International Journal of Social Sciences

Caucasus International University
Volume 6, Issue 3

Journal homepage: http://journal.ciu.edu.ge/

DOI: https://doi.org/10.55367/IYEO2695



*Conference proceedings – **International scientific conference "Contemporary Challenges in International Relations, International Law and Media"** organised by Caucasus International University*
Held on March 12-13, 2026 in Tbilisi

Transnational Financial Fraud and Crypto-Assets: Jurisdictional Challenges in International Criminal Law

Tamta Tsirkvadze [a1]

[a] PhD in Law, Associate Professor,
Caucasus International University

ARTICLE INFO

Keywords:

Crypto-assets

Blockchain

Transnational financial fraud

Territorial jurisdiction

Jurisdictional conflicts

ABSTRACT

In the era of the digital world, one of the most significant challenges is the investigation of transnational crimes, as the ecosystem based on crypto-assets has substantially transformed both the nature of such crimes and the logic of jurisdiction. The purpose of this paper is to analyze how effectively the existing doctrine of international criminal law (territoriality, nationality principles, and the effects doctrine) responds to crypto fraud, and what reforms are necessary to adapt legal systems to technological challenges.

The paper employs doctrinal, comparative legal, and practical analytical research methods. It examines international instruments such as the Budapest Convention, Financial Action Task Force standards, and Markets in Crypto-Assets Regulation, as well as the legal and institutional practice operating in Georgia. The typology of crypto fraud is analyzed, the method of mapping jurisdictional links is applied, and a hybrid evidentiary model (on-chain/off-chain) is assessed.

The findings of the study demonstrate that transnational financial fraud committed through the use of crypto-assets represents a model of "decentralized crime," in which the classical logic of territorial jurisdiction is disrupted, and the elements of conduct, result, and control are distributed across multiple jurisdictions. All of the above significantly complicates effective legal responses to such crimes. The traditional model of territorial jurisdiction

[1] Corresponding author.
E-mail addresses: tamta.tsirkvadze@ciu.edu.ge (T. Tsirkvadze).
ORCID: https://orcid.org/0009-0006-3275-2583

Received: 08/04/2026 Revised: 30/06/2026 Accepted: 20/07/2026 Published: 23/07/2026
E-ISSN 2720-8036 / © 2026 The Author(s). Published in The International Journal of Social Sciences by Caucasus International University.
This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/)

cannot fully ensure either the collection of evidence or the freezing of crypto-assets, while the existing mechanisms of international cooperation (MLA) are not sufficiently sophisticated to match the speed at which blockchain technologies operate.

From a criminal law perspective, the paper analyzes how territorial jurisdiction should be determined in cases of transnational crypto fraud and what reforms are necessary to ensure effective criminal prosecution without violating fundamental human rights. Effective responses to crypto crimes require the introduction of “digital territoriality,” under which priority in determining jurisdiction would be given to the state that has the greatest practical capacity to access evidence, control assets, and apply other procedural mechanisms.

ტრანსნაციონალური ფინანსური თაღლითობა და კრიპტოაქტივები: იურისდიქციის პრობლემები საერთაშორისო სისხლის სამართალში

თამთა წირქვაძე [a2]

[a] სამართლის დოქტორი, ასოცირებული პროფესორი,
კავკასიის საერთაშორისო უნივერსიტეტი

სტატიის შესახებ

საკვანძო სიტყვები:

კრიპტოაქტივები

ბლოკჩეინი

ტრანსნაციონალური ფინანსური თაღლითობა

ტერიტორიული განსჯადობა

იურისდიქციის კონფლიქტები

აბსტრაქტი

ციფრული სამყაროს ეპოქაში მნიშვნელოვან გამოწვევას წარმოადგენს ტრანსნაციონალური დანაშაულების გამოძიების საკითხი, ვინაიდან კრიპტოაქტივებზე დაფუძნებულმა ეკოსისტემამ მნიშვნელოვნად შეცვალა აღნიშნული დანაშაულების ბუნება და იურისდიქციული ლოგიკა. ნაშრომის მიზანია გააანალიზოს, თუ რამდენად ეფექტურად პასუხობს კრიპტო-თაღლითობებს საერთაშორისო სისხლის სამართლის მოქმედი დოქტრინა (ტერიტორიულობა, მოქალაქეობის პრინციპები, ეფექტის დოქტრინა) და რა რეფორმებია საჭირო სამართლებრივი სისტემის ტექნოლოგიურ გამოწვევებთან ადაპტაციისათვის.

ნაშრომში გამოყენებულია დოქტრინალური, შედარებით-სამართლებრივი და პრაქტიკული ანალიზის კვლევის მეთოდები. განხილულია ისეთი საერთაშორისო ინსტრუმენტები, როგორებიცაა ბუდაპეშტის კონვენცია, FATF სტანდარტები, MiCA რეგულაცია, ასევე საქართველოში მოქმედი სამართლებრივი და ინსტიტუციური პრაქტიკა. გაანალიზებულია კრიპტო-თაღლითობის ტიპოლოგია, გამოყენებულია იურისდიქციული კავშირების რუკირების მეთოდი და შეფასებულია ჰიბრიდული მტკიცებულებითი მოდელი (on-chain/off-chain).

კვლევის შედეგები ცხადყოფს, რომ კრიპტოაქტივების გამოყენებით ჩადენილი ტრანსნაციონალური ფინანსური თაღლითობა წარმოადგენს „დეცენტრალიზებული დანაშაულის“ მოდელს, სადაც ირღვევა კლასიკური ტერიტორიული იურისდიქციის ლოგიკა და ქმედების, შედეგისა და კონტროლის ელემენტები ნაწილდება სხვადასხვა ქვეყნის იურისდიქციაში. ყოველივე ზემოაღნიშნული მნიშვნელოვნად ართულებს დანაშაულზე ეფექტიან სამართლებრივ რეაგირებას. ტრადიციული ტერიტორიული იურისდიქციის მოდელი სრულფასოვნად ვერ უზრუნველყოფს ვერც მტკიცებულებების მოპოვებას და ვერც კრიპტო აქტივების გაყინვას, ხოლო საერთაშორისო თანამშრომლობის არსებული მექანიზმები (MLA), არ არის იმდენად დახვეწილი, რომ უპასუხოს ბლოკჩეინ ტექნოლოგიების მუშაობის სისწრაფეს.

[2] Corresponding author.
E-mail addresses: tamta.tsirkvadze@ciu.edu.ge (თ. წირქვაძე)
ORCID: https://orcid.org/0009-0006-3275-2583

ნაშრომში, სისხლის სამართლებრივი პერსპექტივიდან გაანალიზებულია ის, თუ როგორ უნდა გადაწყდეს ტერიტორიული განსჯადობა ტრანსნაციონალური კრიპტო-თაღლითობების დროს და რა რეფორმებია საჭირო ეფექტური სისხლისსამართლებრივი დევნის განსახორციელებლად, ისე, რომ არ დაირღვეს ადამიანის ფუნდამენტრი უფლებები. კრიპტო დანაშაულებზე ეფექტური რეაგირება საჭიროებს „ციფრული ტერიტორიულობის“ დანერგვას, რომელიც იურისდიქციის განსაზღვრისას უპირატესობას მიანიჭებს იმ ქვეყნის იურისდიქციის გამოყენებას, რომელსაც მეტად აქვს მტკიცებულებებზე წვდომის, აქტივების კონტროლისა და სხვა პროცესუალური მექანიზმების გამოყენების საშუალება.

1. Introduction

The rapid integration of crypto-assets into the financial market has created a paradox: technology has simplified financial operations, but has complicated the localization of legal responsibility. The classical criminal law response to crime has historically relied on the unity of two “pillars” — (a) the territorial connection of the act or its result, and (b) the practical ability of the state to exercise coercive power. In fraud based on crypto-assets, these two components often extend beyond the boundaries of a single state: the perpetrator, the victim, the infrastructure (exchanges, hosting, nodes), the circulation of assets, and the result may fall within several jurisdictions. As a result, legal response becomes dependent on cooperation, the speed of evidence gathering, and functional criteria for the choice of jurisdiction (Houben & Snyers, 2018; Zetzsche et al., 2019).

The research question of the paper is to what extent the existing jurisdictional doctrine of international criminal law (territoriality, active/passive nationality, protective principle, etc.) ensures an effective response to transnational financial fraud committed through crypto-assets, and what reforms are necessary for the legal system to adapt to a decentralized environment.

For the purposes of this paper, the term “international criminal law” is used in its broad sense. It is not confined only to the core international crimes, namely genocide, crimes against humanity, war crimes, and the crime of aggression, but also encompasses elements of transnational criminal law, including matters of inter-state cooperation.

2. Literature Review

The literature addresses distinct dimensions of crypto-assets that should not be conflated. Baur et al. (2018) examine Bitcoin's use as an investment asset, whereas Foley et al. (2019) investigate illicit activity using transaction data. These studies inform the economic and empirical context; neither establishes a rule allocating criminal jurisdiction. Zetzsche et al. (2019) analyse the regulatory challenges of initial

coin offerings, while Houben and Snyers (2018) examine the legal implications of cryptocurrencies for financial crime.

Institutional sources address the relationship between prevention and investigation. The Financial Action Task Force (FATF, 2021) focuses on risk-based supervision of virtual asset service providers (VASPs). MiCA regulates defined crypto-asset activities and service providers within its scope (European Union, 2023). The Budapest Convention provides procedural and cooperation mechanisms for electronic evidence (Council of Europe, 2001). These instruments perform complementary functions, but regulatory status does not itself confer authority to prosecute or compel disclosure abroad.

Eurojust (2016) already identifies the location of criminality and loss, the suspect's location, access to evidence and victims' interests as considerations in selecting a prosecuting forum. The research gap is therefore not the absence of coordination criteria. It concerns their application where ledger information, identity records and control over assets lie with different actors in different states.

This article connects those dimensions through a qualitative sequence: establish legal competence, identify the authorities able to execute particular measures, and justify the allocation of the prosecution. Its contribution is an adaptation of existing coordination principles to crypto-asset fraud, with separate attention to evidentiary access and asset control. It does not claim that technical capacity can replace a lawful jurisdictional connection.

3. Materials and Methods

The study employs doctrinal legal analysis and functional comparative analysis. The documentary corpus comprises the international instruments, regulatory materials, academic publications and official case reports cited in the article. Contemporary sources extend through 2025, alongside historical jurisdictional authority. Selection is purposive and based on relevance to criminal jurisdiction, attribution, electronic evidence, asset restraint and cooperation. The review is thematic rather than an exhaustive systematic survey.

Doctrinal analysis distinguishes the authority to prescribe criminal rules, adjudicate alleged offences and execute enforcement measures. Treaty provisions and legislation are examined separately from supervisory guidance and institutional recommendations. The comparative inquiry considers the function of each framework: preventive oversight under FATF guidance and VASP regulation, market governance under MiCA, and cooperation concerning electronic evidence under the Budapest Convention. Georgian criminal-law provisions and regulatory materials supply the national context.

The proposed coordination framework is evaluated qualitatively against the location of conduct and harm, access to suspects and evidence, practical control over assets, and procedural safeguards. Eurojust's 2016 guidelines provide the reference point for forum allocation. The analysis then distinguishes decisions about the main prosecution from decisions about individual assistance measures. No numerical weighting is assigned to these factors, since their legal relevance and operational significance depend on the circumstances of the case.

Two official case reports illustrate different stages of enforcement: Eurojust's account of the November 2022 investment-fraud operation involving Georgia, and the Crown Prosecution Service's January 2025 report of confiscation orders following convictions connected with an Australian cryptocurrency exchange. These are institutional accounts, not substitutes for the full judgments or case files. Allegations, convictions and recovery orders are distinguished, and the examples are not used to infer general success rates.

The study does not include interviews, confidential investigative records or quantitative measurement. Its conclusions are doctrinal and institutional, subject to the selective source base and the limits of public reporting. The hypothetical application below tests the internal coherence of the proposed framework rather than its empirical effectiveness. Legality, proportionality and the ability to contest evidence and restrictive measures form constraints on the framework, rather than factors that may be displaced by operational convenience.

4. Discussion of Findings

The findings demonstrate that crypto-asset fraud operates as a model of decentralized crime in which conduct, harm, infrastructure, and control may be divided among several states. As a result, classical territorial jurisdiction remains important but is insufficient when applied only through formal territorial links.

The article therefore supports a functional approach to jurisdiction. Priority should be given to the state that can most effectively obtain evidence, preserve or freeze assets, coordinate with service providers, and ensure that criminal prosecution is conducted without violating fundamental rights.

4.1. Transnational Financial Fraud in the Crypto-Ecosystem

Transnational financial fraud, in the classical sense, refers to obtaining financial benefit through deception in such a way that the essential elements of the crime are connected to more than one state. The perpetrator may operate from the territory of one country, the victim may be located in another country, while the transfer of financial assets may take place within the jurisdiction of a third state.

As for transnational financial fraud committed through the use of crypto-assets, it additionally creates new dimensions in terms of the typology of crime. These dimensions include the decentralization of jurisdiction, the pseudonymity of offenders, and financial instruments based on algorithms (Houben & Snyers, 2018; Europol, 2022).

Common models of crypto-fraud include:

1. **Investment fraud.** Under such schemes, victims are offered high-yield returns on crypto investments; however, in reality, instead of being placed into an investment fund, the invested money is transferred directly into electronic wallets controlled by the offenders.

2. **OTC or escrow fraud.** In such cases, the perpetrator presents themselves as an intermediary in a crypto transaction and ultimately misappropriates the funds.

3. **Phishing and account takeovers.** Offenders gain access to crypto wallets or exchange accounts and subsequently transfer the assets.

4. **DeFi fraud.** In decentralized finance, manipulation of smart contracts often occurs, whereby project creators misappropriate investors' funds.

In risk analysis, it is important to emphasize that crypto-assets are not merely "anonymous money"; in fact, transactions on the blockchain are visible, while identity is not. This creates a situation in which law enforcement authorities must carry out a complex chain of "de-anonymization": through coordinated use of on-chain analysis, off-chain data (exchange KYC, IP logs, device identifiers), and international requests. It is precisely here that the practical importance of jurisdictional choice arises: which state is able to obtain data most rapidly, apply provisional measures, or block the movement of assets (Foley et al., 2019; Europol, 2022).

4.2. Criminal Law Analysis of Crypto-Fraud

4.2.1. Doctrinal Foundations of Jurisdiction and Their Transformation in the Digital Space

In criminal law, the determination of jurisdiction has traditionally been based primarily on the principle of territoriality, since this principle protects state sovereignty while simultaneously granting law enforcement authorities a real opportunity to respond to crime and conduct the relevant investigation. However, in the case of crypto-transactions, the situation becomes more complex, and the specific location of the criminal act is no longer easily identifiable. A single financial operation may simultaneously be connected to several states. The offender may be located in one country, the exchange or service provider may be registered in another, servers and blockchain nodes may be situated in a third, harm may be suffered by a citizen of a fourth state, while actual control over the misappropriated financial assets may fall within yet another jurisdiction.

In such circumstances, the classical principle of territoriality often transforms in practice into "functional territoriality." This means that priority is given to the jurisdiction of the state that is genuinely capable of obtaining evidence quickly, restricting or controlling assets, and taking effective legal measures against the responsible persons. (Eurojust, 2016; Zetzsche et al., 2019)

The Lotus case (1927) generally recognized that a state enjoys broad discretion in determining jurisdiction, provided that international law does not prohibit it in the particular circumstances (PCIJ, 1927). In the context of digital reality, this approach may be applied by analogy where several states simultaneously claim jurisdiction on the basis of the victim's location, the offender's location, or the place where the harmful result occurred. Such situations create competing jurisdictional claims and often lead to parallel or duplicated investigations. In many cases, however, the opposite problem arises: a legal vacuum is created in which no state initiates an effective investigation, or states avoid taking responsibility for opening one at all.

The active nationality principle allows a state to respond to crimes committed abroad by its own nationals, while the passive nationality principle enables a state to protect its citizens against crimes committed in foreign countries. However, in cases of crypto fraud, we often encounter what may be described as "digital distance," where those involved in the offence are nationals of different countries

acting in an organized manner, while victims are simultaneously located across dozens of states. In such circumstances, reliance on nationality principles alone is no longer sufficient, as they cannot ensure a coherent and effective investigation of the case. In situations like these, there is a clear need for a coordination mechanism capable of determining which country should exercise the role of lead jurisdiction during the investigative process, how the case should be allocated among the different states involved, how parallel and uncoordinated investigations should be avoided, and under what common standards evidence should be collected and shared among the competent authorities. (Eurojust, 2016) In modern practice, the "effects" approach is widely recognized, according to which jurisdiction belongs to the state where the substantial result of the offence occurred. In cases of crypto fraud, this issue becomes more complex, as the harm is often spread simultaneously across several countries. For this reason, particular attention is given to the "center of gravity" of the harm, that is, the place where the offence had its most significant impact. This may be the country where the greatest financial loss was suffered, where a large number of victims are located, or from where the main part of the fraudulent communications was carried out.

4.2.2. Evidence, Attribution, and Procedural Challenges in the Investigation of Crypto-Fraud

The investigation of crypto-related crime is rarely a purely technical matter; in reality, it is one of the most difficult tests of jurisdiction and international cooperation. The first important stage is attribution, namely linking a specific wallet or address to a real individual. In practice, this is usually done through a combination of two methods. On the one hand, investigators rely on on-chain analysis, such as tracing transaction flows, clustering addresses, analyzing chains of transfers, and identifying mixing services. On the other hand, off-chain information is also required, including KYC documentation, login records, IP data, and other metadata. This is where the first serious difficulty arises: the relevant information is often held by foreign service providers, disclosure rules vary from one jurisdiction to another, and time is critically important, since in the digital environment assets can be moved very quickly (Europol, 2022).

The second problem is that traditional investigative procedures often cannot keep pace with the speed of blockchain systems. Classical Mutual Legal Assistance (MLA) requests may take weeks or even months, whereas crypto-assets can be transferred from one address to another within minutes. For this reason, rapid cooperation mechanisms are particularly important, including 24/7 contact networks, emergency communication channels, and pre-agreed forms that allow essential information to be transmitted immediately upon request, even before the formal letter of request is sent. This practical need is addressed by the Budapest Convention, which provides for a 24/7 network mechanism under Article 35.

The third issue concerns the temporary freezing of assets and their subsequent confiscation. Where the case involves a custodial exchange, in which the platform controls the user's assets, suspending an account or address is relatively realistic. However, in a non-custodial DeFi environment, such intervention is often impossible. As a result, one of the key current questions is how the concept of "control" should be interpreted and who should bear responsibility for parts of the infrastructure where genuine governance exists, such as front-end platforms, administrative keys, or oracles.

Mutual Legal Assistance (MLA) remains the principal legal instrument for obtaining evidence and tracing assets. However, in crypto-related cases its effectiveness largely depends on how quickly the

request is sent, whether the format is standardized, and where the relevant data is located — whether in the country of the exchange's registration, the server location, or another jurisdiction. The Budapest Convention is intended to simplify this process by creating a procedural framework for the rapid collection of electronic evidence, subject to its conditions and safeguards (Council of Europe, 2001).

In cases of transnational fraud, extradition also frequently becomes an issue. In relation to crypto-assets, however, problems of dual criminality often arise. The same conduct may be classified in one country as financial fraud, in another as money laundering, in a third as a cybercrime, and elsewhere under a completely different legal category. For that reason, extradition requests should be based not only on legal terminology, but also on the factual core of the conduct, so that a corresponding legal basis exists in both jurisdictions.

European practice shows that the most effective model is the so-called lead jurisdiction, where one country directs the main investigation while other states provide rapid assistance. They may supply evidence, carry out searches, conduct interviews, or implement asset-freezing measures. Eurojust has repeatedly emphasized in its reports that such coordination is particularly decisive in cases involving crypto-assets, where simultaneous action in several countries is often required. (Eurojust, 2016).

The FATF's updated guidance (2021) and "travel rule" practices emphasize that VASPs must be licensed/registered and must implement AML/CFT controls to reduce the misuse of cryptoassets. (Financial Action Task Force (FATF, 2021; Council of Europe, 2001). These standards are particularly important in transnational fraud, as they create an "infrastructure" for data availability for law enforcement purposes.

The EU Markets in Crypto-Assets Regulation (MiCA) creates a single set of rules for the crypto-asset market, including the supervision of service providers (CASPs) and requirements for white papers. MiCA aims to ensure market transparency, protect consumers and reduce systemic risks, and, in a jurisdictional context, to reduce forum shopping through a "single rulebook". (European Union, 2023; European Securities and Markets Authority, nd) The gradual implementation of MiCA (including the application of ART/EMT provisions from mid-2024) shows that the regulation is trying to adapt quickly to market dynamics . (European Banking Authority, 2024) However, MiCA cannot solve a global problem: if part of the crypto-infrastructure is located outside the EU, international cooperation is still needed. MiCA should therefore be considered as a "regional harmonization model" that can influence other jurisdictions (e.g., export of compliance requirements due to market weight), but cannot replace the international conventional level.

Crypto-fraud investigations often require intensive intrusions into private life: monitoring communications, examining devices, requesting data from providers. It is important to balance two parallel goals: effective investigation and protection of human rights. Article 6 of the European Convention protects the right to a fair trial, while Article 8 protects the right to privacy; therefore, the collection of data must be lawful, necessary and proportionate. (Council of Europe, 1950, Articles 6 and 8).

The freezing/confiscation of crypto-assets raises issues related to property rights (First Additional Protocol). The proportionality test requires: (a) a legal basis; (b) a legitimate aim; (c) necessity and an assessment of a less restrictive alternative; and (d) the protection of the individual balance. In practice, this means that the decision to freeze must be justified by the degree of nexus of the asset and the future prospects of confiscation, while the bona fide interests of third parties (e.g. joint accounts, liquidity of the business) must be assessed.

The Crown Prosecution Service reported on 17 January 2025 that three convicted defendants were ordered to pay more than £23.6 million following fraud and laundering connected with an Australian cryptocurrency exchange. The underlying convictions included proceedings at Preston Crown Court in 2023 (Crown Prosecution Service, 2025). This example shows that crypto-related cross-border conduct can lead to prosecution and confiscation under existing law. It does not establish a general recovery rate or prove that the full ordered amount was collected; the report is an institutional account rather than a published judicial determination of a new jurisdictional doctrine.

4.3. Legal and Institutional Practice of Georgia: Regulation, Investigation, and Challenges

The regulation of virtual asset service providers in Georgia is linked to the AML/CFT framework. The National Bank of Georgia (NBG) implements mandatory registration, supervision and sanctioning mechanisms for VASPs. (National Bank of Georgia, 2023; National Bank of Georgia, 2025) This practice is of crucial importance from a jurisdictional perspective, since when a VASP is registered in Georgia, law enforcement authorities have faster access to the data necessary for the investigation, while supervisory bodies gain leverage to enforce compliance.

The regulation approved by the National Bank of Georgia in 2024 concerning the determination and enforcement of financial penalties against VASPs demonstrates that regulators are prepared to apply proportionate and effective sanctions while taking into account the specific risks of the sector (National Bank of Georgia, 2024; NBG, 2025). These steps are highly significant for the prevention of transnational fraud, as inter-agency practice often begins precisely with warning signals issued by the regulator.

A concrete cooperation example is Eurojust's report of the operation on 8–9 November 2022 against an alleged investment-fraud network involving cryptocurrencies. Across the participating states, 15 call centres were searched and five suspects arrested; five of the call centres and one arrest were in Georgia (Eurojust, 2022). Eurojust supported judicial coordination and assistance requests. The report demonstrates Georgia's participation in a coordinated operation, but it does not establish guilt or identify the eventual forum and outcome for every suspect. It therefore supports a limited conclusion about cooperation rather than a general claim about national enforcement effectiveness.

In Georgian crypto-fraud cases, the most common problem is operational cooperation with foreign exchanges and achieving a quick freeze. Working with custodial infrastructure requires MLA requirements or direct operational communication (fast contact channels), while in a non-custodial environment, the investigation depends on on-chain analysis and subsequent procedural actions after the identification of the perpetrator. Therefore, the practical recommendation is: (a) strengthening specialized digital asset units in investigative bodies; (b) pre-agreed memorandums of cooperation with critical

VASPs; (c) active use of the mechanisms of the Budapest Convention; and (d) introduction of “fast” tools for the protection of evidence (e.g., preservation orders).

5. Conclusion

The crypto-asset ecosystem has created a reality of “decentralized crime”, where classical jurisdiction often loses its power and becomes formal. In such a situation, an effective response requires doctrinal flexibility (“functional/digital territoriality”), coordination between institutions (MLA + 24/7 + lead jurisdiction) and regulatory harmonization (FATF, MiCA). In relation to the above issues, the VASP supervision of the National Bank and the active use of international instruments play an important role in Georgia, although the in-depth specialization of personnel and the consolidation of international judicial practice remain a problem.

Through the application of the concept of “digital territoriality” proposed in this paper, it becomes possible, in each individual case, to identify the most effective jurisdiction. Jurisdiction should be granted to the state that has the greatest capacity to obtain evidence rapidly, is able to impose temporary restrictions or freezing measures on financial assets, possesses regulatory leverage over critical technological infrastructure, and where a significant proportion of the victims fall within its jurisdiction - in other words, the country that constitutes the central locus of harm. This approach does not undermine the principles of classical jurisdiction, but ensures their compliance with technological reality. An effective response to crypto crimes is possible only if the determination of jurisdiction is based on functional criteria, and not only on formal territorial connection. The model of “digital territoriality” in this direction represents an important doctrinal development that combines access to evidence, control of assets and procedural efficiency.

Despite the instruments currently in place (UNTOC Rules of Engagement, Budapest Convention, FATF Standards), crypto-fraud requires more concrete norms, such as: a common standard for quick freeze, minimum rules for confiscation of digital assets, a framework for the exchange of information between VASPs, and the harmonization of digital forms of evidence.

As for Georgia, in order to improve the current situation in the fight against the above-mentioned crimes, it is important to strengthen VASP supervision, using a risk-based approach. Specialization and continuous retraining of employees of investigative bodies are necessary. It is also necessary to transfer international coordination mechanisms to operational channels and develop judicial practice in the direction of qualification, seizure and confiscation of crypto-assets.

Finally, the fight against crypto-crime is not only a technical or legal issue. It is a test of the fundamental legal system's ability to adapt to the realities of the digital age. To pass this test successfully, doctrinal innovation, institutional flexibility, and the maintenance of clear standards for the protection of human rights are essential.

The statement regarding the usage of AI: Artificial intelligence (AI) tools were used solely for language editing, stylistic refinement, and improving the clarity and readability of the manuscript. Specifically, OpenAI's ChatGPT was utilized to assist with grammar correction, sentence structure improvement, and enhancement of academic writing style. I have reviewed, verified, and take full responsibility for all content, interpretations, analyses, and conclusions presented in this article.

Funding: This research received no external funding.

Conflict of Interests: There is no conflict of interest regarding this study.

References

1. Baur, D. G., Hong, K., & Lee, A. D. (2018). Bitcoin: Medium or speculative? *Journal of International Financial Markets, Institutions and Money*, *54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004
2. Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*, Articles 6 and 8. Retrieved from www.echr.coe.int
3. Council of Europe. (1952). *Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms*, Article 1. Retrieved from www.echr.coe.int
4. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*.
5. Crown Prosecution Service. (2025, January 17). *Money launderers ordered to pay back over £23m in a high value cryptocurrency scam*. Retrieved from www.cps.gov.uk
6. Eurojust. (2016). *Guidelines for deciding 'Which jurisdiction should prosecute?'*
7. Eurojust. (2022, November 10). *Eurojust coordinates action against massive investment fraud with hundreds of thousands of victims worldwide*. Retrieved from www.eurojust.europa.eu
8. European Banking Authority. (2024). *MiCA implementation statements*.
9. European Securities and Markets Authority. (n.d.). *Markets in Crypto-Assets Regulation (MiCA)*. Retrieved from www.esma.europa.eu
10. European Union. (2023). *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets*. *Official Journal of the European Union*, L 150, 40–205. Retrieved from eur-lex.europa.eu
11. Europol. (2022). *Cryptocurrencies: Tracing the evolution of criminal finances*. Europol Spotlight Report series. Publications Office of the European Union. Retrieved from www.europol.europa.eu
12. Financial Action Task Force. (2021). *Updated guidance for a risk-based approach to virtual assets and VASPs*. Retrieved from www.fatf-gafi.org
13. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, *32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015
14. Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*. European Parliament. https://doi.org/10.2861/263175
15. National Bank of Georgia. (2023). *Rule on Registration of Virtual Asset Service Providers*.
16. National Bank of Georgia. (2024). *Regulation on Sanctions for VASPs*.
17. National Bank of Georgia. (2025). *National Bank of Georgia urges citizens not to engage in virtual asset services with unregistered entities*. Retrieved from nbg.gov.ge
18. Permanent Court of International Justice. (1927). *The Case of the S.S. Lotus (France v. Turkey)*, Series A No. 10.
19. United Nations. (2000). *United Nations Convention against Transnational Organized Crime*, Annex I to General Assembly Resolution 55/25, Articles 3 and 15–19. Retrieved from mandates.un.org
20. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2019). *The ICO gold rush*. *Journal of Banking Regulation*, *60*(2), 267–315. Retrieved from hdl.handle.net