June 2022 (№22)
Volume 8; Issue 2; Page No. 116-130
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/8.2.8

Cryptocurrency-Related Cybercrime Types and Threats

Irakli Nadareishvili
Doctor of Law, Affiliated Associated professor of Caucasus International University, Head of The Department to Investigate Offenses Committed in the Course of Legal Proceedings, The Office of The General Prosecutor of Georgia

Shota Kakulia
Master of Law, Prosecutor of The Department to Investigate, Offenses Committed in the Course of Legal Proceedings

ARTICLE INFO

Article History:

Received 10.05.2022
Accepted 24.06.2022
Published 30.06.2022

Keywords:

Cryptocurrency, Cryptojacking, Cyber-Cartel, Digital Economics, Cybercrime

ABSTRACT

This article emphasizes the types and threats of cybercrime related to cryptocurrencies. The necessity of implementing legislative regulations and invention of administrative control mechanisms in connection with the growth of the digital economy is also discussed. The presented article also elucidates features of cyber-cartels and their new instruments, such as "Auction Robots", for committing illicit activities as the new type of the organized crime in a digital world. This work also focuses on describing certain categories of cybercrime, such as cryptojacking, which is a scheme to use people's devices (computers, smartphones, tablets and etc.), without their consent or knowledge, to secretly mine cryptocurrency on the victim's dime. To analyze the growth in demand, this work highlights the index of the whole capitalization and the exchange rates of the cryptocurrencies. Article also underlines the threat of the element of anonymity related to cryptocurrencies as the main instrument for criminals to either disguise terrorism financing or evade paying taxes. Some valuable examples of amendments developed and introduced by the US and Great Britain legislations to regulate crypto market and control tax evasion are also cited.

კრიპტოვალუტასთან დააკავშირებული კიბერდანაშაულის სახეები და საფრთხეები

ირაკლი ნადარეიშვილი

სამართლის დოქტორი, კავკასიის საერთაშორისო უნივერსიტეტის აფილირებული ასოცირებული პროფესორი. საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის უფროსი

შოთა კაკულია

სამართლის მაგისტრი, საქართველოს გენერალური პროკურატურის სამართალწარმოების პროცესში ჩადენილი დანაშაულის გამოძიების დეპარტამენტის პროკურორი

საკვანძო სიტყვები: კრიპტოვალუტა, კრიპტოჯეკინგი, კიბერკარტელი, ციფრული ეკონომიკა, კიბერდანაშაული

აბსტრაქტი

სტატიაში განხილულია კრიპტოვალუტასტან დაკავშირებული კიბერდანაშაულის სახეები და საფრთხეები. ციფრული ეკონომიკის ზრდის ფონზე, საკანონმდებლო რეგულაციებისა და ადმინისტრაციული კონტროლის მექანიზმების შექმნის საჭიროებები. ასევე განხილულია კიბერკარტელები, როგორც ორგანიზებული დანაშაულის ახალი მიმართულება ციფრულ სამყაროში და მათი დანაშაულებრივი საქმიანობის ერთ-ერთი მთავარი ინსტრუმენტი ე.წ „სააუქციონო რობოტები". მიმოხილულია კრიპტოვალუტასთან დაკავშირებული კიბერდანაშულის ახალი სახე „კრიპტოჯეკინგი" (ინგლ. Cryptojacking), რომლის დროსაც ხორციელდება სხვისი კუთვნილი კომპიუტერული მოწყობილობების გამოთვლითი შესაძლებლობების ფარული გამოყენება სხვადასხვა სახის კრიპტოვალუტის საწარმოებლად. სტატიაში განხილულია კრიპტოვალუტებისთვის დამახასიათებელი ანონიმურობის ელემენტი, რომელიც წარმოადგენს როგორც ტერორიზმის დაფინანსების შენიღბვის, ისე გადასახადებისთვის თავის არიდების ერთ-ერთ საშუალებას. ხაზგასმულია ქართული საკანონმდებლო ბაზის სიმწირე და სარეკომენდაციო მაგალითების სახით მოყვანილია ამერიკის შეერთებული შტატებისა და დიდი ბრიტანეთის მიერ შემუშავებული და განხორციელებული საკანონმდებლო ცვლილებები კრიპროვალუტის ბაზრის კონტროლისა და გადასახადებით დაბეგვრის რეგულაციებთან დაკავშირებით.

შესავალი

კრიპტოვალუტა მაღალტექნოლოგიური განვითარების პროდუქტია და მას რამდენიმე სახელით მოიხსენიებენ: მომავლის ფული, ელექტრონული ფული ან/და ციფრული ფული. იგი დაფუძნებულია ბლოკჩეინ ბაზაზე და უნაღდო ანგარიშსწორებისათვის გამოიყენება. ამგვარი ვალუტით ვაჭრობა ძირითადად ელექტრონული, ონლაინ სავაჭრო პლატფორმების მეშვეობით ხორციელდება. დღეისთვის ყველაზე პოპულარულ და მასშტაბურ პლატფორმებს წარმოადგენენ Etoro, BInance, Coinbase, Kriptomat და სხვა პლატფორმები, სადაც ასეულობით სხვადასხვა სახის კრიპტოვალუტა ტრიალებს, თუმცა მის ყველაზე ძველ და პოპულარულ სახეობად Bitcoin ითვლება, რომელიც თავის მხრივ Bitcoin XT, Bitcoin Classic, Bitcoin unlimited, Parity Bitcoin და BTC1-ს აერთიანებს. მისი მწარმოებლებისა და წარმოების ბუნდოვანების გამო საზოგადოებაში აზრი გაყოფილია, ამას ემატება მისი დეცენტრალიზებული ხასიათი და სახელმწიფოების ეროვნული ბანკების კონტროლის მიღმა არსებობის ფაქტორი, რაც მისი, როგორც ვალუტის სიმყარისა და სტაბილურობისადმი კითხვის ნიშნებს აჩენს. კრიპტოვალუტამ თავისი შესაძლებლობებით გამოჩენივესთანავე მიიქცია კიბერდამნაშავეთა განსაკუთრებული ყურადღება და მათთვის ერთ-ერთ პრიორიტეტულ სამიზნედ იქცა. როგორც ყოველგვარ ტექნოლოგიურ სიახლეს, მასაც აქვს თავისი დადებითი და უარყოფითი მხარეები, მაგრამ ჩვენთვის ის საინტერესოა კიბერდანაშაულისა და მასთან დაკავშირებული შესაძლებლობებიდან გამომდინარე პოტენციური საფრთხეების ზრდის თვალსაზრისით, როგორც ტრანსნაციონალური დანაშაულის განხორციელების ობიექტი და საშუალება. კრიპტოვალუტა განსაკუთრებით საინტერესოა უკანონო შემოსავლის ლეგალიზაციის კუთხით, რამაც, სხვადასხვა საერთაშორისო ორგანიზაციების ანგარიშების თანახმად, შემაშფოთებლად გლობალური მასშტაბი მიიღო. მიმდინარე წელს, 2021 წელთან შედარებით, მისი 30%-იანი ზრდა ფიქსირდება და დაახლოებით, 9 მლრდ დოლარი შეადგინა.[1] აღსანიშნავია, რომ თავად კრიპტოვალუტის ღირებულებამ, ელექტრონული ბაზრის ერთიან ბრუნვაში, დღეის მდგომარეობით 1,67 ტრილიონ აშშ დოლარს მიაღწია.[2]

ციფრული ეკონომიკა და ადმინისტრაციული კონტროლის მექანიზმები

ხელშეკრულებები, ტრანზაქციები და ფინანსური ჩანაწერები წარმოადგენენ თანამედროვე კულტურული, პოლიტიკური და ეკონომიკური ურთიერთობების ქვაკუთხედს. მათი საშუალებით ხდება საქმიანი ურთიერთობების ჩარჩოების ჩამოყალიბება და ფინანსური აქტივების დაცვა, პირების იდენტიფიცირება და მოვლენათა ქრონოლოგიის ასახვა. სახელმწიფოების მიერ სხვადასხვა კრიტიკულად მნიშვნელოვანი ფინანსური ინსტრუმენტების ჩამოყალიბებისა და მათ გამოსაყენებლად შემუშავებული საერთაშორისო ბიუროკრატიული წესების ერთობლიობის მიუხედავად, უნდა აღინიშნოს, რომ ისინი ვერ უწყობენ ფეხს ეკონომიკის ციფრული ტრანსფორმაციის მისწრაფებებს. როგორც მარკო ლანციტი თავის ნაშრომში აღნიშნავს: *„აღნიშნული ფინანსური ინსტრუმენტები სულ უფრო და უფრო ემსგავსებიან პიკი საათის დროს შექმნილ საცობს, რომელიც ცდილობს შეაკავოს ფორმულა 1-ის ბოლიდი“.*

ციფრული ტექნოლოგიების ეპოქაში იცვლება ადმინისტრაციული კონტროლის მექანიზმებიც. სწორედ მსგავსი ტიპის მექანიზმს წარმოადგენს ე.წ. „ბლოკჩეინი“ – ბლოკების ჯაჭვის ჩანაწერები (ინგლ. Blockchain), რომლის საშუალებითაც ხდება კრიპტოვალუტებით ვაჭრობისას განხორციელებული ტრანზაქციების ჩანაწერების წარმოება და გადამოწმება. „ბლოკჩეინთან“ ერთად შეგვიძლია წარმოვიდგინოთ სამყარო, რომელშიც მხარეებს შორის გაფორმებული ხელშეკრულებები ინტეგრირებულია ციფრულ კოდში

1 Marshal J., (2 თებერვალი, 2022), „US$8.6 billion worth of crypto-currency laundered by cybercriminals in 2021“, International Security Journal. <https://internationalsecurityjournal.com/cryptocurrency-laundered-in-2021/> [ბოლო წვდომა: 6 მაისი, 2022]

2 Coinmarketcap, (2022, მაისი 6). კრიპტოვალუტის ბრუნვისა და კურსის საინფორმაციო ვებგვერდი. <https://coinmarketcap.com/> [ბოლო წვდომა: 6 მაისი, 2022]

და ინახება გამჭვირვალე, საჯაროდ გაზიარებულ მონაცემთა ბაზაში, სადაც ისინი დაცულია წაშლისგან, გაყალბებისგან ან სხვა სახის უკანონო ხელყოფისგან. როგორც აღინიშნა, „ბლოკჩეინი“ არის კრიპტოვალუტებით განხორციელებული ტრანზაქციების მონაცემთა ბაზა. ტიპური მონაცემთა ბაზის ნაცვლად, სადაც ინფორმაცია ინახება ე.წ. საქაღალდეებში, მოცემულ შემთხვევაში, განხორციელებული ტრანზაქციების ჯგუფებით იქმნება ე.წ. „ბლოკები“. თითოეულ მსგავს „ბლოკს“ გააჩნია გარკვეული მოცულობა ტრანზაქციების შესანახად და როდესაც შეივსება, ემატება წინა „ბლოკს“ და ამგვარად ქმნის ტრანზაქციების ჯაჭვს, რომელიც ცნობილია „ბლოკჩეინის“ სახელწოდებით. აღნიშნული პრინციპით იქმნება ტრანზაქციების ქრონოლოგიური ისტორია (ელექტრონული წიგნის ჩანაწერების სახით), დაწყებული პირველი ტრანზაქციით პირველ „ბლოკში“, დასრულებული ბოლო ტრანზაქციით უახლეს „ბლოკში“. „ბლოკჩეინის“ მოქნილობას განსაზღვრავს ის, რომ იგი ინახავს ყველა ტრანზაქციას, არის გამჭვირვალე და ხელმისაწვდომი ნებისმიერი მომხმარებლისთვის.

ცალსახად უნდა აღინიშნოს, რომ კრიპტოვალუტებთან დაკავშირებულია ძალიან ბევრი პასუხგაუცემელი კითხვა და ბუნდოვანება. დღეის მდგომარეობით, კრიპტოვალუტების საერთაშორისო ბაზარზე მიმდინარე განვითარების პროცესი ადასტურებს, რომ კრიპტოვალუტებში ჩადებული ინვესტიციები არსებითად მაღალი რისკის შემცველია. მათ შეძენასთან ასოცირდება როგორც დიდი მატერიალური მოგება, ასევე, მნიშვნელოვანი ფინანსური დანაკარგებიც, რაც განპირობებულია ბაზრის არასტაბილურობითა და სენსიტიურობით.

კრიპტოვალუტის შექმნამ თავისი ასახვა ჰპოვა საქართველოს ეკონომიკასა და კანონმდებლობაშიც, კერძოდ: საქართველოს ფინანსთა სამინისტროს 2019 წლის 28 ივნისის №201 გადაწყვეტილებით – *„კრიპტოაქტივის და მის მოსაპოვებლად გამოთვლითი სიჩქარის (სიმძლავრის) მიწოდების ოპერაციების გადასახადებით დაბეგვრის თაობაზე“* განისაზღვრა მისი მიწოდებისას დღგ-ით და საშემოსავლო გადასახადით დაბეგვრის საკითხები.[3] მიუხედავად აღნიშნული რეგულაციისა, ქართული კანონმდებლობა თავისი სიმწირით აშკარად ვერ პასუხობს იმ გამოწვევებს, რაც ეკონომიკაში ელექტრონული ბაზრის შემოსვლასთან და მის დამკვიდრებასთან არის დაკავშირებული.

კიბერდანაშაულის სახეები და საფრთხეები

უშუალოდ კრიპტოვალუტის გამოყენებით ან მის უკანონოდ მოსაპოვებლად ჩადენილი დანაშაულებრივი ქმედებების განხილვამდე აუცილებელია შევიქმნათ წარმოდგენა, თუ როგორ ხდება კრიპტოვალუტის გამომუშავება და რეალიზაცია, რა სახის ტექნოლოგიებთან გვაქვს საქმე და რას ენიჭება მატერიალური ღირებულება.

მსოფლიო საზოგადოება უკვე შეთანხმდა, რომ კრიპტოვალუტა არის ციფრული აქტივი, რომელსაც შეუძლია რეალურ ვალუტასთან პარალელურად ფუნქციონირება, როგორც გაცვლის საშუალებას. საკუთრივ სახელიც გვკარნახობს, რომ კრიპტოვალუტები უსაფრთხო და ვერიფიცირებული ტრანზაქციების განხორციელებისას, ასევე, კრიპტოვალუტის ახალი ერთეულის შესაქმნელად იყენებენ კრიპტოგრაფიის (დაშიფვრის) მეთოდოლოგიას.[4] კერძოდ, ტრანზაქციაში მონაწილე მხარეებს აქვთ ე.წ. „საჯარო და პირადი გასაღებები“, რომლებიც წარმოადგენენ შემთხვევითობის პრინციპით დაშიფრული ციფრებისა და ასოების ნაკრებებს. საჯარო გასაღები ფაქტობრივად წარმოადგენს მისამართს, რომელზეც საბოლოოდ უნდა მოხდეს ტრანზაქციით გადაგზავნილი აქტივის ასახვა, ხოლო პირადი გასაღების მიზანი და დანიშნულება არის საჯარო გასაღების გაშიფვრა და ტრანზაქციის დასრულება – ფულის მიღება. მეტი სიცხადისთვის, შეგვიძლია წარმო-

3 საქართველოს საკანონმდებლო მაცნე, (01.07.2019), საქართველოს ფინანსთა სამინისტროს 2019 წლის 28 ივნისის №201 გადაწყვეტილება, საქართველოს საკანონმდებლო მაცნე. <https://matsne.gov.ge/ka/document/view/4601215?publication=0> [ბოლო წვდომა: 6 მაისი, 2022]

4 Weiss. P., (2019). “Cryptocurrency”. Rifkind, Wharton & Garrison LLP (Multinational Law Firm). p. 1.

ვიდგინოთ საფოსტო ყუთი, სადაც წერილის განთავსება შეუძლია ნებისმიერ პირს, თუმცა მხოლოდ საფოსტო ყუთის მესაკუთრეს აქვს გასაღები, რომლის საშუალებითაც შეუძლია გახსნას ყუთი და მიიღოს მისთვის გაგზავნილი შეტყობინება. მსგავსი პრინციპი მოქმედებს კრიპტოვალუტებით ვაჭრობის შემთხვევაშიც, ნებისმიერ პირს აქვს წვდომა სხვა პირის ელექტრონული საფულის მისამართზე (ე.წ. „საჯარო გასაღები“) და შეუძლია განახორციელოს ტრანზაქცია, ხოლო მიმღებს გააჩნია შესაბამისი „პირადი გასაღები“, რომელსაც შეუძლია გაშიფროს ალგორითმი, რომელიც საკუთარ თავში მოიცავს ციფრულ აქტივს – კრიპტოვალუტას.[5] კიბერტექნოლოგიების განვითარებამ ავტომატურად გამოიწვია ციფრული ეკონომიკის განვითარებაც. ამ სფეროში ვაჭრობისა და მოთხოვნა-მიწოდების ბრუნვის ზრდამ წარმოშვა ახალი კრიმინალური მონოპოლიები, რომლებიც ციფრული კარტელების, იგივე კიბერკარტელების სახელით არის ცნობილი. ასეთი კარტელები ციფრული ბაზრის სისტემატური კვლევით არიან დაკავებულნი და ურთიერთშეთანხმების საფუძველზე ახდენენ ფასთა/ღირებულებათა ალგორითმების მანიპულაციის გზით, მათთვის საინტერესო სფეროში და სასურველ პროდუქტზე ფასების ზრდას ან/და არსებულის მოჩვენებით შენარჩუნებას. ეკონომიკურ პლატფორმაზე ციფრული ტრანსფორმაციის ტალღის ზრდა შეუქცევად ხასიათს ატარებს, თუმცა ამ სფეროში ანტიმონოპოლიური სამსახურების რეაგირება სათანადო ეფექტს ვერ იძლევა. ოფიციალურად, პირველი კიბერკარტელური გარიგება ელექტრონულ ბაზარზე 2011 წელს დაფიქსირდა, გარიგების საგანს წარმოადგენდა სახელმწიფო შესყიდვისას მოთხოვნილ პროდუქტზე ფასის ხელოვნური „დაჭერა“, თუმცა ამ ფაქტიდან დღემდე კიბერკარტელების საქმიანობის მეთოდებმა მნიშვნელოვანი „პროგრესი“ განიცადეს.[6]

კიბერკარტელების დანაშაულებრივი საქმიანობის ერთ-ერთი მთავარ ინსტრუმენტს წარმოადგენს ე.წ „სააუქციონო რობოტები“. ეს არის ერთგვარი პროგრამული მოდული, რომელიც ავტომატურ რეჟიმში უზრუნველყოფს ელექტრონული ვაჭრობისას ე.წ „ბიჯის“ ზრდას მათთვის სასურველ ზედა ზღვრამდე. უნდა აღინიშნოს, რომ ამ მოდულის პარალელურად კიბერკარტელები იყენებენ ე.წ „კონკურენტთა იდენტიფიცირებისა და გზიდან ჩამოცილების“, ასევე „კვალის წაშლის“ ელექტრონულ პროგრამებს, რაც გაცილებით ართულებს მათ მხილებას.[7] აღნიშნული პროგრამების გამოყენებით, ახდენენ რა ფასების მონოპოლიზაციას, ისინი ხელოვნურად უზრუნველყოფენ პროდუქტის საბაზრო ფასზე ძვირად რეალიზაციას და ხელოვნურად იზრდიან მოგებას სახელმწიფოს, თუ სხვა მუნიციპალური ორგანოების მიერ გამოცხადებულ ტენდერებში (ან პირიქით, ხელოვნურად ამცირებენ პროდუქტის სააუქციონო ღირებულებას, მისი შეძენის ინტერესის არსებობისას), რაც პირდაპირ აზარალებს სახელმწიფო ბიუჯეტს. მხოლოდ რუსეთის ფედერაციაში 2021 წლის სექტემბერში 10 კიბერკარტელი იქნა იდენტიფიცირებული და მათ მიმართ ფედერალურმა ანტიმონოპოლიურმა სამსახურმა გამოძიება დაიწყო.[8] აღნიშნული სამსახურის მიერ კიბერკარტელებთან ეფექტური ბრძოლის მიზნით შექმნილი იქნა IT სისტემა სახელწოდებით „დიდი ციფრული კატა“, რომელიც დღემდე გამოიყენება ელექტრონულ ბაზარზე საეჭვო გარიგებების იდენტიფიცირებისა და მიკვლევის მიზნით.

აღსანიშნავია, რომ კრიპტოვალუტამ გარკვეულწილად შეცვალა კიბერდანაშაულის განვითარების მიმართულება და კიბერდამნაშავეთა ინტერესის ობიექტად გადაიქცა. ის გახდა, როგორც უკანონო შემოსავლის ლეგალიზაციის საშუალება, ასევე, განსაკუთრებით მძიმე კატეგორიის დანაშაულებრივი ქმედებების დაფინანსების წყარო. კიბერდა-

5 World Crypto Index. (2018). “How Cryptography is used in cryptocurrency”. World Crypto Index, <https://www.worldcryptoindex.com/how-cryptography-is-used-cryptocurrency/> [ბოლო წვდომა: 6 მაისი, 2022]

6 Тесленко А. В., Кониева Ф. И., (2019). „Роботизация торгов – новый вызов в борьбе с картелями”. Из.Юстицинформ. сборник научных трудов., С. 112–122.

7 Иващенко К. А., (2021). „Цифровые картели как новая разновидность киберпреступлений“. Сборник – Киберпреступность: риски и угрозы., С. 84.

8 TADVISER. (2021). Картели на ИТ-рынке России. TADVISER. <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B0%D1%80%D1%82%D0%B5%D0%BB%D0%B8_%D0%BD%D0%B0_%D0%98%D0%A2-

ნაშაულის მიზნებისთვის კრიპტოვალუტა შესაძლოა იყოს, როგორც დანაშაულის ჩადენის საშუალება, ასევე, ობიექტი ან ე.წ. „სატყუარა“, რომელიც გამოყენებულია სენსიტიური ინფორმაციის ფიშინგის (უკანონო მოპოვება) მიზნით. ორგანიზებული კრიმინალური სამყარო დაინტერესებულია კრიპტოვალუტებით, რადგან ის საუკეთესო საშუალებაა დანაშაულებრივი ქმედებებისა და დანაშაულებრივი გზით მოპოვებული აქტივების შესანიღბად. კიბერდამნაშავეების მიერ კრიპტოვალუტა აქტიურად გამოიყენება ე.წ. „დარკ ვებზე“ კიბერდანაშულის ჩასადენად საჭირო ინსტრუმენტების, მონაცემებისა და მომსახურებებით ვაჭრობისას აუცილებელი გადახდების შესასრულებლად.

კრიპტოვალუტის ბაზარი მისი დაარსების დღიდან დაახლოებით 300 000 %-ით გაიზარდა. სწორედ აღნიშნულმა განაპირობა დეველოპერებისა და ინვესტორების მხრიდან გაზრდილი ინტერესი. ბიტკოინისა და სხვა კრიპტოვალუტების ღირებულების ელვისებურმა მატებამ, რა თქმა უნდა, კიბერდამნაშავეების ყურადღებაც მიიპყრო. კრიპტოვალუტასთან დაკავშირებული კიბერდანაშაულის ერთ-ერთი გავრცელებული სახეა კიბერგამოძალვა. როგორც ბოლო წლებში დამკვიდრებული პრაქტიკა გვაჩვენებს, დამნაშავეები მსხვერპლისგან თანხების გამოძალვას ახდენენ კრიპტოვალუტების საშუალებით. კიბერდამნაშავეების მიერ გამოყენებული გამოძალვის მეთოდებს შორის ლიდერობს ე.წ. „რენსომევეარი“ (ინგლ. Ransomware). ეს არის მავნე პროგრამა, რომელიც შიფრავს მსხვერპლის მიერ კომპიუტერში დაცულ მონაცემებს და გამომძალველები ინფორმაციის გასაშიფრად აუცილებელი კოდის სანაცვლოდ მსხვერპლისგან გამოსასყიდს ძირითადად კრიპტოვალუტაში ითხოვენ, რაც ფაქტობრივად სამართალდამცავ ორგანოებს მომავალში დამნაშავეების იდენტიფიცირების შესაძლებლობას უსპობს. აღნიშნული მავნე პროგრამა გლობალური ეკონომიკის ერთ-ერთ მთავარ გამოწვევადაა მიჩნეული.[9]

„რენსომვეარის“ კიბერშეტევის ერთ-ერთი ყველაზე ცნობილი შემთხვევის სახელწოდებაა “WannaCry”, რომელიც 2017 წლის მაისით თარიღდება. აღნიშნული კიბერშეტევა განხორციელდა მსოფლიო მასშტაბით იმ კომპიუტერებზე, რომლებიც ფუნქციონირებდნენ „მაიქროსოფთ ვინდოუსის“ (ინგლ. Microsoft Windows) ოპერატიულ სისტემაზე და არ ჰქონდათ ჩატვირთული უსაფრთხოების განახლება. კერძოდ, აღნიშნული გლობალური კიბერშეტევის განხორციელებამდე დაახლოებით 2 თვით ადრე, ჰაკერული ჯგუფის (ინგლ. Shadow Brokers) მიერ საჯაროდ გამოქვეყნდა ინფორმაცია პროგრამულ სისუსტეზე, რომლითაც ხასიათდებოდა ზემოხსენებული ოპერატიული სისტემა. პროგრამული ხარვეზის აღმოსაფხვრელად კომპანიამ გამოუშვა პროგრამა უსაფრთხოების განახლების მიზნით, თუმცა ყველა ორგანიზაციამ თუ ინდივიდმა არ ჩამოტვირთა აღნიშნული განახლება, რითაც კიბერდამნაშავეებმა ისარგებლეს და დაახლოებით 230 000 კომპიუტერის დაინფიცირება და მონაცემების დაშიფვრა მოახდინეს. თითოეულ შემთხვევაში კიბერდამნაშავეები დაშიფრული ინფორმაციის გასაშიფრად მომხმარებლებისგან გამოსასყიდის სახით თანხას ბიტკოინებში ითხოვდნენ. აღნიშნული გლობალური კიბერშეტევის შედეგად მიყენებულმა ზიანმა შეადგინა დაახლოებით 4 მლრდ აშშ დოლარი.[10] კრიპტოვალუტის ბუნების გათვალისწინებით, შესაბამისი დარგის ექსპერტები მივიდნენ დასკვნამდე, რომ კრიპტოვალუტების არსებობამ და პოპულარობამ ცალსახად შეუწყო ხელი „რენსომვეარის“ შეტევების ზრდას. კრიპტოვალუტებში ტრანზაქციების სიმარტივემ, დანაშაულებრივი გზით მიღებული შემოსავლების შესაბამის ანგარიშზე გადათავსების სისწრაფემ, ელექტრონული გადარიცხვებისას მესამე პირებისგან კონტროლის არარსებობამ და სამართალდამცავი ორგანოებისთვის ტრანზაქციების მიკვლევადობის სირთულემ კიბერდამნაშავეებისთვის „რენსომვეარის“ შეტევების განხორციელება და გამოსასყიდის ბიტკოინებში მიღება გაცილებით მიმზიდველი გახადა. კიბერდანაშაულის

%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8> [ბოლო წვდომა: 6 მაისი, 2022]

9 Lapuh Bele J., (2021). “Cryptocurrencies as facilitators of cybercrime”. SHS Web of Conferences Volume 111. pp. 1-6.

10 Kaspersky lab. (2022). “What is Wannacry Ransomware”. Mimicast, <https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/> [ბოლო წვდომა: 6 მაისი, 2022]

ცნობილი შემთხვევებიდან აღსანიშნავია კომპანია „კოლონიალ პაიპლაინის“ (ინგლ. Colonial Pipeline) საქმე, რომელიც პასუხისმგებელია აშშ-ის აღმოსავლეთ სანაპიროსთვის აუცილებელი საწვავის დაახლოებით ნახევრის მიწოდებაზე. აღნიშნული კომპანია 2021 წელს გახდა „რენსომვეარის“ შეტევის მსხვერპლი და იძულებული გახდა, კომპიუტერული მონაცემების გასაშიფრად კიბერდამნაშავეებისთვის 4.4 მილიონი აშშ დოლარის ღირებულების კრიპტოვალუტა გადაერიცხა. არანაირი ოფიციალური ცნობა კიბერდამნაშავეების აღმოჩენისა და მათი სისხლისსამართლებრივი პასუხისმგებლობის თაობაზე ამ დრომდე არ მოიპოვება. ასევე, ხორცის გადამამუშავებელი, მსოფლიოს უმსხვილესი კომპანია „JBS“ იძულებული გახდა კიბერდამნაშავეების რუსული დაჯგუფებისთვის გამოსასყიდის სახით გადაერიცხა 11 მილიონი აშშ დოლარის ღირებულების კრიპტოვალუტა, „რენსომვეარის“ შეტევის შედეგად 13 ქარხანაში შეჩერებული წარმოების განსაახლებლად.[11]

კრიპტოვალუტის სავაჭრო ბირჟებზე კიბერდანაშაულის მზარდი სტატისტიკა არსებითად საზიანოა კრიპტოვალუტის ბიზნესის განვითარებისთვისაც, რადგან ამცირებს მომხმარებლის ნდობას და ზრდის აქტივების დაკარგვის რისკს. მკვლევრების მიერ შესწავლილი იქნა 2011-2021 წლებში კიბერდამნაშავეების მიერ ჩადენილი ყველაზე დიდი მასშტაბის კრიპტოვალუტების ქურდობისა და თაღლითურად დაუფლების 30 შემთხვევა. აღნიშნული შემთხვევების ანალიზის შედეგად დადგინდა, რომ ჰაკერული შეტევების დაჯგუფება შესაძლებელია 3 ძირითად კატეგორიად: 1. პლატფორმების უსაფრთხოების სისტემაში სისუსტეების აღმოჩენა, მასში შეღწევა და კრიპტოვალუტების უკანონოდ მოსაპოვებლად მომხმარებლების შესახებ აუცილებელი ინფორმაციის მოპოვება; 2. ე.წ. „ადამიანური შეცდომა“, რა დროსაც კრიპტოვალუტის მფლობელები ხდებიან ჰაკერების მიერ გამოგზავნილი ვირუსის მსხვერპლი და უნებლიედ უზიარებენ კიბერდამნაშავეებს მათი ელექტრონული საფულის პირად გასაღებს, რითაც აძლევენ წვდომას მატერიალურ აქტივებზე; 3. მესამე ტიპის კრიპტოვალუტის ქურდობა დაკავშირებული არ არის ადამიანურ დაუდევრობასთან ან პლატფორმების არასრულფასოვან უსაფრთხოების სისტემებთან, არამედ განპირობებულია კრიპტოვალუტების ვაჭრობისთვის განკუთვნილი პლატფორმების დამფუძნებლების ან სხვა დასაქმებული პირების კიბერდამნაშავეებთან თანამშრომლობასთან (ინსაიდერული ინფორმაციის გამოყენება კიბერშეტევის განსახორციელებლად). აღნიშნული ტიპის კრიპტოვალუტის ქურდობის პრევენცია პრაქტიკულად შეუძლებელია. კრიპტოვალუტების გახშირებული ქურდობის გამო, ზოგიერთმა პლატფორმამ მომხმარებლებისთვის აქტივების დაზღვევის გარკვეული ფორმების შეთავაზებაც კი დაიწყო.

ჩატარებული კვლევის საფუძველზე დადგინდა, რომ 2011-2021 წლებში ჩადენილი კრიპტოვალუტების ქურდობის 30 ყველაზე მასშტაბური კიბერდანაშაულიდან 20 განაპირობა ჰაკერების მიერ უსაფრთხოების სისტემაში აღმოჩენილმა სისუსტემ, რა დროსაც სავაჭრო პლატფორმებზე მომხმარებლების მაიდენტიფიცირებელი მონაცემები და მათი ელექტრონული საფულეების „პირადი გასაღებები“ არ იყო სათანადოდ დაცული. 5 შემთხვევა გამოწვეული იყო „ადამიანური შეცდომით“, რა დროსაც მომხმარებლები გაუცნობიერებლად ხდებოდნენ ჰაკერების მიერ გამოგზავნილი ვირუსის ან/და მავნე პროგრამის მსხვერპლი, რის შემდეგაც კიბერდამნაშავეებს უნებლიედ აძლევდნენ წვდომას კომპიუტერულ მოწყობილობაზე, სადაც დაცული იყო მათ საკუთრებაში არსებული კრიპტოვალუტის მოსაპოვებლად საჭირო ინფორმაცია. დანარჩენ 5 შემთხვევაში კრიპტოვალუტის ქურდობა ჩადენილია ბირჟის „ინსაიდერის“ (პირი, რომელიც დასაქმებულია სავაჭრო პლატფორმაზე და ფლობს კრიტიკულად მნიშვნელოვან ინფორმაციას მომხმარებლების თაობაზე) მიერ. კრიპტოვალუტის მესაკუთრეებისთვის მიყენებული მატერიალური ზიანის ოდენობის მხრივ ყველაზე დიდი მასშტაბით ხასიათდება სავაჭრო პლატფორმების „ინსაიდერების“ მიერ ჩადენილი კიბერდანაშაული, რომლებიც ძირითადად მოქმედებენ სხვა კიბერდამნაშავეებთან

11 Arista Networks. (2021). “The Role of Cryptocurrency in Ransomware Attacks”. ARTISTA. <https://www.untangle.com/inside-untangle/the-role-of-cryptocurrency-in-ransomware-attacks/> [ბოლო წვდომა: 6 მაისი, 2022]

ერთად. სტატისტიკის თანახმად, უკანასკნელი 10 წლის განმავლობაში, კიბერდამნაშავეების მიერ ჩადენილი კრიპტოვალუტების ქურდობის 30 მასშტაბური შემთხვევის შედეგად უკანონოდ დაუფლებული აქტივების საერთო ღირებულებამ (თუ გავითვალისწინებთ, რომ მათი გადაცვლა ქაღალდის ფულში მოხდა დანაშაულის ჩადენიდან უახლოეს პერიოდში) დაახლოებით 7 მლრდ დოლარი შეადგინა. [12]

კრიპტოვალუტასთან დაკავშირებული კიბერდანაშაულის კიდევ ერთ ახალ სახეს წარმოადგენს ე.წ. „კრიპტოჯეკინგი“ (ინგლ. Cryptojacking). აღნიშნული დანაშაულის ჩადენის მიზანი არის სხვისი კუთვნილი კომპიუტერული მოწყობილობების გამოთვლითი შესაძლებლობების ფარული გამოყენება სხვადასხვა სახის კრიპტოვალუტის საწარმოებლად. კერძოდ, კიბერდამნაშავეები ავრცელებენ სხვადასხვა მავნე აპლიკაციებსა და ვირუსებს პოტენციურ მსხვერპლთა კომპიუტერულ მოწყობილობებში მოხვედრის მიზნით. სპეციალური ცოდნის გარეშე მომხმარებელმა, შესაძლოა, ვერც შეამჩნიოს, რომ „კრიპტოჯეკინგის“ მსხვერპლია, რადგან პროგრამული უზრუნველყოფის აღმოჩენა, რომელსაც კიბერდამნაშავეები იყენებენ, მაქსიმალურად რთულია. თუმცა, უნდა აღინიშნოს, რომ არსებობს კომპონენტები, რომლებზეც დაკვირვების შემთხვევაში, მომხმარებლებს შეუძლიათ დაადგინონ – არის თუ არა მათი მოწყობილობა დავირუსებული. „კრიპტოჯეკინგის“ მეთოდით გამოთვლითი რესურსების ქურდობა ანელებს ელექტრონულ მოწყობილობაზე მიმდინარე სხვა კომპიუტერულ პროცესებს, მომხმარებელს საგრძნობლად ეზრდება ელექტროენერგიის გადასახადი და მცირდება მოწყობილობის ვარგისიანობის ვადა. კიბერდამნაშავეებს იზიდავს „კრიპტოჯეკინგი“, რადგან აღნიშნული დანაშაულის ერთადერთ მიზანს წარმოადგენს დიდი შემოსავლის მიღება ყოველგვარი დანახარჯების გარეშე. არსებობს „კრიპტოჯეკინგის“ განხორციელების ორი გავრცელებული მეთოდი: 1. კიბერდამნაშავეები კლასიკურად ელექტრონული ფოსტით აგზავნიან დავირუსებულ ინტერნეტ ბმულს, რომელზეც ხელის დაჭერის შემთხვევაში მომხმარებლის კომპიუტერში ავტომატურად იტვირთება კრიპტოვალუტის მომპოვებელი კოდი; 2. მეორე გავრცელებული მეთოდის შემთხვევაში, კიბერდამნაშავეები არჩევენ ვებგვერდებს, რომლებსაც მრავლად სტუმრობენ მომხმარებლები და აღნიშნულ ვებგვერდებზე ცდილობენ იპოვონ პროგრამული სისუსტე, რომლის აღმოჩენის შემთხვევაში ტვირთავენ მავნე პროგრამის კოდს. შემდგომში, ინტერნეტ მომხმარებლის ნებისმიერი ელექტრონული მოწყობილობა, რომელიც ესტუმრება დავირუსებულ ვებგვერდს, ავტომატურად დაინფიცირდება და კიბერდამნაშვეები შეძლებენ მისი გამოთვლითი რესურსის მიმართვას კრიპტოვალუტის საწარმოებლად. 2017-2018 წლების შემდეგ „კრიპტოჯეკინგი“ საკმაოდ გავრცელებული კიბერდანაშაულის სახეობა გახდა. ცნობილია „კრიპტოჯეკინგის“ რამდენიმე მსხვილმასშტაბიანი შემთხვევა, მათ შორის, ევროპის წყალმომარაგების მართვის სისტემის ოპერატიულ-ტექნოლოგიური ქსელის გამოთვლითი რესურსის გამოყენება. ასევე, ცნობილი შემთხვევა დაფიქსირდა რუსეთის ფედერაციაში, როდესაც რუსი მეცნიერების ჯგუფმა გამოიყენა სუპერშესაძლებლობების მქონე კომპიუტერი კვლევითი და ბირთვული ქობინების ობიექტის გამოთვლითი რესურსების ასათვისებლად და ბიტკოინის მოსაპოვებლად.[13]

კრიპტოვალუტასთან დაკავშირებული კიბერდანაშაულების ზრდის სტატისტიკისა შესამცირებლად, მათი პრევენციისა და ბრძოლის ეფექტიანი მექანიზმების დასანერგად, ევროპარლამენტი ცდილობს შეიმუშავოს გარკვეული რეკომენდაციები ევროკავშირის წევრი ქვეყნებისთვის. რეკომენდაციის თანახმად, კრიპტოვალუტის მომხმარებელთა ანონიმურობის გამოსავლენად განიხილება ერთიანი სავალდებულო რეგისტრაციის შექმნის იდეა. ევროკავშირი განიხილავს კრიპტოვალუტების ისეთი მახასითებლების შექმნაზე აკრძალვის დაწესებას, რომელიც შეუძლებელს ხდის მათი მომხმარებლების დადგენას/გადამოწმებას. ასევე, წამოჭრილია ფინანსური ტრანზაქციების რეგულაციის ფარგლების გაფართოების საკითხი, კრიპტოვალუტით გა-

12 Bernardi M., Charoenwong B., (2022). “A Decade of Cryptocurrency Hacks: 2011-2021”, Business School, National University of Singapore, pp. 1-6.

13 Malwarebytes Company. (2022). “Cryptojacking – What is it?”. Malwarebytes. <https://www.malwarebytes.com/cryptojacking> [ბოლო წვდომა: 6 მაისი, 2022]

ნხორციელებული ფინანსური ტრანზაქციების შემოწმების მიზნით, ფულის გათეთრებისა და ტერორიზმის დაფინანსების რისკების გამოსარიცხად. თუმცა, რეკომენდაციებში ასევე ცალსახად აღნიშნულია, რომ ფოკუსირება უნდა მოხდეს კრიპტოვალუტების უკანონო გამოყენების შემთხვევებზე და „ბლოკჩეინის“ დადებითი ეფექტი და მისი განვითარების პერსპექტივა არ უნდა იყოს ნიველირებული.

მსოფლიო თანხმდება, რომ კრიპტოვალუტების ბაზრის განვითარების პროპორციულად გაიზარდა ფულის გათრეთრებისა და ტერორიზმის დაფინანსების შემთხვევები. აღნიშნული, განსაკუთრებით მძიმე კატეგორიის დანაშაულების ჩადენის რისკის შესამცირებლად, კრიპტოვალუტით მოვაჭრე დამნაშავეების გამოსავლენად აუცილებელია ანონიმურობასთან დაკავშირებული პრობლემის აღმოფხვრა/დარეგულირება. ანონიმურობა ხელს უშლის სამართალდამცავ ორგანოებს, რათა უზრუნველყონ კრიპტოვალუტის ტრანზაქციების ადეკვატური მონიტორინგი, რაც იძლევა „საეჭვო“ ტრანზაქციების განხორციელებელის შესაძლებლობას მარეგულირებელი პერიმეტრის მიღმა. აღნიშნული სისტემა ფაქტობრივად ქმნის ნოყიერ ნიადაგს კრიმინალური ორგანიზაციებისთვის, რომ კრიპტოვალუტის ბაზრის გამოყენებით ჰქონდეთ მარტივი და მოქნილი წვდომა „სუფთა, ნაღდ ფულზე“.[14]

რაც შეეხება ტერორიზმის დაფინანსებასა და კრიპტოვალუტის ანონიმურობის ნეგატიურ როლს აღნიშნულთან მიმართებით, ნათელ მაგალითს წარმოადგენს ალი შუქრი ამინის მიერ 2015 წელს სოციალურ ქსელ „ტვიტერზე“ საჯაროდ გაზიარებული ინსტრუქცია, თუ როგორ შეიძლებოდა „დაეშის“ (ისლამური სახელმწიფო) დაფინანსების შენიღბვა ბიტკოინის გამოყენებით. ალი შუქრის მიერ გამოქვეყნებულ ინფორმაციაში მითითებული იყო, როგორ უნდა გამოყენებინათ კრიპტოვალუტები ჯიჰადისტების დასაფინანსებლად. ის დეტალურად უხსნიდა მიმდევრებს, რას წარმოადგენდა კრიპტოვალუტა, აძლევდა რჩევებს, რათა გამოეყენებინათ ე.წ. „Dark Wallet“ („ბნელი საფულე“), რომელიც ხასიათდება სრული ანონიმურობით. ინფორმაცია ასევე შეიცავდა დეტალებს, თუ როგორ უნდა შეექმნათ ყალბი შემოწირულობის ფონდები ტერორიზმის დაფინანსების შესანიღბად. აღნიშნული აგიტაციის საფუძველზე ალი შუქრი ამინი ცდილობდა მოეძიებინა, წაეხალისებინა და დაეფინანსებინა პირები სირიაში წასასვლელად და ისლამური სახელმწიფოს მხარეს საბრძოლველად. ზემოხსენებული დანაშაულებრივი ქმედებებისთვის 2015 წლის 28 აგვისტოს, ამერიკის შეერთებული შტატების ფედერალური სასამართლოს გადაწყვეტილებით, ალი შუქრი ამინს მიესაჯა 11 წლით თავისუფლების აღკვეთა (სასჯელის მოხდის შემდეგ, სიცოცხლის ბოლომდე, პოლიციის ზედამხედველობის ქვეშ ყოფნის პირობით).[15]

კრიპტოვალუტასთან დაკავშირებული სამართლებრივი მექანიზმები და რეგულაციები

კრიპტოვალუტებისთვის დამახასიათებელი ანონიმურობის ელემენტი წარმოადგენს პრობლემურ საკითხს გადასახადებისთვის თავის არიდების შემთხვევების იდენტიფიცირების თვალსაზრისითაც. კერძოდ, კრიპტოვალუტებით გადასახადის გადახდის გარეშე განხორციელებული ოპერაციები ცალსახად წარმოადგენს გადასახადებისგან თავის არიდების ფაქტებს. მაშინ როცა საგადასახადო ორგანოსთვის უცნობია დასაბეგრი ოპერაციის განმახორციელებელი მხარე, ფაქტობრივად შეუძლებელია შესაბამისი პასუხისმგებლობის საკითხის დაყენება. კრიპტოვალუტის გამოყენებით ტერორიზმის დაფინანსების, ფულის გათეთრებისა და სხვა დანაშაულებრივი ქმედებების გამოვლენა დიდ სირთულეებთან არის დაკავშირებული, ვინაიდან დამნაშავეების მხრიდან ტრანზაქციების განხორციელება სხვადასხვა ქვეყნებს შორის არ მოითხოვს დიდ ძალისხმევას. ზემოხსენებული დანაშაულების წინააღმდეგ ბრძოლას

14 Dr. Houben R., Snyers A., (2018). “Legal contexts and implications for financial crime, money laundering and tax evasion”, European Parliament (Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies), p. 9.

15 Financial Action Task Force (FATF) Report. (October, 2015). “Emerging Terrorists Financial Risks”. FATF <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> [ბოლო წვდომა: 6 მაისი, 2022]

აფერხებს კრიპტოვალუტების გამოყენებით განხორციელებული ტრანზაქციებისა და საკუთრივ კრიპტოვალუტის ემისიის მარეგულირებელი სისტემის არარსებობა. საზოგადოდ დამკვიდრებული აზრის თანახმად, დაშიფვრის მეთოდი, რომელსაც ითვალისწინებს კრიპტოვალუტის კონფიდენციალურობის პოლიტიკა, წარმოადგენს მოქალაქეებისა და ბიზნესისთვის ჰაკერების შემოტევისგან, პერსონალური მონაცემების ქურდობისგან, თაღლითობისგან და სხვა სახის კიბერსაფრთხეებისგან თავის დაცვის ეფექტურ საშუალებას. თუმცა, აქვე აღსანიშნავია, რომ სწორედ კრიპტოვალუტებთან დაკავშირებული კონფიდენციალურობა და ანონიმურობა ქმნის კიბერდამნაშავეების მიერ აღნიშნული „პრივილეგიებით“ არალეგიტიმურად სარგებლობის მომეტებულ საფრთხეს. ზემოაღნიშნული ფაქტორებიდან გამომდინარე, არსებითად მნიშნელოვანია ოქროს შუალედის პოვნა დაშიფვრის მეთოდოლოგიასთან მიმართებით, ერთი მხრივ, კონფიდენციალურობისა და ანონიმურობის შენარჩუნების მიზნით, მომხმარებლების კიბერუსაფრთხოებისა და პირადი ინფორმაციის შემცველი მონაცემების დაცვის უზრუნველსაყოფად და მეორე მხრივ, სამართალდამცავი ორგანოებისთვის ლეგიტიმური წვდომის შესაძლებლობების შექმნის აუცილებლობიდან გამომდინარე.

კრიპტოვალუტის ბაზრის ზრდის პროპორციულად მსოფლიო მასშტაბით იზრდება სახელმწიფოების ინტერესი, რომ შეიმუშავონ გარკვეული სახის სამართლებრივი რეგულაციები ციფრული ბაზრის სამართავად.

აღსანიშნავია, რომ მიუხედავად განვითარების დონისა, არც ამერიკის შეერთებულ შტატებს გააჩნია ერთიანი სამართლებრივი რეგულაციები კრიპტოვალუტასთან მიმართებით და იგი დღემდე აგრძელებს მუშაობას ერთიანი ფედერალური კანონმდებლობის შემუშავების მიმართულებით. ფინანსური დანაშაულების აღსრულების ქსელი (FinCEN) არ აღიარებს კრიპტოვალუტას, როგორც გადახდის ლეგალურ საშუალებას, თუმცა მიიჩნევს, რომ კრიპტოვალუტა არის „ფულის გადაცემის საშუალება“, რადგან მას გააჩნია ღირებულება, რომელიც ანაცვლებს ფულის ერთეულს. აშშ-ის შემოსავლების სამსახურიც არ აღიარებს კრიპტოვალუტას, როგორც გადახდის კანონიერ საშუალებას, მაგრამ განსაზღვრავს მას, როგორც „ღირებულების ციფრულ წარმოდგენას, რომელიც ფუნქციონირებს როგორც გაცვლის საშუალება, ანგარიშის ერთეული". შემოსავლების სამსახური მას აღიქვამს, როგორც ქონებას, რომელიც ექვემდებარება საერთო წესის შესაბამისად დაბეგვრას. კრიპტოვალუტის გადაცვლა ლეგალურია შეერთებულ შტატებში და ექცევა ბანკის საიდუმლოების აქტის (BSA) რეგულაციის ფარგლებში. ეს ნიშნავს, რომ პრაქტიკაში კრიპტოვალუტის გადაცვლის მომსახურების მიმწოდებლები უნდა დარეგისტრირდნენ ფინანსური დანაშაულების აღსრულების ქსელში (FinCEN), შეინარჩუნონ შესაბამისი ჩანაწერები და საჭიროების შემთხვევაში წარუდგინონ ანგარიშები ხელისუფლების წარმომადგენლებს. აშშ-ის ფასიანი ქაღალდებისა და ბირჟის კომისიამ (SEC) განაცხადა, რომ იგი კრიპტოვალუტებს მიიჩნევს ფასიან ქაღალდებად და ფასიანი ქაღალდების კანონებს სრულყოფილად გამოიყენებს ციფრულ საფულეებსა და სავაჭრო ბირჟებთან მიმართებით. განსხვავებული და რბილი მიდგომა შეიმუშავა აშშ-ის „საქონლის ფიუჩერსების სავაჭრო კომისიამ“ (CFTC), რომელმაც მიიღო რა ე.წ. „არ დააზიანოს" სახის ნორმა, აღწერა ბიტკოინს, როგორც მატერიალური ღირებულების მქონე პროდუქტი. კომისია საჯაროდ ვაჭრობის საშუალებას აძლევს ნებისმიერ პირს. ფინანსური დანაშაულების წინააღმდეგ ბრძოლის სახელმწიფოთაშორისი ორგანიზაციის (FATF) მიერ 2019 წლის ივნისში მიღებული მითითებების საპასუხოდ, ფინანსური დანაშაულების აღსრულების ქსელმა (FinCEN) კატეგორიულად განაცხადა, რომ მას აქვს ლეგიტიმური მოლოდინი, რომ კრიპტოვალუტების სავაჭრო ბირჟები დაიცავენ ე.წ. „მოგზაურობის წესს“, რაც გულისხმობს კრიპტოვალუტების გამოყენებით განხორციელებული ტრანზაქციების, მათი შემქმნელებისა და ბენეფიციარების შესახებ ინფორმაციის გაზიარებას. აღნიშნულმა ორგანიზაციამ კრიპტოვალუტის გადაცვლის მოქმედებები გაათანაბრა ტრადიციული ფულის გადაცვლის მოქმედებებთან და მოაქცია ბანკის საიდუმლოების აქტში (BSA) გაწერილი რეგულაციების კატეგორიაში. აშშ-ის ხაზინის დეპარტამენტმა ხაზგასმით აღნიშნა გლობალური და შიდა დანაშაულებრი-

ვი საქმიანობის წინააღმდეგ საბრძოლველად კრიპტორეგულაციების გადაუდებელი საჭიროება. 2020 წლის დეკემბერში FINCEN-მა დაიანონსა კრიპტოვალუტის ახალი რეგულაცია, კრიპტოვალუტის ბირჟებიდან და საფულეებიდან მონაცემთა შეგროვების მოთხოვნების დაწესების მიზნით. არსებობს საფუძვლიანი მოლოდინი, რომ ახალი რეგულაცია ძალაში შევა 2022 წლის შემოდგომაზე და კრიპტოვალუტების სავაჭრო პლატფორმებს დაუწესებს რეგულაციას, რომლის თანახმადაც, საეჭვო აქტივობის ანგარიშებზე 10 000 აშშ დოლარზე მეტი ღირებულების ტრანზაქციის განხორციელების შემთხვევაში, მათ გაუჩნდებათ ინფორმაციის გადაგზავნის ვალდებულება. ასევე, ახალი რეგულაციების შესაბამისად, კრიპტოვალუტის მფლობელებს მოუწევთ საკუთარი თავის იდენტიფიცირება ერთჯერადად 3 000 აშშ დოლარზე მეტი ოდენობის ტრანზაქციის განხორციელების შემთხვევაში.

2021 წელს კონგრესმა ასევე განიხილა კრიპტოვალუტის მომსახურების მომწოდებლების სტატუსი. ბაიდენის ადმინისტრაციის მიერ ინფრასტრუქტურის კანონპროექტში შეტანილი ახალი წესების თანახმად, კრიპტოვალუტის ბირჟები განიხილებიან, როგორც ბროკერები და მათი საქმიანობა უნდა შეესაბამებოდეს შესაბამის კანონმდებლობას და ითვალისწინებდეს ანგარიშების წარდგენისა და შესაბამისი ჩანაწერების შენახვის ვალდებულებებს.

დიდ ბრიტანეთს არ გააჩნია კრიპტოვალუტასთან დაკავშირებით შემუშავებული კონკრეტული სამართლებრივი აქტები, თუმცა კანონმდებლობის შესაბამისად, კრიპტოვალუტა აშშ-ის მსგავსად არ ითვლება გადახდის აღიარებულ კანონიერ საშუალებად. სავაჭრო პლატფორმებს დაწესებული აქვთ რეგისტრაციის მოთხოვნები, შემოსავლების სამსახურმა განმარტა, რომ კრიპტოვალუტებს გააჩნიათ „უნიკალური იდენტობა“ და არ შეიძლება მათი შედარება ჩვეულებრივ ინვესტიციებთან და გადახდის ტრადიციულ ფორმებთან. გადასახადებით დაბეგვრა უნდა განხორციელდეს თითოეული აქტივობისა და საქმიანობაში ჩართული მხარეების იდენტიფიცირების საფუძველზე. კრიპტოვალუტების ვაჭრობით მიღებული მოგება ექვემდებარება გადასახადით დაბეგვრას. ევროკავშირის დატოვების შემდეგ, დიდმა ბრიტანეთმა საკუთარ კანონმდებლობაში ასახა ფულის გათეთრების წინააღმდეგ ბრძოლის საერთაშორისო რეკომენდაციები და აღნიშნულის ფარგლებში განმარტა, რომ კრიპტოვალუტის გადაცვლის მომსახურების მიმწოდებლები ექვემდებარებიან სავალდებულო რეგისტრაციას ფინანსური სამქიანობის ორგანიზაციაში (FCA) და მათ უნდა უზრუნველყონ საქმიანობის ამსახველი ანგარიშების შენახვა/წარდგენის ვალდებულებების შესრულება. მიუხედავად იმისა, რომ არ არის შემუშავებული სპეციალური დებულებები გადაცვლის მომსახურების მიმწოდებლებისთვის, FCA ხაზს უსვამს, რომ ნებისმიერმა კრიპტოვალუტებთან დაკავშირებულ საქმიანობაში მონაწილე სუბიექტმა უნდა შეასრულოს ფულის გათეთრების, ტერორისტული ორგანიზაციების დაფინანსებისა და თანხების ტრანზაქციებთან (ინფორმაცია გადამხდელის შესახებ) დაკავშირებით 2017 წელს შემუშავებული რეგულაციების მოთხოვნები (მათ შორის ჩანაწერების შენახვის თაობაზე).

კრიპტოვალუტასთან დაკავშირებული რეგულაციების მიმოხილვის საფუძველზე შეიძლება დავასკვნათ, რომ განვითარებული ქვეყნები ცდილობენ შეიმუშავონ ისეთი სამართლებრივი მექანიზმები, რომლებიც არ დაუკარგავენ მიმზიდველობას კრიპტოვალუტას, როგორც დეცენტრალიზებულ საანგარიშსწორებო ინსტრუმენტს და, ამავდროულად, სამართალდამცავ ორგანოებს მიეცემათ საეჭვო ტრანზაქციებში ჩართული სუბიექტების იდენტიფიცირების შესაძლებლობა.[16]

დასკვნა

დღეის მდგომარეობით საქართველოში ფაქტობრივად არ არსებობს კრიპტოვალუტასთან დაკავშირებული სამართლებრივი რეგულაციები, რაც დააზღვევდა კრიპტოვალუტასთან დაკავშირებულ საფრთხეებს. ამასთან, რეგულაციების შემოღებისას აუცილებლად უნდა გავითვალისწინოთ ის ფაქტორი, რომ

16 Comply Advantage. (2022). “Cryptocurrency Regulations around the World”. Comply Advantage. <https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/> [ბოლო წვდომა: 6 მაისი, 2022]

კრიპტოვალუტა ამჟამად წარმოადგენს მსოფლიო ტრენდს და შესაბამისად, მისი ბრუნვის გარკვეულწილად შეზღუდვამ, აკრძალვამ ან მასზე დაწესებულმა მკაცრმა რეგულაციებმა შესაძლოა მომავალში დიდი ზიანი მიაყენოს ისეთი პატარა ქვეყნის ეკონომიკას, როგორსაც საქართველო წარმოადგენს. როგორც ზემოთ აღვნიშნეთ, მსოფლიო მოწინავე სახელმწიფოებიც დიდი სიფრთხილით ეკიდებიან ახალი რეგულაციების შემუშავებას და მაქსიმალურად ცდილობენ, არ დააროვიონ ე.წ. „ოქროს შუალედი“. ამასთანავე, არანაკლებ პრიორიტეტულია განსაკუთრებით საშიში ხასიათის დანაშაულების (ფულის გათეთრება, ტერორიზმის დაფინანსება და განსაკუთრებით დიდი ოდენობის გადასახადებისგან თავის არიდება) პრევენციაზე ზრუნვა და კრიპტოვალუტების გამოყენებით აღნიშნული დანაშაულების ჩადენის რისკების მაქსიმალურად შემცირება. აღნიშნული ორი ფაქტორის გათვალისწინებით, აუცილებელია, რომ საქართველომ, განვითარებული ქვეყნების მაგალითებზე დაყრდნობით, შეიმუშავოს საკანონმდებლო ჩარჩო, რომელიც უზრუნველყოფს როგორც კრიპტოვალუტის ბაზრის თავისუფლებას, ასევე, გარკვეულ ბერკეტებს მისცემს სამართალდამცავ ინსტიტუტებს, რათა მოახდინონ საეჭვო ტრანზაქციების მყისიერი იდენტიფიცირება, გადამოწმება და საჭიროების შემთხვევაში, მოახდინონ შესაბამისი რეაგირება. ციფრული ეკონომიკის ზრდის შეუქცევადობა და მასთან დაკავშირებული კიბერდანაშაულის საფრთხეების პირდაპირ პროპორციული ზრდა სახელმწიფოს მხრიდან განსაკუთრებული ყურადღების საგანი უნდა გახდეს, რაც არა მხოლოდ სათანადო საკანონმდებლო რეგულაციების შემოღებას, არამედ შესაბამისი მაკონტროლებელი ინსტიტუტების შექმნასა და ფუნქციონირებას საჭიროებს.

ბიბლიოგრაფია:

გამოყენებული საკანონმდებლო აქტები:

1. საქართველოს საკანონმდებლო მაცნე, (01.07.2019), საქართველოს ფინანსთა სამინისტროს 2019 წლის 28 ივნისის №201 გადაწყვეტილება, საქართველოს საკანონმდებლო მაცნე. <https://matsne.gov.ge/ka/document/view/4601215?publication=0>

კვლევები:

1. ბერნარდი, მ. და ჩაროენვონგი, ბ., (2022). „2011-2021 წლების კრიპტოვალუტასთან დაკავშირებული კიბერდანაშაულის კვლევა“, სინგაპურის ეროვნული უნივერსიტეტი.

უცხოენოვანი ლიტერატურა:

1. Weiss. P., (2019). “Cryptocurrency”. Rifkind, Wharton & Garrison LLP (Multinational Law Firm);
2. Тесленко А. В., Кониева Ф. И., (2019). „Роботизация торгов – новый вызов в борьбе с картелями”. Из.Юстицинформ. сборник научных трудов;
3. Иващенко К. А., (2021). „Цифровые картели как новая разновидность киберпреступлений“.

BIBLIOGRAPHY:

Legal Acts:

1. Legislative Herald of Georgia, (01.07.2019), Decision of the Ministry of Finance of Georgia of June 28, 2019 №201, Legislative Herald of Georgia. <https://matsne.gov.ge/ka/document/view/4601215?publication=0> (In Georgian)

Researches:

1. Bernardi M., Charoenwong B., (2022). “A Decade of Cryptocurrency Hacks: 2011-2021”, Business School, National University of Singapore. (In Georgian)

Used Literature:

1. Weiss. P., (2019). “Cryptocurrency”. Rifkind, Wharton & Garrison LLP (Multinational Law Firm). (In English)
2. Teslenko A.V., Konieva F. I., (2019). “Robotization of sales – new challenge to combat the cyber-cartels”. Iustitsinform. Collection of scientific works. (In Russian)
3. Ivashenko K.A., (2021). “Digital Cartels as the new type of cybercrime”. Collection – Cybercrime: Risks and threats. (In Russian)
4. Dr. Houben R., Snyers A., (2018). “Legal contexts and implications for financial crime, money

Сборник – Киберпреступность: риски и угрозы;
4. Dr. Houben R., Snyers A., (2018). “Legal contexts and implications for financial crime, money laundering and tax evasion”, European Parliament (Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies).
5. Lapuh Bele J., (2021). “Cryptocurrencies as facilitators of cybercrime”. SHS Web of Conferences Volume 111.

ინტერნეტ რესურსები:

1. Marshal, J., (2022, თებერვალი 2), ,,US$8.6 billion worth of crypto-currency laundered by cybercriminals in 2021“, International Security Journal. <https://internationalsecurityjournal.com/crypto-currency-laundered-in-2021/>
2. Coinmarketcap, (2022, მაისი 6). კრიპტოვალუტის ბრუნვისა და კურსის საინფორმაციო ვებგვერდი. <https://coinmarketcap.com/>
3. World Crypto Index. (2018). “How Cryptography is used in cryptocurrency”. World Crypto Index. <https://www.worldcryptoindex.com/how-cryptography-is-used-cryptocurrency/>
4. TADVISER. (2021). Картели на ИТ-рынке России. TADVISER. <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B0%D1%80%D1%82%D0%B5%D0%BB%D0%B8_%D0%BD%D0%B0_%D0%98%D0%A2-%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8>
5. Kaspersky lab. 2022. “What is Wannacry Ransomware”. Mimicast, <https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/>
6. Arista Networks. 2021. “The Role of Cryptocurrency in Ransomware Attacks”. ARTISTA. <https://www.untangle.com/inside-untangle/the-role-of-cryptocurrency-in-ransomware-attacks/>
7. Malwarebytes Company. (2022). “Cryptojacking – What is it?”. Malwarebytes. <https://www.malwarebytes.com/cryptojacking>
8. Financial Action Task Force (FATF) Report. (2015, ოქტომბერი). “Emerging Terrorists Financial Risks”. FATF <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>
9. Comply Advantage. (2022). “Cryptocurrency Regulations around the World”. Comply Advantage. <https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/>

laundering and tax evasion”, European Parliament (Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies). (In English)
5. Lapuh Bele J., (2021). “Cryptocurrencies as facilitators of cybercrime”. SHS Web of Conferences Volume 111.

Internet Resources:

1. Marshal J., (2022, February 2), US$8.6 billion worth of crypto-currency laundered by cybercriminals in 2021“, International Security Journal. <https://internationalsecurityjournal.com/crypto-currency-laundered-in-2021/> (In English)
2. Coinmarketcap, (2022, May 6). Web-site showing the capitalization and exchange rates of cryptocurencies. <https://coinmarketcap.com/> (In English)
3. World Crypto Index. (2018). “How Cryptography is used in cryptocurrency”. World Crypto Index <https://www.worldcryptoindex.com/how-cryptography-is-used-cryptocurrency/> (In English)
4. TADVISER. 2021. Cartels in Russian IT market. TADVISER. <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B0%D1%80%D1%82%D0%B5%D0%BB%D0%B8_%D0%BD%D0%B0_%D0%98%D0%A2-%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8> (In English)
5. Kaspersky lab. 2022. “What is Wannacry Ransomware”. Mimicast, <https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/> (In English)
6. Arista Networks. 2021. “The Role of Cryptocurrency in Ransomware Attacks”. ARTISTA. <https://www.untangle.com/inside-untangle/the-role-of-cryptocurrency-in-ransomware-attacks/> (In English)
7. Malwarebytes Company. 2022. “Cryptojacking – What is it?”. Malwarebytes. <https://www.malwarebytes.com/cryptojacking> (In English)
8. Financial Action Task Force (FATF) Report. (2015, October). “Emerging Terrorists Financial Risks”. FATF <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> (In English)
9. Comply Advantage. 2022. “Cryptocurrency Regulations around the World”. Comply Advantage. <https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/> (In English)

NOTES:

1. Marshal, J., (2 February, 2022). US$8.6 billion worth of crypto-currency laundered by cybercriminals in 2021“, *International Security Journal*. <https://internationalsecurityjournal.com/cryptocurrency-laundered-in-2021/> [Last seen: 6 May, 2022]
2. Coinmarketcap, (6 May, 2022). Web-site showing the capitalization and exchange rates of cryptocurencies. <https://coinmarketcap.com/> [Last seen: 6 May, 2022]
3. Legislative Herald of Georgia, (1 July, 2019). Decision of the Ministry of Finance of Georgia of June 28, 2019 №201, Legislative Herald of Georgia. <https://matsne.gov.ge/ka/document/view/4601215?publication=0> [Last seen: 6 May, 2022]
4. Weiss, P., (2019). “Cryptocurrency”. Rifkind, Wharton & Garrison LLP (Multinational Law Firm). P.1
5. World Crypto Index. (2018). “How Cryptography is used in cryptocurrency”. World Crypto Index, <https://www.worldcryptoindex.com/how-cryptography-is-used-cryptocurrency/> [Last seen: 6 May, 2022]
6. Тесленко А. В., Кониева Ф. И., (2019). ,,Роботизация торгов – новый вызов в борьбе с картелями”. Из. Юстицинформ. сборник научных трудов., С. 112-122.
7. Иващенко К. А., (2021). „Цифровые картели как новая разновидность киберпреступлений“. Сборник – Киберпреступность: риски и угрозы., С. 84.
8. TADVISER. 2021. Cartels in Russian IT market. TADVISER. <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B0%D1%80%D1%82%D0%B5%D0%BB%D0%B8_%D0%BD%D0%B0_%D0%98%D0%A2-%D1%80%D1%8B%D0%BD%D0%BA%D0%B5_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8> [Last seen: 6 May, 2022]
9. Lapuh Bele J., (2021). “Cryptocurrencies as facilitators of cybercrime”. SHS Web of Conferences Volume 111. P. 1-6.
10. Kaspersky lab. 2022. “What is Wannacry Ransomware”. Mimicast, <https://www.mimecast.com/blog/all-you-need-to-know-about-wannacry-ransomware/> [Last seen: 6 May, 2022]
11. Arista Networks. 2021. “The Role of Cryptocurrency in Ransomware Attacks”. ARTISTA. <https://www.untangle.com/inside-untangle/the-role-of-cryptocurrency-in-ransomware-attacks/> [Last seen: 6 May, 2022]
12. Bernardi, M., Charoenwong, B., (2022). “A Decade of Cryptocurrency Hacks: 2011-2021”, Business School, National University of Singapore, P. 1-6.
13. Malwarebytes Company. 2022. “Cryptojacking – What is it?”. Malwarebytes. <https://www.malwarebytes.com/cryptojacking> [Last seen: 6 May, 2022]
14. Dr. Houben R., Snyers A., (2018). “Legal contexts and implications for financial crime, money laundering and tax evasion”, European Parliament (Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies), P. 9
15. Financial Action Task Force (FATF) Report. (2015, October). “Emerging Terrorists Financial Risks”. FATF. <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf> [Last seen: 6 May, 2022]
16. Comply Advantage. (2022). “Cryptocurrency Regulations around the World”. Comply Advantage. <https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/> [Last seen: 6 May, 2022]