

LEGAL MECHANISMS FOR RESOLVING JURISDICTIONAL CONFLICTS IN INTERNATIONAL DIGITAL MONEY TRANSACTIONS

 <https://doi.org/10.52340/26679434/H.13.2>

Nino Jolia

PhD in Economics, PhD student at the Faculty of Law at Caucasus International University, Assistant and Invited Lecturer at the Faculty of Law at Caucasus International University, Invited Lecturer at the Faculty of Business and Technology at Caucasus International University, Georgia, Tbilisi

E-mail: nino.jolia@ciu.edu.ge

ORCID: ID <https://orcid.org/0009-0009-1454-650X>

ABSTRACT

The article analyses the cross-border legal challenges arising from the use of digital money and crypto-assets, as well as the possible legal mechanisms for addressing them. The central thesis of the article is that the classical instruments of private international law remain relevant but are insufficient where a transaction is carried out through a distributed ledger, a smart contract, or a virtual asset service provider. The research examines the absence of a uniform legal standard for digital money, the cross-border nature of blockchain-based transactions, the uneven implementation of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) mechanisms, issues of legal liability in cybersecurity, and the regulatory challenges associated with central bank digital currencies and stablecoins. Particular attention is given to challenges relevant to Georgian law, including the supervision of virtual asset service providers and the coordination of financial regulation, data protection, and anti-money laundering mechanisms. The article concludes that resolving legal conflicts in the field of digital money is not limited to determining the applicable law. It requires an interconnected assessment of legal classification, supervision, data protection, Anti-Money Laundering and Countering the Financing of Terrorism requirements, and financial stability. Accordingly, effective regulation should be based on a harmonized, risk-based, and technologically appropriate legal framework.

Keywords: Blockchain, Regulatory harmonization, Stablecoin, Cybersecurity, Cross-border payments, Decentralized liability

შესავალი

ციფრული ფულის სამართლებრივი რეგულირება თანამედროვე ფინანსური სამართლის ერთ-ერთ ყველაზე დინამიკურ მიმართულებად ჩამოყალიბდა. ბლოკჩეინის ინფრასტრუქტურა, ვირტუალური აქტივების გლობალური ბრუნვა, ციფრული გადახდის სერვისები, სტიბლკოინები და ცენტრალური ბანკის ციფრული ვალუტების განვითარების პერსპექტივა ტრადიციულ სამართლებრივ კატეგორიებს ახალ კონტექსტში აყენებს. სამართალი, რომელიც ისტორიულად ეფუძნებოდა ტერიტორიულობის პრინციპს, რეგულირებული სუბიექტის იდენტიფიცირებასა და ცენტრალიზებული ფინანსური შუამავლის არსებობას, დღეს ფუნქციონირებს არსებითად განსხვავებულ ტექნოლოგიურ გარემოში. ასეთ გარემოში ტრანზაქცია შესაძლოა, ერთდროულად უკავშირდებოდეს რამდენიმე იურისდიქციას, ხოლო მისი განხორციელებისთვის გამოყენებული ტექნოლოგიური ინფრასტრუქტურა არ იყოს მკაფიოდ მიბმული რომელიმე კონკრეტული სახელმწიფოს ტერიტორიასთან ან სამართლებრივ წესრიგთან.

წინამდებარე სტატიის მიზანია ციფრული ფულის საერთაშორისო ტრანზაქციებში წარმოშობილი იურისდიქციული კოლიზიების გადაწყვეტის სამართლებრივი მექანიზმების ანალიზი. „იურისდიქციული კოლიზია“ მოცემულ კონტექსტში არ განიხილება მხოლოდ ვიწრო პროცესუალური მნიშვნელობით, როგორც სასამართლოს კომპეტენციის ან განსჯადობის საკითხი. ციფრული ფულის სფეროში იგი წარმოადგენს მრავალმხრივ სამართლებრივ პრობლემას, რომელიც მოიცავს როგორც გამოსაყენებელი სამართლისა და მარეგულირებელი რეჟიმის განსაზღვრას, ისე ზედამხედველობის, ლიცენზირების, ფინანსური მონიტორინგისა და მომხმარებელთა დაცვის საკითხებს.

კერძოდ, იურისდიქციული კოლიზია აჩენს კითხვებს, თუ რომელი სახელმწიფოს მარეგულირებელი ჩარჩო უნდა გავრცელდეს კონკრეტულ ტრანზაქციაზე; რომელ ორგანოს უნდა ჰქონდეს ზედამხედველობის განხორციელების უფლებამოსილება; სად უნდა დარეგისტრირდეს ან მოიპოვოს ლიცენზია მომსახურების პროვაიდერმა; რომელი ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სტანდარტებს უნდა დაექვემდებაროს ტრანზაქცია; როგორ უნდა დაბალანსდეს ფინანსური მონიტორინგის მოთხოვნები პერსონალურ მონაცემთა დაცვის ვალდებულებებთან; და რა მექანიზმებით უნდა იყოს უზრუნველყოფილი მომხმარებლის ან ინვესტორის დაცვა იმ შემთხვევაში, როდესაც მომსახურების გაწევა ფაქტობრივად საზღვრებს მიღმა ხორციელდება.

კვლევის აქტუალობა განპირობებულია რეგულირების ფრაგმენტულობით. ციფრული ფულის სამართლებრივი სტატუსი სხვადასხვა იურისდიქციაში არაერთგვაროვანია: ერთ სისტემაში იგი შეიძლება აღიქმებოდეს როგორც გადახდის საშუალება, მეორეში – როგორც საინვესტიციო აქტივი, მესამეში – როგორც ვირტუალური აქტივი ან კერძო ციფრული ფული. აღნიშნულ არაერთგვაროვნებას ემატება ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის, კიბერუსაფრთხოების, მონაცემთა დაცვისა და მომხმარებელთა დაცვის განსხვავებული მოთხოვნები. შედეგად, იურისდიქციული კოლიზია არ არის მხოლოდ თეორიული პრობლემა; იგი ქმნის პრაქტიკულ რისკებს ზედამხედველობის, აღსრულების, მომხმარებლის დაცვისა და ფინანსური სტაბილურობისთვის.

სტატიის მეთოდოლოგიურ საფუძველს წარმოადგენს სისტემური, შედარებითი და ფუნქციური ანალიზი. სისტემური მიდგომა საჭიროა იმისთვის,

რომ ციფრული ფული შეფასდეს როგორც ფინანსური, ტექნოლოგიური და სამართლებრივი ფენომენი. შედარებითი ანალიზი ავლენს, თუ როგორ ცდილობენ საერთაშორისო და რეგიონული სტანდარტები იურისდიქციული ფრაგმენტაციის შემცირებას. ფუნქციური ანალიზი კი საშუალებას იძლევა, აქტივი შეფასდეს მისი ეკონომიკური და სამართლებრივი ფუნქციის მიხედვით და არა მხოლოდ ტექნოლოგიური ფორმით. სტატიის ძირითადი თეზისია, რომ ციფრული ფულის საერთაშორისო ტრანზაქციებში იურისდიქციული კოლიზიების გადაწყვეტა მოითხოვს მრავალმრიან მოდელს: აქტივის ფუნქციურ კლასიფიკაციას, ვირტუალური აქტივის მომსახურების პროვაიდერების (VASP) იდენტიფიკაციას, ფულის გათვრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სტანდარტების ჰარმონიზაციას, კიბერუსაფრთხოებისა და მონაცემთა დაცვის მოთხოვნების ინტეგრაციას და ეროვნული ზედამხედველობის საერთაშორისო კოორდინაციას.

1. ციფრული ფულის სამართლებრივი ბუნება და იურისდიქციული კოლიზიის წარმოშობის საფუძველი

ციფრული ფულის სამართლებრივი ბუნება იურისდიქციული კოლიზიის საწყის წერტილს წარმოადგენს. ტრადიციული ფული, როგორც წესი, დაკავშირებულია სახელმწიფოს სუვერენულ

უფლებამოსილებასთან, ცენტრალურ ბანკთან, საბანკო ინფრასტრუქტურასთან და ტერიტორიულად განსაზღვრულ გადახდის სისტემებთან. ციფრული ფული და ვირტუალური აქტივები კი ხშირად ფუნქციონირებენ დეცენტრალიზებულ ინფრასტრუქტურაზე, რომელიც არ ემთხვევა სახელმწიფო საზღვრებს. ბლოკჩეინი ხასიათდება ტრანზაქციების გამჭვირვალობით, უცვლელობითა და განაწილებული ჩანაწერის სისტემით, თუმცა, სწორედ ეს მახასიათებლები ქმნის კლასიკური რეგულირების შეზღუდვებს.¹

ციფრული ფულის სამართლებრივი შეფასება რთულდება მისი ფუნქციური მრავალფეროვნებით. ერთი და იგივე ციფრული აქტივი შეიძლება გამოყენებულ იქნეს ანგარიშსწორებისთვის, საინვესტიციო მიზნებისთვის, ღირებულების შესანახად ან სავაჭრო ოპერაციებისთვის. თუ აქტივი გადახდის საშუალებად გამოიყენება, სამართლებრივი შეფასების ცენტრალურ საკითხებად გადახდის უსაფრთხოება, მომხმარებელთა დაცვის უზრუნველყოფა და AML/CFT კონტროლის მექანიზმები გამოდის. თუ იგი გამოიყენება საინვესტიციო მიზნებისთვის, აქტუალური ხდება ინვესტორის დაცვა, ინფორმაციის გამჭვირება და ბაზრის ზედამხედველობა. თუ აქტივი მიბმულია ფიატ ვალუტაზე ან სხვა აქტივებზე, მისი რეგულირება უახლოვდება სტეიბლკოინის პრობლემატიკას, სადაც ცენტრალური საკითხებია რეზერვები, გამოსყიდვის უფლება, ლიკვიდობა და ფინანსური სტაბილურობა.²

1 Al Mashhour, O.F., Abd Aziz, A.S. and Mohd Noor, N.A., 2022. Blockchain and its Entire Eco-System: A Legal Consideration to an International Cross-Border Technology. International Journal of Multidisciplinary Sciences and Advanced Technology, 3(3), გვ. 15. [ინტერნეტი] ხელმისაწვდომია: https://www.researchgate.net/publication/363645357_Blockchain_and_its_Entire_Eco-System_A_Legal_Consideration_to_an_International_Cross-Border_Technology [წვდომის თარიღი 15.05.2026].

2 Gorton, G.B. and Zhang, J.Y., 2023. Taming Wildcat Stablecoins. University of Chicago Law Review, 90(3), გვ. 909. [ინტერნეტი] ხელმისაწვდომია: <https://chicagounbound.uchicago.edu/uclrev/vol90/iss3/3/> [წვდომის თარიღი 15.05.2026].

სწორედ ეს ფუნქციური მრავალფეროვნება წარმოშობს იურისდიქციულ კოლიზიას. ერთი ტრანზაქცია შეიძლება ერთდროულად დაექვემდებაროს რამდენიმე სამართლებრივ რეჟიმს: გადახდის მომსახურების წესებს, ვირტუალური აქტივების რეგულირებას, AML/CFT სტანდარტებს, მონაცემთა დაცვის მოთხოვნებს და მომხმარებელთა დაცვის ნორმებს. ამასთან, სხვადასხვა სახელმწიფო ერთსა და იმავე აქტივს განსხვავებულად აფასებს. თუ ერთი იურისდიქცია მას გადახდის ინსტრუმენტად მიიჩნევს, ხოლო მეორე – საინვესტიციო პროდუქტად, ტრანზაქციის მონაწილეები დგანან სამართლებრივი გაურკვევლობის წინაშე.

კოლიზიის გადაწყვეტის პირველი მექანიზმი უნდა იყოს ფუნქციური კლასიფიკაცია. სამართალმა ციფრული ფული უნდა შეაფასოს არა მხოლოდ ტექნოლოგიური ფორმით, არამედ მისი რეალური ეკონომიკური ფუნქციით. ასეთი მიდგომა ამცირებს ფორმალურ გაურკვევლობას და ეხმარება მარეგულირებელს განსაზღვროს, რომელი წესები უნდა გავრცელდეს კონკრეტულ ტრანზაქციაზე. ამავდროულად, ფუნქციური კლასიფიკაცია არ გამორიცხავს ერთდროულ რეგულირებას. პირიქით, ციფრული ფულის ჰიბრიდული ბუნების გამო შესაძლებელია, მასზე გავრცელდეს რამდენიმე რეჟიმი, მაგრამ ეს უნდა მოხდეს მკაფიო პრიორიტეტებით და არა ფრაგმენტულად.

მეორე მექანიზმი არის რეგულირებადი სუბიექტის იდენტიფიკაცია. სრულად დეცენტრალიზებულ ქსელზე პირდაპირი სამართლებრივი ზემოქმედება რთულია, თუმცა პრაქტიკაში მომხმარებლისა და ბაზრის სამართლებრივი დაცვის მნიშვნელოვანი ნაწილი ხორციელდება შუამავლების, პლატფორმების,

გაცვლის სერვისების, საფულის მომსახურების მიმწოდებლებისა და სხვა ვირტუალური აქტივის მომსახურების პროვაიდერების (VASP) მეშვეობით. სწორედ აღნიშნული სუბიექტები შეიძლება იქცნენ იურისდიქციის განსაზღვრის პრაქტიკულ წერტილად, რადგან მათ მიმართ შესაძლებელია რეგისტრაციის, ლიცენზირების, იდენტიფიკაციის, ანგარიშგების, უსაფრთხოების და მომხმარებელთა დაცვის მოთხოვნების დაწესება.

2. ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სტანდარტები, ვირტუალური აქტივის მომსახურების პროვაიდერები და საზედამხებო კომპეტენციის გადაკვეთა

ციფრული ფულის საერთაშორისო ტრანზაქციებში იურისდიქციული კოლიზიის ყველაზე პრაქტიკული გამოვლინება AML/CFT სფეროში გვხვდება. დეცენტრალიზებული ციფრული აქტივები, ფსევდონიმურობა და გლობალური გადარიცხვების სისწრაფე ზრდის უკანონო ფინანსური საქმიანობის რისკს. ამ მიზეზით, AML/CFT სტანდარტები ციფრული ფულის სამართლებრივი კონტროლის ერთ-ერთ მთავარ ინსტრუმენტად იქცა.³

ფინანსური ქმედების სპეციალური ჯგუფის (FATF) მიდგომის ძირითადი მნიშვნელობა მდგომარეობს იმაში, რომ იგი ცდილობს ვირტუალური აქტივებისა და VASP-ების მიმართ გამოიყენოს ის AML/CFT ლოგიკა, რომელიც ტრადიციულ ფინანსურ ინსტიტუტებზე ვრცელდება. ამ მიდგომის თანახმად, ვირტუალური აქტივი

3 შეადარე. Al-Tawil, T.N., 2023. Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*, 26(6), გვ. 1150. [ინტერნეტი] ხელმისაწვდომია: <https://doi.org/10.1108/JMLC-07-2022-0109> [წვდომის თარიღი 15.05.2026].

შეიძლება იყოს ღირებულების ციფრული გამოხატულება, რომელიც გამოიყენება გადახდის, ინვესტიციის ან გადარიცხვის მიზნებისთვის, ხოლო VASP არის ის სუბიექტი, რომელიც ბიზნეს საქმიანობის ფარგლებში უზრუნველყოფს გაცვლას, გადარიცხვას, შენახვას, ადმინისტრირებას ან სხვა შესაბამის მომსახურებას.⁴

VASP-ის კონცეფცია იურისდიქციულად მნიშვნელოვანია, რადგან სამართლებრივი ზედამხედველობა ხშირად ვერ ხორციელდება თვითონ დეცენტრალიზებულ პროტოკოლზე, მაგრამ შესაძლებელია განხორციელდეს იმ სუბიექტებზე, რომლებიც მომხმარებლებს ციფრული აქტივის შეძენის, გაცვლის, შენახვის ან გადარიცხვის საშუალებას აძლევენ. ამდენად, VASP წარმოადგენს რეგულირების ე.წ. „დამაგრების წერტილს“. სახელმწიფოს შეუძლია განსაზღვროს, როდის მიიჩნევა მომსახურების მიმწოდებელი მის იურისდიქციასთან დაკავშირებულად: მაგალითად, თუ იგი მომსახურებას სთავაზობს ადგილობრივ მომხმარებლებს, იყენებს ადგილობრივ ვალუტას, ახორციელებს მარკეტინგს ადგილობრივ ბაზარზე ან ამუშავებს ადგილობრივი მომხმარებლების პერსონალურ მონაცემებს.

FATF-ის მიერ დადგენილი „ინფორმაციის თანმხლები გადაცემის წესი“ (Travel Rule) ამ მოდელის ცენტრალური ნაწილია. მისი მიზანია გადარიცხვასთან დაკავშირებული გამგზავნისა და მიმღების

ინფორმაციის შენახვა და გადაცემა ისე, რომ ტრანსსასაზღვრო ოპერაცია არ დარჩეს სამართლებრივი კონტროლის მიღმა.⁵ თუმცა, ციფრული ფულის სფეროში ეს წესი განსაკუთრებულ სირთულეებს აჩენს. ერთი მხრივ, AML/CFT მიზნებისთვის საჭიროა ინფორმაციის შეგროვება და გაზიარება; მეორე მხრივ, ბლოკჩეინის გარემოში ტრანზაქციის მონაწილე შეიძლება არ იყოს ტრადიციული საბანკო ანგარიშის მფლობელი, ხოლო საფულებს შორის გადარიცხვა შეიძლება განხორციელდეს რეგულირებული შუამავლის გარეშე.

ამ კონტექსტში იურისდიქციული კოლიზიის გადაწყვეტა უნდა დაეფუძნოს სამ საფეხურს. პირველი საფეხურია მინიმალური საერთო AML/CFT სტანდარტის აღიარება – მომხმარებლის იდენტიფიკაცია, ბენეფიციარის შესახებ ინფორმაციის შეგროვება, საექვო ოპერაციების მონიტორინგი და ანგარიშგება. მეორე საფეხურია ზედამხედველობის კოორდინაცია იმ შემთხვევებში, როდესაც ერთი ტრანზაქცია რამდენიმე სახელმწიფოს ეხება. მესამე საფეხურია რისკზე დაფუძნებული მიდგომა, რადგან ყველა ციფრული აქტივის ტრანზაქცია ერთნაირ საფრთხეს არ წარმოშობს.⁶

რისკზე დაფუძნებული მიდგომა განსაკუთრებით მნიშვნელოვანია იმისთვის, რომ რეგულაციამ არ შეაფერხოს ინოვაცია და ამავედროულად არ დატოვოს მაღალი

4 Financial Action Task Force, 2014. Virtual Currencies: Key Definitions and Potential AML/CFT Risks. Paris: FATF. [ინტერნეტი] ხელმისაწვდომია:

<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> [წვდომის თარიღი 15.05.2026].

5 Financial Action Task Force, 2019. FATF Recommendation 15: New Technologies. Paris: FATF. [ინტერნეტი] ხელმისაწვდომია:

<https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> [წვდომის თარიღი 15.05.2026].

6 Financial Action Task Force, 2024. Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. Paris: FATF. [ინტერნეტი] ხელმისაწვდომია:

<https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html> [წვდომის თარიღი 15.05.2026].

რისკის ოპერაციები კონტროლის გარეშე. ასეთი მიდგომა საჭიროებს ტრანზაქციის მოცულობის, მხარეთა რისკ-პროფილის, იურისდიქციის რეპუტაციის, მომსახურების ტიპისა და ტექნოლოგიური მახასიათებლების შეფასებას. მხოლოდ ამ გზით შეიძლება AML/CFT ვალდებულებები იყოს პროპორციული და ეფექტიანი.

აღნიშნული სამსაფუხურიანი მოდელის პრაქტიკული მნიშვნელობა განსაკუთრებით მკაფიოდ ვლინდება იმ შემთხვევაში, როდესაც საქართველოს რეზიდენტი მომხმარებელი ტრანსსასაზღვრო გადარიცხვის მიზნით იყენებს უცხოური ვირტუალური აქტივის მომსახურების პროვაიდერსა და სტაბილურ ვირტუალურ აქტივს. ასეთ ვითარებაში, ფინანსურ ქმედებათა სპეციალური ჯგუფის სტანდარტების შესაბამისად, ვირტუალური აქტივის მომსახურების პროვაიდერს ეკისრება გამგზავნისა და მიმღების საიდენტიფიკაციო მონაცემების შეგროვებისა და მათი გადაცემის ვალდებულება „ინფორმაციის თანმხლები გადაცემის წესის“ ფარგლებში, მათ შორის, უცხო ქვეყნის პარტნიორი მომსახურების მიმწოდებლისთვის. აღნიშნული ვალდებულება არ ქარწყლდება იმ გარემოებით, რომ ტრანზაქცია ტექნიკური თვალსაზრისით შესაძლოა, განხორციელდეს დეცენტრალიზებულ ბლოკჩეინზე დაფუძნებული ინფრასტრუქტურის მეშვეობით.

შესაბამისად, მაშინაც კი, როდესაც ტრანზაქციის განხორციელების ტექნიკური ადგილი მკაფიოდ არ იდენტიფიცირდება, ზედამხედველობის სამართლებრივი და პრაქტიკული „მიზნის წერტილი“ ყალიბდება მომსახურების მიმწოდებელ ვირტუალური აქტივის პროვაიდერთან. სწორედ ეს სუბიექტი წარმოადგენს იმ რეგულირებად შუამავალს, რომლის მე-

შვეობითაც დეცენტრალიზებული ტექნოლოგიური გარემო უკავშირდება სახელმწიფო ზედამხედველობის სისტემას. ამდენად, მოდელი ეფუძნება არა უშუალოდ ბლოკჩეინის ქსელის ტერიტორიულ ლოკალიზაციას, არამედ იმ რეგულირებადი სუბიექტის იდენტიფიცირებას, რომელიც მომხმარებელს აძლევს ვირტუალურ აქტივებზე წვდომას და უზრუნველყოფს ტრანზაქციის განხორციელებას. აღნიშნული მიდგომა შეესაბამება როგორც FATF-ის მე-15 რეკომენდაციის ლოგიკას, ისე ვირტუალური აქტივებისა და მათი მომსახურების პროვაიდერების შესახებ 2024 წლის მიზნობრივი განახლებით გაძლიერებულ საერთაშორისო სტანდარტებს.

3. ევროკავშირის მოდელი: MICA, GDPR, PSD2 და NIS2 – როგორც კოლიზიის შემცირების ინსტრუმენტები

ევროკავშირის სამართლებრივი ჩარჩო ციფრული ფულის იურისდიქციული კოლიზიების შემცირების ერთ-ერთ ყველაზე განვითარებულ მაგალითს წარმოადგენს. კრიპტოაქტივების ბაზრების შესახებ რეგულაცია (Markets in Crypto-Assets Regulation (MiCA)) ქმნის ერთიან რეჟიმს კრიპტოაქტივებისა და კრიპტოაქტივების მომსახურების მიმწოდებლებისთვის ევროკავშირის ბაზარზე. მისი მნიშვნელობა იმაში მდგომარეობს, რომ იგი ცდილობს ერთიანი ბაზრის ფარგლებში შეამციროს რეგულაციური ფრაგმენტაცია და წინასწარ განსაზღვროს ავტორიზაციის, გამჭვირვალობის, ორგანიზაციული და მომხმარებელთა დაცვის მოთხოვნები.⁷

MiCA-ს მიდგომა ციფრული აქტივების კლასიფიკაციის მიმართულებით განსაკუთ-

7 European Parliament and Council, 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets. [ინტერნეტი] ხელმისაწვდომია: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114> [წვდომის თარიღი 15.05.2026].

რებით რელევანტურია იურისდიქციული კოლიზიებისთვის. რეგულაცია განასხვავებს სხვადასხვა ტიპის კრიპტოაქტივებს, მათ შორის, აქტივებით უზრუნველყოფილ ტოკენებსა და ელექტრონული ფულის ტოკენებს. ასეთი კლასიფიკაცია ეხმარება სამართალს განსაზღვროს, რომელი რეჟიმი უნდა გავრცელდეს კონკრეტულ აქტივზე. ამავდროულად, MiCA არ წყვეტს ყველა კოლიზიურ საკითხს, რადგან ციფრული აქტივების ტრანზაქციები ხშირად სცდება ევროკავშირის ტერიტორიას და უკავშირდება მესამე ქვეყნებში არსებულ პლატფორმებს ან მომხმარებლებს.

ამ კონტექსტში დამოუკიდებელ სამართლებრივ პრობლემად წარმოჩნდება მონაცემთა დაცვის ზოგადი რეგულაციის (General Data Protection Regulation (GDPR)) როლი, ვინაიდან ფინანსური მონიტორინგის მიზნებისთვის მონაცემთა შეგროვებისა და გადაცემის ვალდებულება უნდა დაბალანსდეს პერსონალურ მონაცემთა დაცვის, მიზნობრიობის, პროპორციულობისა და მონაცემთა მინიმიზაციის პრინციპებთან. ციფრული ფულის ტრანზაქცია ხშირად მოიცავს პერსონალურ მონაცემებს, ხოლო ფინანსური მონიტორინგი მოითხოვს მომხმარებლის იდენტიფიკაციას, მონაცემთა შენახვას და საჭიროების შემთხვევაში მათ გაზიარებას. GDPR მოითხოვს მონაცემთა დამუშავების კანონიერ საფუძველს, პროპორციულობას, უსაფრთხოებას და „privacy by design“

და „privacy by default“ მიდგომებს.⁸ ციფრული ფულის სფეროში ეს პრინციპები უნდა შეესაბამებოდეს AML/CFT მოთხოვნებს, რაც მარტივი არ არის. თუ AML/CFT ლოგიკა ითხოვს ინფორმაციის შენახვასა და გადაცემას, მონაცემთა დაცვის ლოგიკა ითხოვს დამუშავების მინიმიზაციას, მიზნობრიობას და უსაფრთხოებას.

გადახდის მომსახურების მეორე დირექტივა (PSD2)⁹ ციფრული გადახდების უსაფრთხოების თვალსაზრისით მნიშვნელოვანი სტანდარტია. იგი მოითხოვს მომხმარებლის გაძლიერებულ ავთენტიფიკაციას და ქმნის ოპერაციული და უსაფრთხოების რისკების მართვის ჩარჩოს.¹⁰ ციფრული ფულის ტრანზაქციებში ეს ნიშნავს, რომ იურისდიქციის საკითხი ვერ შეფასდება მხოლოდ ფინანსური სამართლის ფარგლებში; აუცილებელია ტექნიკური უსაფრთხოების მოთხოვნების გათვალისწინება. თუ მომხმარებელი ერთ სახელმწიფოშია, მომსახურების მიმწოდებელი – მეორეში, ხოლო ტექნოლოგიური ინფრასტრუქტურა – მესამე იურისდიქციაში, უსაფრთხოების დარღვევა ერთდროულად შეიძლება შეეხოს რამდენიმე მარეგულირებელ რეჟიმს.

ქსელისა და ინფორმაციული სისტემების უსაფრთხოების მეორე დირექტივა (NIS2)¹¹ ამ ლოგიკას კიდევ უფრო ავითარებს და კრიტიკული სექტორებისთვის კიბერუსაფრთხოების საერთო დონეს ადგენს. ციფრული ფინანსური სერვისე-

8 Voigt, P. and von dem Bussche, A., 2024. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer.

9 European Parliament and Council of the European Union, 2015. Directive (EU) 2015/2366 on payment services in the internal market. Official Journal of the European Union, L 337, გვ. 35. [ინტერნეტი] ხელმისაწვდომია: <<https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng>> [წვდომის თარიღი 15.05.2026].

10 European Banking Authority, 2017. Guidelines on the Security Measures for Operational and Security Risks of Payment Services under Directive (EU) 2015/2366, EBA-GL-2017-17.

11 European Parliament and Council of the European Union, 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, L 333, გვ. 80. [ინტერნეტი] ხელმისაწვდომია: <<https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>> [წვდომის თარიღი 15.05.2026].

ბი კიბერუსაფრთხოების მაღალი რისკის სფეროა, სადაც ინციდენტი შეიძლება გადაიზარდოს მომხმარებლის ზიანში, ბაზრის ნდობის დაკარგვასა და სისტემურ საფრთხეში. ამიტომ იურისდიქციული კოლიზიის გადაწყვეტა მოითხოვს არა მხოლოდ იმის დადგენას, რომელმა ფინანსურმა ორგანომ უნდა იმოქმედოს, არამედ იმასაც, რომელი კიბერუსაფრთხოების სტანდარტი და ინციდენტის შეტყობინების ვალდებულება გავრცელდება კონკრეტულ სუბიექტზე.

ევროკავშირის მოდელი აჩვენებს, რომ ციფრული ფულის სამართლებრივი რეგულირება მრავალსექტორულია. ფინანსური რეგულირება, AML/CFT, მონაცემთა დაცვა და კიბერუსაფრთხოება ერთმანეთისგან იზოლირებულად ვერ იმუშავებს. სწორედ ამიტომ, იურისდიქციული კოლიზიების შემცირების ეფექტიანი მექანიზმი უნდა იყოს ინტეგრირებული – ერთდროულად უნდა პასუხობდეს აქტივის სამართლებრივ ბუნებას, მომსახურების მიმწოდებლის სტატუსს, მომხმარებლის დაცვას, პერსონალურ მონაცემებს და ოპერაციულ მდგრადობას.

4. CBDC და სთეიბლკოინები: განსხვავებული სამართლებრივი ბუნება და განსხვავებული კოლიზიური რისკები

ციფრული ფულის ყველა ფორმა ერთნაირ იურისდიქციულ პრობლემას არ წარმოშობს. ცენტრალური ბანკის ციფრული ვალუტა (CBDC) და სთეიბლკოინი ამ

მხრივ განსხვავებული სამართლებრივი კატეგორიებია. CBDC უკავშირდება სახელმწიფოს მონეტარულ სუვერენიტეტს და ცენტრალური ბანკის უფლებამოსილებას, ხოლო სთეიბლკოინი – კერძო ემიტენტს, რეზერვებს, გამოსყიდვის მექანიზმს, გადახდის ფუნქციასა და ფინანსური სტაბილურობის რისკებს.

CBDC-ის შემთხვევაში იურისდიქციული კოლიზია ნაკლებად ეხება ემიტენტის იდენტიფიკაციას, რადგან ემიტენტი ცენტრალური ბანკია. მთავარი პრობლემაა, თუ როგორ დაბალანსდეს ცენტრალური ბანკის ფუნქცია, მომხმარებლის კონფიდენციალურობა, მონაცემთა დაცვა და AML/CFT მოთხოვნები. CBDC-ის ტექნოლოგიური ინფრასტრუქტურა შეიძლება იძლეოდეს ტრანზაქციების უფრო მაღალი ხარისხით მიკვლევადობის შესაძლებლობას, რაც სასარგებლოა ფინანსური მონიტორინგისთვის, მაგრამ ამავედროულად ზრდის პერსონალური მონაცემების დამუშავების მასშტაბს.¹²

CBDC-ის სამართლებრივი ბუნება კლასიკურ კატეგორიებს სრულად არ ემთხვევა. იგი შეიძლება განიხილებოდეს როგორც ცენტრალური ბანკის ფულის ციფრული ფორმა, მაგრამ მისი გამოყენება განსხვავდება ფიზიკური ნაღდი ფულისგან, რადგან დაკავშირებულია ტექნოლოგიურ ინფრასტრუქტურასთან, მონაცემთა დამუშავებასთან და ოპერაციულ კონტროლთან.¹³ აქედან გამომდინარე, CBDC-ის სამართლებრივი ჩარჩო უნდა განსაზღვრავდეს არა მხოლოდ გამოშვებისა და გამოყენების წესებს, არამედ მონაცემთა დაცვის, უსაფრთხოების, ხელმისაწვდომობისა და მომხმარებელთა დაცვის გარანტიებს.

12 Auer, R. and Böhme, R., 2020. The Technology of Retail Central Bank Digital Currency. BIS Quarterly Review, March, გვ. 85. [ინტერნეტი] ხელმისაწვდომია: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm [წვდომის თარიღი 15.05.2026].

13 European Central Bank, 2020. Report on a Digital Euro. Frankfurt am Main: ECB. [ინტერნეტი] ხელმისაწვდომია: https://www.ecb.europa.eu/euro/digital_euro/report/html/index.en.html [წვდომის თარიღი: 15.05.2026].

სტეიბლკოინების შემთხვევაში კოლიზიური რისკი განსხვავებულია. ისინი კერძო ციფრული ფულის ფორმას უახლოვდება და შეიძლება ერთდროულად ასრულებდეს გადახდის, ღირებულების შენახვისა და საინვესტიციო ფუნქციას. სტეიბლკოინების რეგულირებისას განსაკუთრებით მნიშვნელოვანია რეზერვების ხარისხი, მათი გამჭვირვალობა, გამოსყიდვის უფლება, ემიტენტის პასუხისმგებლობა და მომხმარებელთა დაცვა.¹⁴

სტაბილური ვირტუალური აქტივი იურისდიქციულ სირთულეს ქმნის, რადგან ემიტენტი, რეზერვის აქტივები, მომხმარებელი, სავაჭრო პლატფორმა და ტექნოლოგიური ინფრასტრუქტურა შესაძლოა, სხვადასხვა სახელმწიფოს უკავშირდებოდეს. ასეთ პირობებში ბუნდოვანი ხდება, რომელმა სახელმწიფომ უნდა განახორციელოს ზედამხედველობა, რომელი მომხმარებელთა დაცვისა და ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის წესები უნდა გავრცელდეს და როგორ უნდა აღსრულდეს მოთხოვნა რეზერვის აქტივებზე. MiCA-ს მიერ აქტივებით უზრუნველყოფილი ტოკენებისა და ელექტრონული ფულის ტოკენების განსხვავება ამ პრობლემის შემცირების მცდელობაა, თუმცა, გლობალური ტრანზაქციების დონეზე იგი სრულ გადაწყვეტას ვერ უზრუნველყოფს.¹⁵

მაგალითად, თუ აქტივით უზრუნველყოფილი სტეიბლკოინის ემიტენტი რეგისტრირებულია ევროკავშირის წევრ სახელმწიფოში და ექვემდებარება MiCA-ს, მისი რეზერვის აქტივები ინახება მესამე ქვეყნის საბანკო სესხსა ან

ობლიგაციებში, ხოლო მომხმარებელი და სავაჭრო პლატფორმა საქართველოს იურისდიქციასთან არიან დაკავშირებულნი, ზედამხედველობისა და მომხმარებელთა დაცვის ცალკეული ელემენტები გაყოფილია სხვადასხვა რეჟიმებს შორის. ემიტენტზე ვრცელდება MiCA-ს მიერ დადგენილი მოთხოვნები რეზერვების ხარისხზე, გამჭვირვალობასა და გამოსყიდვის უფლებაზე, მაშინ როდესაც საქართველოს მომხმარებელთა დაკავშირებული სამოქალაქო-სამართლებრივი მოთხოვნები და მომხმარებელთა დაცვის სტატუსი უნდა განისაზღვროს ეროვნული სამოქალაქო და ფინანსური კანონმდებლობის საფუძველზე, რომელიც შესაძლოა ჯერ კიდევ არ ასახავდეს სტეიბლკოინის სპეციფიკას. ამასთან ერთად, თუ გადახდა ხორციელდება ტრანსსასაზღვრო რეჟიმში, AML/CFT მოთხოვნები უკვე მოითხოვენ FATF-ის სტანდარტების, მათ შორის, ვირტუალური აქტივებისა და VASP-ების შესახებ 2024 წლის განახლებული რეკომენდაციების, კოორდინირებულ იმპლემენტაციას როგორც ევროკავშირის, ისე საქართველოს ზედამხედველი ორგანოების მხრიდან.

სტეიბლკოინების მაგალითი აჩვენებს, რომ იურისდიქციული კოლიზიის გადაწყვეტისათვის საჭიროა რეზერვებზე, ემიტენტსა და მომხმარებელზე ორიენტირებული კომბინირებული მიდგომა. თუ აქტივი ფართოდ გამოიყენება გადახდისთვის, რეგულაციამ უნდა უზრუნველყოს გამოსყიდვის სანდოობა და მომხმარებელთა დაცვა. თუ იგი სისტემურად მნიშვნელოვანი ხდება, საჭიროა ფინანსური სტაბილურობისა და მონეტარული

14 Berentsen, A. and Schär, F., 2019. Stablecoins: The Quest for a Low-Volatility Cryptocurrency. In: Fatás, A., "ed." The Economics of Fintech and Digital Currencies. London: CEPR Press, გვ. 70. [ინტერნეტი] ხელმისაწვდომია: <https://cepr.org/system/files/publication-files/60138-the-economics-of-fintech-and-digital-currencies.pdf> [წვდომის თარიღი: 15.05.2026].

15 European Parliament and Council, 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets. [ინტერნეტი] ხელმისაწვდომია: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114> [წვდომის თარიღი 15.05.2026].

პოლიტიკის რისკების გათვალისწინება. თუ იგი გამოიყენება ტრანსსასაზღვრო გადარიცხვებში, აუცილებელია AML/CFT და მონაცემთა დაცვის რეჟიმების კოორდინაცია.

5. ქართული სამართლის სამომავლო განვითარების მიმართულებები

ციფრული ფულის საერთაშორისო ტრანზაქციები საქართველოსთვის, როგორც წესი, ტრანსსასაზღვრო ელემენტს შეიცავს: მომხმარებელი შესაძლოა, საქართველოში იმყოფებოდეს, მომსახურების მიმწოდებელი – სხვა იურისდიქციაში, ტექნოლოგიური ინფრასტრუქტურა – გლობალურ ქსელში, ხოლო აქტივი ისეთი ფორმით არსებობდეს, რომელსაც ეროვნული კანონმდებლობა ჯერ მკაფიოდ არ განსაზღვრავს. ამიტომ ქართული სამართლისთვის ძირითადი ამოცანაა არა მხოლოდ ციფრული ფულის ზოგადი აღიარება, არამედ ისეთი სამართლებრივი მექანიზმების ჩამოყალიბება, რომლებიც განსაზღვრავს მარეგულირებელ კომპეტენციას, ზედამხედველობის ფარგლებს, მომხმარებელთა დაცვის წესებსა და ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის შესაბამისობას.

პირველი სამომავლო საკანონმდებლო მიმართულება¹⁶ არის ციფრული ფულისა და ვირტუალური აქტივების ფუნქციური კლასიფიკაციის დანერგვა. ეროვნულმა სამართალმა უნდა განასხვავოს ციფრული აქტივი, რომელიც გამოიყენება გადახდისთვის; აქტივი, რომელიც ქმნის საინვესტიციო მოლოდინს; სტიმულკოინი, რომელიც უკავშირდება რეზერვებსა და გამოსყიდვის უფლებას;

და CBDC, როგორც ცენტრალური ბანკის ფულის ციფრული ფორმა. ასეთი კლასიფიკაცია აუცილებელია იმისთვის, რომ ზედამხედველმა ორგანოებმა იცოდნენ, რომელი რეჟიმი უნდა გავრცელდეს კონკრეტულ პროდუქტზე.

მეორე მიმართულება არის VASP-ების მარეგულირებელი სტატუსის მკაფიო განსაზღვრა. ქართული სამართლისთვის მნიშვნელოვანია დადგინდეს, რა შემთხვევაში ექვევა უცხოური VASP საქართველოს მარეგულირებელი ინტერესის ქვეშ. ასეთი კავშირი შეიძლება წარმოიშვას მაშინ, როდესაც მომსახურება აქტიურად მიემართება საქართველოს მომხმარებლებზე, გამოიყენება ქართული ენა ან ადგილობრივი გადახდის არხები, მუშავდება საქართველოს მომხმარებელთა პერსონალური მონაცემები ან იქმნება AML/CFT რისკი საქართველოს ფინანსური სისტემისთვის.

მესამე მიმართულება არის AML/CFT ვალდებულებების ტექნოლოგიურად შესაბამისი მოდელი. ვირტუალური აქტივების მომსახურების მიმწოდებელმა უნდა შეასრულოს მომხმარებლის იდენტიფიკაციის, ტრანზაქციის მონიტორინგის, საექსპოზიციო რისკების ანგარიშგების, მონაცემთა შენახვისა და საჭირო ინფორმაციის გადაცემის ვალდებულებები. ამასთან, რეგულაცია უნდა იყოს რისკზე დაფუძნებული და არ უნდა აწესებდეს ერთნაირ სიმძიმეს დაბალი და მაღალი რისკის ოპერაციებზე.

მეოთხე მიმართულება არის კიბერუსაფრთხოებისა და პერსონალურ მონაცემთა დაცვის ინტეგრაცია ფინანსურ რეგულირებაში. ციფრული ფულის ტრანზაქცია ერთდროულად არის ფინანსური ოპერაცია და მონაცემთა დამუშავების პროცესი. ამიტომ მარეგულირებელმა ჩაიჩინა უნდა მოითხოვოს შესაბამისი ტექ-

16 De lege ferenda (ლათ. „სამომავლო კანონის თვალსაზრისით“) – აღნიშნავს იმ წინადადებებს, თუ როგორი უნდა იყოს სამართალი.

ნიკური და ორგანიზაციული ზომები, ინციდენტების მართვის პროცედურები, უსაფრთხოების აუდიტი და მომხმარებელთა მონაცემების პროპორციული დამუშავება.¹⁷

მეხუთე მიმართულება არის ზედამხედველ ორგანოთა კოორდინაცია. ციფრული ფულის სფეროში შეიძლება ერთდროულად იყოს ჩართული ფინანსური ზედამხედველობა (მათ შორის, AML/CFT, კიბერუსაფრთხოების კომპეტენტური უწყებები), პერსონალურ მონაცემთა დაცვის ორგანო. თუ მათი კომპეტენციები არ იქნება კოორდინირებული, იურისდიქციული კოლიზია შეიძლება წარმოიშვას არა მხოლოდ საერთაშორისო, არამედ შიდა სამართლებრივ დონეზეც. ამიტომ საჭიროა ინფორმაციის გაცვლის, ერთობლივი ზედამხედველობისა და საგანგებო ინციდენტებზე რეაგირების პროცედურების წინასწარ განსაზღვრა.

დასკვნა

ციფრული ფულის საერთაშორისო ტრანზაქციებში იურისდიქციული კოლიზიების გადაწყვეტა მოითხოვს სამართლებრივი აზროვნების გადანაცვლებას ტერიტორიულად შეზღუდული მოდელიდან ფუნქციურ და რისკზე დაფუძნებულ მოდელზე. ციფრული ფინანსური ურთიერთობა არ არის მხოლოდ გადახდა ან მხოლოდ ინვესტიცია; იგი ხშირად აერთიანებს გადახდის, საინვესტიციო, ტექნოლოგიურ, მონაცემთა დაცვისა და კიბერუსაფრთხოების ელემენტებს. სწორედ ამიტომ, ერთმნიშვნელოვანი და ერთსაფეხურიანი გადაწყვეტა საკმარისი არ არის.

სტატიის ძირითადი დასკვნაა, რომ იურისდიქციული კოლიზიების გადაწყვეტის

ეფექტიანი სამართლებრივი მექანიზმი მრავალშრიანი უნდა იყოს. პირველ საფეხურზე საჭიროა ციფრული აქტივის ფუნქციური კლასიფიკაცია. მეორე საფეხურზე უნდა განისაზღვროს რეგულირებადი სუბიექტი, განსაკუთრებით ვირტუალური აქტივის მომსახურების პროვაიდერი. მესამე საფეხურზე აუცილებელია ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის სტანდარტების, მათ შორის, „ინფორმაციის თანმხლები გადაცემის წესის“, პროპორციული და ტექნოლოგიურად შესაბამისი დანერგვა. მეოთხე საფეხურზე ფინანსური რეგულირება უნდა დაუკავშირდეს კიბერუსაფრთხოებასა და პერსონალურ მონაცემთა დაცვას. მეხუთე საფეხურზე ცენტრალური ბანკის ციფრული ვალუტა და სტაბილური ვირტუალური აქტივები უნდა მოწესრიგდეს მათი განსხვავებული სამართლებრივი ბუნების გათვალისწინებით.

ქართული სამართლისთვის აღნიშნულ ანალიზს პრაქტიკული მნიშვნელობა აქვს. ციფრული ფულის საერთაშორისო ტრანზაქცია საქართველოს იურისდიქციას შეიძლება დაუკავშირდეს მომხმარებლის, მომსახურების მიმწოდებლის, მონაცემთა დამუშავების, ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ ბრძოლის რისკის ან ფინანსური სტაბილურობის საფუძველზე. ამდენად, საჭიროა ისეთი ეროვნული ჩარჩო, რომელიც ციფრული ფულის სპეციფიკურ რისკებს ცალკე, სისტემურად და საერთაშორისო სტანდარტებთან კოორდინირებულად მოაწესრიგებს.

17 Anderson, R., Böhme, R., Clayton, R. and Moore, T., 2008. Security Economics and European Policy. In: Johnson, M.E., "ed." Managing Information Risk and the Economics of Security. New York: Springer, გვ. 55.

ბიბლიოგრაფია

გამოყენებული ლიტერატურა:

1. გაბისონია, ზ., 2019. ბიტკოინის, როგორც ციფრული ვალუტის სამართლებრივი რეგულირების კონცეპტუალური ასპექტები, შედარებითი სამართლის გერმანულ-ქართული ჟურნალი, 2.
2. Al Mashhour, O.F., Abd Aziz, A.S. and Mohd Noor, N.A., 2022. Blockchain and its Entire Eco-System: A Legal Consideration to an International Cross-Border Technology. International Journal of Multidisciplinary Sciences and Advanced Technology, 3(3). [ინტერნეტი] ხელმისაწვდომია: https://www.researchgate.net/publication/363645357_Blockchain_and_its_Entire_Eco-System_A_Legal_Consideration_to_an_International_Cross-Border_Technology [წვდომის თარიღი 15.05.2026].
3. Al-Tawil, T.N., 2023. Anti-money laundering regulation of cryptocurrency: UAE and global approaches. Journal of Money Laundering Control, 26(6). [ინტერნეტი] ხელმისაწვდომია: <https://doi.org/10.1108/JMLC-07-2022-0109> [წვდომის თარიღი 15.05.2026].
4. Anderson, R., Böhme, R., Clayton, R. and Moore, T., 2008. Security Economics and European Policy. In: Johnson, M.E., „ed.“ Managing Information Risk and the Economics of Security. New York: Springer, გვ. 55.
5. Auer, R. and Böhme, R., 2020. The Technology of Retail Central Bank Digital Currency. BIS Quarterly Review, March. [ინტერნეტი] ხელმისაწვდომია: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm [წვდომის თარიღი 15.05.2026].
6. Berentsen, A. and Schär, F., 2019. Stablecoins: The Quest for a Low-Volatility Cryptocurrency. In: Fatás, A., ed. The Economics of Fintech and Digital Currencies. London: CEPR Press. [ინტერნეტი] ხელმისაწვდომია: https://cepr.org/system/files/publication-files/60138-the_economics_of_fintech_and_digital_currencies.pdf [წვდომის თარიღი 15.05.2026].
7. European Central Bank, 2020. Report on a Digital Euro. Frankfurt am Main: ECB. [ინტერნეტი] ხელმისაწვდომია: www.ecb.europa.eu/euro/digital_euro/report/html/index.en.html [წვდომის თარიღი 15.05.2026].
8. Financial Action Task Force, 2014. Virtual Currencies: Key Definitions and Potential AML/CFT Risks. Paris: FATF. [ინტერნეტი] ხელმისაწვდომია: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> [წვდომის თარიღი 15.05.2026].
9. Financial Action Task Force, 2019. FATF Recommendation 15: New Technologies. Paris: FATF. [ინტერნეტი] ხელმისაწვდომია: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> [წვდომის თარიღი 15.05.2026].
10. Financial Action Task Force, 2024. Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. Paris: FATF. [ინტერნეტი] ხელმისაწვდომია: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html> [წვდომის თარიღი 15.05.2026].
11. Gorton, G.B. and Zhang, J.Y., 2023. Taming Wildcat Stablecoins. University of Chicago Law Review, 90(3). [ინტერნეტი] ხელმისაწვდომია: <https://chicagounbound.uchicago.edu/uclev/vol90/iss3/3/> [წვდომის თარიღი 15.05.2026].
12. Voigt, P. and von dem Bussche, A., 2024. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer.

ნორმატიული მასალა:

1. საქართველოს კანონი საერთაშორისო კერძო სამართლის შესახებ, 1998. [ინტერნეტი] ხელმისაწვდომია: <https://matsne.gov.ge/ka/document/view/93712> [წვდომის თარიღი 15.05.2026].
2. საქართველოს სამოქალაქო კოდექსი, 1997. [ინტერნეტი] ხელმისაწვდომია: <https://matsne.gov.ge/ka/document/view/31702> [წვდომის თარიღი: 15.05.2026].
3. საქართველოს კანონი ელექტრონული დოკუმენტისა და ელექტრონული სანდო

- მომსახურების შესახებ, 2017. [ინტერნეტი] ხელმისაწვდომია: <https://matsne.gov.ge/ka/document/view/3654557> [წვდომის თარიღი 15.05.2026].
4. საქართველოს კანონი ფულის გათვრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ, 2019. [ინტერნეტი] ხელმისაწვდომია: <https://matsne.gov.ge/ka/document/view/4690334> [წვდომის თარიღი 15.05.2026].
 5. European Parliament and Council of the European Union, 2015. Directive (EU) 2015/2366 on payment services in the internal market. Official Journal of the European Union, L 337, გვ. 35. [ინტერნეტი] ხელმისაწვდომია: <https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng> [წვდომის თარიღი 15.05.2026].
 6. European Parliament and Council of the European Union, 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, L 333. [ინტერნეტი] ხელმისაწვდომია: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> [წვდომის თარიღი 15.05.2026].
 7. European Parliament and Council of the European Union, 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets. [ინტერნეტი] ხელმისაწვდომია: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114> [წვდომის თარიღი 15.05.2026].
 - regulation of cryptocurrency: UAE and global approaches. Journal of Money Laundering Control, 26(6). [Online] available at: <https://doi.org/10.1108/JMLC-07-2022-0109> [Accessed 15.05.2026]. (in English)
 3. Anderson, R., Böhme, R., Clayton, R. and Moore, T., 2008. Security Economics and European Policy. In: Johnson, M.E., ed. Managing Information Risk and the Economics of Security. New York: Springer. (in English)
 4. Auer, R. and Böhme, R., 2020. The Technology of Retail Central Bank Digital Currency. BIS Quarterly Review, March. [Online] available at: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm [Accessed 15.05.2026]. (in English)
 5. Berentsen, A. and Schär, F., 2019. Stablecoins: The Quest for a Low-Volatility Cryptocurrency. In: Fatás, A., ed. The Economics of Fintech and Digital Currencies. London: CEPR Press. [Online] available at: https://cepr.org/system/files/publication-files/60138-the_economics_of_fintech_and_digital_currencies.pdf [Accessed 15.05.2026]. (in English)
 6. European Central Bank, 2020. Report on a Digital Euro. Frankfurt am Main: ECB. [Online] available at: https://www.ecb.europa.eu/euro/digital_euro/report/html/index.en.html [Accessed 15.05.2026]. (in English)
 7. Financial Action Task Force, 2014. Virtual Currencies: Key Definitions and Potential AML/CFT Risks. Paris: FATF. [Online] available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> [Accessed 15.05.2026]. (in English)
 8. Financial Action Task Force, 2019. FATF Recommendation 15: New Technologies. Paris: FATF. [Online] available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> [Accessed 15.05.2026]. (in English)
 9. Financial Action Task Force, 2024. Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. Paris: FATF. [Online] available at: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html> [Accessed 15.05.2026]. (in English)
 10. Gabisonia, Z., 2019. Conceptual Aspects of Le-

BIBLIOGRAPHY

Used Literature:

1. Al Mashhour, O.F., Abd Aziz, A.S. and Mohd Noor, N.A., 2022. Blockchain and its Entire Eco-System: A Legal Consideration to an International Cross-Border Technology. International Journal of Multidisciplinary Sciences and Advanced Technology, 3(3). [Online] available at: https://www.researchgate.net/publication/363645357_Blockchain_and_its_Entire_Eco-System_A_Legal_Consideration_to_an_International_Cross-Border_Technology [Accessed 15.05.2026]. (in English)
2. Al-Tawil, T.N., 2023. Anti-money laundering

- gal Regulation of Bitcoin as a Digital Currency, German-Georgian Journal of Comparative Law, 2. (in Georgian)
11. Gorton, G.B. and Zhang, J.Y., 2023. Taming Wildcat Stablecoins. University of Chicago Law Review, 90(3). [Online] available at: <https://chicagounbound.uchicago.edu/uclrev/vol90/iss3/3/> [Accessed 15.05.2026]. (in English)
 12. Voigt, P. and von dem Bussche, A., 2024. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer. (in English)

at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114> [Accessed 15.05.2026]. (in English)

Normative Materials:

1. Law of Georgia on Private International Law, 1998. [Online] available at <https://matsne.gov.ge/ka/document/view/93712> [Accessed 15.05.2026]. (in Georgian)
2. Civil Code of Georgia, 1997. [Online] available at <https://matsne.gov.ge/ka/document/view/31702> [Accessed 15.05.2026]. (in Georgian)
3. Law of Georgia on Electronic Document and Electronic Trust Services, 2017. [Online] available at <https://matsne.gov.ge/ka/document/view/3654557> [Accessed 15.05.2026]. (in Georgian)
4. Law of Georgia on the Promotion of Prevention of Money Laundering and Terrorism Financing, 2019. [Online] available at <https://matsne.gov.ge/ka/document/view/4690334> [Accessed 15.05.2026]. (in Georgian)
5. European Parliament and Council of the European Union, 2015. Directive (EU) 2015/2366 on payment services in the internal market. Official Journal of the European Union, L 337, p. 35. [Online] available at: <https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng> [Accessed 15.05.2026]. (in English)
6. European Parliament and Council of the European Union, 2022. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. Official Journal of the European Union, L 333, p. 80. [Online] available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> [Accessed 15.05.2026]. (in English)
7. European Parliament and Council of the European Union, 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets. [Online] available