PERIODICA
Journal of Modern Philosophy, Social Sciences and Humanities
ISSN NO:2720-4030 Volume 48 November 2025

Sanctions For Crypto-Asset Offences In Uzbek Criminal Law: Limits Of Imprisonment And Fines And The Case For A Targeted Digital Restriction

Primov Bakhtiyor Olim ugli
Independent Researcher, Tashkent State University of Law
Doctor of Philosophy (PhD) in Law
ORCID: 0000-0002-8970-9029
e-mail: baxti13051993@gmail.com

ABSTRACT

In January 2024 Uzbekistan introduced criminal liability for repeated violations of crypto-asset legislation (Article 278-8) and for unlawful mining (Article 278-9). The sanctions for both offences follow the conventional ladder of fines, correctional labour, restriction of liberty and imprisonment. This article examines whether that ladder suits offences committed remotely, through accounts, devices and platforms. It combines a doctrinal analysis of the two articles and the regulatory market around them with a comparative review of sources from the United States, the United Kingdom, Germany, Russia, the European Union and South Korea, read against deterrence research and the standards of the Financial Action Task Force. The analysis shows that the ladder contains no measure aimed at the offender's access to the market, and that the existing deprivation of a specific right does not reach a person who trades for himself. Comparative sources suggest two correctives: financial sanctions linked to proceeds, and time-limited, individually reasoned restrictions on dealings. Court and human-rights material shows that blanket restrictions on internet use fail the proportionality test, while narrowly defined ones can stand. On this basis the article proposes a "digital restriction" as an additional penalty, limited to one to five years and reasoned in each case. The proposal is legislative and has not been tested empirically.

ARTICLE INFO

Received: 20th September 2025
Accepted: 14th October 2025

KEYWORDS: crypto-assets; criminal sanctions; digital restriction; proportionality; deterrence; unlawful mining.

Introduction

Crypto-assets have become a routine part of criminal finance. Chainalysis estimated that illicit addresses received at least USD 40.9 billion in 2024 and expected the final figure to rise to about USD 51.3 billion as further addresses are identified [1]. Legislators therefore face a question that is separate from what to criminalise: what should happen to the offender once convicted. For offences committed through accounts, devices and platforms the answer is not obvious. Imprisonment and fines act on the offender's body and wealth, while the offence depends on access to a market.

Uzbekistan built that market through regulation before it built criminal liability around it. Presidential Decree No. UP-121 of 27 April 2022 reorganised the National Agency of Perspective Projects (NAPP) and

gave it authority over crypto-asset circulation [2]. Service providers now operate under licences issued by the Agency, mining is open only to registered legal entities, and a provider's management and ownership are subject to the licensing body's control [3]. Criminal law arrived later. Law No. ÖRQ-899 of 19 January 2024 added Article 278^8 (violation of legislation on crypto-asset turnover) and Article 278^9 (unlawful mining activity) to the Criminal Code [4]. Both follow a two-stage model: an administrative penalty comes first, and criminal liability arises when the conduct is repeated.

Practice has started to follow. Press reports of 2026 investigations describe unlicensed trading run through a purpose-built site on social media with 229 bank cards among the items seized, trading through an account on a foreign exchange that holds no Uzbek licence, and turnover measured in billions of soums. These cases are at the investigation stage and no sentences have been reported, so it is too early to judge how courts will use the sanctions. It is not too early to ask whether the sanctions are well designed.

Scholarly attention to the new provisions has gone mainly to their elements and to the line between them and neighbouring offences. The author's own earlier work compared liability models for crypto-asset offences in selected foreign systems [5]. The structure of the sanctions has not been examined as a design problem. That gap matters. A person who has already paid an administrative fine for trading without a licence is by definition someone for whom the first-stage response failed. The criminal sanction should therefore do something the fine did not.

This article asks two questions. First, how are the sanctions for Articles 278^8 and 278^9 constructed, and do they reach the means by which these offences are committed? Second, if they do not, can a narrowly drawn restriction on participation in the crypto-asset market be justified under the proportionality standards that courts and treaty bodies apply to similar measures, and can it be enforced in Uzbekistan's market? The article argues that the answer to the first question is largely no, and that the answer to the second is yes if the restriction is defined by conduct, limited in time, reasoned case by case, and enforced through the licensed gateways that already exist. The main part first states the sources and limits of the study, then describes the Uzbek framework, draws design criteria from deterrence research and the FATF standards, reviews comparative and human-rights material, and finally presents and tests the proposal.

Main part

The study is doctrinal and comparative. The Uzbek provisions are read through the amending law and the Criminal Code [6] and through published professional commentary on their sanctions. Sanction figures are given in base calculation values (BCV), the unit used in those sources, and should be read against the official text of the Code. The regulatory background is taken from the decree and licensing regulation as reported by the Agency and by legal advisers [7] and from press reports of 2026 amendments and investigations [8].

The comparative material was chosen to represent distinct approaches to the same problem. The United States was selected because its federal courts have produced the most detailed case law on restrictions of computer and internet use imposed as part of a sentence. The decisions used are Packingham, which sets the constitutional standard, and one recent application (Savastio). The United Kingdom was selected for its ancillary order that restricts an offender's dealings after conviction. Germany and Russia were selected because their criminal codes contain the closest doctrinal relatives of the Uzbek deprivation of a specific right. The European Union and South Korea were selected for their penalty provisions on market abuse in crypto-assets. Two international human-rights sources, the Human Rights Committee's General Comment No. 34 and the case law of the European Court of Human Rights, are used as persuasive standards for proportionality.

The sanctions are read against two bodies of research: the empirical literature on deterrence [9] and the standards of the Financial Action Task Force on the licensing and supervision of virtual asset service providers [10].

Four limits should be stated. No sentencing statistics for Articles 278^8 and 278^9 were available, so the study makes no claim about how courts apply them. The 2026 case reports describe the conduct alleged by investigators and are used only to illustrate how the offences are committed, not to establish facts about any person. The deterrence findings come from research on crime in general, not on crypto-asset offences

specifically. Finally, the Binance example discussed below is a single illustration drawn from court and agency reports and news coverage, and it concerns a different offence.

Decree No. UP-121 defined the categories of crypto-asset service providers: crypto-exchanges, mining pools, crypto-depositories and crypto-stores. The licensing regulation registered under No. 3380 on 15 August 2022 requires a separate licence for each category and obliges providers to keep records of transactions and participants for five years and to exclude hidden mining and operations with anonymous crypto-assets. The Agency reported that by January 2024 fourteen providers were operating: two exchanges, two depositories and ten stores. Mining is limited to legal entities, which must register electronically with the Agency and mine only at the registered address.

This structure matters for sanction design in two ways. The number of licensed gateways is small, so a court-ordered restriction could be communicated to all of them. And the gateways already carry duties that depend on knowing the customer. In June 2026 the licensing rules were amended so that a provider cannot be managed by persons resident in or registered in jurisdictions that do not take part in international anti-money-laundering cooperation, and so that changes of ownership and key management need the licensing body's approval. In August 2026 the Agency published draft amendments to the internal-control rules that allow providers to use a third party to identify and verify clients and require suspicious-transaction reports to go to the Economic Crime Combating Department under the Prosecutor General's Office [11]. The market therefore has an identification and reporting layer on which a restriction could rely.

For Article 278^{8} the commentary describes three tiers [12]. The first part provides a fine of up to 100 BCV, or correctional labour for two to three years, or restriction of liberty for up to one year, or imprisonment for up to one year. The second part covers repeated acts, acts by a dangerous recidivist, large amounts and prior conspiracy by a group, and provides a fine of 300 to 400 BCV, or restriction of liberty or imprisonment for up to three years. The third part covers very large amounts, abuse of official position and organised groups, and provides imprisonment for three to five years. The administrative stage that precedes these tiers consists of confiscation of the crypto-assets and instruments used, administrative detention of up to 15 days, or a fine of 20 to 30 BCV, and criminal liability arises if the same conduct is repeated within one year.

For Article 278^{9} the reports describe the same type of ladder. A repeated violation of the mining procedure within a year carries a fine of up to 100 BCV (about UZS 34 million), correctional labour, restriction of liberty or imprisonment of up to one year. Covert mining carries a fine of 100 to 300 BCV or restriction of liberty or imprisonment of up to two years, and the aggravated forms carry a fine of 300 to 400 BCV or restriction of liberty or imprisonment of up to three years [13]. The sources differ on how the parts are numbered, but they agree on the ladder.

Three investigations reported in 2026 show the setting in which the sanctions will operate. In March 2026 two persons were detained for running unlicensed crypto trading through a special site on social media, with turnover of 793,000 USDT (UZS 9.7 billion) over about six months. The seized items included a computer assembly, 22 mobile phones, three SIM cards and 229 bank cards [14]. In July 2026 police reported a case of illegal turnover of about USD 578,000 conducted with special devices and software, with a laptop, a telephone, bank cards and a computer seized [15]. In September 2026 a criminal case was opened under Article 278^{8}, part 3, against a man alleged to have made nearly 700 buy-and-sell transactions between 2021 and 2025 through an account on a foreign exchange without a licence, with an initial value of USD 683,000 [16]. All three cases were at the investigation stage when reported.

Three features stand out. Two of the three cases describe conduct repeated over months or years and run on a standing set-up of accounts, devices and payment cards. Bank cards appear among the seized items in two cases. And one case involved a foreign platform outside the licensing system. A sanction designed for this setting should act on the set-up and not only on the person's freedom or wealth, and it should not assume that every account is held with a licensed provider.

Read against these cases, the ladder reaches and leaves out the following.

(a) The ladder consists of four conventional measures: a fine, correctional labour, restriction of liberty and imprisonment. None is directed at the access through which the offence is committed. The one measure

aimed at the means appears at the administrative stage, where crypto-assets and instruments may be confiscated. The reported sanction provisions of the two articles contain nothing comparable.

(b) The General Part does provide a measure of the right kind in principle: deprivation of a specific right (Article 45 of the Code). The commentary describes it as a court-ordered ban, for a set period, on holding a named post or engaging in a named lawful activity, it requires the offence to be linked to the convicted person's post or activity, and it covers lawful activity only, so a court cannot ban a person from conduct that is itself unlawful [17]. That design fits a provider's manager, a miner's director or an employee who abused a position. It fits less well a person who trades for himself, who holds no post and carries on no registered activity, and it cannot be used against unlicensed trading as such, because that activity is already unlawful. The reported sanctions of Articles 278^8 and 278^9 also do not list it as an additional penalty.

(c) Fines are fixed in BCV and do not vary with the proceeds of the offence. The cases described above involve turnover of several billion soums, against fine ceilings of 100 to 400 BCV, or about UZS 34 to 136 million at the conversion reported for Article 278^9. A fixed ceiling is blind to the size of the gain.

(d) Restriction of liberty and correctional labour are built around the convict's place of residence and place of work. An offender who trades or mines through online accounts and remote equipment can comply with conditions of that kind and continue the same activity. Correctional labour, for its part, works through withholding a share of earnings from regular employment, so it has little to attach to when the offender earns elsewhere or irregularly.

The point is not that these sanctions are useless. Imprisonment retains its place in the aggravated tiers. The point is that in the lower and middle tiers, where most repeat offenders of the kind described above will be sentenced, the ladder offers nothing that changes the offender's access to the market once the sentence has been served or the fine paid.

Nagin's review of the deterrence literature, summarised for practitioners by the National Institute of Justice, finds that the certainty of being caught deters more than the severity of the sentence, and that increases in already lengthy sentences add at best a modest deterrent effect [18]. Crypto-asset offending shifts the balance further. Pseudonymous transactions and cross-border platforms make detection the weak point, so a legislator who responds to the problem by lengthening prison terms is pulling the lever that research finds least effective. A measure that increases the chance that a prohibited attempt is noticed works on the element that matters more.

The Financial Action Task Force expects countries to license or register virtual asset service providers and to supervise them, and has issued guidance on the licensing and the so-called travel rule. Its 2024 targeted update is a caution. It found that 75 percent of the jurisdictions surveyed were only partially compliant or not compliant with the standard on virtual assets, that nearly one third of respondents had not passed legislation implementing the travel rule, and that where such legislation exists supervision and enforcement remain low [19]. A gateway-based measure is only as good as the supervision behind it. This is a reason to design the measure around the small, supervised set of gateways Uzbekistan has, and not around an assumption that every part of the market can be reached.

The research supports four criteria for a sanction aimed at crypto-asset offenders. It should work on certainty and not only on severity. It should act at a chokepoint that can be supervised. It should be narrow, time-limited and reasoned for the individual offender, because that is the condition on which comparable measures survive judicial review (see the comparative material below). And it should be enforceable through duties that already exist, so that it does not depend on new institutions. The proposal presented below is built to meet these criteria.

The comparative material starts with the United States, where courts review the conditions that accompany a sentence. Under 18 U.S.C. § 3583(d) a condition of supervised release must be reasonably related to the sentencing factors and must involve no greater deprivation of liberty than is reasonably necessary [20]. The cases below apply that standard to restrictions on computer and internet use.

In Packingham v. North Carolina the Supreme Court struck down a statute that made it a felony for registered sex offenders to access commercial social networking sites. Justice Kennedy reasoned that the government may not suppress lawful speech as the means to suppress unlawful speech, and the Court

described the sites as a modern public square [21]. The statute applied to persons who had completed their sentences. In Savastio the Second Circuit later distinguished Packingham on that ground and upheld conditions that required the defendant to join a computer and internet monitoring programme and limited him to one internet-capable device, because the conditions did not ban access. The decision is a non-precedential summary order, but it shows the line courts draw [22].

The pattern is consistent. Blanket and open-ended bans on technology fail. Narrow, individualised and monitored conditions, tied to the offence and explained by the court, can be sustained.

Under Part 1 of the Serious Crime Act 2007 (sections 19 to 21) the Crown Court may, on conviction for a serious offence, make a serious crime prevention order if there are reasonable grounds to believe that it would protect the public by preventing, restricting or disrupting the person's involvement in serious crime [23]. The order may restrict financial, property and business dealings, working arrangements, communications and association, the use of premises, and travel. It cannot exceed five years, and breach is a criminal offence punishable by up to five years' custody [24]. The order is general and not specific to crypto-assets. Its value for present purposes is structural: it shows a court restricting the means of offending without custody, on a stated test, for a limited time, with breach independently punishable.

Section 70 of the German Criminal Code allows a court to prohibit a person from exercising a profession or trade where he has been convicted of an unlawful act committed in abuse of it, and where a comprehensive evaluation of the offender and the offence shows a danger of further serious unlawful acts of that kind. The prohibition runs for one to five years, may not be shorter than three months after deduction of any provisional disqualification, and may be made permanent only if there is reason to believe that the statutory maximum would not avert the danger [25].

Article 47 of the Russian Criminal Code provides for deprivation of the right to hold certain posts or engage in certain activities. The term is one to five years as a principal punishment and six months to three years as an additional one, and up to twenty years only as an additional punishment where the Special Part so provides. Under its third part a court may impose the deprivation as an additional punishment even when the Special Part article does not list it, if the nature and danger of the offence and the offender's personality mean that he cannot be allowed to keep the right [26].

Both provisions are close relatives of Article 45 of the Uzbek Code. They share a design: a ban linked to the offence, a fixed term in a band of one to five years, and a danger test or reasoning requirement. The Russian model adds one feature of practical value, namely the possibility of imposing the ban even where the sanction clause is silent. None of the three, however, reaches a private person who uses a market for himself. They address roles and occupations, which is the supplier side of the market.

Article 111 of Regulation (EU) 2023/1114 requires administrative penalties for market abuse that reach at least EUR 5 million for natural persons and at least EUR 15 million or 15 percent of annual turnover for legal persons, together with maximum fines of at least three times the profit gained or loss avoided where these can be determined. Member States may leave these infringements to criminal law only if they were already criminal offences by 30 June 2024 [27]. South Korea's Virtual Asset User Protection Act, in force from 19 July 2024, prohibits the use of undisclosed material information, price manipulation and other unfair trading. According to the Financial Services Commission, the criminal penalties are at least one year's imprisonment or a fine of three to five times the unfair profit, and an administrative surcharge of up to twice the profit may be added [28]. Both systems tie the size of the financial sanction to the gain, and both treat the financial sanction as a principal tool, not an afterthought.

The case of Changpeng Zhao is not an Uzbek analogue, since it concerned a failure to maintain an effective anti-money-laundering programme under the Bank Secrecy Act. It illustrates what happens when custody and fines meet control of a platform. On 30 April 2024 Mr. Zhao was sentenced to four months' imprisonment and a USD 50 million fine. Prosecutors had asked for three years, and the guidelines range was 12 to 18 months. Binance was ordered to pay USD 4.3 billion in fines and forfeiture [29]. In November 2023 the Commodity Futures Trading Commission had announced a proposed consent order that included a USD 150 million civil penalty against Mr. Zhao and a permanent injunction against evading the Commodity Exchange Act [30]. Mr. Zhao was not required to give up his stake in the company, but he was barred from

operating Binance for three years and stepped down as chief executive [31]. In October 2025 he received a presidential pardon [32].

Two observations follow. First, the criminal process itself reached for a time-limited bar on a role, which is the logic of the German and Russian provisions. Second, the bar left ownership untouched, and the pardon shows that the whole package can be reopened by executive decision. A restriction that depends on a plea agreement or on clemency is not a reliable instrument. It needs a statutory basis and a fixed term.

Uzbekistan is a party to the International Covenant on Civil and Political Rights [33]. The Human Rights Committee's General Comment No. 34 states that restrictions on expression must be necessary and proportionate, that they must be the least intrusive instrument among those that might achieve the protective function, and that generic bans on the operation of certain sites and systems are incompatible with the Covenant [34]. The European Court of Human Rights, whose case law Uzbekistan is not bound by but which is a useful comparator, held in Ahmet Yıldırım v. Turkey that blocking all of Google Sites to reach one offending site was a disproportionate interference, because the domestic court did not weigh the collateral effects [35]. In Kalda v. Estonia it found a violation where a prisoner was denied access to specific legal-information websites without a convincing showing that the restriction was necessary [36].

These sources concern freedom of expression and information, and a restriction on participation in the crypto-asset market is a restriction on financial dealings, not on speech. They are still useful, for two reasons. They state the method that reviewing bodies use: ask what the restriction is for, whether a narrower one would do, and what it does to people who are not the target. And they point in the same direction as the American cases. A broad, undifferentiated restriction on a technology is difficult to defend, and a restriction defined by a specific service, reasoned for the individual and limited in time is far easier to defend.

Table 1. Comparative sources and their relevance to Articles 278^{8} **and** 278^{9}

Jurisdiction	Instrument	Core feature	Lesson for the Uzbek provisions
United States	18 U.S.C. § 3583(d); Packingham, Savastio	Judicial control of conditions: reasonable relation to sentencing purposes, no greater deprivation of liberty than necessary	Blanket and indefinite bans fail; narrow, reasoned and monitored conditions can stand
United Kingdom	Serious Crime Act 2007, ss. 19-21	Order on conviction restricting dealings, communications, premises and travel; up to 5 years; breach is an offence	A court can restrict the means of offending without custody, on a stated test
Germany	Criminal Code, s. 70	Ban on a profession or trade abused in the offence; 1 to 5 years; danger test; permanent only exceptionally	Term band and danger test are workable; limited to occupations
Russia	Criminal Code, Art. 47	Ban on posts or activities; 1 to 5 years (principal), 6 months to 3 years (additional); may be added even if the sanction is silent	Ancillary imposition when the sanction is silent; limited to posts and activities

Jurisdiction	Instrument	Core feature	Lesson for the Uzbek provisions
European Union	Regulation (EU) 2023/1114, Art. 111	Fines of at least EUR 5 million (natural persons), EUR 15 million or 15% of turnover (legal persons), and at least three times the profit	Financial sanctions can be tied to the proceeds of the offence
South Korea	Virtual Asset User Protection Act, in force 19 July 2024	Imprisonment of at least one year or a fine of three to five times the unfair profit; surcharge up to twice the profit	Penalties scale with the gain; a fixed fine in BCV does not

The comparative material shows a gap that is easy to miss. Occupational bans of the kind found in Article 45 of the Uzbek Code, Article 47 of the Russian Code and section 70 of the German Code act on the supplier side of a market. They remove a manager from a provider, a director from a mining company, a professional from his trade. Many offenders under Article 278^8 are on the user side or run informal operations without a licence. The offence covers unlawful acquisition, transfer or exchange of crypto-assets and operations with anonymous crypto-assets as well as unlicensed provision of services, and the 2026 cases involve individuals who traded with their own accounts, devices and cards and not as employees or managers of a licensed provider. For them an occupational ban has nothing to bite on, and a ban on unlicensed trading would only repeat the offence, because Article 45 reaches lawful activity only. What is needed is a restriction on participation in the lawful market, defined by conduct and not by status, which a person convicted of abusing that market can be denied for a period.

The author proposes an additional penalty called "digital restriction", with the following elements.

1. Scope by conduct. The convicted person is prohibited from participating in crypto-asset operations of any kind, including opening or using accounts with crypto-asset service providers and holding crypto-assets through them; from founding, managing or financing a crypto-asset service provider or a mining entity; and from operating mining equipment. The measure does not restrict internet use in general or ordinary banking, which is the lesson of Packingham.

2. Term. A fixed term of one to five years, set by the court by reference to the gravity of the offence and the offender's role. This is the band used in section 70 of the German Code and in Article 47 of the Russian Code, and five years is also the ceiling of the British order.

3. Test and reasons. The court may impose the measure where it finds reason to believe that continued participation would lead to further offences of the same kind, and it must state in the judgment why the scope and the term are necessary in the individual case. This borrows the danger test of the German provision and the public-protection test of the British order, and it makes the finding of necessity visible in the judgment.

4. Application by tier. The measure should be available in every part of both articles, but its use should differ by tier, as shown in Table 2.

5. Variation. The convicted person may apply to the court to shorten or end the restriction after part of the term has been served, and the court may vary its scope. The British order has a variation procedure for this purpose.

6. Basis. The measure should be listed expressly in the sanctions of Articles 278^8 and 278^9 and defined in the General Part alongside Article 45. The Russian rule allowing imposition when the sanction is silent is a useful fallback, but an express listing removes doubt.

7. Link with the financial sanction. Fines in these cases should be set by reference to the proceeds, as in the European and Korean models, and not only as a fixed amount in BCV. Where restriction of liberty is imposed, its conditions should be tied to specific services and not to the offender's location.

Table 2. Illustrative application of the digital restriction by tier

Case	Principal sanction range as reported	Digital restriction (illustrative)	Reason
Part 1, first criminal conviction after the administrative stage	Fine up to 100 BCV, correctional labour, restriction of liberty or imprisonment up to 1 year	Discretionary; 1 to 2 years where trading was regular or used a standing set-up of accounts and devices	The administrative response has already failed once; the aim is to close the lawful route back into the market
Part 2: repeated acts, recidivists, large amounts, group conspiracy	Fine of 300 to 400 BCV, restriction of liberty or imprisonment up to 3 years	Court must consider it and give reasons if it does not impose it; 2 to 4 years	Pattern and scale suggest continued risk
Part 3: very large amounts, official position, organised groups	Imprisonment of 3 to 5 years	Presumptive; up to 5 years, running after release	Restriction operates when custody ends
Repeat conviction under either article	As above	Presumptive; upper half of the band	Prior conviction is the strongest indicator of risk

The measure can be enforced through four channels that already exist or are being built. First, a register of persons subject to the restriction, kept by the Agency and available to licensed providers. Second, the providers themselves: they already identify customers, keep records for five years and report suspicious transactions, and the August 2026 draft rules extend these controls. A check against the register is a small addition to a due-diligence routine that exists. Third, the licensing system, in which the licensing body approves changes in ownership and key management and could refuse approval to a person who is subject to the restriction. Fourth, payment channels. Bank cards appear among the items seized in two of the 2026 cases, so the register should also be available, under a legal basis to be defined, to financial institutions for their own due-diligence purposes.

Breach should carry its own consequence. The legislator could treat participation in breach of the restriction as an aggravating factor in any later case, as a ground for replacing the unserved part with a stricter measure, or as a separate offence, in the way that breach of the British order is. The choice is a matter for drafting and should reflect Uzbek rules on non-execution of court decisions.

A draft formulation, for insertion in the General Part next to Article 45 and for cross-reference in the sanctions of Articles 278^8 and 278^9, would read:

> "In cases under Articles 278^8 and 278^9 of this Code, where there is reason to believe that the convicted person's continued participation in crypto-asset operations would lead to further offences of the same kind, the court may, in addition to the principal punishment, prohibit him for a term of one to five years from opening or using accounts with crypto-asset service providers and holding crypto-assets through them, from founding, managing or financing a crypto-asset service provider or a mining entity, and from operating mining equipment. The court shall state in the judgment the grounds for the scope and term of the prohibition."

Five objections deserve an answer.

Circumvention. The most obvious objection is that an offender can go to a foreign platform, trade peer to peer, or hold assets in a wallet that no provider controls. That is true, and the third case described above involved a foreign platform. The restriction is therefore not a technological barrier. It does three other things.

It closes the lawful route, so that an offender cannot continue or resume through a licensed provider while the sentence is formally served. It converts any continued participation, wherever it occurs, into a breach of a court order with its own consequence, which gives investigators a ground to act that does not depend on proving the original offence again. And it gives licensed providers and the Agency the information they need to refuse and to report. The measure complements detection and does not replace it, and the deterrence literature suggests that raising the chance of detection is where the benefit lies.

Proportionality. A restriction on a defined category of financial services, for a fixed term, reasoned for the individual and open to variation, is a long way from the social-media statute that failed in Packingham. It leaves the offender free to use the internet, to bank, to work and to communicate. The proposal also follows the method of General Comment No. 34 and of the European Court: it asks for the least intrusive instrument that serves the protective aim and requires the court to weigh the effect on the individual. The risk of overreach is real if the scope is later widened to digital activity in general, and the draft provision is worded to prevent that.

Enforcement capacity. The FATF's 2024 update shows that supervision is weak in many jurisdictions. The Uzbek position is better placed than most for this particular measure because the licensed market is small, a single agency licenses and supervises it, and the 2026 amendments strengthen control of ownership and management. A register of restricted persons checked by a small group of licensed providers (fourteen in January 2024) is a manageable task. Whether it works in practice is an empirical question to be tested once the measure is in use.

Excess for minor cases. A first-time offender who traded a modest amount may reasonably say that a restriction of up to five years is out of scale. The tiered use in Table 2 addresses this: in the first part the measure is discretionary and short, and it is aimed at regular and organised trading, not at isolated acts. A judge who finds no risk of further offences should not impose it, and the reasons requirement makes that finding visible.

Relation to the administrative stage. Because criminal liability follows an administrative penalty, a person reaches Article 278^8 only after one failed response. That supports the proposal. If the administrative stage included a short, similar restriction, the criminal stage would build on it. That is a possible further reform, but it is outside the scope of this article, which is confined to criminal sanctions.

Conclusion

Articles 278^8 and 278^9 of the Uzbek Criminal Code rely on a conventional ladder of sanctions. The ladder contains no measure aimed at the access through which crypto-asset offences are committed. The deprivation of a specific right in Article 45 is tied to posts and activities and does not reach a person who trades for himself. Fines are fixed in BCV and do not follow proceeds. Restriction of liberty and correctional labour are built around residence and employment and leave online conduct untouched.

The comparative sources suggest two correctives. Financial sanctions can be linked to the gain, as the European Union and South Korea do. Restrictions on dealings can be imposed for a limited time on a stated test, as the United Kingdom, Germany and Russia do in different forms. American case law and international human-rights standards add the conditions under which such restrictions survive review: they must be defined by a specific service or activity, limited in time, reasoned for the individual and open to variation. Blanket restrictions on technology fail.

Three recommendations follow. First, introduce an additional penalty of digital restriction, defined by conduct, for a term of one to five years, imposed with reasons and open to variation, and list it in the sanctions of both articles. Second, link fines in these cases to the proceeds of the offence. Third, create a register of restricted persons and a corresponding duty on licensed providers, and consider making the register available to financial institutions, so that the restriction can be enforced through the market's existing gateways. These proposals are legislative. They should be tested against sentencing data and enforcement experience as they become available, and the study's main limit, the absence of such data, should be remedied first.

References

1. Chainalysis. The 2025 Crypto Crime Report. Chainalysis Inc., 2025.
2. National Agency of Perspective Projects. The institutional structure of the national crypto-market is expanding (news item, 3 January 2024; title translated from Uzbek). https://napp.uz/en/news/milliy-kripto-bozor-institutsional-tizimi-kengaymoqda
3. GRATA International. Regulation on the procedure for licensing service providers in the field of crypto-assets approved in Uzbekistan (Regulation registered No. 3380, 15 August 2022). Mondaq. https://mondaq.com/fin-tech/1225010/there-has-been-approved-the-regulation-on-the-procedure-for-licensing-service-providers-in-the-field-of-crypto-assets-in-uzbekistan.
4. Law of the Republic of Uzbekistan No. ÖRQ-899 of 19 January 2024 "On amendments and additions to the Criminal Code, the Code of Criminal Procedure and the Code of Administrative Responsibility of the Republic of Uzbekistan" (title translated from Uzbek). National Database of Legislation, 20.01.2024.
5. Primov B.O. A comparative legal analysis of liability for criminal offenses related to crypto-assets in the criminal legislation of selected foreign countries. Journal of Law Research, 2026, vol. 11, issue 8.
6. Criminal Code of the Republic of Uzbekistan (adopted 22 September 1994, as amended). Bulletin of the Oliy Majlis of the Republic of Uzbekistan, 1995, No. 1.
7. Kinstellar. Uzbekistan liberalises regulatory framework for mining of crypto-assets. Mondaq, 16 May 2022 (describing Presidential Decree No. UP-121 of 27 April 2022). https://www.mondaq.com/fin-tech/1192946/uzbekistan-liberalizes-regulatory-framework-for-mining-of-crypto-assets.
8. Spot.uz. Rules on licensing of crypto-service providers amended (news item, 30 June 2026; title translated from Uzbek). https://www.spot.uz/oz/2026/06/30/crypto-service/.
9. Nagin D.S. Deterrence in the twenty-first century. Crime and Justice, 2013, vol. 42, no. 1, pp. 199-263.
10. Financial Action Task Force. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris, 28 October 2021. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html
11. Spot.uz. Draft amendments to internal-control rules for crypto-service providers published (news item, 12 August 2026; title translated from Uzbek). https://www.spot.uz/oz/2026/08/12/crypto-services-aml/
12. Khudoykulov F. Do you know there is liability for violating legislation in the sphere of crypto-asset turnover? (title translated from Uzbek). yuz.uz, 1 April 2024. https://yuz.uz/oz/news/kripto-aktivlar-aylanmasi-sohasidagi-qonunchilikni-buzganlik-uchun-javobgarlik-borligini-bilasizmi
13. Punishments being introduced for illegal mining and cryptocurrency trading. Kun.uz, 20 January 2024. https://kun.uz/en/news/2024/01/20/punishments-being-introduced-for-illegal-mining-and-cryptocurrency-trading.
14. Spot.uz. Illegal crypto trading detected in Tashkent (news item citing the Tashkent City Internal Affairs Department, 24 March 2026; title translated from Uzbek). https://www.spot.uz/oz/2026/03/24/illegal-crypto/
15. Spot.uz. Illegal crypto-asset turnover investigated in Tashkent (news item, 22 July 2026; title translated from Uzbek). https://www.spot.uz/oz/2026/07/22/turnover-crypto-assets/
16. Spot.uz. Criminal case opened over unlicensed crypto trading (news item citing the Cybercrime Department of the Ministry of Internal Affairs, 14 September 2026; title translated from Uzbek). https://www.spot.uz/oz/2026/09/14/turnover-crypto-assets/
17. Muayyan huquqdan mahrum qilish qanday jazo? (commentary on Article 45 of the Criminal Code of Uzbekistan; title translated from Uzbek). yuz.uz. https://yuz.uz/oz/news/muayyan-huquqdan-mahrum-qilish-qanday-jazo
18. National Institute of Justice. Five Things About Deterrence. Washington, DC: U.S. Department of Justice, Office of Justice Programs, May 2016 (NCJ 247350).

19. Financial Action Task Force. Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Paris, 9 July 2024. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html
20. 18 U.S.C. § 3583(d) (conditions of supervised release).
21. Packingham v. North Carolina, 582 U.S. 98 (2017).
22. United States v. Savastio, No. 17-2149 (2d Cir. June 11, 2019) (summary order).
23. Serious Crime Act 2007 (United Kingdom), Part 1, ss. 19-21.
24. Sentencing Council for England and Wales. Serious crime prevention order on conviction (explanatory material). https://sentencingcouncil.org.uk/ancillary-suppl-information-text/serious-crime-prevention-order-on-conviction/
25. German Criminal Code (Strafgesetzbuch), section 70 (prohibition from exercising a profession), English translation. UNODC SHERLOC Case Law Database. https://sherloc.unodc.org/cld/es/legislation/deu/german_criminal_code/general_part_-_chapter_three/section_70/section_70.html
26. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ, статья 47 «Лишение права занимать определенные должности или заниматься определенной деятельностью». https://rulaws.ru/uk/Razdel-III/Glava-9/Statya-47/
27. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, Art. 111. OJ L 150, 9.6.2023, pp. 40-205.
28. Financial Services Commission (Republic of Korea). FSC to ensure thorough preparation for the enforcement of the Act on the Protection of Virtual Asset Users. Press release, 8 February 2024. https://fsc.go.kr/eng/pr010101/81698
29. Binance founder Changpeng Zhao sentenced to 4 months in prison after plea deal. CNBC, 30 April 2024. https://www.cnbc.com/2024/04/30/binance-founder-changpeng-zhao-cz-sentenced-to-four-months-in-prison-.html
30. U.S. Commodity Futures Trading Commission. Press Release No. 8825-23, 21 November 2023 (proposed consent order with Binance and Changpeng Zhao). https://www.cftc.gov/PressRoom/PressReleases/8825-23
31. Binance founder sentenced to 4 months in prison. Axios, 30 April 2024. https://www.axios.com/2024/04/30/cz-binance-changpeng-zhao-founder-sentenced.
32. US President Trump pardons Binance founder Changpeng Zhao. Ada Derana, 24 October 2025. https://www.adaderana.lk/news/113901/us-president-trump-pardons-binance-founder-changpeng-zhao.
33. International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.
34. United Nations Human Rights Committee. General Comment No. 34: Article 19, Freedoms of opinion and expression. CCPR/C/GC/34, 2011, paras 33-34, 43.
35. Ahmet Yıldırım v. Turkey, application no. 3111/10, European Court of Human Rights (Second Section), judgment of 18 December 2012.
36. Kalda v. Estonia, application no. 17429/10, European Court of Human Rights, judgment of 19 January 2016.