IRSTI 10.77.51
UDC 343.721
JEL K14

https://doi.org/10.46914/2959-4197-2026-1-3-151-163

ZHUMAGULOVA Sh.R.,[1]
c.l.s., associate professor.
e-mail: jumagulova_sholpan@mail.ru
ORCID ID: 0000-0002-2033-6260
SARTAYEVA K.R.,[2]
c.l.s., professor.
e-mail: galiya_1305@list.ru
ORCID ID: 0000-0002-7177-1369
BERDIYAROVA Zh.S.,[3]
c.l.s., associate professor.
e-mail: berdiyarova_zhs@enu.kz
ORCID ID: 0000-0002-4949-9522
AUESHOVA B.T.,*[4]
c.l.s., associate professor.
*e-mail: bagdataueshova@gmail.com
ORCID ID: 0000-0003-1449-9941
[1]Korkyt Ata Kyzylorda University,
Kyzylorda, Kazakhstan
[2]Auezov University,
Shymkent, Kazakhstan
[3]Gumilev University,
Astana, Kazakhstan
[4]Yessenov University,
Aktau, Kazakhstan

DIGITAL ASSETS AS THE SUBJECT OF CRIME: PROBLEMS OF QUALIFICATION OF THEFT AND FRAUD

Abstract

The article examines problems of criminal-law qualification of acts in which digital assets appear as the subject of crime or are used to conceal the criminal origin of property in the Republic of Kazakhstan. It is substantiated that, for criminal law, a digital asset should be regarded first and foremost as a proprietary value rather than pure information. In theft, decisive significance attaches to the victim's loss of control over the asset; in fraud, to a defect of will be caused by deception or abuse of trust; and in laundering, to financial operations aimed at giving a lawful appearance to the origin and movement of the asset. The current criminal legislation of Kazakhstan already contains norms capable of covering principal forms of encroachment upon digital assets; however, law enforcement requires clearer qualification criteria, a uniform approach to digital traces, and a special methodology of proof. The greatest difficulties in practice are connected with determining the subject of crime, distinguishing secret taking from taking by deceit, establishing the moment of completion of theft, and proving the value, control, and origin of the digital asset. A practice-oriented model for qualification of crimes related to digital assets is proposed.

Keywords: digital asset, crypto-asset, cryptocurrency, subject of crime, theft, fraud, laundering of criminal proceeds.

Introduction

For Kazakhstani law, the digital asset has already ceased to be exclusively a technological term or a particular plot of financial regulation. After the adoption of the Law of the Republic of Kazakhstan "On Digital Assets in the Republic of Kazakhstan," the legislator established an independent legal regime for secured and unsecured digital assets, the licensing of certain kinds of activity in this sphere,

as well as a special infrastructure of circulation, above all in the part concerning unsecured digital assets. By this, a step was taken which has principled significance for criminal law: an object that until recently was perceived as something lying "outside the law" entered the sphere of normatively recognized proprietary relations [1].

However, criminal legislation was not rewritten anew for the digital environment. The Criminal Code of the Republic of Kazakhstan still relies on the classical categories of "property," "right to property," "proceeds obtained by criminal means," "deception," "abuse of trust," "financial transactions," and "other property." This creates methodological tension. On the one hand, criminal law does not know a special general corpus delicti concerning the theft of digital assets. On the other hand, the absence of such a corpus delicti does not in itself yet mean that digital assets fall outside criminal-law protection. On the contrary, the question shifts to another plane: to what extent the traditional norms of Articles 188, 189, 190, and 218 of the Criminal Code of the Republic of Kazakhstan are capable of covering encroachments upon digital assets without the artificial construction of "exotic" characterizations [2].

Kazakhstani civil-law doctrine has already approached the point that is key for criminal law: digital assets are reducible neither to a thing in the physical sense nor to a pure informational message. In the literature, it is rightly emphasized that the legislation of the Republic of Kazakhstan classifies digital assets as property; yet at the same time the very construction of the secured and unsecured digital asset shows that law is confronted not with a familiar object, but with a special digital form of proprietary value. For criminal-law analysis this is important because the subject of crime here must be determined not through the material carrier, but through the legally significant loss of control over a proprietary good [3].

Additional confirmation of the proprietary nature of digital assets is also given by the official tax position of the state. The State Revenue Committee directly indicates that the income of individuals from the sale of digital assets is classified as proprietary income, and that the positive difference between the sale value and the acquisition value is subject to taxation. For criminal law, this thesis has independent significance: if the state recognizes the digital asset as an object of valuation, circulation, and proprietary income, it is already impossible consistently to deny its suitability to be the subject of crime [4].

At the same time, it is precisely here that not simplification begins, but complication of characterization. Kazakhstani studies devoted to the legal regulation of the production and circulation of digital assets and to counteracting commercial fraud show that a digital asset easily becomes an element of schemes in which an investment legend, tokenization, a pseudo-exchange environment, and a digital interface are used not for lawful circulation, but for the deceitful taking of proprietary value. Therefore, for criminal law the problem lies not only in recognizing the digital asset as property, but also in properly distinguishing where there is secret taking, where there is voluntary transfer under the influence of deceit, and where there is the subsequent concealment of the criminal origin of the asset through a chain of transfers, exchanges, and transit wallets [5].

Materials and methods

The methodological basis of the article consists of formal-legal, systemic, comparative-legal, and doctrinal methods. The formal-legal method was used to analyze the current norms of criminal and special digital legislation; the systemic method was used to identify the connection between the private-law status of the digital asset, its financial-law regime, and criminal-law protection; the comparative-legal method was used to compare the Kazakhstani approach with international standards of counteracting abuses in the sphere of virtual assets; the doctrinal method was used to evaluate the proposals of Kazakhstani researchers concerning the legal nature of digital assets, cryptocurrency schemes, and new forms of criminal conduct. In the part concerning the characterization of fraud, the study also relies on the current normative resolution of the Supreme Court of the Republic of Kazakhstan, since it is precisely this that sets the guidelines binding for law enforcement in matters of deception, abuse of trust, and the distinction between criminally punishable fraud and other forms of proprietary conflicts [6].

For the analysis of the block connected with the laundering of criminal proceeds, the study uses the provisions of the Law of the Republic of Kazakhstan "On Counteracting the Legalization (Laundering)

of Proceeds Obtained by Criminal Means, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction," as well as FATF international standards and practice-oriented OSCE materials. This choice is not accidental. It is precisely in the sphere of laundering criminal proceeds that the digital asset most vividly reveals the intersectoral nature of the problem: without taking into account the rules of financial monitoring, identification standards, the control mechanisms of VASP providers, and the specifics of digital transfers, criminal-law characterization risks remaining formal and evidentially vulnerable [7].

Results and discussion

Digital Asset as the Subject of Crime: The Initial Problem of Legal Characterization. The first and probably most fundamental problem consists in the fact that, in cases involving digital assets, the law enforcer often attempts to substitute technical vocabulary for legal analysis. Meanwhile, for criminal law it is of primary importance not what variety of blockchain, token, or protocol is at issue, but whether the corresponding object possesses the attributes of proprietary value, whether it can be within the sphere of control of a specific person, and whether its unlawful taking entails proprietary damage. The Law on Digital Assets already provides the necessary starting point: it distinguishes between secured and unsecured digital assets, introduces the regime of their issuance and circulation, and, with respect to unsecured assets, allows lawful circulation within a special infrastructure. For criminal law, this is sufficient to proceed from the presumption that a digital asset is not "empty code," but an economically significant good capable of being the object of criminal encroachment [1].

But recognizing the digital asset as the subject of crime does not mean that in all cases it should be mechanically assimilated to a thing. Kazakhstani literature quite rightly notes that a secured digital asset certifies a right to material, intellectual services and assets, whereas an unsecured digital asset is not connected with independent material backing in the habitual sense. From this follows a methodological conclusion which criminal law cannot ignore: in some cases, the encroachment is directed against the digital asset itself as an independent digital value; in others, through the digital asset a broader proprietary interest is in fact affected, confirmed by it or mediated by it. Consequently, in characterization it is necessary to establish not only the fact of the asset's departure, but also what specific proprietary good was withdrawn from the victim's sphere of control [3].

Kazakhstani research on the problems of regulating blockchain and cryptocurrencies also leads to an important conclusion: the legal regime of tokens, cryptocurrencies, and other digital forms of value cannot be described by one universal formula. Different types of digital assets are included in circulation in different ways and are differently connected with the issuer, the platform, the backing, and user access. From this there follows a criminal-law consequence as well: the characterization of an act should not be built merely on the colloquial word "crypto." For the court and the investigation, it is important to establish what exactly turned out to be the object of criminal impact: an asset on an exchange account, a token in a wallet, access to a custodial service, a right to dispose of an account, or proprietary value already withdrawn from circulation [8].

Theft of Digital Assets: The Moment of Completion and the Limits of Proprietary Taking**.** When the matter concerns the theft of digital assets, the first temptation of the law enforcer consists in treating as a completed crime already the mere fact of obtaining access to a wallet, an exchange account, a seed phrase, or a private key. Such an approach appears convenient, but juridically it is excessively coarse. For crimes against property, decisive significance still attaches not to the offender's abstract acquaintance with access credentials, but to the victim's actual loss of control over the proprietary value and the transfer of this possibility to the offender. In other words, the copying of a key and the unlawful taking of a sheet containing a seed phrase are not yet always identical to the completed theft of the digital asset itself. Until the transfer of control over the asset or its actual removal from the victim's dominion is established, the question of the moment of completion of the corpus delicti must be decided cautiously [2].

The high-technology environment, of course, changes the mode of taking. Theft of a digital asset may be committed through hacking into an exchange account, phishing interception of credentials, remote access to a device, substitution of a wallet address at the moment of transaction, the use of malicious software, manipulation of browser extensions, or exploitation of vulnerabilities of a wallet

service. However, the digital technique of the encroachment does not remove the proprietary content of the act. If the result was the gratuitous and unlawful withdrawal of the digital asset from the sphere of control of the owner, what remains before criminal law is precisely a crime against property, and not a "pure" computer violation. The error here is typical: the technical method begins to be taken as an independent object of characterization and thereby blurs the core of the proprietary harm [9].

A special place is occupied by the situation in which the offender does not withdraw an already existing digital asset belonging to the victim, but uses another's computing resources, software infrastructure, or devices for the unlawful mining of digital assets. Kazakhstani authors who analyzed the unlawful extraction of digital assets have convincingly shown that such acts should not be confused with the classical theft of another's digital asset. Here the harm may be connected with the unlawful use of computing power, disruption of the operation of equipment, expenditures on electricity, wear and tear of hardware, interference with information infrastructure, but not necessarily with the taking of an asset already belonging to the victim. For characterization, this distinction is fundamental: cryptojacking, unlawful mining, and secret withdrawal of an existing asset are not identical constructions, and their conflation only weakens the precision of the accusation [10].

From a practical standpoint, particular difficulty is created by the value of the stolen asset. With material objects, value is usually fixed comparatively more easily; a digital asset is volatile, traded around the clock, and may have different prices on different platforms. t is precisely for this reason that significance attaches to the official mechanism for determining and publishing the value of digital assets, established by the Order of the Minister of Finance of the Republic of Kazakhstan of 25 September 2025 No. 531. For a criminal case, such a procedure does not replace expert examination, but provides a legal reference point enabling the amount of damage to be tied to a specific date and a specific type of digital asset. Without this, qualifying features depending on the amount of damage risk turning into a dispute over an arbitrary quotation [11].

Finally, in cases of theft of digital assets, one must not lose sight of the situation of entrusted possession. If access to the digital asset was entrusted to an employee, the administrator of a corporate wallet, the operator of a platform, or another person by virtue of official, contractual, or factual position, the subsequent taking of the asset should not automatically be described only as theft. Depending on the structure of access, the scope of entrusted powers, and the nature of disposal of the asset, another solution is possible here – up to characterization as misappropriation or embezzlement. Consequently, for crimes involving digital assets, a technical description of access does not yet answer the characterization question; it is first necessary to establish the legal nature of the access itself – whether it was external, secretly overcome, or initially entrusted [2].

Fraud Involving Digital Assets: When the Digital Interface Masks a Defect of the Victim's Will. Fraud in the digital environment often appears outwardly as a voluntary action of the victim himself or herself: the victim transfers the asset to a specified address, communicates recovery credentials, confirms "verification," signs a transaction through a mobile application, connects a wallet to a site perceived as a lawful platform. It is precisely for this reason that the normative resolution of the Supreme Court in fraud cases acquires special significance here. The judicial approach proceeds from the premise that what is determinative is not the external form of the transfer of property, but the existence of deception or abuse of trust which conditioned a defect in the victim's will and led to the proprietary departure. For digital assets this thesis is especially important: the formal "activity" of the victim does not yet exclude fraud if his or her decision was provoked by a false digital shell, a fictitious service, or a knowingly false representation regarding the purpose of the transaction [6].

Kazakhstani literature has already drawn attention to the fact that the digital asset market is weakly protected from dishonest investment schemes, pseudo-tokenization, and commercial fraud. In such models, the digital asset is used not simply as an object of trade, but as an instrument for instilling trust: the potential victim is shown a "modern" platform, promised access to a closed market, presented with algorithmic profitability, and references are made to technological novelty and to the fact that the state allegedly has not yet managed fully to "adjust" the rules. As a result, the digital shell substitutes for verification of the real proprietary content of the transaction. For criminal law this means one thing: the technological complexity of the project cannot be regarded as an argument in favor of its civil-law neutrality; on the contrary, it often becomes a means of strengthening the deceptive impact [5].

Official information from the Financial Monitoring Agency shows that for Kazakhstan this problem has long since ceased to be hypothetical. According to the data of the AFM, in 2024 thirty-six illegal crypto-exchangers with a total turnover of 60 billion tenge were liquidated; assets in the amount of 4.8 million USDT were frozen and confiscated; in addition, schemes using cryptocurrency for the attraction of investments were uncovered. For the characterization of fraud, these data are significant not in a statistical, but in a typological sense: digital assets become part of deceptive constructions in which the victim either immediately transfers the asset to the fraudster, or is misled as to the legality of the platform, the status of the exchanger, the source of profitability, and the real guarantees for the return of funds [12].

A characteristic example is also the case in which the AFM reported the return from abroad of crypto-assets of a financial pyramid scheme in the amount of 250 million tenge stolen from citizens of Kazakhstan. This report is important because it graphically demonstrates the staged structure of digital fraud. First, the victim is persuaded voluntarily to invest value into a pseudo-lawful project; then the asset is fragmented, dispersed through transit wallets, and withdrawn into another digital environment; further, there begins no longer merely the retention of what was obtained, but the concealment of its origin. In other words, in a real case the digital asset appears at once in several roles: as the subject of the initial deceitful taking and as a means of the subsequent breaking of the trace of the property's origin [13].

At the same time, for precise characterization it is important not to fall into the opposite extreme. Not every dispute concerning a digital asset constitutes fraud. Volatility of the rate, an unsuccessful investment, a technical error in a protocol, a dispute over the content of a token, failure to perform promised profitability in the absence of proven initial deception – all this does not in itself transform private-law or market risk into a criminally punishable act. Therefore, in cases concerning digital assets, the investigation must prove not merely the victim's financial failure, but the initial deceptive scenario: the falsity of information, the conscious creation of a fictitious digital infrastructure, the concealment of substantial circumstances, or the intention, absent from the outset, to perform what was promised [6].

A separate problem remains the distinction between fraud and theft in cases where deception is used only to obtain access, while the taking of the asset itself is later committed secretly. If the victim is convinced of the necessity of an "official verification," communicates a one-time code, after which the offender independently initiates a transaction and withdraws the digital asset, the criminal-law picture becomes more complex. Here deception does not fully coincide with the act of disposing of the property; it merely prepares the subsequent secret taking. Consequently, the mechanical rule "if the victim handed over something himself or herself, then it is always fraud" turns out to be too primitive in the digital environment. For correct characterization, it is necessary to analyze at exactly what stage the proprietary departure occurred and what the immediate mechanism of causing it consisted in [2].

Laundering of Criminal Proceeds in the Digital Environment: Where Retention of the Stolen Ends and "Laundering" Begins**.** For Article 218 of the Criminal Code of the Republic of Kazakhstan, what is central is not simply the fact that a person possesses property of criminal origin, but the commission of financial operations and other transactions aimed at giving a lawful appearance to the possession, use, and disposal of such property. In the digital environment, this boundary becomes especially fine. One and the same wallet, one and the same exchange, and even one and the same series of transactions may in one case signify the simple retention of the criminal result, and in another already an independent stage of concealing the origin of the property. Therefore, with digital assets, laundering cannot be inferred automatically from any subsequent transaction with the stolen asset; it is necessary to establish the special function of the relevant operations – the concealment of the source, beneficiary, route of movement, or economic trace of the property [7].

FATF international standards have long proceeded from the premise that virtual assets and service providers dealing with them should fall within a full AML/CFT contour. In the updated 2021 guidance, FATF emphasized the necessity of licensing or registration of VASPs, the application of customer due diligence measures, compliance with the Travel Rule, and the removal of regulatory "loopholes" allowing virtual assets to be used for laundering criminal proceeds. For the criminal law of Kazakhstan, this is important not as an external recommendation, but as a guideline for the logic of characterization: if a criminal asset is moved through such services, the evaluation of the act

cannot be confined only to the predicate offense; what is required is an analysis of whether the digital infrastructure was used precisely to break the link between the property and its criminal source [14].

The sixth targeted FATF review, published in 2025, shows that the problem is not weakening, but becoming more complex. FATF notes the further growth of risks associated with stablecoins, offshore VASPs, difficulties of identifying the real operators of such services, and the uneven implementation of the Travel Rule; it is separately emphasized that a significant part of on-chain illicit activity today is connected precisely with stablecoins. For Kazakhstani criminal law, this means that laundering in the digital environment will increasingly take the form not of a single exchange of "crypto into fiat," but of a complex chain of transfers, changes of tokens, transit through different jurisdictions, and the use of weakly controlled platforms. Consequently, Article 218 requires not formal, but technologically sensitive application [15].

The practical OSCE guide for law enforcement agencies, published in 2025, confirms the same conclusion, but on an applied plane. The guide separately identifies typical crypto-crimes, methods of investigation using blockchain analytics, the significance of international cooperation, work with victims, and means of increasing the effectiveness of tracing digital routes of the asset. For the characterization of laundering, this material is especially valuable: it shows that proving "laundering" in cases involving digital assets is impossible without understanding the mechanics of multistage transfers, custodial and non-custodial wallets, exchange services, and the role of analytical tools. Otherwise, Article 218 will remain a fine formula without sufficient procedural support [16].

From this there follows an important distinction. If the offender stole a digital asset and simply retains it at his or her own address or transfers it to the nearest wallet controlled by him or her without an obvious purpose of masking its origin, the criminal-law core of the act still lies in the sphere of the predicate offense. But if there is then constructed a sequence of fragmenting sums, using several transit addresses, converting into other tokens, entering illegal exchangers, subsequently withdrawing into fiat, or investing into other assets for the purpose of making it difficult to identify the origin of the property, then an autonomous criminal function already manifests itself – giving the criminal asset an outwardly lawful appearance. It is precisely this that should become the criterion for imputing laundering [7].

Problems of Proof: Control, Value, Origin, Digital Trace. In practice, the greatest difficulties arise not at the level of verbal characterization, but at the level of proof. In cases involving digital assets, the investigation and the court must establish who controlled the wallet address, who initiated the transaction, from what device and through what service it was done, to whom the recovery credentials belonged, at what stage the victim lost the ability to dispose of the asset, and when exactly the damage arose. The OSCE guide rightly proceeds from the premise that the investigation of crypto-crimes requires the early collection of digital traces, correct fixation of addresses, requests to providers, the use of blockchain analytics, and careful work with metadata. For Kazakhstani practice, this means one simple thing: in a digital case, the traditional set of evidence is no longer sufficient [16].

No less difficult is the question of value. The official rules for determining and publishing the value of digital assets, approved by Order of the Minister of Finance No. 531, create an important support for tying value to a concrete calendar date and a concrete type of asset. But even this mechanism does not remove all questions. The investigation must take into account on what exact date the damage is fixed: at the moment of the unlawful debiting of the asset, at the moment of its withdrawal from the exchange, at the moment the victim lost access, or at the moment the crime was discovered. In addition, the platform on which the asset circulated is also significant, since the real liquidity and execution price may differ from the average market benchmark. Therefore, the official procedure should be regarded as a basis rather than as an automatic substitute for expert evaluation [11].

Official AFM materials on the liquidation of illegal crypto-exchangers also show that, in such cases, the digital trace is not confined to a single transaction. The blocking of more than 3.5 thousand illegal online crypto-exchangers, the freezing and confiscation of assets in USDT, and the detection of cryptocurrency components of financial pyramid schemes demonstrate that criminal schemes are built on the use of a network of intermediaries, addresses, and services, rather than on one "direct" transfer. From this there also follows an evidentiary consequence: without fixation of the entire chain of movement of the digital asset, there is a great danger either of failing to prove laundering, or, conversely, of substituting a full establishment of the route with general assumptions about "suspicious blockchain movement" [12].

The AFM's report on the return of stolen crypto-assets in the case of a financial pyramid scheme shows even more vividly the significance of tracing. Here the law-enforcement result was achieved not because the digital asset is "transparent in itself," but because the chain of transit wallets was reconstructed and the connection between the initial taking and the subsequent distribution of the asset was established. For criminal-law characterization, this has dual significance. First, the very fact of the asset's departure from the victim's control becomes provable. Second, a real basis appears for distinguishing the main offense and the subsequent operations aimed at concealing the origin of the property. Without such reconstruction, the case risks remaining either at the level of a hypothesis or at the level of excessively general characterization [13].

An additional and often underestimated element of proof is connected with the tax and financial trace of the digital asset. Since the state already regards income from the sale of digital assets as proprietary income and constructs a special block of tax administration of digital assets, in a criminal case this may be used not only for evaluation of value, but also for comparison of the digital and fiat trace. Where the digital asset was withdrawn, exchanged, sold, or otherwise converted into a proprietary result, the tax, banking, and financial-monitoring contour ceases to be optional: it becomes part of the evidentiary base in a case of theft, fraud, or laundering [4].

Directions for Improving Legal Characterization and Law Enforcement. From the analysis carried out, it follows that Kazakhstan is hardly in need of a single new corpus delicti of "theft of digital assets" as a universal answer to all digital threats. Such a step would look impressive, but in methodological terms it would be too coarse. The current criminal legislation already contains the principal constructions suitable for protecting proprietary interests in the digital environment as well. The problem lies elsewhere: in the absence of uniform criteria for when a digital asset is considered the subject of crime, when unlawful access to credentials turns into completed theft, where the boundary lies between fraud and concealed taking, and what specific operations testify to laundering rather than simply to the retention of the criminal result [1].

For the fraud block, it is advisable to rely on a stricter judicial standard: in cases involving digital assets, it is necessary to analyze not only promises and correspondence, but also the architecture of the digital scheme – who created the interface, in what manner the "verification" was organized, what exactly the victim was required to do, to whom the transaction was actually directed, and whether his or her expression of will may be regarded as free and conscious. Without such focus, even the current normative resolution of the Supreme Court on fraud will be applied too abstractly. The digital environment does not abolish the classical sign of deception, but it substantially complicates the forms in which it is realized [6].

In the part concerning the laundering of criminal proceeds, the further development of practice must inevitably proceed along the path of a closer linkage of criminal characterization with the institutions of financial monitoring, control over VASP providers, compliance with the Travel Rule, and the mechanisms of international cooperation. Otherwise, criminal law will react only to the initial theft or fraud, but not to the financial infrastructure that makes digital criminal schemes scalable and stable. For Kazakhstan, this is especially relevant against the background of the growth of illegal crypto-exchangers, the use of stablecoins, and the cross-border character of digital transfers, to which both FATF materials and AFM reports directly attest [7].

No less important is the procedural part. For cases involving digital assets, there is an urgent need to form a stable practice of the early arrest of digital assets, standardized requests to crypto-platforms, the consolidation of minimum requirements for a blockchain-analytical opinion, and a careful approach to the seizure of devices, seed phrases, hardware wallets, and backup keys. If this is not done, the law-enforcement system will either lose the digital trace in the first hours after the crime, or become excessively dependent on random technical specialists. In the final analysis, the issue here already turns not only on the norm, but also on the institutional readiness of the state to regard the digital asset as a full-fledged object of criminal-law protection [16].

Practical Qualification Framework for Criminal Offenses Involving Digital Assets. The analysis of criminal offenses involving digital assets demonstrates that the main challenge for law enforcement does not lie in the complete absence of applicable criminal-law norms, but in the absence of a unified approach to their application. Digital assets introduce new technical forms of circulation and transfer of value; however, the criminal-law assessment of such acts should remain focused on legally significant

circumstances rather than on technological characteristics alone. Therefore, the qualification of offenses involving digital assets requires a consistent framework based on the identification of the object of encroachment, the determination of control over the asset, the mechanism of its unlawful transfer, and the subsequent movement of the obtained value.

The first element of such a framework is the identification of the specific object affected by the criminal act. In practice, the term "digital asset" may refer to different legal and technological phenomena, including a secured digital asset, an unsecured digital asset, access credentials, or the possibility of disposing of a digital account or wallet. For criminal-law purposes, however, the decisive issue is not the technical form of the asset, but the existence of an economically valuable object capable of belonging to the sphere of control of a particular person. Establishing this circumstance allows the investigation and the court to distinguish between an actual property-related encroachment and actions that affect only information or technical access without causing proprietary harm.

The second element concerns the determination of legally relevant control over the digital asset. Unlike traditional property, where possession is usually connected with physical domination over an object, digital assets are characterized by the ability to authorize transactions and dispose of value through technological instruments. Consequently, the central question is not whether the offender obtained technical access to a digital environment, but whether such access resulted in the acquisition of the actual ability to dispose of the asset. The unlawful acquisition of credentials, access to a wallet, or information necessary for authentication may therefore have different criminal-law significance depending on whether it only created a possibility for future interference or already resulted in the loss of the victim's control over the proprietary value.

The third element relates to the mechanism through which the transfer of control occurred. This criterion is particularly important for distinguishing theft from fraud involving digital assets. Where the offender removes the asset from the victim's sphere of control without a conscious transfer of value by the victim, the legal assessment should focus on unlawful taking. In contrast, where the victim performs actions leading to the transfer of the asset because of deception, abuse of trust, or a false representation concerning the transaction, the central issue becomes the defect of the victim's will. Thus, the external digital form of the transaction cannot by itself determine qualification. The same technical operation, such as the transfer of cryptocurrency to another wallet, may receive different legal assessments depending on the circumstances preceding it.

The fourth element concerns the differentiation between the original criminal acquisition of a digital asset and subsequent actions aimed at concealing its origin. The movement of digital assets after the commission of theft or fraud does not automatically constitute laundering of criminal proceeds. For the purposes of Article 218 of the Criminal Code of the Republic of Kazakhstan, it is necessary to establish that subsequent transactions had an independent criminal purpose connected with disguising the source, ownership, or route of movement of the asset. Accordingly, the analysis of blockchain transactions should focus not only on the fact of transfer but also on the function of such transfer within the overall criminal scheme.

The fifth element of the qualification framework concerns evidence. The digital nature of the asset requires a comprehensive assessment of evidence, combining technological and legal analysis. The fact of a blockchain transaction alone does not establish all circumstances necessary for criminal qualification. It is necessary to determine the person exercising control over the relevant wallet or account, the circumstances of access, the moment of loss of control by the victim, the value of the asset, and the relationship between individual transactions and specific persons. Therefore, digital traces should be considered as a system of interconnected evidence rather than isolated technical information.

The proposed framework allows the existing criminal-law mechanisms of Kazakhstan to be applied more consistently to offenses involving digital assets. Its main purpose is not to create a separate category of crimes based solely on technological characteristics, but to ensure that digital assets are assessed within traditional criminal-law categories while taking into account their specific features. Such an approach makes it possible to avoid both the unjustified exclusion of digital assets from the sphere of property protection and the excessive perception of them as an entirely separate legal phenomenon beyond existing criminal-law constructions.

Table 1 – Practical Qualification Framework for Criminal Offenses Involving Digital Assets

Qualification stage	Key question	Legal significance
Identification of the object	What digital value became the object of encroachment?	Determines whether the act affects a legally protected proprietary interest
Determination of control	Who had the ability to dispose of the digital asset?	Establishes the relevant sphere of proprietary control
Mechanism of transfer	How was control transferred or lost?	Differentiates unlawful taking from transfer caused by deception
Subsequent transactions	Did further operations conceal the criminal origin of the asset?	Distinguishes retention of criminal proceeds from laundering
Evidence assessment	What digital and financial traces confirm the circumstances?	Ensures reliable criminal-law qualification
Note: Compiled by the authors.		

Conclusion

Digital assets in the law of the Republic of Kazakhstan are no longer located in a "gray zone" between the economy and technology. The legislator has recognized them as a special object of regulation, state bodies account for them as a source of proprietary income, financial monitoring regards them as a channel for the movement and concealment of criminal funds, and law-enforcement practice encounters real cases in which the digital asset appears now as the target of encroachment, now as the instrument of the subsequent masking of the criminal result. It is precisely for this reason that, for criminal law, the old position is no longer possible, under which crypto-assets were described as an exotic phenomenon not requiring precise work of characterization [1].

The principal conclusion of the article is the following: in Kazakhstani criminal law, a digital asset should be regarded as a proprietary value capable of being the subject of theft, fraud, and laundering; however, the characterization of such acts should be built not according to digital terminology, but according to the factual mechanism of causing harm. If the victim lost control over the asset as a consequence of its secret withdrawal from his or her wallet or account, the central point lies in a crime against property. If the asset or the possibility of disposing of it was transferred under the influence of deception, fraud takes priority. If, however, after the predicate offense special operations are committed aimed at concealing the origin, route, and ownership of the digital asset, there arises an independent question of laundering criminal proceeds [2].

At the same time, the law enforcer must refuse two equally mistaken extremes. The first is the reduction of the digital asset to "mere information," by reason of which the proprietary content of the crime is lost. The second is the opposite mystification, in which the digital asset is declared such a special object that the existing criminal-law constructions are supposedly inapplicable to it. Neither extreme withstands verification by law, doctrine, or official practice. Current legislation already makes it possible to cover the principal forms of criminal encroachment upon digital assets, but it requires subtler thinking in characterization and higher-quality proof [3].

From this there also follows a practical guideline. In cases involving digital assets, the court and the investigation must each time answer not a technological, but a juridically organized set of questions: what exactly constituted the subject of crime; in whose sphere of control the asset was located; in what manner this control was lost; whether there was a defect in the victim's will; which subsequent operations had the character of retention, and which of concealment of the origin of the property; how the value of the asset was established; and how the connection between the digital route and the concrete person was proved. Only such an approach makes it possible to transfer the discussion of digital assets from the zone of declarations to the zone of precise criminal-law characterization.

REFERENCES

1 On digital assets in the Republic of Kazakhstan Law of the Republic of Kazakhstan №. 193-VII LRK of February 6, 2023. URL: https://adilet.zan.kz/eng/docs/Z2300000193 (accessed: 06.06.2026)

2 Criminal Code of the Republic of Kazakhstan dated 3 July 2014 No. 226-V ZRK. URL: https://adilet.zan.kz/eng/docs/K1400000226 (accessed: 06.06.2026)

3 Жанабилова А.Б. Правовое регулирование оборота цифровых активов в Республике Казахстан и возможность их наследования // Вестник Института законодательства Республики Казахстан. – 2024. – № 3(78). – С. 124–134.

4 On Issues of the Sale of Digital Assets. URL: https://kgd.gov.kz/ru/news/po-voprosam-realizacii-cifrovyh-aktivov-1-142592 (accessed: 06.06.2026)

5 Романенко С.В. Вопросы регулирования правоотношений в сфере производства и обращения цифровых активов, противодействия коммерческому мошенничеству // Вестник КазНУ. Серия Юридическая. – 2023. – № 2(106). – С. 47–55.

6 On Judicial Practice in Cases of Fraud: Normative Resolution of the Supreme Court of the Republic of Kazakhstan dated 29 June 2017 No. 6. URL: https://adilet.zan.kz/eng/docs/P170000006S (accessed: 06.06.2026)

7 On Counteracting the Legalization (Laundering) of Proceeds Obtained by Criminal Means, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction: Law of the Republic of Kazakhstan dated 28 August 2009 No. 191-IV. URL: https://adilet.zan.kz/eng/docs/Z090000191_ (accessed: 06.06.2026)

8 Қойшыбайұлы Қ., Копбаев Д.З., Бидайшиева А.Б. Правовое регулирование блокчейн и криптовалют: проблемы и перспективы выпуска токенов и их оборот на территории Республики Казахстан // Вестник Института законодательства Республики Казахстан. – 2023. – № 1(72). – С. 98–107.

9 Kan A.G., Korzhumbaeva T.M., Abdullina S.Kh. Features of the Use of Cryptocurrencies in the Commission of Crimes in the Sphere of High Technologies // Bulletin of L.N. Gumilyov Eurasian National University. Law Series. 2024. Vol. 147. No. 2. P. 230–241.

10 Заркенов М.С., Жемпиисов Н.Ш. Уголовная ответственность в области неправомерной добычи цифровых активов // Вестник Академии правоохранительных органов. – 2021. – № 2(20). – С. 48–55.

11 Приказ Министра финансов Республики Казахстан от 25 сентября 2025 года № 531 «Об утверждении Правил определения, опубликования стоимости цифровых активов и перечня их видов». URL: https://adilet.zan.kz/rus/docs/V2500036938 (дата обращения: 06.06.2026)

12 Ликвидация структур по отмыванию денег через криптовалюту. URL: https://www.gov.kz/memleket/entities/afm/press/news/details/913888?lang=ru (дата обращения: 06.06.2026)

13 АФМ первыми на пространстве СНГ возвратило похищенные средства от зарубежного эмитента цифровых активов. URL: https://www.gov.kz/memleket/entities/afm/press/news/details/820233?lang=ru (дата обращения: 06.06.2026)

14 FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (accessed: 06.06.2026)

15 FATF Urges Stronger Global Action to Address Illicit Finance Risks in Virtual Assets // FATF. 26.06.2025. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html (accessed: 06.06.2026)

16 Decoding Crypto Crime – A Guide for Law Enforcement. URL: https://oceea.osce.org/oceea/587475 (accessed: 06.06.2026)

REFERENCES

1 On digital assets in the Republic of Kazakhstan. Law of the Republic of Kazakhstan No. 193-VII LRK of February 6, 2023. URL: https://adilet.zan.kz/eng/docs/Z2300000193 (accessed: 06.06.2026) (In English)

2 Criminal Code of the Republic of Kazakhstan dated 3 July 2014 No. 226-V ZRK. URL: https://adilet.zan.kz/eng/docs/K1400000226 (accessed: 06.06.2026) (In English)

3 Zhanabilova A.B. (2024) Pravovoe regulirovanie oborota cifrovyh aktivov v Respublike Kazahstan i vozmozhnost' ih nasledovanija // Vestnik Instituta zakonodatel'stva Respubliki Kazahstan. No. 3(78). P. 124–134. (In Russian)

4 On Issues of the Sale of Digital Assets. 2026. URL: https://kgd.gov.kz/ru/news/po-voprosam-realizacii-cifrovyh-aktivov-1-142592 (accessed: 06.06.2026) (In Russian)

5 Romanenko S.V. (2023) Voprosy regulirovanija pravootnoshenij v sfere proizvodstva i obrashhenija cifrovyh aktivov, protivodejstvija kommercheskomu moshennichestvu // Vestnik KazNU. Serija Juridicheskaja. No. 2(106). P. 47–55. (In Russian)

6 On Judicial Practice in Cases of Fraud Normative Resolution of the Supreme Court of the Republic of Kazakhstan dated 29 June 2017. No. 6. URL: https://adilet.zan.kz/eng/docs/P170000006S (accessed: 06.06.2026) (In English)

7 On Counteracting the Legalization (Laundering) of Proceeds Obtained by Criminal Means, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction: Law of the Republic of Kazakhstan dated 28 August 2009 No. 191-IV. URL: https://adilet.zan.kz/eng/docs/Z090000191_ (accessed: 06.06.2026) (In English)

8 Qoişybaiūly Q., Kopbaev D.Z., Bidajshieva A.B. (2023) Pravovoe regulirovanie blokchejn i kriptovaljut: problemy i perspektivy vypuska tokenov i ih oborot na territorii Respubliki Kazahstan // Vestnik Instituta zakonodatel'stva Respubliki Kazahstan. No. 1(72). P. 98–107. (In Russian)

9 Kan A.G., Korzhumbaeva T.M., Abdullina S.Kh. (2024) Features of the Use of Cryptocurrencies in the Commission of Crimes in the Sphere of High Technologies // Bulletin of L.N. Gumilyov Eurasian National University. Law Series. Vol. 147, no. 2, pp. 230–241. (In English)

10 Zarkenov M.S., Zhempiisov N.Sh. (2021) Ugolovnaja otvetstvennost' v oblasti nepravomernoj dobychi cifrovyh aktivov // Vestnik Akademii pravoohranitel'nyh organov. No. 2(20). P. 48–55. (In Russian)

11 Prikaz Ministra finansov Respubliki Kazahstan ot 25 sentjabrja 2025 goda № 531 «Ob utverzhdenii Pravil opredelenija, opublikovanija stoimosti cifrovyh aktivov i perechnja ih vidov». 2025. URL: https://adilet.zan.kz/rus/docs/V2500036938 (data obrashhenija: 06.06.2026) (In Russian)

12 Likvidacija struktur po otmyvaniju deneg cherez kriptovaljutu. 2026. URL: https://www.gov.kz/memleket/entities/afm/press/news/details/913888?lang=ru (data obrashhenija: 06.06.2026) (In Russian)

13 AFM pervymi na prostranstve SNG vozvratilo pohishhennye sredstva ot zarubezhnogo jemitenta cifrovyh aktivov. 2026. URL: https://www.gov.kz/memleket/entities/afm/press/news/details/820233?lang=ru (data obrashhenija: 06.06.2026) (In Russian)

14 FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF. 2021. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (accessed: 06.06.2026) (In English)

15 FATF Urges Stronger Global Action to Address Illicit Finance Risks in Virtual Assets // FATF. 2025. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html (accessed: 06.06.2026) (In English)

16 Decoding Crypto Crime – A Guide for Law Enforcement. 2026. URL: https://oceea.osce.org/oceea/587475 (accessed: 06.06.2026) (In English)

ЖҰМАҒҰЛОВА Ш.Р.,[1]
з.ғ.к., қауымдастырылған профессор.
e-mail: jumagulova_sholpan@mail.ru
ORCID ID: 0000-0002-2033-6260
САРТАЕВА К.Р.,[2]
з.ғ.к., профессор.
e-mail: galiya_1305@list.ru
ORCID ID: 0000-0002-7177-1369
БЕРДИЯРОВА Ж.С.,[3]
з.ғ.к., қауымдастырылған профессор.
e-mail: berdiyarova_zhs@enu.kz
ORCID ID: 0000-0002-4949-9522
АУЕШОВА Б.Т.,*[4]
з.ғ.к., қауымдастырылған профессор.
*e-mail: bagdataueshova@gmail.com
[1]Қорқыт Ата ат. Қызылорда университеті,
Қызылорда қ., Қазақстан
[2]М.О. Әуезов ат.
Оңтүстік Қазақстан университеті,
Шымкент қ., Қазақстан
[3]Л.Н. Гумилев ат.
Еуразия Ұлттық Университеті
Астана қ., Қазақстан
[4]Ш. Есенов ат. университеті,
Ақтау қ., Қазақстан

ЦИФРЛЫҚ АКТИВТЕР ҚЫЛМЫСТЫҢ ПӘНІ РЕТІНДЕ: ҰРЛЫҚ ПЕН АЛАЯҚТЫҚТЫ САРАЛАУДЫҢ МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада Қазақстан Республикасының құқығында цифрлық активтер қылмыс заты ретінде көрінетін не мүліктің қылмыстық шығу тегін жасыру құралы ретінде пайдаланылатын іс-әрекеттерді қылмыстық-құқықтық

саралау мәселелері зерттеледі. Негізгі мәселе зат нысанында өмір сүрмейтін, бірақ мүліктік құндылыққа ие және қылмыстық схемаларға қатыса алатын объектіге қатысты ұрлық, алаяқтық және заңдастырудың дәстүрлі конструкцияларының қалай қолданылатынында болып табылады. Қылмыстық құқық үшін цифрлық актив ең алдымен таза ақпарат ретінде емес, мүліктік құндылық ретінде қарастырылуы тиіс екені негізделді. Ұрлық кезінде шешуші мән жәбірленушінің активке бақылауын жоғалтуына, алаяқтық кезінде – алдау немесе сенімді теріс пайдалану салдарынан туындаған ерік ақауына, ал заңдастыру кезінде – қылмыстық активтің шығу тегі мен қозғалысына құқыққа сай сипат беруге бағытталған қаржылық операциялардың болуына тиесілі екені көрсетілді. Қазақстанның қолданыстағы қылмыстық заңнамасында цифрлық активтерге қол сұғушылықтың негізгі нысандарын қамтуға қабілетті базалық нормалар қазірдің өзінде бар деген қорытынды жасалады, алайда құқық қолдану қызметі неғұрлым дәл саралау өлшемдеріне, цифрлық іздерге бірыңғай тәсілге және дәлелдеудің арнайы әдістемесіне мұқтаж. Тәжірибе үшін ең үлкен қиындықтар қылмыс затын айқындаумен, жасырын алып қоюды алдау арқылы иеленуден ажыратумен, ұрлықтың аяқталу сәтін белгілеумен, сондай-ақ цифрлық активтің құнын, бақылауын және шығу тегін дәлелдеумен байланысты екені анықталды. Цифрлық активтермен байланысты қылмыстарды саралаудың тәжірибеге бағдарланған моделі ұсынылды.

Тірек сөздер: цифрлық актив, криптоактив, криптовалюта, қылмыс заты, ұрлық, алаяқтық, қылмыстық кірістерді заңдастыру.

ЖУМАГУЛОВА Ш.Р.,[1]
к.ю.н., ассоциированный профессор.
e-mail: jumagulova_sholpan@mail.ru
ORCID ID: 0000-0002-2033-6260
САРТАЕВА К.Р.,[2]
к.ю.н., профессор.
e-mail: galiya_1305@list.ru
ORCID ID: 0000-0002-7177-1369
БЕРДИЯРОВА Ж.С.,[3]
к.ю.н., ассоциированный профессор.
e-mail: berdiyarova_zhs@enu.kz
ORCID ID: 0000-0002-4949-9522
АУЕШОВА Б.Т.,*[4]
к.ю.н., ассоциированный профессор.
*e-mail: bagdataueshova@gmail.com
ORCID ID: 0000-0003-1449-9941
[1]Кызылординский университет им. Коркыт Ата,
г. Кызылорда, Казахстан
[2]Южно-Казахстанский университет
им. М.О. Ауэзова,
Шымкент, Казахстан
[3]Евразийский национальный университет
им. Л.Н. Гумилева,
Астана, Казахстан
[4]Университет им. Ш. Есенова,
Актау, Казахстан

ЦИФРОВЫЕ АКТИВЫ КАК ПРЕДМЕТ ПРЕСТУПЛЕНИЯ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ ХИЩЕНИЯ И МОШЕННИЧЕСТВА

Аннотация

В статье исследуются проблемы уголовно-правовой квалификации деяний, в которых цифровые активы выступают предметом преступления либо используются как средство сокрытия преступного происхождения имущества в праве Республики Казахстан. Обосновано, что цифровой актив для уголовного права должен рассматриваться прежде всего как имущественная ценность, а не как чистая информация. Показано, что при хищении решающим является утрата потерпевшим контроля над активом, при мошенничестве – дефект воли, вызванный обманом или злоупотреблением доверием, а при легализации – наличие финансовых операций,

направленных на придание правомерного вида происхождению и движению преступного актива. Сделан вывод, что действующее уголовное законодательство Казахстана уже содержит базовые нормы для охвата основных форм посягательств на цифровые активы, однако правоприменение нуждается в более точных критериях квалификации, единообразном подходе к цифровым следам и специальной методике доказывания. Установлено, что наибольшие трудности для практики связаны с определением предмета преступления, разграничением тайного изъятия и обманного завладения, установлением момента окончания хищения, а также доказыванием стоимости, контроля и происхождения цифрового актива. Предложена ориентированная на практику модель квалификации преступлений, связанных с цифровыми активами.

Ключевые слова: цифровой актив, криптоактив, криптовалюта, предмет преступления, хищение, мошенничество, легализация преступных доходов.

Article submission date: 01.07.2026