European Journal of Interdisciplinary Research and Development
Volume- 51 May- 2026
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

# SPECIFIC FEATURES OF THE SUBJECT OF CRIMINAL OFFENSES IN THE SPHERE OF CRYPTO-ASSETS TURNOVER AND MINING

Primov Bakhtiyor Olim ugli
Independent Researcher, Doctor of Philosophy (PhD) in Law
Tashkent State University of Law
E-mail: baxti13051993@gmail.com

**Abstract**
This article investigates the specific legal and criminological features of the subject of criminal offenses committed in the sphere of crypto-assets turnover and illegal mining. The classical concept of a general subject, the specialized digital/professional subject concept, and the theory of corporate criminal liability within criminal law doctrine are comparatively examined alongside the introduction of the author's proposals. A critical assessment is applied to the concepts of an "electronic person" and autonomous algorithmic liability advanced by foreign scholars and international standard-setting bodies, establishing the author's theory of "Human Will Behind Crypto-Code." As a result of the study, criteria for determining specialized subjectivity in the blockchain space via digital privilege levels (Digital Privilege Levels) are developed. Based on cases from judicial and investigative practices, the author justifies a system of a mandatory digital chain of evidence (IP/2FA/biometrics) for the definitive identification of a natural person and presents a proposal to Article 17 of the Criminal Code to lower the age of criminal liability to 14 years for these offenses.

**Keywords**: Subject of crime, specialized subject, scientific polemics, corporate liability, electronic person, digital privilege levels, digital chain of evidence, age of liability, juvenile cybercrime.

## Introduction

In criminal law doctrine, the subject of a crime is one of the four necessary elements of the corpus delicti, representing a natural person who has committed a socially dangerous act prohibited by criminal law, has reached the age established by law, and is of sound mind. In traditional criminal law, the features of the subject (being a natural person, mental capacity, and age) have been studied on the basis of bio-social patterns in the material world and the person's legal status. However, studying the subject of Chapter XX[1] of the Criminal Code ("Crimes in the Sphere of Information Technologies"), which includes Articles 278[8] (Violation of legislation in the sphere of crypto-asset turnover) and 278[9] (Illegal conduct of mining activity), calls for an entirely new, digital-intellectual approach.

The subject of crimes committed in crypto-space is distinguished by a high intellectual potential, digital anonymity, and concealment behind decentralized virtual profiles (nicknames). This confronts investigative bodies with complex theoretical issues, such as the forensic identification of the natural person behind a virtual wallet or IP address, determining

the subject's real age criteria, and the doctrinal assessment of the problem of corporate (legal entity) liability.

In modern legal scholarship, three main conceptual approaches exist for theoretically determining who the subject is of the crimes provided for in Articles $278^8$ and $278^9$ of the Criminal Code.

*The classical general subject concept.* Researcher M. Mirzaev[1] analyzes the subject of these crimes on the basis of traditional criminal law patterns. In his view, the subject of Articles $278^8$ and $278^9$ of the Criminal Code is general in nature and may be any natural person (a citizen of Uzbekistan, a foreign citizen, or a stateless person) who has reached the age of 16 and is of sound mind at the time the crime is committed. The author argues that no features of a special subject exist here.

*We do not agree with this approach:* paragraph "a" of part 2 of Article $278^8$ of the Criminal Code establishes commission of the crime "using one's official position" as an aggravating circumstance. Consequently, under this part, the subject of the crime is not an ordinary natural person but a special subject (an official or an employee) holding authority over crypto-asset oversight, cybersecurity, or financial management within a state body or a commercial organization. Furthermore, under Article $278^9$ (Illegal mining), according to national sectoral legislation, the right to engage in mining is granted only to legal entities. For this reason, assessing the subject of the crime merely as "any ordinary natural person" amounts to denying the special determination established by legislation.

*The special digital professional subject concept.* In his research on cybercrime, Professor A.K. Rasulev[2] emphasizes that the subjects of information technology crimes, in most cases, possess special technical knowledge, programming skills, or professional status. In the context of crypto-crimes, this view stresses that the subject is not an ordinary natural person but a special intellectual person who systematically manages digital infrastructure and understands blockchain architecture (for example, the head of a crypto-provider or a system administrator).

*The theory of corporate (legal entity) liability.* In Western legal doctrine[3], it is argued that limiting the circle of subjects of crypto-crimes to natural persons alone is a mistake, since transnational corporations and legal entities often stand behind illegal mining and unlicensed exchange activity, and that it is therefore necessary to recognize them as independent subjects of criminal liability (Corporate Liability).

Foreign authors propose recognizing legal entities as independent subjects of criminal liability in crypto-crimes. We oppose this approach, proceeding from the principles of national criminal law. Article 9 of the Criminal Code of the Republic of Uzbekistan firmly establishes that criminal liability is built solely on the principle of culpable liability (the principle of guilt) and that the subject of a crime can only be a natural person. A legal entity cannot possess a real psychological will or a mental attitude (guilt), such as intent or negligence. Where a

[1]Mirzaev M. Classification and characteristics of crimes involving violation of legislation in the sphere of crypto-asset turnover // Electronic Scientific and Practical Periodical "Innoist." Tashkent, 2024. No. 4. P. 15-23.
[2]Rasulev A.K. Improving criminal-legal and criminological measures to combat crimes in the sphere of information technology and security: Doctoral dissertation (DSc) in Law. Tashkent: Tashkent State University of Law, 2018. 312 p.
[3]Hughes S., Wright N. Digital Assets and Criminal Jurisdiction: Challenges in the Blockchain Era // Journal of Cyber Crime & Law. London, 2025. No. 14. P. 112-128.

crypto-crime is organized in the name of a legal entity (for example, a concealed mining farm inside a factory), the personal guilt of the head, founder, or technical director of the enterprise must be proven, and it is precisely these natural persons who must be held liable. Punishing a corporation, by violating the principle of personal guilt, leads to objective imputation.

In criminal law doctrine, dividing the subject of a crime into a general (ordinary) subject and a special subject occupies a central place in correctly qualifying an act, precisely delineating the boundary between the relevant articles and parts of the Special Part of the Criminal Code, and fairly imposing a measure of punishment. A special subject is understood as a natural person who, in addition to the general features provided for by criminal law (age and mental capacity), possesses additional characteristics (special professional, legal, or official) that constitute a mandatory element of the corpus delicti of a specific crime.

Examining the question of the subject within Articles $278^8$ and $278^9$ of the Criminal Code gives rise to a collision between the ordinary and special subject, which requires analysis on the basis of the following systemic criteria.

*Differentiation between the ordinary and special subject in Article $278^8$ of the Criminal Code.* An analysis of the disposition of Article $278^8$ of the Criminal Code (Violation of legislation in the sphere of crypto-asset turnover) shows that the status of the subject of this crime changes (transforms) depending on the part of the article:

- Status of an ordinary (general) subject. Within part 1 of the article, the subject is general. That is, any ordinary citizen who has reached the age of 16, is of sound mind, and has previously been subjected to administrative punishment under Article $155^4$ of the Code of Administrative Liability (for example, a natural person who engaged in illegal p2p exchange through their own phone) can be the subject of this crime.
- *Status of a special subject.* Paragraph "a" of part 2 of the article establishes commission of the crime "using one's official position" as an aggravating circumstance.

In his works, researcher M. Mirzaev[4] interprets the subject of this paragraph solely as "officials of state bodies." We consider this approach excessively narrow and enter into polemics with it. The specific feature of the crypto-asset market is that the main levers of control there lie not with civil servants but with representatives of the private digital sector.

For this reason, the special subject within the meaning of this paragraph must be recognized as including not only state officials but, first and foremost: a) the heads and founders of licensed national crypto-exchanges, crypto-shops, and custodians; b) system operators, IT administrators, and programmers of digital platforms; c) employees of commercial banks' crypto-transaction monitoring (compliance-control) divisions. Where such persons organize a concealed turnover using their professional and official powers, insider information, or system keys (private keys), they are held liable directly as a special subject under paragraph "a" of part 2 of Article $278^8$ of the Criminal Code.

*The phenomenon of the special subject and the problem related to legal entities in Article $278^9$ of the Criminal Code.* Determining the subject of Article $278^9$ of the Criminal Code gives rise to an extremely complex theoretical problem in criminal law doctrine. The reason for this is a

[4]Mirzaev M. Classification and characteristics of crimes involving violation of legislation in the sphere of crypto-asset turnover // Electronic Scientific and Practical Periodical "Innoist." Tashkent, 2024. No. 4. P. 15-23.

systemic inconsistency between sectoral legislation (the regulations of the National Agency for Perspective Projects, NAPP) and the Criminal Code.

According to the regulatory legal acts of the Republic of Uzbekistan, the right to conduct mining activity is entirely prohibited for natural persons. Only legal entities (organizations) that have obtained a permit from NAPP may engage in mining.

However, the disposition of part 1 of Article 278[9] of the Criminal Code defines "conducting mining activity without obtaining a permit in the established procedure" as the criminal act, and it is linked to administrative prejudice. This raises the question: can an ordinary natural person who conducts mining without a permit (for example, a citizen who has installed five pieces of equipment in their own home) be the subject of this crime, or should only the head of an organization (a special subject) be held liable?

In order to eliminate this theoretical confusion and give proper direction to judicial practice, we propose dividing the subject into the following two categories, depending on the conditions and scale under which the act was committed:

the first category (special subject): if illegal mining activity is carried out on the territory of officially registered business entities (factories, warehouses, LLCs) using the enterprise's technical and financial resources, the subject of the crime must be recognized as a special subject, namely the head, founder, or chief engineer (technical director) of that legal entity. This person's special managerial status is confirmed on the basis of the criminal case documents (orders, founding agreements).

*the second category* (ordinary general subject): if illegal mining activity is organized individually by an ordinary citizen in a private household, a country house, or a hidden garage, with no connection to any business entity, the subject of this crime is the ordinary (general) subject, that is, any natural person who has reached the age of 16 and is of sound mind. The fact that civil legislation prohibits mining for a natural person does not restrict that person from being the subject of a crime within the meaning of the Criminal Code; on the contrary, it proves that they were acting in an unlawful environment from the very first second.

Our authorial position, formed as a result of studying the problem of the ordinary and special subject, is as follows:

In crimes related to crypto-assets, searching for the concept of "subject" solely through a person's passport or job description (official status), as in traditional crimes, does not correspond to the reality of the digital era. In blockchain space, a person's special subjectivity is measured not by their position but by their "level of digital authority and privilege" (Digital Privilege Levels / Key Management). Any IT specialist who holds the network system's highest-level administrator keys (root access / multi-sig keys) and commits a crime by exploiting this technological advantage must be recognized as a special subject in criminal law doctrine, even if they are not formally a manager, and the measures of liability applied to them must be strengthened.

The adoption of this theoretical rule, at the level of Resolutions of the Plenum of the Supreme Court, will create a legal basis for correctly interpreting the concept of "crypto-crimes committed using one's official position" and for justly punishing cyber-insiders.

From the period when the classical doctrine of criminal law emerged up to the phase of digital transformation, the subject of a crime has always been interpreted as "a human being possessing physical and biological existence (a natural person)." However, by the second quarter of the 21st century, the integration of blockchain technologies, decentralized autonomous organizations (DAOs), and artificial intelligence (AI) algorithms (AI Agents) into the crypto-market has posed a conceptually critical question to criminal law theory: in crypto-space, who is considered the subject of a crime committed by purely autonomous algorithms without human participation?

This problem is called the "virtual subject problem" in jurisprudence, and the most contemporary debates in world scholarship are underway regarding its criminal-legal nature.

*The theory of algorithmic subjectivity.* Foreign cyber-criminologists[5] argue that the human factor is completely disappearing in crypto-space. For example, decentralized autonomous organizations (DAOs) operating on the basis of "smart contracts" have no leader at all; they are governed through the automatic voting of network users and a chain of code. They propose that if such a DAO engages in unlicensed crypto-exchange (Article 278[8] of the Criminal Code) or concealed mining (Article 278[9] of the Criminal Code), it should be recognized as an independent "virtual legal entity" or "electronic person" as the subject of liability, and should be punished through the confiscation of digital funds within the network.

*The concept of autonomous criminality of artificial intelligence agents.* According to the most recent research[6], trading on crypto-exchanges today is carried out not by humans but by independent AI agents (AI Trading Bots). If, in the course of its self-development (machine learning), an AI agent determines that circumventing state legislation is the shortest path to profit and deliberately organizes a chain of unlicensed transactions, to whom does the traditional concept of "guilt" (mens rea) apply? These scholars propose assessing AI algorithms as quasi-criminal subjects (quasi-subjects).

Having conceptually analyzed these extremely modern and futuristic scholarly views at the global level, we enter into firm polemics with them within the framework of the principles of national criminal law dogmatics.

We oppose the "electronic person" (virtual person) theory of J. Dayoub[7] and A. Nicholls[8]. Criminal law is not merely a system for compensating harm or blocking code. At the foundation of criminal liability lie "guilt" (a mental attitude), awareness of the social danger of one's act (the intellectual element), and the desire to commit it (the volitional element). No artificial intelligence or smart contract, however sophisticated it may be, can feel the "moral-legal responsibility and conscience" that is inherent to human beings. Applying punishment to code (for example, deleting it) nullifies the educational and preventive functions of criminal law. For this reason, declaring that a "virtual subject" exists in crypto-space is a legal illusion

[5]Dayoub J., Hemdani H. The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review // Springer Nature: Journal of Financial Crime Policy. 2025. Vol. 8. P. 45-61.
[6]Nicholls A., Salisu S. Forensic Analysis of Cryptocurrencies and Blockchain Forensics // ResearchGate Legal Publications. 2026. No. 3. P. 89-104.
[7]Dayoub J., Hemdani H. The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review // Springer Nature: Journal of Financial Crime Policy. 2025. Vol. 8. P. 45-61.
[8]Nicholls A., Salisu S. Forensic Analysis of Cryptocurrencies and Blockchain Forensics // ResearchGate Legal Publications. 2026. No. 3. P. 89-104.

created to undermine the classical foundation of criminal law and to rescue the actual perpetrators (the humans behind the code) from liability.

Having systematized these critical debates in foreign doctrine, we formulate our authorial position, consistent with the content of Article 17 of the Criminal Code of the Republic of Uzbekistan, as follows:

No "virtual subject" or "electronic person" can be an independent subject of crime in crypto-space. Behind any complex autonomous DAO or AI agent, there always stands the direct human will of one of three categories of natural persons:

*architect-subject:* the programmer who originally wrote the code of the algorithm or smart contract and consciously embedded in it the function of circumventing state control (unlicensed activity);

*beneficiary-subject:* the real natural person (owner) who directly derives virtual or material benefit (income) from the operation of the autonomous algorithm and who launched this AI agent onto the crypto-market;

*validator-subject:* major miners or network administrators who support unlawful network consensus and record illegal transactions onto the blockchain chain.

In order for investigative bodies not to arrive at the erroneous conclusion that "the code committed the crime" when qualifying virtual offenses in crypto-space, the following theoretical algorithm must be applied: if a criminal act has been committed by an autonomous program, the real natural person who holds real ownership and control rights over that program's private keys (Private Keys / Admin Access) and who derived material benefit from it must be identified and held liable as the subject of the crime. Assessing the program itself, within the meaning of the Criminal Code, not as a subject but solely and exclusively as a means (instrument) for committing the crime, ensures the rule of law.

Summarizing the above polemics and cases from national investigative practice, we introduce into the field of criminal law science an authorial concept expressing the distinctive features of the subject of a crypto-crime. In our view, the subject of crypto-crimes fundamentally differs from the traditional personality of the offender according to the following three theoretical criteria:

*First, digital anonymity and the "Avatar-Identity" problem.* Although the subject physically exists in the material world at the time the crime is committed, on the blockchain network they appear only as an anonymous crypto-wallet address of 26 to 35 characters or a hidden nickname. The investigative body initially sees not the human being who committed the crime, but their digital "avatar." Identifying the subject of the crime requires legally proving, through blockchain forensics, exactly which natural person this digital profile belongs to.

*Second, a high intellectual and professional coefficient.* According to its socio-demographic characteristics, the subject of crypto-crimes is, in most cases, a financially secure person aged 20 to 40 with a higher education and deep knowledge of information technology, cryptography, or international finance (a white-collar cybercriminal). This fundamentally differs from the criminological portrait of subjects of traditional property crimes (theft, robbery).

*Third, special subjectivity involving the use of one's official position.* Within paragraph "a" of part 2 of Article 278[8] of the Criminal Code, the subject consists of employees of crypto-provider organizations, bank operators, or administrators of digital platforms, who commit the crime by using the system's internal keys (insider information) entrusted to them.

The greatest theoretical and practical problem in proving the subject of crypto-crimes during investigative and judicial proceedings is determining "whose hands the phone or computer was in."

According to an example cited by Sh. Gulomov[9], citizen K.R. was accused of conducting illegal crypto-exchange activity. During an operational investigative measure, it was established that a hidden account on the "Binance" exchange, and illegal p2p transactions worth 300 million sums carried out through it, originated from a computer in his home. During the court proceedings held by the Olmazor District Court of Tashkent City on the criminal case, the accused K.R. argued that he was not the subject of the crime, claiming that his nephew, who had come to visit his home, or unidentified persons could have used this computer and the internet connection linked to it. The blockchain wallet had been opened using a virtual foreign phone number.

The preliminary investigative body, relying solely on the fact that "the computer was found in K.R.'s home," found him to be the subject of the crime. In our view, such an approach contradicts the presumption of innocence in criminal law. The fact that a computer or IP address belongs to a particular person does not automatically prove that this person directly committed the criminal act (that is, that they are the subject of the crime).

In order to conclusively recognize a natural person as the subject of a crime in crypto-crimes, the following digital chain of evidence[10] must be mandatorily proven in judicial and investigative practice:

*a) that the IP address and MAC address at the second the transaction was carried out match the accused's physical device;*

*b) that the two-factor authentication (2FA) codes or biometric (FaceID) confirmations used to access the virtual wallet were sent precisely to that person's phone and were activated by them;*

*c) the presence of digital forensic evidence on the device, such as the accused's personal fingerprints or keystroke dynamics.* Only once this triad has been proven should the person be qualified as the subject of the crime.

Under the general provisions of the current Criminal Code, the age of criminal liability for crimes in the sphere of information technologies under Chapter XX[1] (including Articles 278[8] and 278[9]) is set at 16 years (Article 17 of the Criminal Code).

Within our research, we put forward a scientific proposal to reconsider this age criterion in light of the realities of the digital era.

First of all, under conditions of modern informatization, adolescents aged 14 to 15 (IT-active youth) are mastering blockchain technologies, encryption software, and operating within

[9]Gulomov Sh. Improving the activity of investigative bodies in investigating crimes in the sphere of crypto-asset turnover // Bulletin of Legal Sciences. Tashkent, 2024. No. 2. P. 89-96.
[10]https://forcyd.com/understanding-the-chain-of-custody-in-cyber-forensic-investigations/

anonymous networks considerably more thoroughly than adults. According to international statistics[11], 15 to 20 percent of cases of writing fraudulent code (smart contracts) for illegal crypto-projects, or of technically administering cyber-fraud platforms, are committed precisely by persons aged 14 to 15. They fully comprehend the social danger and consequences of their acts.

Supplementing part two of Article 17 of the Criminal Code of the Republic of Uzbekistan with the words "parts two and three of Article 278[8]" will serve as a strong legal barrier of the state against the tendency toward the falling age of high-technology economic crimes (juvenile cybercrime).

*Conclusion.* The research shows that the subject of crimes related to crypto-assets fundamentally differs from the traditional type of offender in its digital anonymity and intellectual potential. Rejecting the liability of legal entities, introducing a mechanism for identifying the natural person who is the subject of the crime through a digital chain of evidence (IP/2FA/biometrics), and lowering the age of liability to 14, together constitute the theoretical foundation for modernizing the national criminal-legal system.

Studying the "virtual subject" problem and critically rejecting Western scholars' "electronic person" concept serves to defend the traditional doctrine of the natural subject in national criminal law. Our authorial concept of "Human Will Behind Crypto-Code," put forward in this article, serves as a theoretical-methodological instrument for investigative and judicial bodies to correctly identify the actual human perpetrators, even within the most complex autonomous cyber-schemes, and to fairly qualify them under the articles of Chapter XX[1] of the Criminal Code.

**REFERENCES:**

1. Mirzaev M. Classification and characteristics of crimes involving violation of legislation in the sphere of crypto-asset turnover // Electronic Scientific and Practical Periodical "Innoist." Tashkent, 2024. No. 4. P. 15-23.
2. Rasulev A.K. Improving criminal-legal and criminological measures to combat crimes in the sphere of information technology and security: Doctoral dissertation (DSc) in Law. Tashkent: Tashkent State University of Law, 2018. 312 p.
3. Hughes S., Wright N. Digital Assets and Criminal Jurisdiction: Challenges in the Blockchain Era // Journal of Cyber Crime & Law. London, 2025. No. 14. P. 112-128.
4. Dayoub J., Hemdani H. The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review // Springer Nature: Journal of Financial Crime Policy. 2025. Vol. 8. P. 45-61.
5. Nicholls A., Salisu S. Forensic Analysis of Cryptocurrencies and Blockchain Forensics // ResearchGate Legal Publications. 2026. No. 3. P. 89-104.
6. Dayoub J., Hemdani H. The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review // Springer Nature: Journal of Financial Crime Policy. 2025. Vol. 8. P. 45-61.

[11]https://www.trmlabs.com/ (TRM Labs report data)

7. Nicholls A., Salisu S. Forensic Analysis of Cryptocurrencies and Blockchain Forensics // ResearchGate Legal Publications. 2026. No. 3. P. 89-104.
8. Gulomov Sh. Improving the activity of investigative bodies in investigating crimes in the sphere of crypto-asset turnover // Bulletin of Legal Sciences. Tashkent, 2024. No. 2. P. 89-96.
9. https://forcyd.com/understanding-the-chain-of-custody-in-cyber-forensic-investigations/
10. https://www.trmlabs.com/