შალვა ბიწაძე | თინათინ ქაროსანიძე
თბილისის თავისუფალი უნივერსიტეტი
sbits21@freeuni.edu.ge | t.karosanidze@freeuni.edu.ge

კრიპტოვალუტა, როგორც ტერორისტული დაფინანსების ახალი ინსტრუმენტი: ანონიმურობისა და რეგულაციების ნაკლებობის გამოწვევები გლობალური უსაფრთხოებისთვის

რეზიუმე

ტერორიზმის დაფინანსება თანამედროვე სამყაროში გლობალური უსაფრთხოების სერიოზული გამოწვევაა. ტექნოლოგიური განვითარების ფონზე, საფინანსო ტრანზაქციების ახალი ფორმები არა მხოლოდ ეკონომიკის განვითარებას უწყობს ხელს, არამედ ახალ შესაძლებლობებს და სხვა ტექნოლოგიურ უპირატესობებს აძლევს კრიმინალურ თუ ტერორისტულ ორგანიზაციებს. ერთ-ერთი ასეთი ტექნოლოგიური ინოვაცია კრიპტოვალუტაა: დეცენტრალიზებული და ნაწილობრივ ანონიმური ფულადი სისტემა, რომელიც ტრადიციული ფინანსური არხებისგან ძალიან განსხვავებულად მუშაობს. საკვლევი თემის სენსიტიურობა ართულებს პირდაპირი მონაცემების შეგროვებას, რაც გულისხმობს ტერორისტული ორგანიზაციების დაფინანსების მექანიზმების შესწავლას კრიმინალურ სუბიექტთან კონტაქტით, რაც არა მხოლოდ ეთიკურად, არამედ იურიდიულადაც დაუშვებელია.

საკვანძო სიტყვები: კრიპტოვალუტა, ტერორიზმის დაფინანსება, ანონიმურობა, გლობალური უსაფრთხოება.

შესავალი

ტერორიზმი არის მუდმივად განვითარებადი ფენომენი. ჩვენ როდესაც ვსაუბრობთ ტერორისტებზე, მხოლოდ ბოლო რამდენიმე წლის შემთხვევები არ უნდა გვახსენდებოდეს. ჯერ კიდევ ძველ ეპოქებში არსებობდა ჯგუფები, რომლებიც ძალადობრივ ქმედებებს პოლიტიკური ან რელიგიური მიზნებისათვის იყენებდნენ (მაგალითად ზილოტები ან ასასინები). მე-19 საუკუნეში ანარქისტული ტერორიზმი ევროპასა და რუსეთში აქტიურად გავრცელდა, ხოლო მე-20 საუკუნეში უკვე მასობრივმა ტერორიზმის ფორმებმა მოიკიდეს ფეხი. როგორც წარსულში, ისე დღესაც, ტერორისტული აქტები მიმართულია საზოგადოებისათვის პოლიტიკური ან იდეოლოგიური გზავნილის მიტანაზე, თუმცა დროთა განმავლობაში მნიშვნელოვნად შეიცვალა მათი მასშტაბი, გავლენა და განხორციელების ტექნოლოგიური საშუალებები.

ბოლო წლების განმავლობაში ტერორიზმი გახდა გლობალური პრობლემა, რომელიც მრავალი ათწლეულია უკვე საფრთხეს უქმნის საერთაშორისო სტაბილურობას, განსაკუთრებულად კი 21-ე საუკუნეში არიან გააქტიურებულნი. ტერორისტები მსგავსი საფრთხის შემცველნი არიან, რადგან მათი ამოცნობა და შესაბამისი რეაგირება არის საკმაოდ რთული და დროში გაწელილი პროცესი. გაჩნდება კითხვა იმასთან დაკავშირებით, თუ რატომ არის ასეთი რთული ტერორისტის ამოცნობა? განსხვავების გაკეთება ძალიან მარტივია, როდესაც უყურებ ორ ერთმანეთისგან რადიკალურად განსხვავებულ პირს,

მაგალითად სამხედროს და ჩვეულებრივ მოქალაქეს, თუმცა ამ შემთხვევაში ჩვენ გვაქვს შეხება ისეთ ადამიანებთან, რომელთა განსხვავებაც ჩვეულებრივი მოქალაქისგან არის თითქმის შეუძლებელი. ასეთ ტერორისტულ ორგანიზაციებში მონაწილეობენ არამხოლოდ მამაკაცები, არამედ ქალებიც და ზოგ შემთხვევაში ბავშვებიც. ასეთ დროს კი ამოცნობა ხდება რთული. არსებობს ძალიან ბევრი ტერორისტული ორგანიზაცია, რომელიც ერთმანეთისგან განსხვავდება ზომით, სტრუქტურით, ოპერატიული შესაძლებლობებით, მთავარი მიზნით, რეკრუტირების ხერხებითა და შესაძლებლობებით. მიუხედავად იმისა, რომ მათი მიზნები და ხერხები შეიძლება იყოს განსხვავებული, მათ ერთი რამ მაინც აერთიანებთ. ეს არის ფინანსური რესურსების საჭიროება, რათა მათი მიზნები, იდეები და გეგმები რეალურ ტერორისტულ აქტებად გარდაქმნან. ეს განსაკუთრებულად მნიშვნელოვანია მსხვილი მასშტაბის ორგანიზაციებისთვის, რომლებიც მიზნად ისახავენ ტერიტორიების გაკონტროლებას და გავლენის გაფართოებას. მათი ფინანსური მდგომარეობა უშუალოდ განსაზღვრავს ოპერაციულ შესაძლებლობებს. შესაბამისად, მსგავსი ორგანიზაციები მუდმივად ცდილობენ რესურსების სტაბილური ნაკადის უზრუნველყოფას. თითოეული ჯგუფის ფინანსური სტრატეგია არის განსხვავებული. თუმცა, საერთო მიზანი არის ინფრასტრუქტურის განვითარება, ოპერაციული მოცულობის გაფართოება, შესაბამისი იარაღის და სამხედრო ტექნიკის ქონა. ტერორისტულ ორგანიზაციებს აქვთ რამდენიმე გზა იმისთვის, რომ ფინანსები მუდმივად შემოსდიოდეთ, რათა ოპერაციები დროულად განახორციელონ (FAFT 2015: 9-10).

ტერორისტული ორგანიზაციები მიმართავენ ფინანსების გადაადგილების ტრადიციულ მეთოდებს. ბანკის დახმარებით რიცხავენ თავიანთი თანხის საკმაოდ დიდ რაოდენობას. ისინი სპეციალურად ირჩევენ ისეთ კომპანიებს, რომლებიც ოფიციალურად დარეგისტრირებულნი არ არიან და მოქმედებენ AML/CFT (Anti-Money Laundering and Counter-Terrorism Financing Act) წესების გარეშე. ასეთ არარეგისტრირებულ კომპანიებს ხშირად სამიზნედ ირჩევს ალ-კაიდა, ISIS და მსგავსი დაჯგუფებები, რადგან მათი ნებისმიერი ქმედება არის მონიტორინგის ქვეშ და ამ კომპანიების დახმარებით უსაფრთხოდ შეუძლიათ გადარიცხვა. გარდა ამისა, სულ უფრო აქტიური ხდება P2P (person-to-person) გადახდის პლატფორმები, როგორიცაა Venmo, CashApp, Zelle. ამ პლატფორმების საშუალებით მომხმარებლებს აღარ უწევთ თავიანთი საბანკო დეტალების მითითება და აგზავნიან თანხას მხოლოდ ტელეფონის ნომრის ან ელ-ფოსტის მეშვეობით, რაც ფულის მიმოქცევის კვალს ძალიან ბუნდოვანს ხდის და მიგნებას ართულებს. მიუხედავად იმისა, რომ მსგავს პლატფორმებზე აუცილებელია რეგისტრაციის გავლა, მათი დახურული და გამოსაყენებლად მარტივი სტრუქტურის გამო ტერორისტებისთვის მიმზიდველი ხდება.

სტრუქტურირებული გადარიცხვებისას ფულის გადამტან კომპანიებს (MSBs) დიდი როლი აქვთ. მიუხედავად რეგულაციებისა, ზოგი MSB მიზანმიმართულად ან გაუცნობიერებლად ემსახურება ტერორისტულ მიზნებს. ამის მაგალითია ლიბანში დაფუძნებული კომპანია CTEX, რომელმაც მოახერხა ჰეზბოლასთვის მილიონობით აშშ დოლარის გადარიცხვა. MSB-ებს აქვთ SAR (suspicious activity reports) წარდგენის დაბალი ბარიერი ($2,000), ვიდრე სხვა რეგულირებად ფინანსურ ინსტიტუტებს ($5,000). MSB-ებს მოეთხოვებათ, წარადგინონ საეჭვო აქტივობის ანგარიშები (SAR). SAR-ის მოხსენების ანალიზი კი აჩვენებს, რომ 2020 წლიდან 2022 წლამდე, MSB-ებმა შეიტანეს TF-თან (Terrorism Financing) დაკავშირებული ყველა SAR-ის თითქმის 72% (Treasury 2024).

ტერორისტული ორგანიზაციების ტრადიციული დაფინანსების მეთოდები უფრო და უფრო ნაკლებად ეფექტური ხდება, რადგან მათ წინააღმდეგ მოქმედებს სანქციები, რომლებიც ამ პროცესს აფერხებს. სანქციების ხარჯზე უკვე დაფიქსირდა რამდენიმე შემთხვევა, სადაც იმ თანხამ, რომელიც უნდა მოხმარებოდა ტერორისტულ მიზნებს, ვერ მიაღწია დანიშნულების წერტილამდე, რადგან ძალიან ძლიერი წინააღმდეგობა არსებობს სახელმწიფოს მხრიდან და უზრუნველყოფენ, რომ ორგანიზაციებმა ვერ განახორციელონ დასახული გეგმები. მაგრამ, ამ ეტაპზე სახელმწიფოები და ის ორგანოები, რომლებიც ებრძვიან ტერორიზმს, ძალიან დიდი გამოწვევის წინაშე დგანან. სანქციების, რეგულაციების

Anastasia Tsertsvadze, Revaz Topuria Free University of Tbilisi
atser21@freeuni.edu.ge I r.topuria@freeuni.edu.ge

და მუდმივი მონიტორინგის მიუხედავად, თანამედროვე სამყაროში არსებობს თანხის გადარიცხვის ისეთი მეთოდი, რომლის მეშვეობითაც კვალის დატოვება და მიგნება თითქმის შეუძლებელია, რაც ხელსაყრელია ტერორისტებისთვის და მათი მიზნებისთვის. ეს არის კრიპტოვალუტა. დღეს-დღეობით ძალიან ბევრი ელექტრონული ვალუტა არსებობს, თუმცა თავდაპირველად ბაზარზე ბიტკოინის გამოჩენამ გამოიწვია კრიპტოაქტივების და მთლიანობაში ბლოკჩეინის მიმართ ნდობა. პირველად ეს ტექნოლოგია გამოჩნდა 2009 წელს, თუმცა საწყის ეტაპზე ნაკლები სანდოობა ჰქონდა. ბიტკოინი იყო ძალიან იაფი და თანხას დიდწილად არავინ დებდა, თუმცა 2024 წლის მონაცემებით, ბიტკოინის ბაზრის მთლიანი ღირებულება შეადგენდა $1.8 ტრილიონს, ამ ეტაპზე კი უკვე $2.1 ტრილიონი დოლარის (Kerner 2024) უზარმაზარ ინდუსტრიასთან გვაქვს საქმე. თუმცა, ჩნდება კითხვა, რატომ იყენებს მილიონობით ადამიანი ამ სისტემას და რატომ ენდობა მას?

ბლოკჩეინი თანამედროვე ტექნოლოგიების ერთ-ერთი ყველაზე მნიშვნელოვანი ნაწილი გახდა. დღესდღეობით მას საკმაოდ აქტიურად იყენებენ ბიზნესები, ინვესტორები, მთავრობები და ინდივიდუალური პირები. ბლოკჩეინი არის სპეციალური ტიპის ციფრული მონაცემთა ბაზა, რომელიც ერთდროულად ინახავს ინფორმაციას და გამოიყენება ბევრი კომპიუტერის მიერ, რომლებიც ერთმანეთთან ქსელურად არის დაკავშირებული. ბლოკჩეინი ყველაზე მეტად ცნობილია ბიტკოინის გამო, მაგრამ მისი გამოყენება მხოლოდ ამ გზით არ შემოიფარგლება. ის შეიძლება გამოვიყენოთ თითქმის ყველა სფეროში, სადაც გვინდა. იმისთვის, რომ ინფორმაცია იყოს მუდმივად დაცული და უცვლელი. ბლოკჩეინის მთავარი ძალა იმაშია, რომ მასში ერთხელ შეყვანილი ინფორმაცია აღარ იცვლება. შესაბამისად, აღარ არის საჭირო მედიატორები ან მესამე პირები, რომლებსაც უწევთ მონაცემების პერიოდული შემოწმება და საჭიროების შემთხვევაში შესწორებების შეტანა. ბლოკჩეინში სისტემა უზრუნველყოფს სანდოობას.

ბლოკჩეინზე ტრანზაქციები გარკვეული პროცესის მიხედვით ხორციელდება, რაც სხვადასხვა სისტემებში შეიძლება ოდნავ განსხვავდებოდეს. ბიტკოინის შემთხვევაში, პროცესი არის ძალიან გრძელი. თავდაპირველად მომხმარებლის ტრანზაქცია გაიგზავნება მეხსიერების აუზში (Memory pool), სადაც ინფორმაცია შეინახება დროებით მანამ, სანამ სპეციალური კომპიუტერი ამ ინფორმაციას არ აირჩევს, ეს პროცესი არის ჩვენთვის ცნობილი, როგორც „მაინინგი“. ქსელში ჩართული ყველა კომპიუტერი ცალკე მუშაობს საკუთარ ბლოკზე, რადგან ისინი სხვადასხვა ტრანზაქციებს ირჩევენ. თითოეული ცდილობს, ამოხსნას რთული ამოცანა და ამისთვის იყენებს ცვლადს, რომელსაც „nonce” (Number used once) ეწოდება. ეს არის რიცხვი, რომელიც ყოველი გამოყენებისას იზრდება. მაინერი ტესტავს nonce-ს სხვადასხვა მნიშვნელობებს და ახდენს ბლოკის „ჰეშის“ გამოთვლას (როცა ბლოკი ივსება, მის შიგთავსს პროგრამა გარდაქმნის უნიკალურ კოდად, რომელსაც „ჰეში“ ჰქვია. ეს ჰეში ინახება შემდეგ ბლოკში და ასე იქმნება ერთმანეთზე მიბმული ბლოკების ჯაჭვი, საიდანაც წარმოიშვა მისი დასახელება, ბლოკჩეინი). თუ შედეგი არ აკმაყოფილებს სასურველ პირობებს (ე.წ. მიზნობრივი ჰეში), nonce-ს ერთი ემატება და ცდა თავიდან იწყება. ამ ციკლის გამეორება შეიძლება წამში რამდენიმე მილიარდჯერ მოხდეს. საბოლოოდ, ის მაინერი, რომელიც „სწორ“ ჰეშს მიიღებს, „იმარჯვებს“ და იღებს ჯილდოს. ამის შემდეგ ბლოკი ბლოკჩეინში ერთდება და ტრანზაქცია დასრულებულად ითვლება. თუმცა, ტრანზაქცია საბოლოოდ დადასტურებულად ითვლება მხოლოდ მაშინ, როცა მას შემდეგ დამატებული იქნება კიდევ ხუთი ბლოკი. რადგან თითო ბლოკის გამომუშავებას დაახლოებით 10 წუთი სჭირდება, მთლიანი დადასტურების დრო საშუალოდ 1 საათია (ImmuneBytes 2023; Hayes 2024).

ტერორისტული ორგანიზაციების კრიპტოაქტივობა

ტექნოლოგიური სირთულის მიუხედავად, კრიპტოს ინტეგრირება ნებისმიერ საქმიანობაში და მისი სრულად ათვისება ყველასთვის ხელმისაწვდომია. სწორედ ამ მიზეზის გამო, ტერორისტული ორგანიზაციები უკვე საკმაოდ აქტიურად მოიხმარენ კრიპტოს თანხების მოსაზიდად. დღესდღეობით დიჯიტალურ ვალუტასთან დაკავშირებით ინფორმაციის მოპოვება ძალიან მარტივია, რადგან მასზე არის უამრავი სტატია, კვლევა თუ ანგარიშები და მისი საშუალებით ყველა საჭირო ინფორმაციას გაიგებ, რაც კრიპტოს სრული ათვისებისთვის იქნება საჭირო. ორგანიზაციები, როგორიცაა ე.წ. ისლამური სახელმწიფო (ISIS), ალ-კაიდა, ჰუთიები და ჰამასი ყოველდღიურად ასეულობით გადარიცხვებს ახორციელებენ.

ISIS იყო პირველი დაჯგუფება, რომელმაც დაიწყო კრიპტოვალუტის გამოყენება საკუთარი მიზნებისთვის. 2015 წლიდან იყენებენ ელექტრონულ ვალუტებს. 2019-2022 წლებში ერთმა პიროვნებამ მოახერხა ორგანიზაციისთვის $185,000-ზე მეტი შეეგროვებინა და გადაერიცხა. ჯამში 300-ზე მეტი კრიპტოვალუტის საფულე ჰქონდა და ყველას აქტიურად იყენებდა. განსაკუთრებით საინტერესო კი არის ჰამასის შემთხვევა. ISIS ფარულად ცდილობდა, რომ თანხა შეეგროვებინა და გადაეგზავნა, მარა ჰამასის შემთხვევაში ალ-კასამის ბრიგადებმა 2019 წელს თავიანთი ბიტკოინის საფულეების მისამართი გამოაქვეყნეს, სადაც ყველას შეეძლო კონკრეტულ საიტზე გადასვლის შემთხვევაში თანხის გადარიცხვა. ასევე ჰქონდათ თავიანთი ოფიციალური ვებსაიტი, სადაც განთავსებული იყო ბიტკოინის ერთჯერადი მისამართი და მის ქვემოთ იყო წარწერა: „დონაცია ჯიჰადისთვის“ (TRM Blog 2024; TRM Blog 2025).

დაჯგუფებებზე უფრო სახიფათო არიან ე.წ. მარტოხელა მგლები. ისინი მოქმედებენ მარტო, კვალს თითქმის არ ტოვებენ, რადგან მასშტაბი ბევრად მცირეა, მიგნებაც ბევრად რთულდება. მათი მიზნების განსახორციელებლად არ არის საჭირო ფართომასშტაბიანი ლოჯისტიკა და დიდი რესურსები. ე.წ. მარტოხელა მგლები არ არიან უბრალოდ „მარტოხელა მებრძოლები“, ისინი რეალურად ტერორიზმის ისტორიაში იკავებენ ძალიან მნიშვნელოვან ნაწილს, სადაც ერთ ადამიანს შეუძლია მინიმალური ხარჯით მოახდინოს გავლენა საზოგადოებასა და მედიაზე (Hughes 2017; Goldbarsht 2024; Chainalysis, 2020: 73-77).

გლობალური უსაფრთხოების გამოწვევები და მარეგულირებელი პასუხები, ტერორიზმის საწინააღმდეგო ზომები და ტერორიზმის დაფინანსების შეჩერების გზები

ტერორისტულმა ორგანიზაციებმა დიდწილად აითვისეს კრიპტოს გამოყენება, რის გამოც კონტრტერორისტული ორგანოები მზარდი გამოწვევების წინაშე დგანან. ის დაკავშირებულია ახალ და განვითარებად ფინანსური ტექნოლოგიების შექმნასთან და მათ არამიზნობრივად გამოყენებასთან. კონტრდაზვერვის და კონტრტერორისტულმა ორგანოებმა თავდაპირველ ეტაპზე ვერ შეძლეს, ამ უეცარ ცვლილებას დაწეოდნენ და შესაბამისი მეთოდი შეემუშავებინათ, რომელიც დაეხმარებათ მათ დროულ და სწორ რეაგირებაში. გაეროს უშიშროების საბჭოს 2025 წლის დოკუმენტში კონტრტერორიზმის შესახებ აღწერილია: ეს ტექნოლოგიები, მიუხედავად იმისა, რომ საზოგადოებაზე ძალიან დიდ გავლენას ახდენს და კიბერ სივრცის მიმართულებით ძალიან დიდი წინგადადგმული ნაბიჯია, ტერორისტებს კარგ შესაძლებლობებს აძლევს თავიანთი ოპერაციების გლობალურად დაფინანსებისთვის (Bendjama 2025:2–3).

წევრი სახელმწიფოების მიერ რეაგირების შესაძლებლობების გასაუმჯობესებლად, ალჟირის სახელმძღვანელო პრინციპები ადგენს ოთხ ძირითად არასავალდებულო მარეგულირებელ პუნქტს.

Anastasia Tsertsvadze, Revaz Topuria Free University of Tbilisi
atser21@freeuni.edu.ge I r.topuria@freeuni.edu.ge

პირველი არის რისკების გაგება. სახელმწიფოებმა უნდა შეისწავლონ ტერორისტული დაფინანსების რისკები, განსაკუთრებით ახალი ფინანსური ტექნოლოგიების გამოყენებისას. პოტენციური რისკების რუკის არსებობა აძლევს მათ საშუალებას დროულად ამოიცნონ საეჭვო არხები. მეორე პუნქტი ეხება პროპორციულ რეგულაციებს. ინოვაციები არ უნდა ჩაიხშოს, არამედ მართვადი უნდა გახდეს. მნიშვნელოვანია ისეთი ჩარჩოების შექმნა, რომლებიც გამოავლენს არარეგისტრირებულ ერთეულებს ზედმეტი ზედამხედველობის გარეშე. მესამე პუნქტი გულისხმობს ფინანსური ქსელების პროაქტიულ ჩაშლას. სახელმწიფოებმა უნდა გააუმჯობესონ საგამოძიებო შესაძლებლობები, განათავსონ ბლოკჩეინის ანალიტიკა და მონაწილეობა მიიღონ ფინანსური დაზვერვის გლობალურ ქსელში. აქ სასიცოცხლოდ მნიშვნელოვანია ისეთი მექანიზმები, როგორიცაა ინტერპოლის მონაცემთა ბაზების გამოყენება, ციფრული აქტივების კოორდინირებული ჩამორთმევა და სამართლებრივი ურთიერთდახმარების გამარტივებული ხელშეკრულებები. მეოთხე და საბოლოო პუნქტი ეხება კონტრდაფინანსების ღონისძიებების ეფექტურობისა და არასასურველი შედეგების გაზომვას. მიუხედავად იმისა, რომ აუცილებელია მკაცრი აღსრულება, ეს ქმედებები უნდა შეესაბამებოდეს საერთაშორისო კანონებს და არ უნდა დაარღვიოს ლეგიტიმური ფინანსური საქმიანობა. გადაჭარბებულმა რეგულაციამ შეიძლება უნებლიედ მოახდინოს მარტივად მოწყვლადი მოსახლეობისთვის ინოვაციურობის დათრგუნვა და ბევრად უფრო დამაზიანებელი იყოს, რადგან ტექნოლოგიური წინსვლა თითქმის სრულიად შეჩერდება.

ზემოაღნიშნული სახელმძღვანელო პრინციპების თანდმიმდევრულად დანერგვა მნიშველოვანი და აუცილებლი პირობაა, რათა მოხდეს ისეთი ტექნოლოგიების გამოყენება, როგორიცაა ხელოვნური ინტელექტი და მანქანათმცოდნეობა (machine learning) ფინანსურ მონიტორინგში. ვირტუალური აქტივების დაზვერვის სპეციალიზებული ერთეულების შექმნა და უშუალოდ პლატფორმებთან და ბირჟებთან კოორდინაცია ძალიან ეფექტური იქნება ნებისმიერი მასშტაბის ტრანზაქციის დროულად დასაკვირვებლად (Bendjama 2025:7-12).

აშშ-მა მნიშვნელოვანი ნაბიჯები გადადგა კონტრტერორიზმის სფეროში. ყველა ორგანო იყო პასუხისმგებელი, მიეგნოთ რაიმე სახის კვალისთვის, რაც ტერორისტებს შესაძლოა ტრანზაქციების დროს დაეტოვებინათ. თუმცა, იმდენად მალე მოახდინეს ტერორისტებმა ამ ტექნოლოგიების ადაპტაცია, რომ მსგავსმა ორგანოებმა შესაბამისი საფრთხის გამანეიტრალებელი ტექნოლოგია ვერ შეიმუშავეს თავის დროზე. ამიტომაც, ჩამოყალიბდა ახალი ორგანო, ვირტუალური აქტივების განყოფილების (VAU - virtual assets unit), რადგან FBI იყო თითქმის უმოქმედო ამ საკითხთან დაკავშირებით.

VAU-მ გააერთიანა კიბერდანაშაულის, კრიმინალური და კონტრტერორისტული მიმართულების ექსპერტები და ჩამოაყალიბდა ცენტრალიზებულ, ერთობლივ ძალად, რომელიც ამუშავებს კრიპტოსთან დაკავშირებულ საქმეებს ყველა სექტორში: ბავშვების ექსპლუატაციისა და გამოსასყიდის პროგრამებიდან ტერორიზმამდე და თაღლითობამდე. VAU გვაწვდის კრიტიკულ შეხედულებებს იმის შესახებ, თუ როგორ მოხდა ბიუროს სტრუქტურული ადაპტაცია, კრიპტოვალუტის სფეროში, ტერორიზმის დაფინანსების განვითარებადი საფრთხის მოსაგვარებლად. საკვანძო პუნქტი არის VAU-ს ფუნდამენტური ინტეგრაცია FBI-ის კონტრტერორისტულ განყოფილებასთან, კიბერ და კრიმინალურ სამმართველოებთან ერთად. (Wyman 2025)

მომავლის პერსპექტივა და რისკები

აღნიშნული საკითხი წარმოადგენს კომპლექსურ პრობლემას სახელმწიფო სექტორებისთვის, რადგან ვირტუალურ სივრცეში შეღწევისას სპეციალისტს აქვს თითქმის უსაზღვრო შესაძლებლობა, თუმცა ეს შესაძლებლობა ჩნდება მხოლოდ იმ შემთხვევაში, თუ ქსელში შეღწევა იყო წარმატებული. პრობლემა კი სწორედ ამაშია. ამ ქსელებში შესვლა არის ამ ეტაპზე შეუძლებელი და ამიტომაც არის ბლოკჩეინი და

ბიტკოინი ასეთი სანდო, ამიტომ ცდილობენ მის უფრო და უფრო გაუმჯობესებას, რადგან გადარიცხვები გამარტივდეს და დღის ბოლოს ყველაფრის გაციფრულების მხრივ ადამიანის ყოველდღიური შენაძენები და საქმიანობა შედარებით გამარტივდეს. თუმცა, ეს ზრდის ტერორისტებისთვის ახალ შესაძლებლობას. სამომავლო პერსპექტივა ბლოკჩეინის კი არის იმდენად უკიდეგანო, რომ კონკრეტულ მიმართულებას მის განვითარებას ვერ მივცემთ. ამასთან ერთად გაჩნდა ახალი ინიციატივა, ამ ეტაპზე უკვე მიმდინარეობს მუშაობა ხელოვნური ინტელექტის ინტეგრირება ბლოკჩეინში, რის შედეგადაც შეიქმნება „სუპერ-ტექნოლოგია“, რომელსაც შეეძლება აბსოლუტურად ყველაფრის გაკეთება. მისი პოტენციალი სცდება მხოლოდ ფინანსურ ტრანზაქციებს. ის მოიცავს მონაცემთა დაცვას, სმარტ კონტრაქტებს, გლობალურ ლოჯისტიკას, ჯანდაცვასა და უმთავრესად, უსაფრთხოების სისტემების ახალი სტანდარტის ჩამოყალიბებას. თუმცა, ეს უდიდესი ძალა შესაძლოა აღმოჩნდეს როგორც კაცობრიობის პროგრესის, ისე მისი რისკის წყაროდ, განსაკუთრებით მაშინ, როდესაც ტერორისტული დაჯგუფებები აქტიურად ცდილობენ ამ ტექნოლოგიის ათვისებას ფინანსური ნაკადების გასაფანტად, ანონიმურობის შესანარჩუნებლად და მონიტორინგისგან თავის დასაღწევად. სახელმწიფოს მთავარი მოტივი ყოველთვის არის შესაბამისი ხერხების შემუშავება და ამის ტერორისტების წინააღმდეგ ამოქმედება, თუმცა ძალიან დიდი სიფრთხილით უნდა მოეკიდონ ამ საკითხს, რადგან თუ ის აღმოჩნდა ტერორისტის ხელში, ამას საწინააღდეგო ეფექტი ექნება.

სახელმწიფოებსა და საერთაშორისო ორგანიზაციებს ახლა მოუწევთ არა მხოლოდ უკვე არსებული რეგულაციების გადახედვა, არამედ სრულიად ახალი სამართლებრივი ჩარჩოების შექმნა, რომლებიც შეძლებენ ბალანსის დაცვას ინოვაციასა და უსაფრთხოებას შორის. ბლოკჩეინის გაუმჭვირვალე ბუნება იმას ნიშნავს, რომ ვერც ერთი ქვეყანა ინდივიდუალურად ვერ გაუმკლავდება ამ გამოწვევას. საჭიროა კოლექტიური, კოორდინირებული მოქმედება როგორც ტექნოლოგიური, ისე სადაზვერვო და დიპლომატიური ხაზით.