

Specific Features of Investigating the Crime of Digital Bribery

Rajabov Ulugbek Abdurakhmonovich

Independent Researcher at the Law Enforcement Academy of the Republic of Uzbekistan

Received: 26 August 2026; **Accepted:** 22 September 2026; **Published:** 13 October 2026

Abstract: The rapid development of digital technologies and the growing adoption of cryptocurrencies have created new methods of committing corruption-related offences, particularly bribery involving crypto-assets. This article examines the legal, procedural, and forensic challenges associated with proving the receipt of bribes in the form of cryptocurrencies, with particular emphasis on the identification, collection, preservation, examination, and evaluation of digital evidence. The study highlights the specific characteristics of crypto-assets, including decentralisation, pseudonymity, cross-border transferability, transaction irreversibility, and price volatility, which complicate the establishment of the actual ownership of crypto-wallets, the tracing of financial flows, and the determination of the value of a bribe at the time of the offence. Particular attention is paid to the legal regulation of crypto-assets in Uzbekistan and the need to improve investigative and judicial practices concerning bribery involving digital assets. The article also examines relevant foreign experience, including criminal investigations in which blockchain analysis and cryptocurrency exchange records have contributed to establishing the movement of crypto-assets and identifying individuals involved in alleged corruption schemes. The research identifies several key evidentiary challenges, including the use of cryptocurrency mixers and tumblers, the concealment of transaction origins, the encryption or deletion of electronic data, and the absence of unified approaches to documenting cryptocurrency transactions in procedural records. The article substantiates the importance of comprehensive computer-forensic and economic examinations to establish the fact of a cryptocurrency transfer and determine its monetary equivalent. It further analyses the practical value of blockchain analytics, obtaining customer identification and transaction records from cryptocurrency exchanges, forensic examination of computers, smartphones and hardware wallets, and the use of electronic communications and witness testimony in conjunction with blockchain evidence. The study emphasises the importance of conducting urgent investigative actions to preserve digital traces, documenting wallet addresses and complete transaction identifiers, recording transaction amounts and relevant exchange rates, and ensuring the integrity and authenticity of digital evidence. It concludes that improving the investigation of bribery involving crypto-assets requires specialised technical expertise, standardised procedures for documenting and valuing crypto-assets, stronger international cooperation, and the development of appropriate criminal procedure mechanisms. These measures can enhance the reliability of evidence, support the effective investigation of cryptocurrency-related bribery, and strengthen the legal framework for combating corruption in the digital economy.

Keywords: Corruption, bribery, crypto-assets, cryptocurrency, digital evidence, blockchain analysis, cryptocurrency transactions, criminal investigation, forensic examination, computer forensics, digital traces, cryptocurrency wallets, transaction identification, financial investigation, evidence preservation, criminal procedure, anti-corruption measures.

Introduction: In the context of the rapid development of digital technologies and the popularization of cryptocurrencies, new methods of committing corruption crimes are emerging. Receiving a bribe using

crypto-assets creates a particular difficulty for law enforcement agencies in proving the elements of a crime. The development of information technology and the formation of the digital economy are leading to a

shift in bribery methods. Instead of traditional cash or bank transfers, criminals are increasingly using crypto-assets. This creates new problems for law enforcement agencies, as the decentralization, false anonymity, and lack of borders characteristic of cryptocurrencies make them a convenient tool for receiving and giving bribes.

The phrase "use of cryptocurrency in criminal cases in Uzbekistan" should only be understood in the Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan dated July 3, 2020 No. 12 "On amendments and additions to certain resolutions of the Plenum of the Supreme Court of the Republic of Uzbekistan and the Plenum of the Higher Economic Court of the Republic of Uzbekistan" "According to the content of Article 243 of the Criminal Code, money laundering... should be understood. In such cases, any property provided for in Article 169 of the Civil Code of the Republic of Uzbekistan, including, etc., may serve as the object of ownership".

In recent years, there has been an increase in instances of bribery in the form of cryptocurrency, which poses new challenges to law enforcement agencies. Crypto-assets, characterized by anonymity and high returns, are becoming a convenient tool for corrupt activities. The urgency of finding a solution to the problem is explained by the lack of unified investigative and judicial practice in this category of cases, as well as the imperfection of legislative regulation of crypto-assets. In this regard, it is advisable to identify the specific features and problematic aspects of proving bribery using cryptocurrencies and other crypto-assets. This issue is relevant not only for Uzbekistan but also for global law, with Russia, the USA, and EU countries also facing this problem. Therefore, it is advisable to identify the specific features and problematic aspects of proving bribery using cryptocurrencies and other crypto-assets.

According to the results of the study, it was found that there are a number of problems in proving bribery with crypto-assets. In particular, the anonymity and falsity of transaction addresses. Although crypto-asset transactions are typically recorded in blockchain technology, it is difficult to identify their true owner. Cryptocurrency addresses (wallets) are not directly linked to real individuals.

In addition, there is the possibility of destroying digital traces. At the same time, conducting cryptocurrency transactions through mixers (cryptocurrency mixers) or tumblers (tumblers) allows for the concealment of the source of funds. Crypto-assets are cross-border in nature, and their legal regulation varies from country to country.

At the same time, the exchange rate of

cryptocurrencies is sharply volatile, and the question of which time value to take into account to determine the amount of the bribe is complex. This, in turn, requires specialized knowledge in the fields of blockchain technology, cryptography, and digital evidence analysis to investigate cryptocurrency-related crimes.

Our research has shown that there are a number of important features that require detailed consideration in the process of proving bribery with crypto-assets:

First feature - necessity of conducting a comprehensive computer-technical and economic expertise. This expertise must solve two interrelated tasks: establishing the fact of transferring crypto-assets and determining their value equivalent. At the same time, a number of problematic aspects arise. In particular, the high volatility of cryptocurrencies makes it difficult to determine its exact value at the time of receiving a bribe. Existing methods for assessing the value of crypto-assets have not been unified, which leads to different approaches to conducting expert examinations. The solution to this problem lies in developing a unified method for assessing the value of crypto-assets for the purposes of criminal proceedings, taking into account the weighted average exchange rate of the cryptocurrency on the main exchanges at a specific time. In the Russian Federation in 2024, a law enforcement officer was held criminally liable for accepting a bribe. For example, "Marat Tambiyev, the former head of the investigative department of the Investigative Committee for the Tver district of Moscow, was sentenced to 16 years in a maximum-security colony and fined 500 million rubles in a case involving bribery in 2,718 Bitcoin cryptocurrencies (7.3 billion rubles) and 1.5 million dollars". During the investigation, the evidence base was established by identifying the bribe-taker's cryptocurrency wallet, proving the fact of the transaction, and determining the value of the cryptocurrency at that time.

The second feature is the uniqueness of recording digital traces when investigating this category of crimes. Blockchain analysis allows for tracking the movement of crypto-assets between wallets, but it presents difficulties in identifying the owners of these wallets. Furthermore, the use of mixers and anonymous cryptocurrencies significantly complicates the tracking of transactions. "Data obtained from the suspects' electronic devices - computers, smartphones, hardware crypto-wallets - will be an important source of evidence". At the same time, there is a problem of rapid data loss resulting from data deletion by suspects or the use of encryption tools. To solve these problems, it is necessary to: develop technical tools for the forensic investigation of cryptocurrency transactions; implement special software for blockchain analysis;

and improve the tactics of urgent investigative actions aimed at preserving digital traces.

Third feature - documenting the subject of the bribe in the form of crypto-assets. Despite the fact that the status of other property of cryptocurrency is enshrined in legislation, there are difficulties in describing crypto-assets in procedural documents. There are no unified requirements for recording the identification features of cryptocurrency transactions, which creates a risk of invalidating evidence. In Uzbekistan, from April 19, 2024, the provision of crypto services without a license will entail criminal liability. Questions arise regarding the possibility of seizing crypto-assets and their subsequent confiscation. "In the US, in the 2020 'Silk Road' case, a federal agent was found to have received a bribe in Bitcoin cryptocurrency". Investigators identified traces of the crime based on blockchain analysis and data obtained from crypto exchanges. In this case, the immutability and transparency of cryptocurrency transactions served as an important argument.

Although judicial practice regarding bribery using crypto-assets has not yet been established in Uzbekistan, the aforementioned foreign experience can be utilized.

The results of our studies showed that the following methods are effective in proving bribery with crypto-assets:

1. Blockchain analysis. All transactions on the blockchain are kept in a public and immutable list. Companies such as Chainalysis, CipherTrace, and Elliptic provide blockchain data services to law enforcement agencies worldwide. Blockchain analytics data must be prepared in accordance with existing legal standards for documentation in court. Special software can be used to analyze transaction history and identify suspicious addresses and their interconnections.

2. Receiving information from crypto exchanges and cryptocurrency exchange services. Many crypto exchanges conduct customer identification (KYC - Know Your Customer) procedures, which allow for the identification of the real owners of cryptocurrency wallets. FATF Recommendation 15 requires mandatory KYC and transaction monitoring from VASPs. There are more than 512,000 digital asset owners in Uzbekistan, and domestic licensed providers are required to store their identity verification information.

3. Examination of electronic devices. By examining the computer, smartphone, and other devices of a suspect or suspect, one can find keys to cryptocurrency wallets, transaction history, and other important information. Cellebrite UFED is a mobile forensic tool used by law enforcement agencies in

more than 150 countries worldwide, allowing for the recovery of data from messengers, browser history, and cryptocurrency programs. Oxygen Forensic Detective specializes in recovering cryptocurrency wallets and passkeys.

4. Witness statements and information recorded by technical means. Information confirming the facts of receiving and giving bribes with crypto-assets can be obtained through telephone conversations, SMS messages, email correspondence, and messenger messages. The efficiency of the evidentiary base increases when digital evidence is considered in conjunction with traditional evidence (witness testimony, documents).

5. Operational-search activities. Facts of receiving bribes with crypto-assets can be documented through supervised bribery and rapid experimentation. In Russian practice, the tactic of supervised bribery has shown effective results in identifying bribery schemes through crypto-assets.

When investigating cases of this category, the investigator must take into account the fundamental characteristics of crypto-assets as the subject of the crime. The decentralization of cryptocurrency operations implies the absence of a unified management and control center, which significantly complicates the process of asset tracking. The pseudonyms of the operation participants are manifested in the fact that the identities of the crypto wallet owners are not directly disclosed, and their identification requires a complex of investigative actions and operational-search measures. The irreversibility of transactions excludes the possibility of their cancellation or modification once verified on the blockchain, which requires particular caution when documenting the fact of bribery. The high volatility of the value of crypto-assets creates difficulties in determining the amount of the bribe and requires recording the exchange rate at the time of the crime.

Special attention should be paid to the possibilities of using various methods to hide traces of crime, such as cryptocurrency mixers, atomic swaps, the use of anonymous cryptocurrencies, and numerous transfers between different blockchains. Knowledge of these technical aspects is essential for proper investigation planning and gathering an evidence base. The investigator must take into account the growing interconnectedness between digital financial crimes and cybersecurity.

When obtaining information about the fact of receiving a bribe with crypto-assets, it is important to immediately conduct a set of preliminary investigative actions aimed at recording and preserving digital traces

of the crime. Delay can lead to the irreversible loss of key evidence due to the specifics of the operation of cryptocurrency systems.

First of all, the investigator must organize the recording of information about the cryptocurrency wallets of the participants in the crime. This includes saving wallet addresses, transaction history, balances, and related transaction information.

The preservation of digital traces may be ensured by seizing electronic devices, copying data, blocking access to cryptocurrency wallets, and recording the status of cryptocurrency accounts. To do this, it is necessary to pay special attention to the information on the suspects' electronic devices - computers, smartphones, tablets and hardware crypto wallets. It is important to record all available correspondence in messengers and emails, where bribery agreements, terms of transfer, and technical details of crypto-assets are most likely discussed.

To inspect electronic devices, it is required to use specialized software for forensic research, involve a digital forensics specialist, document all actions in the protocol, specifying the software used, and create backup copies of the data. When inspecting electronic devices, specialized forensic research software such as Cellebrite UFED, Oxygen Forensic Detective, or Belkasoft should be used. It is mandatory to involve a specialist in digital forensics who ensures the proper acquisition and storage of digital evidence. All actions must be recorded in detail in the protocol, specifying the software used, its version, the research methods used, and the results obtained. Cellebrite UFED allows you to restore data from messengers (WhatsApp, Telegram, Signal), browser history, and cryptocurrency applications, including deleted data.

The process of documenting cryptocurrency transactions poses a particular challenge, requiring specialized knowledge and adherence to a specific methodology. When drafting the protocol of the investigative action, it is necessary to reflect all technical characteristics of the cryptocurrency transaction as fully and accurately as possible. The protocol must specify the type of crypto-asset (Bitcoin, Ethereum, Tether, etc.), as different cryptocurrencies have their own technical characteristics and require different approaches to analyzing transactions. The transaction identifier (hash) is a unique identifier of a transaction on the blockchain and must be recorded in its full form without abbreviations. The addresses of the sender and the recipient shall be indicated after verifying their accuracy by reconciliation. In addition to the transaction amount in a cryptocurrency unit, its equivalent in the national currency should be recorded

at the exchange rate at the time of the transaction, using data from major cryptocurrency exchanges.

Regarding the determination of the value equivalent of crypto-assets, the investigator must verify the validity of the choice of information sources regarding cryptocurrency exchange rates. The conclusion should contain data from several reputable cryptocurrency exchanges and price aggregators, as well as a methodology for calculating the weighted average exchange rate. It is important to ensure that the expert takes into account the volatility of cryptocurrencies and records the exact time of determining their value.

The uniqueness of crypto-assets as a subject of bribery requires a special approach to the collection, consolidation, and storage of evidence. Digital evidence is characterized by particular vulnerability and the possibility of irreversible loss, which necessitates the creation of backups and ensures their reliable storage. All digital evidence must be stored using methods that exclude the possibility of its alteration or replacement.

REFERENCES

1. Chainalysis. Crypto Crime Report 2024. — URL: <https://go.chainalysis.com/2024-crypto-crime-report.html> (access date: 15.03.2025). In 2023, the volume of illegal cryptocurrency transactions worldwide amounted to more than 24.2 billion US dollars.
2. Resolution of the Plenum of the Supreme Court of the Republic of Uzbekistan dated July 3, 2020, No. 12 "On introducing amendments and additions to certain resolutions of the Plenum of the Supreme Court of the Republic of Uzbekistan and the Plenum of the Higher Economic Court of the Republic of Uzbekistan" // <https://lex.uz/docs/4904177>.
3. Долгиева М.М. Теоретические основы уголовной политики в сфере оборота криптовалюты: диссертация доктора юридических наук. - Тошкент, 2021. - 474 p.
4. <https://www.rbc.ru/society/08/10/2024/6704f99b9a79475102e1f136>
5. Zuyev, S.V. IT investigator in the digital environment of criminal proceedings // Law and order: history, theory, practice. 2024. No 2 (41). PP. 48-54.
6. <https://www.lexology.com/library/detail.aspx?g=91e869a9-e800-455a-aa60-52d50e3d6c87> application date 01.07.2026
7. <https://www.rbc.ru/rbcfreenews/551985d29a794739f3c3e2d5> application date 01.07.2026
8. Tazhanov Kh. Crypto legislation in Uzbekistan:

overview // Law & Digital Economy. 2023. 2. No P. 15-28.

9. Cellebrite DI Ltd. — URL: <https://www.cellebrite.com> (official website). Cellebrite UFED is a professional forensic tool used for obtaining information from mobile devices and is used by law enforcement agencies in more than 150 countries worldwide. Cellebrite UFED Touch2 has been awarded the Forensic 4:cast Award every year since 2009.
10. Oxygen Forensics Inc. Oxygen Forensic Detective. URL: <https://www.oxygen-forensic.com>. Oxygen Forensic Detective is specialized software for researching mobile and computer devices, including cryptocurrency wallets.
11. Tisen O.N. The mechanism of committing crimes using cryptocurrencies: based on the results of the analysis of investigative and judicial practice // Russian Investigator. - 2024. — 5. No - P. 7-11.
12. Nikkel B. Fintech forensics: criminal investigation and digital evidence in financial technologies // Forensic Science International: Digital Investigation. - 2020. Vol. 33. - P. 200908 (Nikkel B. Fintech forensics: criminal investigation and digital evidence in financial technologies).
13. Cellebrite UFED | Access to mobile device data and its collection // <https://cellebrite.com/en/ufed/>
14. <https://www.oxygenforensics.com/en/>
15. Belkasoft: Intelligent Software for Digital Forensics and Cyber Incident Response // <https://belkasoft.com/>