, and preservation therefore require specialized procedural approaches.

The immutability and transparency of blockchain data create opportunities for evidentiary use. Yet the absence of a clear regulatory basis for determining legal relevance, authenticating the data, and evaluating it in court generates practical problems. The criminal-procedural nature of crypto-assets and uniform rules for handling them must therefore be defined.

Academic literature contains competing views on cryptocurrency as the object of offenses against property. Some scholars contend that intangible digital assets do not fit the traditional concept of property because they lack a physical attribute. Classical ownership also assumes that an owner may dispose of property independently of the will of others.

In cryptocurrency relations, however, disposition is validated by network participants through a consensus mechanism. This does not restrict the owner's will; it ensures legal trust in a distributed digital environment. Modern scholarship therefore recognizes cryptocurrency, as a digital asset of economic value, as an object of property rights and, where appropriate, an object of criminal encroachment. Other researchers place cryptocurrency within "other property" and see no legal obstacle to protecting victims.

Data generated in user mode generated through user activity and stored on electronic media have special forensic value in investigations involving cryptocurrency and electronic money. They help establish the criminal mechanism, identify participants, and document their actions.

Particularly important are credentials used to access electronic-wallet and crypto-wallet accounts: usernames, passwords, private keys, two-factor authentication codes, recovery phrases, and other identifiers. These data can reveal digital traces, trace financial operations, and establish their source. Their identification, preservation, and procedural recording are therefore major investigative tasks.

Electronic documents containing registration data from payment systems, crypto-exchanges, and P2P platforms, as well as payment-card details, are also significant. Confirmation emails may contain personal data, registration date and time, the IP address used, temporary passwords, or verification codes. Such information may support an inference that particular persons registered and possibly used the relevant wallet or account help establish that particular individuals registered and potentially used the relevant wallet or account.

Crypto-asset offenses commonly span several jurisdictions: a transaction may begin in one state, pass through another, and end on an exchange or platform in a third. This complicates jurisdiction, mutual legal assistance, and evidence collection.

ISSN: 2224-6878 | Pakistan Volume 6, No. 10.

IF: 14.91 | 2026 http://waerasia.org/index.php/ijtar

Criminal-procedure legislation generally relies on territoriality. In crypto-asset cases, however, the "place of commission" may be difficult to determine because operations occur through platforms and exchanges located in different states. Timely international requests, acquisition of data, and recognition of that data as evidence are therefore problematic.

Secure digital platforms enabling rapid information exchange between law-enforcement bodies and foreign service providers can mitigate this problem. Kodex (kodexglobal.com), for example, enables official electronic requests to crypto-asset service providers, banks, and other organizations and the secure receipt of responsive data, thereby supporting evidence collection in technology-enabled cases.

Electronic information-exchange mechanisms with foreign providers should therefore be expanded. Relevant operational and investigative officers should be registered on the Kodex government-request portal and systematically trained in its procedures and capabilities.

Traditional measures such as search, seizure, attachment, and confiscation also present difficulties. Obtaining digital keys or passwords may be enough to control a crypto-asset sufficient to gain control over crypto-assets, but compelling or acquiring such information raises human-rights and procedural-guarantee issues.

For judicial evaluation of blockchain analysis, the transaction hash, block number, timestamp, wallet address, analytical software, acquisition method, and chain of custody should be mandatory particulars. FATF likewise emphasizes the need for specialized technology and qualified personnel to identify and trace virtual assets.

Preservation of seized crypto-assets and their value is a separate concern. Market volatility can sharply change their price, complicating realization of assets transferred to the state and enforcement of judicial decisions.

Collection of digital evidence in crypto-asset cases must therefore meet specialized technical and procedural requirements. Blockchain analysis, wallet tracing, and requests to exchanges must be based on appropriate procedural decisions.

Integrity and authenticity must be maintained throughout evidence collection. The chain-of-custody principle should be observed and every action documented procedurally; otherwise, the court may find the digital evidence inadmissible or unreliable.

Because crypto-asset crime is transnational, effective detection and investigation require international cooperation and uniform standards. International organizations and individual states are developing specialized legal and institutional mechanisms.

Foreign International practice, particularly in the United Kingdom, United States, and Germany, is relevant to Uzbekistan. It demonstrates mechanisms for identifying, temporarily controlling, freezing, and confiscating crypto-assets and collecting associated digital evidence.

In the United Kingdom, the Economic Crime and Corporate Transparency Act 2023 integrates crypto-assets into the asset-recovery system. Amendments permit law-enforcement agencies to restrain and control them in a manner comparable to tangible property the treatment of tangible assets, recover wallets where necessary, and transfer assets to a law-enforcement-controlled wallet. The legislation also provides pre-conviction mechanisms.

In the United States, blockchain analytics, transaction tracing between crypto-addresses, and civil forfeiture are widely used. In July 2026, federal authorities in the District of Columbia restrained more than USD 25 million in crypto-assets associated with international fraud schemes and sought their forfeiture.

Germany's system permits provisional freezing during investigation and final confiscation by court order, while protecting safeguarding victims' interests where necessary. Under statutory conditions it also permits confiscation of assets whose direct connection to a specific offense has

ISSN: 2224-6878 | Pakistan Volume 6, No. 10.

IF: 14.91 | 2026 http://waerasia.org/index.php/ijtar

not been fully established. The Crypto-Asset Tax Transparency Act adopted in 2025 strengthened identification and reporting mechanisms for crypto-asset service providers.

A common feature of these systems is an integrated chain: prompt identification, blockchain tracing, freezing or control where necessary, acquisition of provider data, and final confiscation. The response is not limited to confiscation after an offense.

FATF is the leading international standard-setting body in this area. Its recommendations require licensing of virtual-asset service providers, customer identification, and reporting of suspicious transactions.

The United Nations and UNODC treat criminal use of crypto-assets as a global threat and recommend adapting criminal-procedure law to digital evidence, equipping investigative enhancing the technical capacity of investigative bodies technically, and strengthening international information exchange. These measures improve transparency and timely access to relevant information and provide a basis for effective evidentiary use.

The following proposals follow from the analysis. First, a regulatory instrument should comprehensively govern the criminal use, identification, attachment, seizure, preservation, valuation, disposal, and procedural status of crypto-assets.

Second, electronic information exchange with foreign service providers and other relevant organizations should be expanded to detect and investigate transnational cybercrime promptly and to collect and preserve digital evidence without delay.

Third, crypto-asset investigations require specialized knowledge and technical capabilities distinct from traditional procedures. A unified investigative and forensic standard should be developed, and specialized investigative-forensic groups should be established within law-enforcement bodies.

Comprehensive implementation of these legal, organizational, and forensic measures would provide a modern system for combating crypto-asset-enabled crime, identifying and procedurally securing criminal proceeds, and improving the quality of transnational cybercrime investigations.

References

1. Europol. Cryptocurrencies: Tracing the Evolution of Criminal Finances. Luxembourg: Publications Office of the European Union, 2022, p. 3. Accessed 8 September 2026.
2. FATF. Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing. Paris: FATF/OECD, 2020, p. 5. Accessed 8 September 2026.
3. Kushnirenko, S. P., and A. G. Kharatishvili. “Cryptocurrency Turnover in the Mechanism of Committing Crimes.” Kriminalist, no. 3 (40), 2022, pp. 77–83.
4. Resolution of the President of the Republic of Uzbekistan No. PP-3832 of 3 July 2018 “On Measures to Develop the Digital Economy and the Sphere of Crypto-Asset Turnover in the Republic of Uzbekistan.”
5. Order No. 33 of the Director of the National Agency for Perspective Projects of 18 July 2022 “On Approval of the Rules for Trading Crypto-Assets on a Crypto-Exchange,” registered by the Ministry of Justice on 15 August 2022, No. 3379.
6. Orlova, A. S. “Cryptocurrency as the Object of Crimes Against Property: Recognize or Exclude?” Evolution of Russian Law: Proceedings of the XIX International Scientific Conference, Yekaterinburg, 2021, pp. 124–128.
7. Korennaya, A. A., and N. V. Tydykova. “Cryptocurrency as an Object and Means of Committing Crimes.” Accessed 11 February 2026.

ISSN: 2224-6878 | Pakistan Volume 6, No. 10.

IF: 14.91 | 2026 http://waerasia.org/index.php/ijtar

8. Melnik, L. L. “Methods of Investigating Crimes Committed Using Cryptocurrencies and Electronic Money: Genesis, Current State, and Development Prospects.” Justice of Belarus, no. 4 (229), 2021, pp. 43–47.
9. Casey, E. Digital Evidence and Computer Crime. 3rd ed. London and San Diego: Academic Press, 2011.
10. UK Home Office. Circular 004/2024: Economic Crime and Corporate Transparency Act—Cryptoasset Confiscation Order Provisions. 26 April 2024. Accessed 8 September 2026.
11. U.S. Department of Justice. “Investigations into Cryptocurrency Scams Result in Seizure of More Than $25 Million.” 21 July 2026. Accessed 8 September 2026.
12. Federal Ministry of Finance, Germany. Crypto-Asset Tax Transparency Act. 22 December 2025. Accessed 8 September 2026.
13. Meighan, S. J. The Regulation of Crypto-assets for Anti-Money Laundering. 2024. Accessed 11 February 2026.
14. Smith, D. Money Laundering, Terrorist Financing and Virtual Assets. Cham: Springer, 2024.