კრიპტო დანაშაულის გაშიფვრა

გზამკვლევი სამართალდამცველთათვის

OSCE ევროპის უსაფრთხოებისა და თანამშრომლობის ოფისი

შენიშვნა

წინამდებარე პუბლიკაცია მომზადდა ავტორის მიერ წარმოდგენილი მასალების საფუძველზე. აღნიშნული მასალების რედაქტირება არ მომხდარა ეუთოს მიერ. გამოთქმულ მოსაზრებებზე პასუხისმგებლობა ეკისრება ავტორს, რამდენადაც ეუთო-ს, მისი მისიების, ან მისი წევრი სახელმწიფოების შეხედულებებს არ წარმოადგენს.

ეუთო, მისი მისიები და წევრი სახელმწიფოები არ იღებენ პასუხისმგებლობას ნებისმიერ შედეგებზე, რაც შეიძლება ამ პუბლიკაციის გამოყენებამ გამოიწვიოს. მოცემულ პუბლიკაციაში არ განიხილება სამართლებრივი თუ სხვა სახის, ნებისმიერი პირის ქმედებისა თუ უმოქმედობის პასუხისმგებლობის საკითხები. პუბლიკაციაში კონკრეტული ქვეყნების ან ტერიტორიების მოხსენიება თუ მითითება არ ნიშნავს ეუთო-ს რაიმე პოზიციას მათი იურიდიული სტატუსის, მმართველი ორგანოების, ინსტიტუტების, ან მათი საზღვრების დადგენის შესახებ.

კრიპტო დანაშაულის გაშიფვრა

გზამკვლევი სამართალდამცველთათვის

ევროპის უსაფრთხოებისა და თანამშრომლობის ოფისი

სარჩევი

აკრონიმები, აბრევიატურები და საკვანძო ტერმინები განმარტებებით

AML-ის მე-5 დირექტივა	ევროპარლამენტისა და ევროსაბჭოს 30.05.2018 წ. დირექტივა 2018/843 რომლის ძალითაც ცვლილებები შედის შემდეგ დირექტივებში: ფულის გათეთრების ან ტერორიზმის ფინანსირებისათვის ფინანსური სისტემების გამოყენების წინააღმდეგ პრევენციის 2015/849 დირექტივაში; ასევე 2009/138/EC და 2013/36/EU დირექტივებში (EEA-ს შესაბამისი ტექსტი). აღნიშნული დირექტივის მოქმედების სფერო გავრცელდა კრიპტოაქტივებზე. 2020წ.10 მაისისათვის ევროკავშირის წევრ-სახელმწიფოებმა უნდა უზრუნველყონ დირექტივის შესაბამისი კანონებისა და რეგულაციების დანერგვა.
AML	Anti-Money Laundering (ფულის გათეთრების წინააღმდეგ ბრძოლა) — აღნიშნავს კანონებს, რეგულაციებსა და პროცედურებს, რომლებიც ემსახურება დანაშაულებრივი გზით მიღებული თანხების ლეგალურ შემოსავლებად გადაქცევის აღკვეთას.
CASP	Crypto-Asset Service Provider (კრიპტო აქტივების მომსახურების პროვაიდერები) - სუბიექტები, რომლებიც საზოგადოებას კრიპტო აქტივებთან დაკავშირებულ სერვისებს სთავაზობენ. ეს სერვისები შეიძლება საქმიანობის ფართო სპექტრს მოიცავდეს, მათ შორის და არა მხოლოდ: 1. ურთიერთგადაცვლის სერვისები: ფიატური ფულით, ან სხვა კრიპტო აქტივებით კრიპტო აქტივების ყიდვის და გაყიდვის უზრუნველყოფა. 2. საფულეთა მიმწოდებლები: სთავაზობენ მომხმარებელს კრიპტო კასტოდიანურ, ან არაკასტოდიანურ საფულეებს აქტივების შესანახად, მართვისა და გადაცემისთვის. 3. გადარიცხვის სერვისები: კრიპტო აქტივების ერთი მისამართიდან ან ანგარიშიდან მეორეზე გადატანა. 4. ფინანსური კონსულტაცია: კრიპტო აქტივების ყიდვის, გაყიდვის ან შენახვის შესახებ რჩევების მიწოდება. 5. შენახვის (ანუ კასტოდიანური) მომსახურება: კლიენტების სახელით კრიპტო აქტივების ფლობა და დაცვა. (მეტი ინფორმაციისთვის იხილეთ გვ. 20).
COE	Council of Europe (ევროპის საბჭო) - საერთაშორისო ორგანიზაცია, რომლის მიზანი ევროპაში ადამიანის უფლებების, დემოკრატიისა და კანონის უზენაესობის დაცვაა.
CTF	Counter-terrorism financing (ტერორიზმის დაფინანსების აღკვეთა) - ეხება პოლიტიკას და ქმედებებს, რომლებიც ტერორისტული საქმიანობის დაფინანსების აღკვეთას ემსახურება. მის მიზანს წარმოადგენს ტერორისტული დაჯგუფებებისთვის განკუთვნილი ლეგალური და არალეგალური ფულადი ნაკადების აღმოჩენა და შეჩერება.
ERC20 ტოკენები	Ethereum Request for Comment 20 Tokens – ეს არის ტექნიკური სტანდარტი, რომელიც ეთერიუმის ბლოკჩეინზე ჭკვიანი კონტრაქტების შესაქმნელად და გასაცემად გამოიყენება. შემოღებულია 2015 წელს.
EU	European Union (ევროკავშირი) - ევროპის 27 ქვეყნის პოლიტიკური და ეკონომიკური ორგანიზაცია.
EPE	ევროპოლის ექსპერტთა პლატფორმა – ევროპოლის მიერ შექმნილი წამყვანი სივრცე სამართალდამცავი ორგანოების ექსპერტებისთვის, რომელიც განკუთვნილია ცოდნის, საუკეთესო პრაქტიკისა და დანაშაულის შესახებ არაპერსონალური მონაცემების გაზიარებისთვის.
EUROPOL	ევროპოლი (ევროკავშირის სამართალდამცავთა თანამშრომლობის სააგენტო) - ევროკავშირის სამართალდამცავი სააგენტო, რომელიც თავის წევრ ქვეყნებს საერთაშორისო დანაშაულისა და ტერორიზმის წინააღმდეგ ბრძოლაში ეხმარება.

FinCEN	The Financial Crimes Enforcement Network (ფინანსურ დანაშაულთან ბრძოლის ქსელი) - შეერთებული შტატების სახაზინო დეპარტამენტის ბიურო, რომელიც ფინანსური ტრანზაქციების შესახებ ინფორმაციას აგროვებს და აანალიზებს.
FIU	Financial Intelligence Unit (ფინანსური დაზვერვის განყოფილება) - სამთავრობო უწყება, რომელიც პასუხისმგებელია ფულის გათეთრებისა და ტერორიზმის დაფინანსების სავარაუდო საქმიანობის შესახებ ფინანსური ინფორმაციისა და დაზვერვის შეგროვებაზე, ანალიზსა და გავრცელებაზე .
IP	Internet Protocol (ინტერნეტ პროტოკოლი) - წესების ერთობლიობა, რომელიც ინტერნეტით, ან სხვა ქსელებით გაგზავნილი მონაცემების ფორმატს არეგულირებს.
LER	Law enforcement request – სამართალდამცავი ორგანოების მიერ გამოძიების ჩასატარებლად საჭირო ინფორმაციის მოთხოვნა კერძო კომპანიებისა ან ფიზიკური პირებისაგან
MiCA	ევროპარლამენტისა და საბჭოს 2023 წლის 31 მაისის რეგულაცია (EU) 2023/1114 კრიპტოაქტივების ბაზრების შესახებ, რომელიც ცვლის რეგულაციებს (EU) No 1093/2010, (EU) No 1095/2010 და დირექტივებს 2013/36/EU, (EU) 2019/1937. ეს არის ევროკავშირის ახალი რეგულაცია, რომელიც არეგულირებს კრიპტოაქტივებს. ის ძალაშია 2024 წლის 30 დეკემბრიდან.
ML	Money Laundering (ფულის გათეთრება) – დანაშაულებრივი ქმედებებით გამომუშავებული დიდი ოდენობით ფულის ლეგალიზების უკანონო პროცესი.
MultiSig Wallet	Multi-Signature cryptocurrency wallet (კრიპტოვალუტის საფულე მრავალი ხელმოწერით) – კრიპტოვალუტის საფულის ტიპი, რომელიც ტრანზაქციის ავტორიზაციისთვის მრავალ პერსონალურ გასაღებს მოითხოვს
OCEEA	The OSCE's Office of the Co-ordinator of Economic and Environmental Activities - ეუთო-ს ეკონომიკური და გარემოსდაცვითი საქმიანობის კოორდინატორის ოფისი
OSCE	Organization for Security and Co-operation in Europe (ევროპის უსაფრთხოებისა და თანამშრომლობის ორგანიზაცია) - ევროპის რეგიონული უსაფრთხოების ორგანიზაცია, რომელიც ორიენტირებულია სამხედრო, პოლიტიკურ, გარემოსდაცვით და ეკონომიკურ განზომილებებში დიალოგისა და ყოვლისმომცველი თანამშრომლობის ხელშეწყობაზე.
OSINT	Open Source Intelligence – საჯაროდ ხელმისაწვდომი წყაროებიდან შეგროვებული ინფორმაცია, რომელიც გამოძიებისას გამოიყენება.
OTC	Over The Counter – ორ მხარეს შორის ვირტუალური აქტივებით ვაჭრობა ცენტრალური ბირჟის ან ბროკერის დახმარებით, ან მათ გარეშე.
UNODC	United Nations Office on Drugs and Crime – გაეროს ფარგლებში მოქმედი ნარკოტიკებისა და დანაშაულის შესახებ მონაცემების წარმოებასა და გავრცელებაზე პასუხისმგებელი უწყება.
VASP	Virtual Asset Service Provider (ვირტუალური აქტივების მომსახურების პროვაიდერი) – FATF-ის მიერ შემოღებული ტერმინი. გულისხმობს პირს, რომელიც საქმიანობას ან ოპერაციებს ვირტუალური აქტივებით ახორციელებს (მეტი ინფორმაციისთვის იხილეთ ნაწილი 20.)
VPN	Virtual Private Network (კერძო ვირტუალური ქსელი) – ტექნოლოგია, რომელიც საშუალებას იძლევა ნაკლებად უსაფრთხო ქსელში, კომპიუტერსა და ინტერნეტს შორის შექმნას უსაფრთხო კავშირი, ხშირად (მაგრამ არა ყოველთვის) პირის ადგილმდებარეობის დამალვით.

შესავალი

გზამკვლევის მიზანი

ეს დოკუმენტი წარმოადგენს ყოვლისმომცველ გზამკვლევს სამართალდამცავებისთვის. მათ შორის პოლიციის ოფიცრებისთვის, პროკურორებისთვის, სახელმწიფო და ფედერალური აგენტებისთვის. ასევე საგადასახადო და სასამართლო ექსპერტიზის სპეციალისტებისთვის, რომლებიც კრიპტოვალუტებს და სხვა ვირტუალურ აქტივებს ახლახან გაეცნენ. ასევე მათთვის, ვისაც კრიპტო აქტივებთან დაკავშირებული დანაშაულის გამოძიება სულ უფრო ხშირად ევალება.

გზამკვლევში ყურადღება გამახვილებულია თაღლითობისა და თაღლითური ქცევის ყველაზე გავრცელებულ ტიპებზე. ოფიცრებისათვის განმარტებულია საუკეთესო მეთოდები, თუ რა ქმედებები განახორციელონ და რა ტიპის ინფორმაციის მიღება და ჩაწერაა შესაძლებელი პოტენციური მსხვერპლისაგან - განსაკუთრებით პირველადი მტკიცებულებების შეგროვების პროცესში, ადგილობრივ პოლიციის განყოფილებაში.

წინამდებარე გზამკვლევი დაიწერა და შემუშავდა როგორც სახელმძღვანელო სამართალდამცავი ორგანოების თანამშრომელთათვის. იგი გამიზნულად არ მოიცავს კრიპტოვალუტის ისეთ სფეროებს, რომლებიც სავარაუდოდ ნაკლებად მნიშვნელოვანია კონკრეტულ მსხვერპლთან დაკავშირებულ საქმეებში. გარდა ამისა, ყურადღება მიზანმიმართულად გამახვილდა ფიზიკურ პირთა და სამართალდამცავ ორგანოთა თანამოქმედებაზე. უგულებელყოფილია ინფორმაცია STR-ების (Suspicious Transaction Reports - საეჭვო ტრანზაქციების ანგარიშები) ან SARs-ების (Suspicious Activity Reports - საეჭვო აქტივობის ანგარიშები) შესახებ, რომლებსაც ფინანსური ინსტიტუტები, ან ფინანსური დაზვერვის ერთეულები (ან მათი ეკვივალენტები) იყენებენ.

კრიპტოვალუტებთან დაკავშირებული საქმეების წარმოების არსებულ მეთოდებში მრავალი პრობლემა გამოვლინდა.

მაგალითად, გამომძიებელთა ინფორმაციით, მონაცემთა არასრულად შეგროვების გამო, მათ მოუწიათ მსხვერპლთან კონტაქტი კრიპტოვალუტების საფულეთა მისამართების შესაგროვებლად. აღნიშნული ინფორმაციის გარეშე გამოძიების წარმოება შეუძლებელია. ოფიცრებმა უნდა იცოდნენ რომელი ინფორმაციაა მნიშვნელოვანი, რა უნდა შეგროვდეს და რა არა. არასწორი კომუნიკაცია ხშირად მრავალდღიან დაგვიანებას იწვევს, რადგანაც მსხვერპლმა შეიძლება ბოლომდე ვერ გაიგოს, სამართალდამცავებისთვის რომელი ინფორმაციაა მნიშვნელოვანი. ცოდნის აღნიშნული ხარვეზი მხოლოდ უხერხულობა არაა; ის კრიმინალებმა გამოიყენეს, რომლებსაც ესმით, რომ ტექნოლოგია პირველივე დღიდან ყველასათვის ხელმისაწვდომია, ხოლო კრიპტოვალუტებთან დაკავშირებული საქმეების გამოძიების მოწინავე მეთოდები კი კვლავ ჩამორჩება. ამ მზარდი გამოწვევის საპასუხოდ ჩვენ შევიმუშავეთ ეს გზამკვლევი, რომელიც ასახავს იმას, თუ როგორ უნდა მოიქცნენ სამართალდამცავი ორგანოები გამოძიებისას და როგორ დაეხმარონ პოტენციურ მსხვერპლს, რომელიც კრიპტოვალუტასთან დაკავშირებული დანაშაულის შესახებ განაცხადებს.

ეუთო-ს სხვადასხვა სახელმწიფოში სამართლებრივი სიტუაციების, მეთოდების მრავალფეროვნების, სამართლებრივი მდგომარეობის და თემის სირთულის გათვალისწინებით ჩვენი მიზანი არა ამომწურავი გზამკვლევის, არამედ პრაქტიკული სახელმძღვანელოს შეთავაზებაა, რომლის გამოყენებაც მყისიერად იქნება შესაძლებელი წინა ხაზზე მომუშავე სამართალდამცავი ორგანოების მიერ მოქალაქეებისაგან მიღებული შეტყობინებების საფუძველზე. გზამკვლევი მიზნად ისახავს მსჯელობის დაწყებას საუკეთესო შიდა პრაქტიკების გაუმჯობესების გზებზე, განსაკუთრებით იმ შემთხვევაში, თუ არსებული სახელმძღვანელოები კრიპტოვალუტებს არ მოიცავს. წინამდებარე სახელმძღვანელოში

ყველაზე გავრცელებული თაღლითური პრაქტიკა შეჯამებულია დღესათვის არსებული სახით და მოცემულია შესავალი მასალა რათა საკითხის უფრო სიღმისეულ გაგებას შეუწყოს ხელი.

წინამდებარე გზამკვლევი ვირტუალური აქტივების მუდმივცვალებადი სამყაროს შესახებ სამართალდამცავი ორგანოების ცოდნის ხარვეზის დასაძლევად გადადგმული

მნიშვნელოვანი ნაბიჯია. ასევე უნდა ვაღიაროთ, რომ კრიპტოვალუტების ოპერირების Web3 სივრცე სწრაფად ვითარდება და წინამდებარე გზამკვლევს დასჭირდება დამატებითი ინფორმაციით შევსება.

წინამდებარე გზამკვლევში განსაკუთრებული ყურადღება ექცევა არა მხოლოდ ეფექტური გამოძიებისათვის აუცილებელ

ინსტრუმენტებსა და სტრატეგიებს, არამედ საზოგადოებასთან თანამშრომლობასა და უწყვეტი სწავლების ხელშეწყობას. სახელმძღვანელოს საბოლოო მიზანია სამართალდამცავების აღჭურვა ცოდნითა და საკუთარი შესაძლებლობების რწმენით, რაც კრიპტოვალუტებთან დაკავშირებული დანაშაულის უნიკალური გამოწვევების დასაძლევად არის საჭირო.

გზამკვლევის სტრუქტურა

წინამდებარე სახელმძღვანელოს მთავარი მიზანი ვირტუალური აქტივების დანაშაულების სფეროში მომუშავე სამართალდამცავი ორგანოების გამოუცდელი თანამშრომლების განათლება და ასეთი დანაშაულის შესახებ განმცხადებელ მსხვერპლთა მხარდაჭერაა. ამ მიზნის გათვალისწინებით

სახელმძღვანელო შემდეგნაირად არის სტრუქტურირებული: პირველ რიგში შემოთავაზებულია ციფრული აქტივების მოკლე მიმოხილვა. ციფრული აქტივები შეიძლება განვიხილოთ, როგორც ფართო ტერმინი, რომელიც ისეთ საკითხებს მოიცავს, როგორიცაა კრიპტოვალუტები, მაგალითად ბიტკოინი და ეთერიუმი. მოცემულია მათი განმარტება, მსგავსება და განსხვავება. განსხვავებები და მსგავსებები მათი სიღრმისეული გაგების უზრუნველსაყოფად განიხილება.

ამასთანავე, განიხილება კრიპტოვალუტების გამოყენებისა თუ არასწორი გამოყენების შესაძლო ფორმებისა და მათი მხარდამჭერი ტექნოლოგიების საკითხები.

ვირტუალური აქტივების შესახებ საბაზისო ცნებების აღწერის შემდეგ, გზამკვლევში მასთან დაკავშირებული გავრცელებული დანაშაულებია წარმოდგენილი. შემდეგ აღწერილია ამ დანაშაულებთან ბრძოლის სტანდარტული პროტოკოლები. განისაზღვრება თუ რომელი დანაშაულის სწრაფად გახსნაა შესაძლებელი და რომელი მოითხოვს უფრო საფუძვლიან გამოძიებას. გზამკვლევი ასევე განიხილავს თითოეული დანაშაულისთვის მტკიცებულებების შეგროვებას, მსხვერპლისთვის დასმულ კითხვებს, ვირტუალური აქტივების

მომსახურებისპროვაიდერებთან გასაზიარებელ მონაცემებს და ინფორმაციას, რომლის მიღებაც შესაძლებელია ვირტუალური აქტივების ბირჟებიდან.

ხელმისაწვდომობა და ენის გამარტივება: თემის სირთულიდან გამომდინარე, ავტორებმა გამარტივებული, არატექნიკური ენა გამოიყენეს, რათა დამწყებთათვის ეს ანგარიში ხელმისაწვდომი ყოფილიყო. ჟარგონების გამოყენებისგან თავის არიდება უზრუნველყოფს იმას, რომ ყველა მკითხველისთვის შინაარსი ნათელი და გასაგები იყოს. დაბოლოს, სახელმძღვანელო გთავაზობთ მსხვერპლის მხარდაჭერის რესურსებს და სხვადასხვა რეკომენდაციებს კრიპტოვალუტასთან დაკავშირებული დანაშაულის პრევენციისთვის.

ზოგადი ცნობები

კრიპტო აქტივებზე ორიენტირებული გამოძიებები თავიდან შეიძლება საფრთხის შემცველი მოგეჩვენოთ, განსაკუთრებით აქტივების აღდგენის სირთულესთან დაკავშირებული მცდარი წარმოდგენების გათვალისწინებით. მითია, რომ მას შემდეგ, რაც ეროვნული ვალუტა ბიტკოინის მსგავს კრიპტოვალუტად გარდაიქმნება, თანხები შეუქცევადად იკარგება, მსხვერპლს უმწეოდ ტოვებს და გამომძიებლებს საქმის დახურვას აიძულებს. რამდენიმე წლის წინ, ეს წარმოდგენა სწორი იყო, მაგრამ დრო შეიცვალა.

ტექნოლოგიურმა პროგრესმა ახალი კარები გააღო. ისევე როგორც დნმ-ის გადამოწმებამ, "გაყინული" შემთხვევების ხელახლა გახსნის და მოგვარების შესაძლებლობა შექმნა, ახლა კრიპტოვალუტების ადრე დახურული საქმეების ხელახლა გახსნა შეგვიძლია. ბლოკჩეინზე კრიპტოვალუტის ტრანზაქციების აღმოსაჩენად და შესამოწმებლად შექმნილი ინსტრუმენტების მზარდი ხელმისაწვდომობა და საერთაშორისო სამართლის ცვლილებები, კრიპტოვალუტასთან დაკავშირებული

სისხლის სამართლის საქმეების დამნაშავეების გამოვლენის საშუალებას იძლევა. ეს ინსტრუმენტები სულ უფრო მოსახერხებელი და ფართოდ გავრცელებულია, რაც საგამოძიებო გარემოს ცვლილებას ნიშნავს.

ყველა ამ ინსტრუმენტის მიუხედავად, ჩვენ ვხედავთ, რომ ბევრი გამოძიება, რომლებსაც ადგილობრივი პოლიციის თანამშრომლები ატარებენ, არასაკმარისი გაგების და ცოდნის გამო, ნაადრევად იხურება. გავრცელებული მოსაზრების მიუხედავად, კრიპტოვალუტების ტრანზაქციების მიკვლევა შესაძლებელია. დასაწყისშივე მონაცემების ზუსტად ჩაწერით, ვირტუალური და მატერიალური მტკიცებულებების ორგანულად გაერთიანებით, იზრდება ტრანზაქციების პოტენციურ ეჭვმიტანილთან დაკავშირების ალბათობა.

ბოლო წლებში, ეუთო-ს რამდენიმე წევრმა სახელმწიფომ, ფინანსური ქმედების სპეციალური ჯგუფის (FATF) მიერ გამოცემული განახლებული სტანდარტების შესაბამისად, ფულის

გათეთრების წინააღმდეგ ეროვნულ რეგულაციებში კრიპტოვალუტების და სხვა ვირტუალური აქტივების ჩართვა დაიწყო. მოვლენათა ასეთი განვითარება ნიშნავს, რომ კომპანიებმა, რომლებიც კრიპტოვალუტებით მუშაობენ, ახლა უნდა გაითვალისწინონ პროცესები, რომლებიც თავდაპირველად ტრადიციული საბანკო ინსტიტუტებისთვის შეიქმნა. მათ სთხოვენ გადაამოწმონ თავიანთი მომხმარებლების ვინაობა, შეამოწმონ დაფინანსების წყაროები და დააკვირდნენ თუ სად იგზავნება კრიპტოვალუტები.

ამ ცვლილებების გათვალისწინებით, ეუთო-ს ვირტუალური აქტივების ექსპერტთა ჯგუფმა გადაწყვიტა ადგილობრივი სამართალდამცავი დანაყოფების წევრებზე მორგებული დამხმარე სახელმძღვანელო გამოსცეს. ეს გზამკვლევი არა მხოლოდ მოგითხრობთ კრიპტოვალუტის გამოძიების ახალ შესაძლებლობებზე, არამედ სამართალდამცავ ორგანოებს აძლევს ცოდნას და ინსტრუმენტებს ასეთ რთულ და მუდმივად განვითარებად სფეროში სამართლიანობის აღსასრულებლად.


30 OSCE MINISTERIAL COUNCIL
osce NORTH MACEDONIA 2021
IT'S ABOUT PEOPLE
SKOPJE
Interpretation Languages
CH 0 - Floor
CH 1 - ENG
CH 2 - FRA
CH 3 - GER
CH 4 - SPA
CH 5 - RUS
CH 6 - ITA
CH 7 - ALB
CH 8 - MKD


OSCE
Valiant Richey
Helga Maria Schmid
OSCE Secretary General
OSCE


Mariia Sulialina
Deputy Head of the Center of Civil Education "Almenda", Ukraine
Hadja Lahbib
Minister of Foreign Affairs of Belgium
Stefano Baldi
Permanent Representative of Italy to the OSCE
Dorota Woroniecka-Krzyżanowska
Polish Center for International

ეუთო-ს შესახებ

ეუთო ევროპის უსაფრთხოებისა და თანამშრომლობის ორგანიზაციაა. ის მოქმედებს როგორც უსაფრთხოების რეგიონული ორგანიზაცია, მიზნად ისახავს დიალოგისა და თანამშრომლობის ხელშეწყობას და უსაფრთხოების ყოვლისმომცველ ხედვას - მოიცავს ყველაფერს, სამხედრო და პოლიტიკურიდან დაწყებული, გარემოსდაცვითი და ეკონომიკური სფეროებით დასრულებული.

ეუთო 1975 წელს, ცივი ომის დროს დაარსდა და ამჟამად 57 წევრი სახელმწიფოსგან შედგება. ეს სახელმწიფოები ძირითადად ევროპაშია, სადაც ეუთო-ს სამუშაოს დიდი ნაწილია თავმოყრილი, მაგრამ ასევე მოიცავს კანადას და შეერთებულ შტატებს ჩრდილოეთ ამერიკაში. ასევე ქვეყნებს, როგორიცაა ყაზახეთი, ყირგიზეთი და უზბეკეთი ცენტრალურ აზიაში. ის ყოვლისმომცველი უსაფრთხოების პრინციპების საფუძველზე მოქმედებს და მოიცავს სამხედრო, პოლიტიკურ, ეკონომიკურ, ეკოლოგიურ და ადამიანის უფლებების სფეროებს.

ევროპაში ეუთო სტაბილურობის ხელშეწყობასა და უსაფრთხოების გამოწვევებზე მუშაობს. მისი მთავარი მიზანი კონფლიქტების თავიდან აცილება და რეგიონული თანამშრომლობის განვითარებაა ისეთი მექანიზმებით, როგორიცაა დიპლომატიური მოლაპარაკებები, კონფლიქტების მოგვარების ინიციატივები და შეიარაღების კონტროლის შეთანხმებები. გარდა ამისა, არის სამუშაო, რომელსაც ეუთო დემოკრატიის და ადამიანის უფლებების მხარდასაჭერად ასრულებს. მაგალითად, არჩევნების მონიტორინგი.

როდესაც საქმე ფინანსური დანაშაულის და კრიპტოდანაშაულის თემას ეხება, ეუთო ამ გამოწვევებთან ბრძოლაში ეხმარება წევრ სახელმწიფოებს და დაზვერვის მონაცემების გაცვლისა და შესაძლებლობების განვითარებას უწყობს ხელს. ეს ტრანსსასაზღვრო ინფორმაციის გაცვლის გაუმჯობესებას ემსახურება. ეს მნიშვნელოვანია, რადგან კრიპტოდანაშაულების ბუნება არ შემოიფარგლება ერთი ქვეყნით ან ვალუტით, ამიტომ, ტრანსსასაზღვრო თანამშრომლობა სასიცოცხლოდ მნიშვნელოვანია.

ეუთო ასევე მოუწოდებს საკანონმდებლო ბაზის და მტკიცე მარეგულირებელი ზომების ჩამოყალიბებისკენ, როგორც კლასიკური ფულის გათეთრებისა და ტერორიზმის დაფინანსების წინააღმდეგ საბრძოლველად, ასევე კრიპტოვალუტების გამოყენებით უკანონო ქმედებების გამოვლენისა და თავიდან აცილების ღონისძიებების განსახორციელებლად. ეს წევრი სახელმწიფოების მიერ ფულის გათეთრების საწინააღმდეგო (AML) და ტერორიზმის დაფინანსების საწინააღმდეგო (CFT) საერთაშორისო სტანდარტების უზრუნველყოფას მოიცავს.

ამისათვის, ეუთო სასწავლო პროგრამებსა და სემინარებს მართავს, რათა ფინანსურ და კრიპტო დანაშაულებებთან დაკავშირებით, სამართალდამცავი უწყებების, ფინანსური ინსტიტუტების და სხვა დაინტერესებული მხარეების გამოცდილება გააუმჯობესოს. ეს ძალისხმევა კიბერდანაშაულისა და კრიპტოდანაშაულის გამოვლენისა მის წინააღმდეგ ბრძოლის მიზნით, საგამოძიებო მეთოდების გაუმჯობესებასა და მოწინავე ტექნოლოგიების გამოყენებისკენ არის მიმართული.

ამ პუბლიკაციის ფარგლებში, ეუთო პასუხობს კონკრეტული წევრი სახელმწიფოების საჭიროებას, რაც ვირტუალური აქტივების დანაშაულებრივი მიზნებისთვის გამოყენებისა და საერთაშორისო სანქციების გვერდის ავლის რისკების აღმოფხვრას უკავშირდება. ამ რისკების აღმოფხვრა არის პროექტის, „პოლიტიკის ინოვაციური გადაწყვეტილებები, ვირტუალურ აქტივებთან დაკავშირებული ფულის გათეთრების რისკების შესამცირებლად“ ძირითადი მიზანი, რომელსაც ეუთო-ს ეკონომიკური და გარემოსდაცვითი საქმიანობის კოორდინატორის ოფისი (OCEEA) ხელმძღვანელობს.

ამ პროექტის საბოლოო მიზანი, ვირტუალური აქტივების კონკრეტული სისუსტეების წინააღმდეგ საბრძოლველად, სახელმწიფო სტრუქტურების შესაძლებლობების ჩამოყალიბებაა.

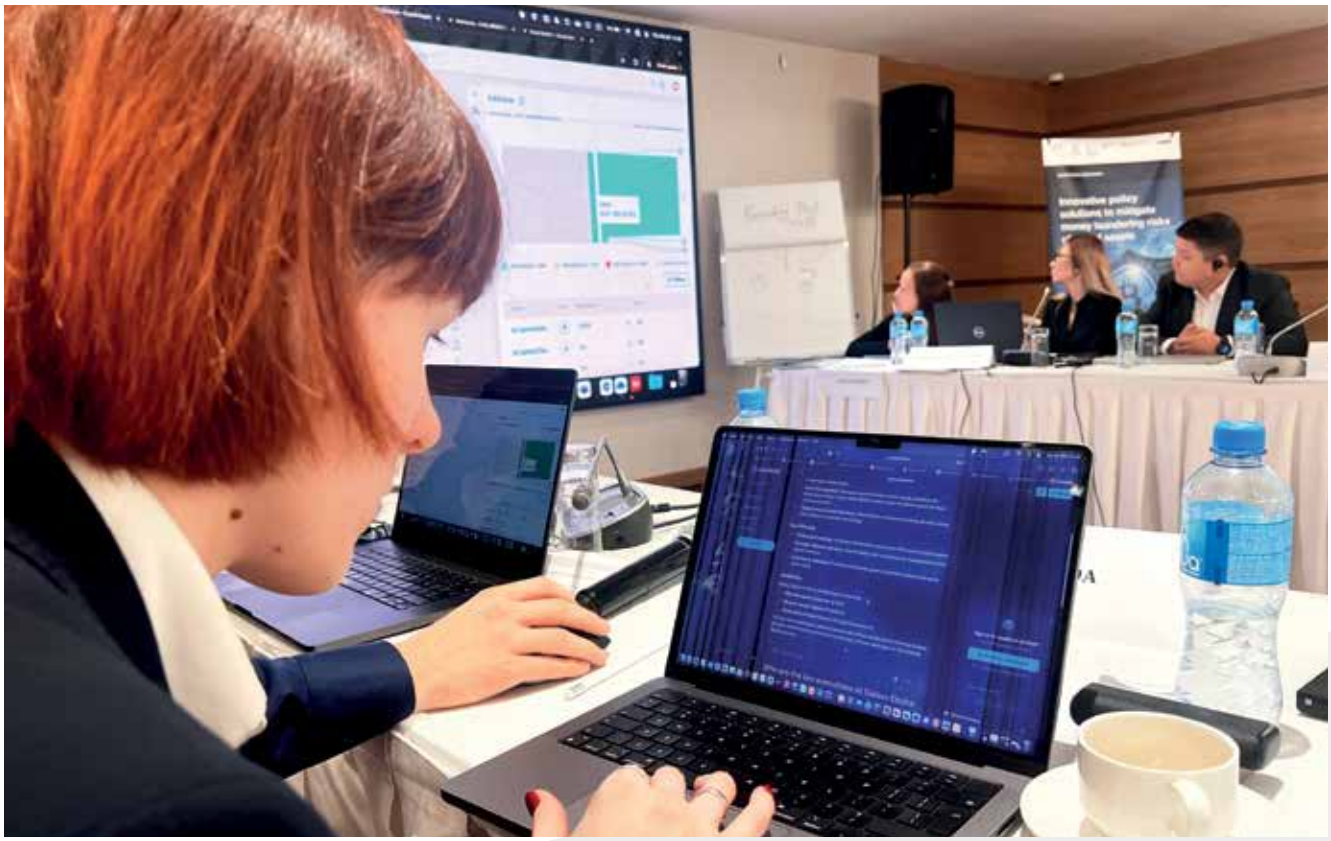
პროექტის განხორციელებისას, OCEEA, გაერო-ს ნარკოტიკებისა და დანაშაულის ოფისის ფულის გათეთრებასთან ბრძოლის გლობალურ პროგრამასთან ერთად (UNODC GPML), აგრძელებს აღმოსავლეთ ევროპისა და კავკასიის ქვეყნების - საქართველოს, მოლდოვას და უკრაინის დახმარებას, რაც ვირტუალურ აქტივებთან (VA) და ვირტუალური აქტივების მომსახურების პროვაიდერებთან (VASP) დაკავშირებით, მათი ნორმატიულ-სამართლებრივი ბაზის, FATF-ის რეკომენდაციებთან შესაბამისობაში მოყვანას ითვალისწინებს და იმავდროულად, ამ ქვეყნების შესაბამის სამართალდამცავ ორგანოებს შესაძლებლობების განვითარებით და ტექნიკური მხარდაჭერით ეხმარება.

პროექტის ეფექტურობის ასამაღლებლად ეუთო-ს გუნდი UNODC-თან თანამშრომლობდა. UNODC-მა კრიპტოვალუტებზე, ფულის გათეთრების (ML) და ტერორიზმის დაფინანსების (TF) რისკებზე, გამოძიებაზე, ამოღებასა და კონფისკაციაზე, რეგულაციასა და მომხმარებელთა წინდახედულებაზე საკუთარი გამოცდილება და პრაქტიკული სასწავლო პროგრამები წარმოადგინა. OCEEA აგრძელებს შესაბამისი ორგანოების მხარდაჭერას, როგორიცაა ცენტრალური ბანკები, ძირითადი ფინანსური ინსტიტუტების შესაბამისობის დეპარტამენტები, ფინანსური დაზვერვის ქვედანაყოფები, გენერალური პროკურატურები, იუსტიციისა და შინაგან საქმეთა სამინისტროები. ის ზემოჩამოთვლილ ორგანიზაციებს პერსონალისთვის რეგულაციებისა და ინსტრუქციების შემუშავებაში ეხმარება, საინფორმაციო-საგანმანათლებლო აქტივობებს უწევს ორგანიზებას და კრიპტოვალუტების გამოყენებით ჩადენილ დანაშაულთა გამოძიებისას, უწყებათაშორის და საერთაშორისო თანამშრომლობას უწყობს ხელს.

წინამდებარე პუბლიკაცია ინოვაციური პოლიტიკური გადაწყვეტილებების პროექტის ნაწილია, რომელიც ვირტუალურ აქტივებთან დაკავშირებული ფულის გათეთრების რისკების შემცირებას ემსახურება და გერმანიის, იტალიის, პოლონეთის, რუმინეთის, გაერთიანებული სამეფოს და შეერთებული შტატების მიერ ფინანსდება.

OSCE ევროპის უსაფრთხოებისა და თანამშრომლობის ოფისი

ყაზახეთში, ასტანაში, გამომძიებელთა სწავლებას გრეტა ბარკაუსკიენე ხელმძღვანელობს — AML ექსპერტი და ლიეტუვის PPP ცენტრის ფულის გათეთრების წინააღმდეგ ბრძოლის ეროვნული ჯგუფის კოორდინატორი. იგი თავის ფართო გამოცდილებას იყენებს, რათა სახელმწიფო და კერძო სექტორის საუკეთესო პრაქტიკა ბენეფიციარი ქვეყნების შესაძლებლობების გაძლიერებას მოემსახუროს.



თბილისში ჩატარებული სემინარები გამომძიებლებისთვის კრიპტოვალუტის აქტივების ჩამორთმევის ძირითად ასპექტებს დაეთმო, მათ შორის — უსაფრთხო ობიექტების მომზადებას პოტენციური კონფისკაციისთვის. სემინარები დაკავშირებული იყო სავარჯიშოსთან, რომელიც ბლოკჩეინზე აქტივების იდენტიფიკაციის, გადაცემისა და აღდგენის უნარების გაძლიერებას ისახავდა მიზნად. ფოტო: Michal Gromek.

წარმოდგენა ციფრულ აქტივებზე: გამარტივებული გზამკვლევი

წარმოდგენა ციფრულ აქტივებზე: გამარტივებული გზამკვლევი

ამ ნაწილში განვიხილავთ განსხვავებებს ციფრულ აქტივებსა, ფიატ ვალუტებსა და კრიპტოვალუტებს შორის. ასევე განვიხილავთ კრიპტოვალუტების განსხვავებულ ტიპებს და მათ ირგვლივ არსებულ ინფრასტრუქტურას.

ხშირად არის ბუნდოვანება იმასთან დაკავშირებით, თუ რა განსხვავებაა ციფრულ აქტივებს, ვირტუალურ აქტივებს, კრიპტო აქტივებსა და კრიპტოვალუტას შორის.

მარტივად რომ ვთქვათ, ციფრული აქტივი ყველაზე ფართო ტერმინია. ეს არის აქტივი, რომელიც ციფრული ფორმით არსებობს. ეს მოიცავს გამოსახულებებს, ვიდეოებს, მუსიკას (მაგ. MP3 ფორმატში), დოკუმენტებს და ვირტუალურ ვალუტას.

ვირტუალური აქტივი ციფრული აქტივების ვიწრო კრებულია. FATF -ის თანახმად ვირტუალური აქტივები (კრიპტო აქტივები) მიეკუთვნება ღირებულების ნებისმიერ ციფრულ გამოხატულებას, რომლითაც ციფრულ ფორმატში ვაჭრობა, გადაცემა, ან გამოყენება არის შესაძლებელი. ის არ მოიცავს ფიატური ვალუტების ციფრულ გამოხატულებას.

ამის საპირისპიროდ, კრიპტო აქტივს კიდევ უფრო ვიწრო ნიშა აქვს. ეს არის აქტივი, რომელსაც ღირებულება აქვს, მაგრამ განაწილებული აღრიცხვის ტექნოლოგიით (DLT) უნდა გადაიცეს. ბლოკჩეინი DLT-ის ტიპია. თქვენ შეგიძლიათ გქონდეთ ვირტუალური აქტივი, მაგალითად, მონეტა ონლაინ თამაშში, რომელიც არ არის კრიპტოაქტივი, რადგან ის მოთამაშეებს შორის, განაწილებული რეესტრის ტექნოლოგიის გამოყენების გარეშე გადაიცემა. ბლოკჩეინი ამჟამად განაწილებული აღრიცხვის ტექნოლოგიის ყველაზე გამორჩეული ტიპია, მაგრამ არსებობს სხვა DLT ტექნოლოგიები, როგორებიცაა Hashgraph, Iota Tangle, R3 Corda და მრავალი სხვა. ამ სახელმძღვანელოს მიზნებისთვის, ჩვენ ყურადღებას ბლოკჩეინზე დაფუძნებულ ფინანსებზე ვამახვილებთ.

ციფრულ აქტივებს შორის მრავალი სხვადასხვა ტიპის აქტივი არსებობს, მათ შორისაა კრიპტოვალუტები, რომლებიც ახალი ტიპის ვალუტებია (ისინი ბლოკჩეინ ტექნოლოგიის გამოყენებით მუშაობენ) და არაჩანაცვლებადი ტოკენები (NFT), რომლებიც ძირითადად გამოსახულებაზე (ნახატი, ვიდეო ა.შ.) დაფუძნებული აქტივებია.

ამგვარად, როგორც კი კრიპტო აქტივი ვაჭრობის, გადაცემის, ან გადახდისთვის გამოსაყენებლად შეიქმნება, ჩვენ მას კრიპტოვალუტას ვუწოდებთ. ასევე შეიძლება შეგხვდეთ ტერმინი ვირტუალური ვალუტა, რომელიც კრიპტოვალუტასთან ურთიერთშენაცვლებით ხშირად გამოიყენება. კრიპტოვალუტასა და ვირტუალურ ვალუტას შორის განმასხვავებელი ფაქტორი ტექნოლოგიაა. კრიპტოვალუტები იყენებენ ბლოკჩეინს, მაშინ როცა ვირტუალური ვალუტები ბლოკჩეინზე აგებული შეიძლება არც იყოს.

ეს გზამკვლევი ძირითადად კრიპტოვალუტით ჩადენილ დანაშაულებზე იქნება ფოკუსირებული.

ავტორის ნებართვით (ალექსანდრა ანდჰოვი, გამოთვლითი სამართალი, კარნოვი, 2022).

1 ფინანსური ქმედებების სპეციალური ჯგუფი, წყარო: https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies (შემოწმდა: 2023 წლის 26 სექტ.).

კრიპტოვალუტებისა და ფიატური ვალუტების შედარება

„FIAT ვალუტად“ ცნობილი ტრადიციული მონეტები და ქაღალდის ფული საუკუნეების განმავლობაში ჩვენი ეკონომიკის ხერხემალი იყო. თუმცა, ტექნოლოგიების განვითარებასთან ერთად გაჩენილმა ფულის ახალმა ფორმებმა მატერიალურსა და ვირტუალურს შორის საზღვრები ბუნდოვანი გახადა. კერძო პირები FIAT ვალუტის ელექტრონული გადარიცხვების დროს (ერთი ადამიანი უგზავნის მეორეს) იყენებენ „ელექტრონულ ფულს“. ელ-ფული, ანუ ელექტრონული ფული, წარმოადგენს ჩვენთვის ნაცნობ FIAT ვალუტას ციფრული ფორმით, რაც ხელს უწყობს ელექტრონულ ტრანზაქციებს მისი ღირებულების შეცვლის გარეშე. ელექტრონული ფული არის ფიატ ვალუტის ციფრული გამოხატულება.

ფიატური ფულისგან განსხვავებით კრიპტოვალუტები დეცენტრალიზებულ გარემოში ფუნქციონირებს. ისინი არ ებმის არცერთ მთავრობას, ან ცენტრალურ ბანკს, და მათ ღირებულებას სხვადასხვა ფაქტორი, მათ შორის მოთხოვნა, ტექნოლოგია და ნდობა, განსაზღვრავს. ასეთი ვალუტების პოტენციალი ამ სფეროში წამყვანმა ვალუტამ - ბიტკოინმა აჩვენა. მისი ღირებულება მნიშვნელოვნად გაიზარდა. ჯერ კიდევ 2021 წელს, მისი თითო მონეტის ფასმა $64 000-ზე მეტს მიაღწია. კრიპტოვალუტები, როგორიცაა ბიტკოინი და ტეზერი, არცერთი მთავრობის ან ცენტრალური ბანკის მიერ გარანტირებული არ არის. მიუხედავად იმისა, რომ ვირტუალური ვალუტები ისეთი ძველი არ არის, როგორც ფიატური ვალუტა, ისინი არც ისე ახალია, როგორც ადამიანების უმეტესობა ფიქრობს. ერთ-ერთი პირველი ვირტუალური ვალუტა „ე-გოლდი“ (E-Gold), თითქმის 30 წლის წინ, 1996 წელს დაინერგა.

E-გოლდის შეჯამება

ერთ-ერთ პირველ პოპულარულ ვირტუალურ ვალუტას „E-Gold“ (ელექტრონული ოქრო) ეწოდებოდა. დაარსდა 1996 წელს, დუგლას ჯექსონისა და ბარი დაუნის მიერ. E-გოლდი მომხმარებლებს საშუალებას აძლევდა გაეხსნათ ანგარიში, რომლის ღირებულებაც ოქროს გრამებში (ან სხვა ძვირფას ლითონებში) გამოისახებოდა და მათ E-გოლდის სხვა ანგარიშებზე, ღირებულების მყისიერი გადარიცხვის შესაძლებლობას აძლევდა.

2005 წელს E-გოლდს 2.5 მილიონი ანგარიშის მფლობელი ჰყავდა, რომლებიც ასრულებდნენ ყოველდღიურ ტრანზაქციას, ჯამში 6.3 მილიონი აშშ დოლარის ღირებულებით. ის ეფექტურობის, დაბალი გადასახადებისა და გლობალური ხელმისაწვდომობის გამო იყო პოპულარული. თუმცა, მკაცრი რეგულაციების არარსებობამ უკანონო საქმიანობასაც შეუწყო ხელი.

2007 წელს, E-გოლდს შეერთებულ შტატებში ბრალი წაუყენა ნაფიც მსაჯულთა სასამართლომ, კომპანიას ბრალი დასდეს ფულის გათეთრებაში, შეთქმულებასა და ფულის არალიცენზირებულად გადაცემის ბიზნესში. ამან საბოლოოდ, 2009 წელს აშშ-ის სასამართლოების მიერ, E-გოლდის დახურვა გამოიწვია.

E-გოლდს ბევრი მიმბაძველი გამოუჩნდა, მაგალითად e-Bullion.com, Pecunix.com და სხვა.[2]

ამ სფეროს განხილვისას მნიშვნელოვანია კონკრეტული ვიყოთ, რადგან ვირტუალური ვალუტები შეიძლება მიეკუთვნებოდეს როგორც ელექტრონულ ვალუტებს, ასევე კრიპტოვალუტებს. ამან შეიძლება დაგაბნიოთ. ამ გზამკვლევში ჩვენ ყურადღებას კრიპტოვალუტებზე ვამახვილებთ.

საბაზისო ტექნოლოგია: ბლოკჩეინი

ბლოკჩეინი არის განაწილებული აღრიცხვის ტექნოლოგიის (DLT) ტიპი. ეს ახალი ტექნოლოგია პირველად 2008 წელს, სატოში ნაკამოტოს[3] მიერ გამოქვეყნებულ "თეთრ ქაღალდში" გამოჩნდა. ის განისაზღვრება, როგორც დეცენტრალიზებული, ვინაიდან მასში არ არსებობს კონტროლის ერთი ცენტრი, ან პასუხისმგებელი პირი. ამის ნაცვლად, ცვლილებების შეტანა ნებისმიერ მომხმარებელს შეუძლია. მაგრამ იმისთვის, რომ ისინი მუდმივი გახდეს, უნდა დაადასტუროს მომხმარებელთა უმრავლესობამ.

ბევრი განსხვავებული ბლოკჩეინი არსებობს. ბლოკჩეინი ეს უბრალოდ ტექნოლოგიაა. თითოეული ბლოკჩეინი წარმოიდგინეთ, როგორც შენობა. მიუხედავად იმისა, რომ თითოეული მათგანი შეიძლება ძალიან განსხვავებულად გამოიყურებოდეს და თითოეულ შენობას განსხვავებული დანიშნულება ჰქონდეს, როდესაც დეტალურად ვათვალიერებთ, თითქმის ყველა შენობა აგურითა და ცემენტითაა აგებული.

ისევე, როგორც შენობების შემთხვევაში, ზოგიერთ ბლოკჩეინზე წვდომა ნებისმიერს, ნებართვის გარეშე შეუძლია. ზოგი კი, სანამ გაწევრიანების უფლებას მოგცემთ, დამტკიცებას მოითხოვს. ამ მხრივ განასხვავებენ საჯარო და კერძო ბლოკჩეინს.

---

2 ფედერალები E-გოლდს კიბერთაღლითების დახმარებაში ადანაშაულებენ“, NBC News, 2007 წლის მაისი.- (ხელმისაწვდომია: http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helpingcybercrooks (შემოწმდა 2023 წლის 24 აგვისტო). „ინტერნეტ ვალუტის ფირმა ფულის გათეთრებაში თავს დამნაშავედ ცნობს“, The Industry Standard, 2008 წლის ივლისი: http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering (შემოწმდა: 2023 წლის 24 აგვისტო). E-გოლდის ტრანზაქციების მიმოხილვა (1996) E-Gold: http://www.e-gold.com/unsecure/synopsis.htm (შემოწმდა: 2023 წლის 24 აგვისტო).

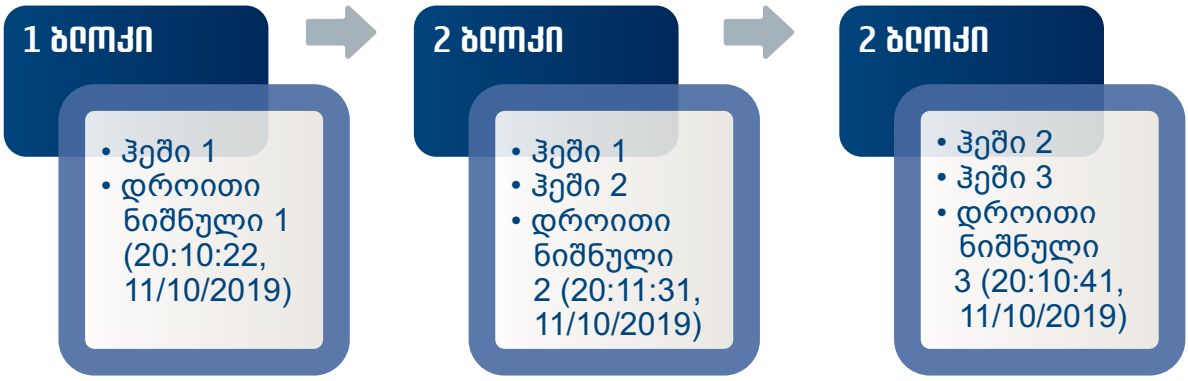
3 ნაკამოტო, ს. (2008) ელექტრონული ერთრანგიანი ფულადი სისტემა, ბიტკოინი: https://bitcoin.org/en/bitcoin-paper (შემოწმდა: 26 აგვისტო, 2023).

განვასხვავებთ საჯარო და კერძო ბლოკჩეინებს. საჯარო ბლოკჩეინებს „უნებართვო“ ეწოდებათ და, როგორც წესი, ნაკლებ გამჭვირვალობას ან კონტროლს საჭიროებენ „ნებართვის მქონე“ ბლოკჩეინებისაგან განსხვავებით, რომლებსაც ხშირად საწარმოს მიზნებისთვის იყენებენ და გაწევრიანების მსურველი პირის დამტკიცებას საჭიროებს. ბლოკჩეინს ასე ჰქვია, რადგან მომხმარებლები ამატებენ ან ცვლიან მონაცემების „ბლოკებს“.

ეს ბლოკები ერთმანეთთან მიბმულია ჯაჭვში (დროის მიხედვით). როდესაც ერთი მომხმარებელი ქმნის ან ატვირთავს ახალ ბლოკს (მაგალითად, ახალი ტრანზაქცია ბიტკოინით), ყველა სხვა მომხმარებელმა ბლოკჩეინზე უნდა დაადასტუროს ახალი ბლოკი „კონსენსუსის მეთოდების“ გამოყენებით (ეს მოიცავს საკმაოდ რთულ მათემატიკურ განტოლებებს, რათა უზრუნველყოფილი იყოს მისი სანდოობა). რადგან ყველა ბლოკი ერთმანეთთანაა დაკავშირებული, თითქმის შეუძლებელია წინა ბლოკზე გადასვლა და მისი შეცვლა. ეს ნიშნავს, რომ სისტემაში ჩარევა შეუძლებელია. ნებისმიერი ახალი ინფორმაცია, მათ შორის ძველი ინფორმაციის ცვლილებები, ახალ ბლოკში ჩაიწერება.

ბლოკჩეინი იმგვარად მუშაობს, რომ ამ ჯაჭვთან დაკავშირებულ ყველა მომხმარებელს ჯაჭვის („ჩანაწერების“) მთელი ისტორიის ნახვის საშუალებას აძლევს. ამიტომ, ბიტკოინის ბლოკჩეინის საშუალებით მომხმარებლებს ყველა განხორციელებული ტრანზაქციის ნახვა შეუძლიათ. ეს გამომძიებლებს გამოძიების ჩატარების საშუალებას აძლევს. რადგანაც ბლოკჩეინის რეესტრი ყველა მომხმარებლისთვისაა ხელმისაწვდომი ბლოკჩეინს „განაწილებული რეესტრის ტექნოლოგია“ ან „გრტ“ (DLT) ეწოდება.

ის „გუგლის ფურცლის“ („Google Sheet“) მსგავსია, რომელზე მუშაობა და წინა ვერსიების ნახვაც ყველას შეუძლია. გამჭვირვალობის, ნდობის და უსაფრთხოების მაღალ ხარისხს განაპირობებს ის, რომ ყველაფერი ჩანს და შეუძლებელია ისე შეიცვალოს, რომ ყველამ ვერ შეძლოს მისი დანახვა. ასევე არის თავდასხმების საწინააღმდეგო მაღალი ხარისხის მდგრადობა: რადგან ყველა ადამიანს აქვს ბლოკჩეინის ასლი და არ არსებობს ცენტრალიზებული ვერსია, მაშინაც კი, თუ ერთ მომხმარებელს („კვანძი“ ბლოკჩეინის ტერმინოლოგიით) თავს დაესხნენ და მწყობრიდან გამოიყვანეს, სისტემა აგრძელებს ფუნქციონირებას.



ავტორის ნებართვით (ალექსანდრა ანდჰოვი, "გამოთვლითი სამართალი", კარნოვი, 2022).

კრიპტოვალუტების ტიპები

კრიპტოვალუტების განსხვავების ორი გზა არსებობს:

- კონვერტირებადია თუ არაკონვერტირებადი
- ცენტრალიზებულია თუ დეცენტრალიზებული

ეს განმასხვავებელი მახასიათებლები უფრო დეტალურად ქვემოთ არის აღწერილი.

კონვერტირებადი და არაკონვერტირებადი ვალუტები

კონვერტირებად ვალუტებს ფიატურ ვალუტაში ეკვივალენტური ღირებულება აქვთ და მათი „ჩვეულებრივ“ ფულზე უკან გადაცვლა შესაძლებელია. ეს კონვერტირებადობა გარანტირებული არ არის, რადგან კრიპტოვალუტებს არცერთი მთავრობა ან ინსტიტუტი მხარს არ უჭერს. კრიპტოვალუტის ფიატურ ვალუტაში კონვერტირებადობას არსებული საბაზრო და კერძო შეთავაზებები განაპირობებს. ეს არის კრიპტოვალუტის ტიპი, რომელიც ყველაზე მეტად ფიგურირებს დანაშაულებებში.

კონვერტირებადი ვალუტების მაგალითებია ბიტკოინი და E-გოლდი. არაკონვერტირებადი ვალუტები ოქროს მონეტების მსგავსია და კომპიუტერულ თამაშში რჩება. ამ ვალუტებით ჩადენილი დანაშაულის ალბათობა ნაკლებია, რადგან მათ რეალური ღირებულება არ აქვთ. თუმცა ზოგიერთი ადამიანი მათი გაცვლის გზას პოულობს იმ თამაშის საზღვრებს გარეთ, სადაც ისინი არსებობენ. ამგვარად, ისინი კონვერტირებადობას იძენენ მაშინაც კი, თუ ეს თამაშის წესებს ეწინააღმდეგება. მაგალითად, ვინმეს შეუძლია თამაშში „შეგროვებული ოქროს მონეტები“ ერთი მოთამაშისგან მეორე მოთამაშეს გადაურიცხოს.

ტრანზაქცია კი ოფლაინ რეჟიმში ნაღდი ფულით გადაიხდება.

ცენტრალიზებული და დეცენტრალიზებული ვალუტები

ცენტრალიზებულ კრიპტოვალუტებს ზედამხედველობას ერთი ორგანო უწევს, რომელიც გამოსცემს ვალუტას, ადგენს მის წესებს, აწარმოებს გადახდის რეესტრს და მიმოქცევიდან მისი ამოღების უფლება აქვს. ცენტრალიზებული ვალუტები შეიძლება კონვერტირებადი, ან არაკონვერტირებადი იყოს. არაკონვერტირებადი ვალუტები ყოველთვის ცენტრალიზებულია (რადგან მაგალითად, თამაშში არ შეიძლება იყოს ვალუტა, თუ თამაში ამ ვალუტას არ აკონტროლებს). ცენტრალიზებული კონვერტირებადი ვალუტის გაცვლისას, გაცვლითი კურსი ბაზრის მიწოდებისა და მოთხოვნის შესაბამისად განისაზღვრება, ან ადმინისტრატორის მიერ ფიქსირდება. E-გოლდი ცენტრალიზებული ვალუტის თვალსაჩინო მაგალითია.

მეორე მხრივ, დეცენტრალიზებულ ვალუტებს ცენტრალური მმართველი არ ჰყავს და Peer-to-Peer (პირიდან-პირზე) ქსელზე დაყრდნობით მოქმედებენ. წარმოიდგინეთ დეცენტრალიზებული სისტემა, როგორიც ინტერნეტია. ისევე, როგორც არ არსებობს ერთი ზედამხედველი, რომელიც მთელ ინტერნეტზე არის პასუხისმგებელი, დეცენტრალიზებულ სისტემასაც ერთი მთავარი მაკონტროლებელი არ ჰყავს. მიუხედავად იმისა, რომ ადამიანების უმეტესობა ყოველდღიურად იყენებს ინტერნეტს, არ არსებობს არც ერთი კომპანია, რომელიც ამაში ფულს იღებს; სამაგიეროდ, სხვადასხვა პროვაიდერს ფულს სხვადასხვა მომსახურებისთვის უხდიან. სწორედ ასე გამოიყენება ბლოკჩეინის ქსელის ტექნოლოგია, რომელიც ისეთ კრიპტოვალუტებს უდევს საფუძვლად, როგორიც ბიტკოინია. ტრანზაქციების მართვა ქსელის მეშვეობით ხდება და რომელიმე ორგანოს მიერ სხვა მონიტორინგი არ ხორციელდება.

2023 წლის 23 აგვისტოს მდგომარეობით, ყველაზე დიდი საბაზრო კაპიტალის მქონე ათი კრიპტოვალუტის სია ქვემოთ, სქოლიო 4-ში მოცემულ ბმულზე დაყრდნობით არის მოყვანილი.[4]

დასახელება	სიმბოლო	საბაზრო კაპიტალიზაცია (2023 წლის 23 აგვისტო)	შემდეგი ქვეყნის მთლიან შიდა პროდუქტს უტოლდება[5]
ბიტკოინი	BTC	$ 514 912 135 787	სუდანი
ეთერიუმი	ETH	$ 201 475 414 760	ჰაიტი
ტეთერი USDt	USDT	$ 82 835 552 223	სომალი
BNB	BNB	$ 33 285 580 473	ანდორა
XRP	XRP	$ 27 991 699 189	კურასაო
USD კოინი	USDC	$ 26 005 195 827	ლესოტო
კარდანოდანო	ADA	$ 9 357 776 591	სენტ-ვინსენტი და გრენადინები
დოგკოინი	DOGE	$ 8 965 846 112	ჩრდილოეთ მარიანის კუძნულები
სოლანა	SOL	$ 8 792 761 272	სამოა
ტრონი	TRX	$ 6 938 358 042	ამერიკის სამოა

ფსევდოვალუტები და კონფიდენციალური მონეტები

ფსევდოანონიმური ვალუტების ანგარიშები მოიცავს ანგარიშებს, რომლებიც იყენებენ ფსევდონიმებს. ეს ნიშნავს იმას, რომ ტრანზაქციებსა და პირად მონაცემებს შორის კავშირის არარსებობის მიუხედავად ზოგი საიდენტიფიკაციო ინფორმაცია მაინც რჩება. მაგალითად, კრიპტოვალუტის შესაძენად გამოსაყენებელი ტიპიური ფიატური ვალუტის საბანკო ანგარიში დაკავშირებულია საიდენტიფიკაციო მონაცემებთან. ამ კატეგორიაში შედის ისეთი მონეტები, როგორიცაა ბიტკოინი და ეთერი.

ამის საპირისპიროდ, კონფიდენციალურობის მონეტები უფრო მეტ ანონიმურობას გვთავაზობენ, რადგან ტრანზაქციის დეტალებისა და მასთან დაკავშირებული ვინაობის დასაფარად მოწინავე კრიპტოგრაფიულ მეთოდებს იყენებენ. ეს ართულებს მათი თავდაპირველი მომხმარებლის კვალის დადგენას.

ასეთი მონეტების მაგალითებია მონერო და ზეროქეში (Zcash).

4 ყველა კრიპტოვალუტა (2023) CoinMarketCap: https://coinmarketcap.com/all/views/all/ (შემოწმდა: 2023 წლის 24 აგვისტოს).

5 მშპ-ის შესახებ მსოფლიო ბანკის მონაცემებზე დაყრდნობით (აშშ დოლარის მიმდინარე კურსი), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false (შემოწმდა 2023 წლის 23 აგვისტოს).

კრიპტო საფულეები

კრიპტოვალუტის საფულე არის ადგილი, სადაც კრიპტოვალუტა ინახება. კარგი ანალოგიაა იმის წარმოსადგენად, თუ როგორ ინახება ფული დღეს მთელ მსოფლიოში.

ფული სხვადასხვა ფორმით არსებობს. მისი ნაწილი მსხვილ ბანკებში ოქროს ზოდებად ინახება. ნაწილი ქაღალდის ბანკნოტების, ონლაინ საბანკო გადარიცხვების, ან კრიპტოვალუტების სახით ბრუნავს. არსებობს კრიპტოვალუტის საფულეების სხვადასხვა ფორმა: ტელეფონის აპლიკაცია, USB დისკის მსგავსი მოწყობილობა, ან უბრალოდ პროგრამული უზრუნველყოფის ნაწილი (თქვენი ელექტრონული ფოსტის მისამართის მსგავსი), რომელზეც წვდომა მომხმარებლის სახელისა და პაროლის შეყვანით გეძლევათ. მიუხედავად იმისა, რომ კრიპტოვალუტის სხვადასხვა სახის საფულეები არსებობს, ისინი ერთსა და იმავე ტექნოლოგიას იყენებენ. უმეტესობას აღდგენის 12, 18, ან 24-სიტყვიანი პაროლი აქვს, რომლითაც შესაძლებელია საფულის ხელახლა გახსნა.

კრიპტოვალუტის საფულეების მისამართები

კრიპტოვალუტის საფულის მისამართები საბანკო ანგარიშის ნომრის მსგავსია. ვინმეს საბანკო ანგარიშის ნომრის ფლობა მის ფულზე წვდომას არ ნიშნავს. კრიპტო საფულის მისამართებს გრძელი, რთული თანმიმდევრობა აქვთ და რეგისტრისადმი მგრძნობიარე ასოებისა და ციფრებისგან შედგებიან. მოცემულია ორი მაგალითი:

კრიპტოვალუტის საფულე ვალუტა ტრონისთვის
TYm3NTSyk85t9UHSd68DY4vGWQADHXpaXJ

კრიპტოვალუტის საფულე ბიტკოინისთვის
Bc1qu5z7kn0v2krhglsnan4c0m5f76xk69p53wjwgh

განსხვავება ტრადიციული საბანკო ანგარიშის ნომრებსა და კრიპტო საფულეების მისამართებს შორის ისაა, რომ კრიპტო საფულის მისამართებთან შედარებით საბანკო ანგარიშის ნომრიდან ბევრი ინფორმაციის შეგროვება შეიძლება. სამართალდამცავ ორგანოებს შეუძლიათ IBAN ნომერი მარტივად გაშიფრონ და შესაბამის ორგანოს დაუკავშირდნენ.

IBAN საერთაშორისო საბანკო ანგარიშის ნომერია. მას შეიძლება 34 ასო და რიცხვი ჰქონდეს. ის იწყება ქვეყნის კოდით, უსაფრთხოების ორნიშნა შემოწმებით და შემდეგ ბანკისა და ანგარიშის დეტალებით. ზოგჯერ, სხვადასხვა ქვეყანაში, ამ საბანკო დეტალებს განსხვავებულად

IBAN:

- LT44 32500 47338696265

  LT ლიეტუვის რესპუბლიკას განსაზღვრავს,

  32500 განსაზღვრავს Revolut Bank UAB-ს

  47338696265 არის მომხმარებლის ანგ. ნომერი[6]

აფორმებენ. მაგალითისთვის: თუ გამოძიებაში IBAN საბანკო ანგარიშის მსგავსი ნომერი გამოჩნდება, ოფიცერს ეცოდინება, რომ ლიეტუვის ბანკ Revolut-ს უნდა დაუკავშირდეს. ამ ინფორმაციის მიღება, ეგრეთ წოდებული „IBAN ვალიდატორებისგან“ შეიძლება (iban.com, ან https://wise.com/gb/iban/checker). შემდეგ შეიძლება ანგარიშის მომხმარებლის შესახებ პირადი ინფორმაციის მოპოვების პროცესი დაიწყოს. ფსევდოანონიმური კრიპტოვალუტებისთვის, როგორიცაა Bitcoin, ვერცერთი სამართალდამცავი ოფისი ვერ შეძლებს ანგარიშის მფლობელის შესახებ პირადი ინფორმაციის იდენტიფიცირებას, ანგარიშის ასეთი ნომრის საფუძველზე: bc1qu5z7kn0v2krhglsnan4c0m5f76xk-69p53wjwgh.

მფლობელის საიდენტიფიკაციო ინფორმაციის მოსაძებნად, სპეციალიზებული პროგრამული უზრუნველყოფაა საჭირო. მაგალითად, ბლოკჩეინ ანალიტიკის პროვაიდერი. იგი გამოიყენება მოპარული კრიპტოვალუტებისთვის. ასეთ პროვაიდერებს შეუძლიათ დაადგინონ, თუ რომელ ფინანსურ ინსტიტუტებს, ან კრიპტო ბირჟებს (VASP – ვირტუალური აქტივების მომსახურებების მიმწოდებლებს) ეკუთვნის ეს

6 IBAN და ფინანსური ინსტიტუტების კოდები, ლიეტუვის ბანკი, , https://www.lb.lt/en/iban-and-financial-institution-codes (2023 წლის 25 სექტემბერი).

საიდენტიფიკაციო ინფორმაცია, რაც იმ ქვეყნის კანონმდებლობაზეა დამოკიდებული, სადაც ისინი მუშაობენ. ამ მიზეზით, საერთაშორისო აქტორები, როგორიცაა ეუთო, თავიანთ წევრ სახელმწიფოებს, ამ სფეროში საუკეთესო საერთაშორისო პრაქტიკის დანერგვაში ეხმარებიან.

კრიპტოსაფულის ექსპლორერები

ვინაიდან წამყვანი ტიპის საჯარო ბლოკჩეინი ყველასთვის ღიაა, ნებისმიერს შეუძლია გადახედოს საფულეში განხორციელებულ ყველა ტრანზაქციას "კრიპტოსაფულის ექსპლორერის" გამოყენებით.

კრიპტოსაფულის ექსპლორერი არის საძიებო სისტემა, რომელიც სპეციალურად ბლოკჩეინის მონაცემებში ნავიგაციისთვისაა შექმნილი. ის იძლევა დეტალურ ინფორმაციას ცალკეული ბლოკების, ტრანზაქციების და დაკავშირებული საფულეების შესახებ. წარმოიდგინეთ ეს როგორც "Google" ბლოკჩეინის ტრაზაქციებისთვის. კრიპტოსაფულის ექსპლორერის ძირითადი გამოყენება:

შენიშვნა

თითოეული ტიპის კრიპტოვა-ლუტისთვის შეიძლება სხვა-დასხვა საფულის ექსპლორერი დაგჭირდეთ. საუკეთესო ვარიანტია კრიპტოვალუტის სახელის აკრეფა, რომლის მოკვლევაც გსურთ. წამყვანი პროვაიდერების მოკვლევის მიზნით, საძიებო სისტემაში სიტყვათშეთანხმება „საფულის ექსპლორერი“ (“Wallet Explorer”) ან „ბლოკჩეინის ექსპლორერი“ („Blockchain Explorer“) აკრიფეთ. როგორც წესი, ასეთი მომსახურება უფასოა.

- ტრანზაქციის შემოწმება:
  საფულის ექსპლორერი მომხმარებლებს განხორციელებული ტრანზაქციის გადამოწმების საშუალებას აძლევს.
  როდესაც ვინმე აცხადებს, რომ კრიპტოვალუტა გადმოგზავნა, ექსპლორერის გამოყენებით შესაძლოა ამის დადასტურება: ტრანზაქციის იდენტიფიკატორის (ID) ან საფულის მისამართის გამოყენებით.

- აუდიტი და აღრიცხვა:
  ფიზიკური პირებისთვის ან ბიზნესებისთვის, რომლებსაც ტრანზაქციების ჩანაწერების შენახვა ესაჭიროებათ, ექსპლორერს შეუძლია დეტალური ინფორმაციის მიწოდება თუ როდის მოხდა ტრანზაქცია, რა თანხა გაიგზავნა და რომელი მისამართებია გამოყენებული.

- კვლევა და ანალიზი:
  შემქმნელები, მკვლევარები და ანალიტიკოსები, ბლოკჩეინის საერთო მდგომარეობის და აქტივობის შესასწავლად საფულის ექსპლორერს ხშირად იყენებენ. მათ შეუძლიათ შესრულებული ტრანზაქციების რიცხვი, ტრანზაქციების მოცულობა და სხვა ბევრი რამ ნახონ.

- საფულის ბალანსი:
  ექსპლორერში საფულის მისამართის შეყვანით შეგიძლიათ კონკრეტული კრიპტოვალუტის საფულის ბალანსი და მისი ტრანზაქციების ისტორია ნახოთ.

კრიპტო საფულეების უფასო ექსპლორერები:

კრიპტოვალუტის თითოეული ტიპის კრიპტო საფულეების პოვნა მარტივად - ჩვეულებრივ ინტერნეტ საძიებო სისტემაში „XXX კრიპტოვალუტის საფულის საუკეთესო უფასო ექსპლორერის“ აკრეფითაა შესაძლებელი.

ამ ინსტრუმენტების გამოყენებით, ბლოკჩეინზე ტრანზაქციების შესწავლა და გადამოწმება ყველას შეუძლია. კრიპტოვალუტის ფლობის, ან ტექნოლოგიის სიღრმისეული ცოდნის გარეშეც. როგორც ინტერნეტში სანდო საძიებო ინსტრუმენტებით შეგვიძლია ძებნა, ზუსტად ისეა შესაძლებელი ბლოკჩეინების მოძებნაც.

კრიპტოვალუტების გაცვლა

„ჩვეულებრივი“ ფულის მსგავსად, ერთი ტიპის კრიპტოვალუტის მეორეზე ან FIAT ვალუტაზე გადასაცვლელად, კონკრეტული პლატფორმის გამოყენებაა საჭირო. არსებობს სამი ძირითადი ტიპის პლატფორმა: თანაბარი დონის ბირჟები (P2P), ცენტრალიზებული ბირჟები (CEX) და დეცენტრალიზებული ბირჟები (DEX).

P2P ნიშნავს პირიდან-პირზე, ან უფრო ხშირად, მომხმარებლიდან მომხმარებელზე (რადგან მომსახურების გამწევ იურიდიულ პირებს შეუძლიათ, თავიანთი აქტივები გაყიდონ ან შესთავაზონ) გაცვლა. აქ მომხმარებლები არა უშუალოდ ბირჟიდან, არამედ სხვა მომხმარებლებისგან ყიდულობენ. ასეთი P2P ბირჟის მაგალითი, რომელმაც ფუნქციონირება შეწყვიტა, იყო ფინური მიმწოდებელი სახელწოდებით LocalBitcoin.com.

ასეთი ბირჟები ყიდიან საკუთარ ვირტუალურ აქტივებს და მომხმარებლებს ერთმანეთთან არ აკავშირებენ.

P2P გადამცვლელები ექვემდებარება AML და CTF რეგულაციებს[7] და უნდა ფლობდნენ მომხმარებლის დეტალურ ინფორმაციას. ასევე მათ უნდა დაიცვან იმ ქვეყნებში, სადაც უწევენ მომსახურებას გარკვეული წესები.

დეცენტრალიზებული ბირჟები დარწმუნებით აცხადებენ, რომ ისინი ავტომატური ფაილების გარდამქმნელების მსგავსად ფუნქციონირებენ (მაგ., .doc to .pdf). ისინი ძირითადად კრიპტოდან-კრიპტოზე ტრანზაქციებისთვის გამოიყენება და ნაკლებად ფიატის კრიპტოვალუტებზე გადაცვლისთვის. დეცენტრალიზებულ ბირჟებში ჩართულ ფონდებს მოსაკვლევად სპეციალიზებული მხარდაჭერა ესაჭიროებათ.

ეს მხოლოდ აისბერგის მწვერვალია. ასევე არსებობს ახალი ტიპის ბირჟები, როგორიცაა ზემოთ ნახსენები დეცენტრალიზებული ბირჟები, OTC ბირჟები, მიქსერები და ტამბლერები. ეს არის სწრაფად განვითარებადი ტექნოლოგია, რომელიც მომხმარებლების ტრანზაქციების კვალის დამალვის მიზნით შეიქმნა. ეუთო-ს ბევრი წევრი სახელმწიფო, ამგვარი ინსტრუმენტების გამოყენების შეზღუდვის მიზნით შესაბამის ქმედებებს ახორციელებს.

მიქსერები და ტამბლერები

მიქსერები და ტამბლერები არის სერვისები, რომლებიც კრიპტოვალუტის ტრანზაქციების კონფიდენციალურობისა და ანონიმურობის გასაძლიერებლად არის შექმნილი. მათი უპირველესი ფუნქცია სხვადასხვა მომხმარებლის ფონდების შერევაა, რითაც ფონდების თავდაპირველი წყარო ინიღბება.

7 იმ ქვეყნებში მოქმედი კრიპტობირჟებისთვის, რომლებმაც FATF-ის 15 რეკომენდაცია შეასრულეს. ეს რეკომენდაციები ქვეყნებს მოუწოდებს კრიპტოვალუტებთან დაკავშირებული ფინანსური სუბიექტები ჩართონ თავიანთ AML და CTF ჩარჩოებში.

მიქსერები

ეს არის ცენტრალიზებული ან დეცენტრალიზებული სერვისები, რომლებიც ახორციელებენ სხვადასხვა წყაროდან მიღებული კრიპტოვალუტის ფონდების შერევას მათი წარმომავლობის დამალვის მიზნით. მომხმარებლები თავიანთ კრიპტოვალუტებს (მაგ., ბიტკოინს) მიქსერში აგზავნიან, რომელიც ამ მონეტებს სხვა მომხმარებლების ან საკუთარ მონეტებთან ურევს. „შერევის პროცესის“ დასრულების შემდეგ, სერვისი მომხმარებლის მისამართზე აგზავნის მონეტების ეკვივალენტურ რაოდენობას საკომისიოს გამოკლებით, რაც ართულებს მონეტების წარმოშობის დადგენას. თუმცა, ცენტრალიზებულ მიქსერებს მართავს ერთი სუბიექტი, რომელსაც პოტენციურად ტრანზაქციის რეგისტრაცია შეუძლია. ევროპოლის EC3 გუნდი გთავაზობთ განცალკევების (განშრევების) კურსებს, რომლებიც ხელმისაწვდომია მხოლოდ ნებადართული სამართალდამცავებისთვის.

მიქსერის მსგავსი მომსახურებანი ტრადიციულ საბანკო საქმეში

მიქსერები ჩვეულებრივი ბანკების მსგავსად ფუნქციონირებს, სადაც თანხები დეპოზიტზე შეაქვთ და გამოაქვთ. განვიხილოთ დიდი ფინანსური ინსტიტუტი, სადაც ცალკეულ პირებს შეაქვთ ფული. თუ ეს ინსტიტუტი გააერთიანებდა ყველა ამ დეპოზიტს და შემდეგ გაანაწილებდა მათ ანგარიშის მფლობელებზე თითოეული დოლარის წარმოშობის დაზუსტების გარეშე, ეს დაემსგავსებოდა შერევის პროცესს. ფონდებს ცნობილი სუბიექტი ზედამხედველობს, როგორიცაა ცენტრალიზებული მიქსერი და მასში შეღწევის შემდეგ ეს თანხები სხვებს შეერევა. ბლოკჩეინ ანალიტიკის წამყვანი პროვაიდერები აცხადებენ, რომ წამყვანი მიქსერების უმეტესობას „დემიქსის“ ავტომატურ, ან მექანიკურ სერვისებს სთავაზობენ. ეს ამ პროვაიდერებს ასეთ ტრანზაქციების გადახედვის საშუალებას აძლევს.[8]

ტამბლერები

ტამბლერები მიქსერების მსგავსია და ბევრ კონტექსტში, ეს ტერმინები ურთიერთშენაცვლებით გამოიყენება. ტამბლერის მთავარი მიზანი ასევე ტრანზაქციის ანონიმურობის გაუმჯობესებაა. ტამბლერებს ზოგიერთი მიქსერის უფრო დახვეწილ ვერსიად განიხილავს. ისინი მოწინავე ალგორითმებს შერეული მონეტების თავდაპირველ წყაროებთან დაკავშირების შეზღუდვის უზრუნველსაყოფად იყენებენ.

ტამბლერის მსგავსი მომსახურებანი ტრადიციულ საბანკო საქმეში

ტამბლერები შეიძლება შევადაროთ ბანკის ანგარიშებს იმ ქვეყნებში, რომლებიც საგადასახადო თავშესაფრებად ითვლებიან, ან ოფშორულ ბანკებს, განსაკუთრებული კონფიდენციალურობისა და პირადულობის დაცვის პოლიტიკით. ასეთი ბანკები, როგორც წესი, იყენებენ რთულ სტრუქტურებსა და სერვისებს, რომლებიც მიზნობრივად შემუშავებულია კონფიდენციალურობისა და აქტივების დასაცავად. კრიპტოვალუტის სფეროში ტრანზაქციების ანონიმურობის შესანარჩუნებლად ტამბლერები უახლეს მათემატიკურ ალგორითმებს იყენებენ, რაც სტანდარტულ მიქსერებთან შედარებით დამალვის უფრო დახვეწილ დონეს უზრუნველყოფს. ტამბლერზე ტრანზაქციის თვალყურის დევნება რთული და შრომატევადია, მაგრამ შეუძლებელი არაა.

განსხვავებები და მსგავსებები

მიუხედავად იმისა, რომ მიქსერებიც და ტამბლერიც ერთსა და იმავე მიზანს - ტრანზაქციების კონფიდენციალურობის გაზრდას ემსახურება, მათ შორის არსებული ნიუანსები ხშირად მათი მეთოდებისა და სირთულის დონემდე დაიყვანება.

ეს ძირითად ვებ-ბრაუზერების იმ ბრაუზერებთან შედარებას ჰგავს, რომლებიც კონფიდენციალურობის გაუმჯობესებულ ფუნქციებს გვთავაზობენ. ორივე ინტერნეტის დათვალიერების საშუალებას გაძლევთ, მაგრამ ანონიმურობის შესანარჩუნებლად ერთი უფრო მოწინავე ინსტრუმენტებს გთავაზობთ.

VASP-ები და CASP-ები

ვირტუალური აქტივების მომსახურების მიმწოდებელი (VASP) შემდეგ აქტივობებს ასრულებს:

- ვირტუალურ აქტივებსა და ფიატურ ვალუტებს შორის გაცვლის ხელშეწყობა;
- ვირტუალური აქტივების ერთ ან რამდენიმე ფორმას შორის გაცვლის ხელშეწყობა;
- ვირტუალური აქტივების ერთი საფულედან მეორეზე გადაცემის ხელშეწყობა;
- ვირტუალური აქტივების გაყიდვასთან დაკავშირებული ფინანსური მომსახურებების უზრუნველყოფა.

VASP-ებთან დაკავშირებით არსებობს მთელი რიგი ტერმინები, რომლებიც ურთიერთშენაცვლებით გამოიყენება. „VASP“-ის შექმნის გადაწყვეტილება, ფულის გათეთრებასთან ბრძოლის ფინანსური ქმედების სპეციალურმა ჯგუფმა (FATF) მიიღო. თუმცა, ევროკავშირში ჩვეულებრივ VASP-ის ნაცვლად „CASP“ გამოიყენება, რომელიც კრიპტო აქტივების მომსახურების მიმწოდებელს ნიშნავს. CASP-ით განსაზღვრული მომსახურებების რაოდენობა უფრო ფართოა, ვიდრე VASP-ით. ზოგჯერ ასევე გამოიყენება ტერმინები - „ბირჟები“ და „ბროკერები“. მაგრამ ისინი VASP-ის ან CASP-ის მრავალი სახეობიდან მხოლოდ ერთს წარმოადგენს.

8 სარედაქციო პუბლიკაციის ვადის გასვლამდე, ავტორმა ამ პრეტენზიების დადასტურება ან უარყოფა ვერ შეძლო.

ციფრულ აქტივებთან დაკავშირებული დანაშაულის მართვის პროტოკოლი

ციფრულ აქტივებთან დაკავშირებული დანაშაულის გამოძიების პროტოკოლი

შესაგროვებელი ინფორმაციის ოთხი ყველაზე მნიშვნელოვანი კომპონენტი

როდესაც პოტენციური მსხვერპლი პოლიციის განყოფილებაში მიდის და აცხადებს, რომ კრიპტოვალუტით თაღლითობას ემსხვერპლა, ოთხი მნიშვნელოვანი ინფორმაცია უნდა შეგროვდეს.

კრიპტოვალუტის ტრანზაქციები შეუქცევადია – როგორც კი ისინი დასრულდება და ბლოკჩეინში მოხვდება, მსხვერპლს ამ თანხების დასაბრუნებლად მნიშვნელოვანი ძალისხმევა დასჭირდება. და მაინც, მიუხედავად იმისა, რომ ძალისხმევა მართლაც მნიშვნელოვანია, ეს შეუძლებელი არ არის.

დრო

პირველი ძირითადი ელემენტი დროა. კრიპტოვალუტით ტრანზაქციები ბლოკჩეინში ყოველთვის დაუყოვნებლივ არ აისახება. ხშირად, ბლოკჩეინში ჩაწერამდე, თანხები გარკვეული დროის განმავლობაში ბანკში, ან კრიპტოვალუტის ლიცენზირებულ ბროკერთან ინახება. იმის დადგენა, ეს ასეა თუ არა, პირველი და ყველაზე გადამწყვეტი საკითხია, რადგან ის ტრანზაქციის გაუქმების შანსს იძლევა.

ფინანსური ინსტიტუტი

შემდეგ ყველაზე მნიშვნელოვანია დაზარალებულს ჰკითხოთ თუ რომელი კრიპტოვალუტის ბროკერი ან ფინანსური ინსტიტუტი გამოიყენა ფიატური ვალუტის გადარიცხვისას. თუ გადარიცხვა განხორციელდა ბროკერთან, დაბალი რისკის იურისდიქციაში, სადაც ფინანსურ ინსტიტუტებზე ფულის გათეთრების საწინააღმდეგო წესები მოქმედებს, არსებობს იმის შესაძლებლობა, რომ ტრანზაქცია შეჩერდება.

ოდენობა

მესამე ყველაზე მნიშვნელოვანი საკითხი ტრანზაქციის ოდენობაა, რადგან მსხვილი თანხები, რომლებიც ფულის გათეთრების საწინააღმდეგო ბარიერს აჭარბებს, VASP-ის ან CASP-ის მხრიდან შემოწმებას ექვემდებარება. თუ მსხვერპლმა ლიცენზირებულ ბირჟაზე დიდი გადარიცხვა განახორციელა, შესაძლებელია ამ ბირჟასთან დაკავშირება და კრიპტოვალუტაზე გადარიცხვის შეჩერება.

კრიპტოვალუტის ტიპი

დაბოლოს, ბოლო საკვანძო საკითხია, თუ რა ტიპის კრიპტოვალუტა ან ვირტუალური აქტივია შეძენილი. ზოგიერთი ტიპის, მაგალითად ბიტკოინის ადვილად მიკვლევაა შესაძლებელი. კრიპტოვალუტის სხვა ტიპები, მაგალითად, ანონიმურ ვალუტებად ცნობილი მონერო და ზეროქეში, შექმნილია იმისთვის, რომ მიკვლევადობა და გამოძიება გაართულოს, მაგრამ გარკვეული ძალისხმევით, მათი მიკვლევაც კი შესაძლებელია.

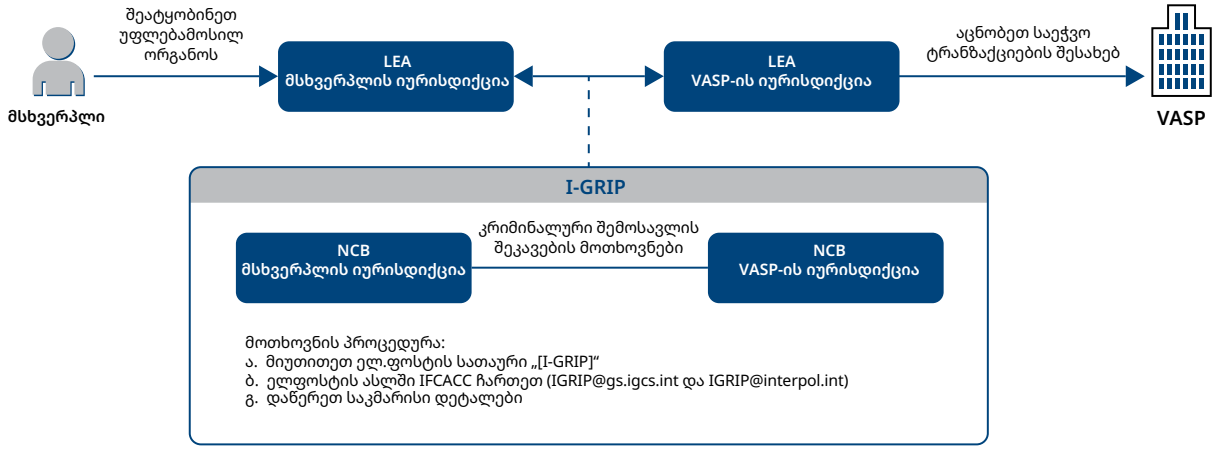
თუ მსხვერპლის საბანკო ანგარიშიდან ტრანზაქცია ძალიან ცოტა ხნის წინ შესრულდა, ბლოკჩეინში მისი შესვლის შეჩერებას ყველანაირი ძალისხმევა უნდა მოხმარდეს. განყოფილებაში საქმის მიღებამ და წინასწარი გამოძიებისთვის სხვა კოლეგებისთვის გადაცემამ, რომლებმაც ის შეიძლება მხოლოდ რამდენიმე დღის შემდეგ აიღონ, წარმატების შანსები შეიძლება მნიშვნელოვნად შეამციროს. სამი მაგალითი, რომელიც ამ კონცეფციისთვის ხშირი და საილუსტრაციოა:

მაგალითი 1: თუ პოტენციური მსხვერპლის შემთხვევაში, საერთაშორისო ბანკიდან ფიატური ვალუტის გადარიცხვა, მაგალითად, პარასკევს საღამოს შესრულდა და ამის შესახებ სამართალდამცავებს შაბათს დილით ეცნობა, მაშინ ბანკთან დაკავშირება და ტრანზაქციის შეწყვეტა მაინც შესაძლებელია. თუ დაზარალებული ბანკს ჯერ კიდევ არ დაუკავშირდა, მან ეს დაუყოვნებლივ უნდა გააკეთოს (იხ. ინტერპოლის IGrip გადაწყვეტა, გვ. 23)

მაგალითი 2: მაშინაც კი, თუ მსხვერპლმა თავისი საბანკო ანგარიშიდან კრიპტოვალუტის ბროკერს დიდი თანხა გადაურიცხა და ამ გადარიცხვამ მსხვერპლის ანგარიში უკვე დატოვა, კლიენტის საბანკო ანგარიშზე შეიძლება დარჩეს ინფორმაცია, რომელიც აჩვენებს VASP/CASP-ის სახელს, რომელზეც გადარიცხვა გაიგზავნა. ამ მაგალითში, თუ გადარიცხვა ერთ-ერთ დიდ ბროკერთან გაიგზავნა, როგორიცაა Binance, მომხმარებელი ჩატის ფანჯრის მეშვეობით, დაუყოვნებლივ მომხმარებელთა სერვისს უნდა დაუკავშირდეს, ან გაუგზავნოს ელ. წერილი სათაურით: **„სასწრაფოდ: შეაჩერეთ გაცვლა – თაღლითობა"** fraud@nameofthebroker.domain ან compliance@nameofthebroker.domain მისამართბზე, რათა აცნობოს მათ, რომ კონკრეტული IBAN-დან, გარკვეული ზომის და კონკრეტულ ვადაში შესრულებული გადარიცხვა არ უნდა დამუშავდეს.

სამართალდამცავებს ასევე შეუძლიათ თანხების შეჩერების მოთხოვნა, მაგალითად, Binance-ის სამთავრობო სამართალდამცავთა მოთხოვნის სისტემის მეშვეობით: https://www.binance.com/en/support/law-enforcement. უფრო მსხვილ ბროკერებს, ან ბირჟებს და სხვა VASP-ებს, როგორც წესი, აქვთ პროცედურა, რომელიც აღმასრულებელ ორგანოებს გადარიცხვის პოვნასა და შეჩერებაში დაეხმარება. ინდუსტრიის მოთამაშეთა უმრავლესობას აქვს ელ.ფოსტის მისამართები, როგორიცაა compliance@name-of-the-broker.com ან fraud@name-on-of-the-broker.com რომელიც შეიძლება გადაუდებელი შემთხვევების შესახებ შეტყობინებისთვის იყოს გამოყენებული.

იმავდროულად, დაზარალებულის იურისდიქციის LEA-ს (Law Enforcement Authority) შეუძლია, გადახდის შეწყვეტის მოთხოვნა ინტერპოლის მეშვეობით, კერძოდ გადახდის გლობალური სწრაფი ინტერვენციის (I-GRIP - Global Rapid Intervention of



წყარო: სქემა ინტერპოლის მიერ არის მოწოდებული

Payment) ინსტრუმენტის გამოყენებით განახორციელოს. ეს არის არხი იმ იურისდიქციის LEA-სკენ, სადაც VASP მდებარეობს. ინტერპოლმა გამოუშვა I-GRIP, რათა აქტივების აღდგენის საწყისი ეტაპების განსახორციელებლად საერთაშორისო თანამშრომლობა საკმარისად დაჩქარდეს.

მას შემდეგ, რაც იმ იურისდიქციის LEA, სადაც VASP მდებარეობს, I-GRIP მოთხოვნას მიიღებს, მათ შეუძლიათ მიიღონ აუცილებელი ზომები, რათა დანაშაულებრივი შემოსავლის შემდგომი დამუშავება მათი ეროვნული კანონმდებლობის შესაბამისად დააბრკოლონ. აუცილებელმა ზომებმა შეიძლება სხვადასხვა ფორმა მიიღოს. მათ შეუძლიათ აცნობონ VASP-ის მიმღებს საეჭვო ტრანზაქციის შესახებ, რათა VASP-მა საეჭვო ანგარიშის შეჩერება, ან ტრანზაქციის გაწვევის ნებაყოფლობითი გადაწყვეტილება მიიღოს.

ასევე, LEA-ებს შეუძლიათ თავიანთი ადმინისტრაციული უფლებამოსილება გამოიყენონ, რათა VASP-ს საეჭვო ანგარიშის შეჩერება დაავალონ. გარდა ამისა, LEA-ს შეუძლია, იმ გამოძიების პარალელურად, რომელსაც I-GRIP-ის მიერ მოთხოვნილი იურისდიქციები ახორციელებენ, საკუთარი შიდა სისხლის სამართლის გამოძიება დაიწყოს და საეჭვო ანგარიშის წინააღმდეგ სისხლის სამართლის ბრძანება გამოსცეს. თუ ეუთო-ს წევრი სახელმწიფოს სამართლებრივი ჩარჩო ამის საშუალებას იძლევა, პოტენციური მსხვერპლის მიერ საჩივრის წარდგენისთანავე საქმის დაუყოვნებლივ აღძვრა წარმატების კიდევ ერთი შესაძლებლობაა, რადგან კრიპტოვალუტასთან დაკავშირებული გამოძიების ერთ-ერთი ყველაზე მნიშვნელოვანი ასპექტი დროა.

მაგალითი 3: თუ პოტენციური მსხვერპლი სრულიად დარწმუნებული არაა თუ რომელ კრიპტოვალუტის ბროკერს გაეგზავნა თანხები, გადარიცხვის რეკვიზიტებზე შეიძლება ნახოთ ასოებისა და ციფრების შემოკლებები, რომლებიც გადარიცხვის მსგავსია: 1C5Eu4UpeK5djG3QiKwhcLELtFwHT146dG. ეს შეიძლება მიუთითებდეს იმაზე, რომ თანხები გადაიცვალა, ან გადაიცვლება კრიპტოვალუტის საფულეზე. ასეთი საფულეები შეიძლება საბანკო ანგარიშებს ან ელექტრონული ფოსტის საფოსტო ყუთს შევადაროთ, სადაც თანხები ინახება.

შესაძლებელია ასეთ საფულეში სახსრების აღდგენა ან გაყინვა მცირე ძალისხმევით. მიუხედავად იმისა, რომ ადამიანებისთვის, ვისთვისაც კრიპტოვალუტები უცხოა, ასოებისა და რიცხვების ასეთი კომბინაცია უჩვეულოდ გამოიყურება, ამ სფეროში გამოცდილების მქონე გამომძიებლებისთვის ასოებისა და რიცხვების ასეთი კომბინაცია, საკრედიტო ბარათის ნომრის მსგავს ინფორმაციას იძლევა. კრიპტოვალუტის საფულის მისამართის ფლობა, საკრედიტო ბარათის ნომრის ფლობას ჰგავს, მაგრამ პერსონალური დეტალების გარეშე, როგორიცაა სახელი, ან ემიტენტი ბანკი.

საკრედიტო ბარათის ნომერი ბარათის გამცემსა და ბარათის ტიპზე მიუთითებს. ანალოგიურად არსებობს საფულის მისამართის კონკრეტულ კრიპტოვალუტასთან, ან კონკრეტულ VASP-თან, ან ფინანსურ შუამავალთან დაკავშირების შესაძლებლობა გარე ინსტრუმენტების დახმარებით (რომელიც ყოველთვის არ არის წარმატებული) მას შემდეგ, რაც მსხვერპლმა სამართალდამცავებს კრიპტოვალუტის საფულის მისამართი შეატყობინა.

(დამატებითი ინფორმაციისთვის, იხილეთ სექცია „ვირტუალური აქტივების დანაშაულის გამოძიების დამატებითი ინსტრუმენტები“, გვ. 47.)

9 ინტერპოლი, ვირტუალური აქტივების ჩამორთმევის სახელმძღვანელო (2023 წლის ოქტომბერი), გვ. 40.

საუკეთესო პრაქტიკა თითოეული ტიპის ტრანზაქციისთვის

არსებობს სამი ტიპის ტრანზაქცია ბლოკჩეინზე, რომელთა შესახებაც გამომძიებლებმა უნდა იცოდნენ, რადგან მათ შეიძლება ვირტუალური აქტივების მომსახურების მიმწოდებლებთან თანამშრომლობა (VASP) დასჭირდეთ.

ტრანზაქციის ტიპი	აღწერა	გამოძიებაზე გავლენა
ფიატ ვალუტა კრიპტო-ვალუტაზე	მსხვერპლმა თანხების კრიპტოვალუტებზე გადამცვლელ VASP-ში გადახდა დაასრულა: საბანკო გადარიცხვით, ბარათით, მობილური ტელეფონით ან ეროვნულ ვალუტის ნაღდი ფულით.	**საუკეთესო პრაქტიკა 1** **თუ ეს შესაძლებელია, შეეცადეთ გადარიცხვა შეაჩეროთ, ან კრიპტოვალუტის ბროკერს დაუბრუნოთ.** ანგარიშგების ეტაპზე ყველაზე სერიოზული ხარვეზი საეჭვო დანაშაულის რეგისტრაციისა და წინასწარ გამოძიებაზე ოფისში პასუხისმგებელი პირის დროულად დანიშვნაა, რის შედეგადაც იგვიანებს მსხვერპლთან პირველი კონტაქტი. დროული რეაგირების შემთხვევაში კი ტრანზაქციის შეჩერება ჯერ კიდევ შესაძლებელია. თუ ტრანზაქცია ბანკის არასამუშაო საათებში, ან შაბათ-კვირას შესრულდა, შესაძლოა გამავალი საბანკო გადარიცხვის განხორციელების შეჩერება მოხერხდეს, რადგან ზოგიერთი ბანკი გადარიცხვებს მომდევნო სამუშაო დღეს ამუშავებს. თუ ტრანზაქცია საგადახდო ბარათის მეშვეობით შესრულდა, შესაძლოა ბარათის გამომშვებ ფინანსურ ინსტიტუტთან დაკავშირება მოხერხდეს, რათა შეჩერდეს ან გაუქმდეს გადახდის ოპერაცია და თანხა უკან დაბრუნდეს. მთავარი იმის გარკვევაა, თუ რომელმა ფინანსურმა ინსტიტუტმა განახორციელა საბანკო გადარიცხვა. ეს ბანკის ამონაწერზე გამოჩნდება. **საუკეთესო პრაქტიკა 2** **თუ ტრანზაქციის შეჩერება ვერ მოხერხდა, შეეცადეთ დაადგინოთ, თუ რომელ VASP-ზე გაიგზავნა გადარიცხვა, რათა მათ, თუ შესაძლებელია, ტრანზაქცია შეაჩერონ და თანხები გაყინონ.** თუ კრიპტოვალუტის ბროკერი დაბალი რისკის ქვეყანაში მუშაობს, სადაც კრიპტოვალუტის აქტივებისთვის AML/CTF რეგულაციებია შემოღებული, მაშინ ბროკერს დაუყოვნებლივ უნდა დაუკავშირდეთ და თანხების გაყინვა ან დაბრუნება მოსთხოვოთ, თუ ისინი უკვე გაცვლილი არ არის. ზოგჯერ ეს პროცესი შეიძლება თავად დაზარალებულებმა წამოიწყონ. ამის შემდეგ ბროკერებმა შეიძლება სახსრების გაცვლა შეაჩერონ, რადგან AML-ის კანონების შესაბამისად, თანხების გადარიცხვა მხოლოდ იმ შემთხვევაშია შესაძლებელი, თუ ცნობილია მათი წარმომავლობა და ასევე ნათელია სად იგზავნება. თუ VASP-ს აცნობებთ, რომ მიმღების კრიპტოვალუტის საფულე დაკავშირებულია თაღლითობასთან, ისინი იძულებულნი იქნებიან გაითვალისწინონ ფულის გათეთრების რეგულაციები და მიიღონ ზომები მის შესაჩერებლად.

ტრანზაქციის ტიპი	აღწერა	გამოძიებაზე გავლენა
		მიუხედავად იმისა, რომ ეს VASP-ის შიდა შესაბამისობის პოლიტიკაზეა დამოკიდებული, რამდენიმე სამუშაო დღით თანხების დროებითი გაყინვა სამართალდამცავებსა და პროკურორებს თანხების დაბრუნების ოფიციალური მოთხოვნით პროცესში ჩართვის საშუალებას მისცემს. ეს შესაძლებელია დროული მოქმედებისა და კრიპტოვალუტის ბროკერისგან სწრაფი უკუკავშირის მიღების შემთხვევაში. თუ ორივე პროცესი ჩაიშალა, მესამე შესაძლებლობაა დაუკავშირდეთ იდენტიფიცირებულ VASP-ს და მათი მონაცემთა ბაზებიდან მოითხოვოთ ინფორმაცია იმ მომხმარებლის ვინაობის შესახებ, რომელმაც ანგარიში შექმნა (რადგან სავარაუდოდ ეს არის თაღლითი ან ყალბი პიროვნება). ასევე შესაძლებელია მოითხოვოთ ყველა მტკიცებულება, მისი საიდენტიფიკაციო ინფორმაცია და ტრანზაქციის ჰეში.
კრიპტო-ვალუტა კრიპტოვა-ლუტაზე	დაზარალებული აცხადებს თაღლითობაზე, რომელიც საკუთრივ ბლოკჩეინ ტექნოლოგიის ფარგლებში ხორციელდება, ფიატური ვალუტების დამუშავების განმახორციელებელ ტრადიციულ ფინანსურ ინსტიტუტებთან რაიმე კავშირის გარეშე. მაგალითად, მოხდა თაღლითობა, რომლის დროსაც მომხმარებელი მოატყუეს და კრიპტოვალუტის სხვა პროდუქტი შეაძენინეს (მაგალითად NFT, Staking და ა.შ.), რასაც ფინანსური ზარალი მოჰყვა.	**საუკეთესო პრაქტიკა 1** **მოძებნეთ პოტენციური ლიცენზირებული ფინანსური შუამავლები, ეგრეთ წოდებული „ცენტრალიზებული ბირჟები“, რომლებიც ჩართულნი იყვნენ გაცვლაში. თუ მათი პოვნა მოხერხდება, მაშინ შესაძლებელი იქნება ამ შუამავლის მეშვეობით ჩართული მხარეების შესახებ პირადობის ინფორმაციის შეგროვება.** **საუკეთესო პრაქტიკა 2** **ხშირად, დაზარალებულები ექვემდებარებიან სოციალურ ინჟინერიას, რაც მნიშვნელოვანი რაოდენობით კიბერუსაფრთხოების კვალს ტოვებს. მაგალითად, ეჭვმიტანილები მსხვერპლს ხშირად სთხოვენ მათთან დისტანციური მართვის აპების, ელფოსტის, სატელეფონო ზარების, საწყისი საბანკო გადარიცხვების, sms-ის, ან საკომუნიკაციო შეტყობინებების მეშვეობით დაკავშირებას.** ამ სცენარში, მსხვერპლს ჩვეულებრივ, ბლოკჩეინზე დაფუძნებულ ფინანსებზე მუშაობის გამოცდილება აქვს. თავდაპირველი ამოცანა გადარიცხვის ყველაზე ზუსტი და განახლებული ინფორმაციის შეგროვებაა: ტრანზაქციის დრო, მსხვერპლის მიერ გამოყენებული ვალუტის ტიპები, ცნობები კრიპტოვალუტის საფულეებზე, ქვითრები, ელ.წერილები, sms შეტყობინებები და სხვა სახის ინფორმაცია. (მეტი დეტალები შეგიძლიათ იხილოთ შემდეგ ნაწილში „მტკიცებულებების შეგროვება“, გვ. 27).

ტრანზაქციის ტიპი	აღწერა	გამოძიებაზე გავლენა
კრიპტოვალუტა ფიატურ ვალუტაზე	მსხვერპლი სახსრების ქურდობის, ან დაკარგვის შესახებ იტყობინება	ამ სცენარში, მსხვერპლი უკვე ფლობდა კრიპტოვალუტებს, რომლებიც გაიგზავნა კრიპტოვალუტის ბირჟაზე და შემდეგ გადაიცვალა ეროვნულ ვალუტაზე, რომელიც სავარაუდოდ, გადახდილი იქნებოდა საბანკო გადარიცხვით, ან ნაღდი ფულით, ფიზიკურ ოფისში. ამ შემთხვევაშიც, ფიატური ვალუტიდან კრიპტოვალუტაში გადარიცხვების მსგავსად, საჭიროა ფინანსური შუამავლის მოძიება, რომელმაც განახორციელა ეროვნულ ვალუტაზე გაცვლა და საბანკო გადარიცხვის ინიცირება. თუ ლაპარაკია დიდ თანხებზე და ფინანსური ინსტიტუტი დაბალი რისკის იურისდიქციაში მდებარეობს, მაშინ ამ ინსტიტუტმა უნდა შეისწავლოს თანხების წარმომავლობა. ეს პროცედურა შესაბამისობის თანამშრომლების მიერ ხელით სრულდება და ტრანზაქციის შემდეგ შეიძლება 24 საათიდან რამდენიმე სამუშაო დღემდე დასჭირდეს. თუ შესაძლებელია, შეიყვანეთ კრიპტოვალუტის საფულის მისამართი ბლოკჩეინ-ექსპლორერში (blockchain-wallet-explorer-ში) მის შესამოწმებლად და გაარკვიეთ, დაკავშირებულია თუ არა ის რომელიმე ფინანსურ შუამავალთან, რომლის მოძიებაც შესაძლებელია (დამატებითი ინფორმაციისთვის იხილეთ სექცია "ვირტუალური დანაშაულის გამომძიებლების დამატებითი ინსტრუმენტები", გვ. 40). თუ ასეთი ძიება უშედეგოა, მიზანშეწონილია სპეციალური პროგრამული უზრუნველყოფის (ბლოკჩეინ ანალიტიკის სერვისის) გამოყენება, რომელიც შესაძლოა მიანიშნებდეს მისამართის კავშირს ცნობილ ფინანსურ ინსტიტუტთან.

მტკიცებულებათა შეგროვება

მტკიცებულებათა შეგროვება

ინფორმაციის მოპოვება კერძო პირისგან

გამოძიებისათვის მნიშვნელოვანი 10 კომპონენტი

- **აქტივის ტიპი:** რომელი კრიპტოვალუტის პროექტი ან NFT იყო ჩართული, მისი სახელის, სიმბოლოს და ძირითადი ტექნოლოგიის სპეციფიკის ჩათვლით.
- **ტრანზაქციის დეტალები:** ინფორმაცია მსხვერპლის მიერ განხორციელებული ტრანზაქციების შესახებ: თარიღი, დრო, თანხის ოდენობა, ვალუტა და ტრანზაქციის ID (მაგალითად, ქვითრები VASP-იდან).
- **საფულის მისამართები:** მსხვერპლისა და სავარაუდო თაღლითის კრიპტოვალუტის საფულეების დეტალები.
- **კომუნიკაციის ჩანაწერები:** ნებისმიერი სახის მიმოწერა, რაც მსხვერპლს ჰქონდა სავარაუდო თაღლითებთან — იქნება ეს ელფოსტა, სოციალური ქსელები, ჩეთის აპლიკაციები, სატელეფონო ზარები თუ ფორუმები.
- **სარეკლამო მასალა**: ვირტუალურ აქტივებთან დაკავშირებული ნებისმიერი სარეკლამო განცხადება, ონლაინ პოსტი ან სხვა სახის რეკლამა, რომელიც მსხვერპლებმა მიიღეს. ელ-ფოსტის წერილების ასლების შენახვისას დარწმუნდით, რომ ბმულები ნარჩუნდება, სასურველია ასლების USB მოწყობილობაზე გადატანა. გაფრთხილება! ასეთი ელექტრონული მასალის შენახვისას არ დააჭიროთ ბმულებზე, რადგან ისინი შესაძლოა ინფიცირებულები იყვნენ.
- **პლატფორმის შესახებ:** ნებისმიერი დეტალი იმ VASP პლატფორმის ან ბირჟის შესახებ (იხილეთ სექცია „VASP-ები და CASP-ები“, გვ. 20), სადაც მსხვერპლმა შეიძინა კრიპტოვალუტის აქტივი. ინფორმაციის მიღების შესახებ მოთხოვნის წესი იხილეთ სექციაში „მონაცემების მოთხოვნა VASP-ისგან“, გვ. 29-ზე.

ბირჟების დასახელებები, როგორც წესი, ტრანზაქციის ქვითრებზეა მოთითებული.

- **რეფერალური ინფორმაცია:** ინფორმაცია თუ როგორ გაიგო მსხვერპლმა აქტივის შესახებ: რეკომენდაციით, ონლაინ რეკლამის საშუალებით, მონაყოლით და სხვ.
- **კოდირების ანომალიები:** ნებისმიერი მტკიცებულება კოდის მანიპულაციის შესახებ, რომელიც უშლის ხელს კრიპტოვალუტის გაყიდვას, ასევე მტკიცებულებები კოდის სხვა ტიპის ანომალიების შესახებ. დამატებით, იურისდიქციის გათვალისწინებით, სამართალდამცავებს პროგრამული უზრუნველყოფის გარკვევაში დაეხმარება დაზარალებულის მიერ საკუთარი ფინანსური მონაცემების გაზიარების დროს სისტემაში შესასვლელად გამოყენებული ნებისმიერი მონაცემი და დანაშაულის ხელშემწყობი ნებისმიერი ვებ-გვერდების ბმულები.
- **ფინანსური ჩანაწერები:** საბანკო ამონაწერები, საკრედიტო ბარათის ამონაწერები, ან სხვა ფინანსური ჩანაწერები, რომლებიც ინვესტიციასთან დაკავშირებული სახსრების გადარიცხვას მოწმობენ.
- **პირადობის დამადასტურებელი ინფორმაცია:** ნებისმიერი დეტალი, რომელიც თაღლითის იდენტიფიცირებაში დაგეხმარებათ, მაგალითად მომხმარებლის სახელები, სოციალური მედიის პროფილები, ელფოსტის მისამართები, ან სხვა საკონტაქტო ინფორმაცია, რომელიც მსხვერპლის კომპიუტერზე, მსხვერპლთან ურთიერთობის დროს იყო გამოყენებული.
- **ტექნოლოგიური ანომალიები:** თაღლითობის პროცესში მსხვერპლმა რაიმე პროგრამული აპლიკაცია დააინსტალირა? ეს პროგრამა წაშლილია, თუ ჯერაც კომპიუტერზეა? პროგრამული უზრუნველყოფის წყაროს, ან წარმოშობის დადგენა შესაძლებელია?

თუ კრიპტოვალუტით განხორციელებული ტრანზაქცია არ შეჩერდა, კრიტიკულად მნიშვნელოვანია იმ საფულის მისამართის მოპოვება, რომელზეც თანხა გაიგზავნა, ან საიდანაც იგი იქნა მიღებული.

კრიპტოვალუტის საფულეების მისამართების შეგროვება

რა არის ბლოკჩეინზე გამოძიებისთვის საჭირო ყველაზე მნიშვნელოვანი მონაცემები?

ტრანზაქციის დეტალები: კრიპტოვალუტის საფულის მისამართი და ჰეშის ნომრები

ვინაიდან კრიპტოვალუტის საფულის მისამართები ასოებისა და რიცხვების გრძელი ჯაჭვისგან შედგება, მათი არასწორი ჩაწერა ერთ-ერთი ყველაზე გავრცელებული შეცდომაა.

მაგალითი 4: კრიპტოვალუტის საფულის მისამართის ჩაწერისას რიცხვი ნული „0“ ადვილად შეიძლება აირიოს ასო O-სთან, ან ასოები q და g. საუკეთესო პრაქტიკაა ჩაწერილი კრიპტოვალუტის საფულის მისამართის შეყვანა ინტერნეტ საძიებო სისტემაში, როგორიცაა google ან bing, რათა ნახოთ მისი იდენტიფიცირება შესაძლებელი თუ არა.

თუ მისამართი დაუყოვნებლივ არ გამოჩნდება, შეგიძლიათ საფულის ძებნის ინსტრუმენტი გამოიყენოთ. (იხილეთ ნაწილი „დამატებითი ინსტრუმენტები ვირტუალური აქტივების დანაშაულის გამომძიებლებისთვის“, გვ. 47).

თუ კრიპტოვალუტის საფულის მისამართი სწორია, ინფორმაცია მყისიერად გამოჩნდება, რომელიც შემდეგი ინფორმაციის ამოღების საშუალებას მოგცემთ:

ბიტკოინის შემთხვევაში ყოველთვის:

- **ტრანზაქციის ოდენობა:** თქვენ შეგიძლიათ ბიტკოინის ის ოდენობა ნახოთ, რომელიც თითოეულ ტრანზაქციაში გაიგზავნა, ან მიიღეს.
- **ტრანზაქციის დრო:** ჩანს დროის ნიშნული, რომელიც მიუთითებს, თუ როდის ჩაირთო ტრანზაქცია ბლოკში.
- **კრიპტოვალუტის საფულის მიმდინარე ბალანსი:** შესაძლებელია რეალურ დროში ნახოთ, თუ რამდენი ბიტკოინია საფულეში მიმდინარე ეტაპზე.
- **ტრანზაქციის ჰეში:** ეს ყოველი ტრანზაქციის უნიკალური იდენტიფიკატორია, როგორც ტრანზაქციის ID, რომელსაც გადახდის მომსახურების პროვაიდერები, „თითის ანაბეჭდივით“ იყენებენ.

ხელმისაწვდომია ზოგიერთ სერვისზე, თუმცა არა ყველა შემთხვევაში.

- **ტრანზაქციის მოცულობა:** ზოგიერთი სერვისი წამყვან ფიატურ ვალუტებში (აშშ დოლარი ან ევრო) დეტალურ ინფორმაციას იძლევა ხშირად გადარიცხვადი ტრანზაქციების მოცულობის შესახებ.
- **დროის სარტყლის მორგება:** ზოგი პლატფორმა, ნაგულისხმევი UTC დროის სარტყლის შეცვლის შესაძლებლობას გვთავაზობს. მაგალითად, მომხმარებლებს შეუძლიათ, ის ადგილობრივ დროის სარტყელის შესაბამისად მომართონ, რაც მტკიცებულებების შეგროვებას შეუწყობს ხელს.

შესაძლებელია თუ არა ერთი კრიპტოვალუტის საფულის მისამართზე სხვადასხვა ტიპის კრიპტოვალუტის შენახვა?

მრავალხელმოწერიანი (MultiSig) საფულის აპლიკაციის გამოყენება მომხმარებელს ერთი და იმავე ავტორიზაციის მონაცემებით სხვადასხვა ვირტუალურ აქტივზე წვდომის საშუალებას აძლევს. MultiSig-ის ტექნოლოგია ასევე საშუალებას აძლევს მომხმარებელს განსხვავებული ვირტუალური აქტივები იმავე ავტორიზაციის დეტალების გამოყენებით ერთი აპლიკაციით მართოს. ასე მარტივდება სხვადასხვა კრიპტოვალუტის ადმინისტრირების პროცესი.

ისევე, როგორც ბანკები აწესებენ უნიკალურ ანგარიშის ნომრებს სხვადასხვა ვალუტისთვის - ერთი აშშ დოლარისთვის, მეორე ევროსთვის, სხვადასხვა ბლოკჩეინ ტექნოლოგიებზე დაფუძნებულ კრიპტოვალუტებსაც, როგორიცაა Bitcoin და Tron, ესაჭიროება უნიკალური საფულის მისამართები.

MultiSig საფულეები მრავალ პირს არ საჭიროებს; ამის ნაცვლად, ტრანზაქციის ავტორიზაციისთვის, ისინი იყენებენ რამდენიმე პირად გასაღებს.

ერთ ადამიანს შეიძლება ჰქონდეს რამდენიმე პირადი გასაღები, ან შეიძლება აქტივების მართვაში რამდენიმე პიროვნება იყოს ჩართული, რომლებსაც თავისი პირადი გასაღები აქვთ.

ამ კონცეფციის ვიზუალიზაცია შეიძლება სმარტფონების ტიპებსა და მათ მიერ მხარდაჭერილ საოპერაციო სისტემებსა, თუ აპლიკაციებს შორის განსხვავებას შევადაროთ. ზოგი აპი ექსკლუზიურად, Apple-ის iOS-ისთვის არის შექმნილი და iPhone-ს საჭიროებს, ზოგი კი Android-ზეა მორგებული და Apple-ის მოწყობილობებზე არ მუშაობს. თუმცა, Android-ის პლატფორმაზე შეიძლება სხვადასხვა პროგრამისტის მიერ შემუშავებულმა სხვადასხვა აპმა იმუშაოს, რომლებსაც Google Play Store-ში ნახავთ. ანალოგიურად, კრიპტოვალუტები, რომლებიც საერთო ტექნოლოგიით არის გაერთიანებული, მაგალითად ERC20 ტოკენები, რომლებიც ეთერიუმის ბლოკჩეინის საფუძველზეა შექმნილი, შეიძლება ეთერიუმზე დაფუძნებული საფულის ერთი მისამართის მეშვეობით იმართებოდეს.

ეს იმას ჰგავს, თუ როგორ უზრუნველყოფს აპლიკაციების ერთი მაღაზია, ერთსა და იმავე პლატფორმაზე შემუშავებული მრავალი აპლიკაციის ჩამოტვირთვას. ამის მსგავსად, ერთ ბლოკჩეინზე, მაგალითად ეთერიუმზე შემუშავებული კრიპტოვალუტები, შეიძლება ეთერიუმზე დაფუძნებული საფულის ერთი მისამართის ფარგლებში იყოს კონსოლიდირებული, რაც მათ მოხმარებას ამარტივებს.

VASP-ებიდან მონაცემების მოთხოვნა:

თუ მსხვერპლმა არ იცის, ვირტუალური აქტივების მომსახურების იმ პროვაიდერის (VASP) დასახელება, რომელსაც ფული გაეგზავნა, მას შეიძლება ჰქონდეს ქვითარი, რომელშიც საფულეების მისამართებია ნაჩვენები. ეს მონაცემები ხშირად ხილულია ბლოკჩეინ ანალიტიკის პროვაიდერის პროგრამული უზრუნველყოფის მეშვეობით. ასეთი პროვაიდერები რეგისტრირებულნი არიან ქვეყნებში, სადაც კანონებით ზუსტადაა განსაზღვრული, რომ ვირტუალური აქტივები ფულის გათეთრების საწინააღმდეგო მოთხოვნებს უნდა შეესაბამებოდეს. ამ წესების შესაბამისად VASP-ებმა მათი მომხმარებლების ვინაობა უნდა გადაამოწმონ და ჩაწერონ ტრანზაქციები. მაგალითად ევროკავშირში, ევროკავშირის მეხუთე AML დირექტივის შესაბამისად, VASP-ები ევროკავშირის წევრ სახელმწიფოებში უნდა დარეგისტრირდნენ და უნდა შეასრულონ ფულის გათეთრების საწინააღმდეგო სხვადასხვა ვალდებულება.

თუ მსხვერპლმა იცის, თანხები რომელ VASP-ზე გაიგზავნა, ან რომლიდან მოვიდა და ავტორიზაციის მონაცემები ჯერ კიდევ აქვს (ან შეუძლია აღადგინოს), მაშინ პირველი ნაბიჯი ბირჟიდან გადარიცხვის ყველა ინფორმაციის ამოღება უნდა იყოს. გადარიცხვის ეს ინფორმაცია მოიცავს განხორციელებულ ტრანზაქციებს, გაგზავნილ კრიპტოვალუტებს და მათი კრიპტოვალუტების საფულეების მისამართებს.

თუ მსხვერპლი დარწმუნებული არ არის, თუ თანხები სად გადაირიცხა, ან საიდან გამოიგზავნა, VASP-ის დასახელება ზოგჯერ შეიძლება მსხვერპლის საბანკო ამონაწერში, ან ბარათის ამონაწერში მოიძებნოს.

ვირტუალური აქტივების ან ბირჟების ზოგიერთი დასახელება მოიცავს PanCake Swap-ს (https://pancakeswap.finance/); Wasabi Wallet-ს (https://wasabiwallet.io); Doge Coin-ს (https://dogecoin.com/); და Shit Coin-ს (https://www.investopedia.com/terms/s/shitcoin.asp). მათთვის, ვინც კრიპტოვალუტის სამყაროში აქტიურად არ არის ჩართული, ეს დასახელებები შეიძლება თავიდანვე გასაგები არ იყოს, თუმცა ისინი ხშირად გამოიყენება. ისეთი პლატფორმებიც კი, რომლებიც სრულ დეცენტრალიზაციას

დეკლარირებენ (მაგ.Uniswap), მომხმარებლებს ტრანზაქციების ისტორიას .csv ფორმატში სთავაზობენ, რაც გამოძიებას უწყობს ხელს.

მსოფლიოში ასობით ბირჟაა. თუმცა, ფართო საზოგადოებისთვის, ან სამართალდამცავებისთვის მხოლოდ რამდენიმე დასახელებაა მეტ-ნაკლებად ცნობილი.

იმ შემთხვევაში, როცა მომხმარებლისთვის VASP-ში საკუთარი ანგარიში მიუწვდომელია, დახმარებისათვის შეუძლია ცენტრალიზებულ VASP-ს, ან კრიპტოვალუტის საფულის სამეურვეო (კასტოდიანურ) მომსახურების პროვაიდერს დაუკავშირდეს.

როგორც წესი, საუკეთესო პრაქტიკის შესაბამისად, VASP-ები არავითარ ინფორმაციას ტელეფონით არ გასცემენ. ამიტომ, საჭიროა სამართალდამცავი ორგანოების მოთხოვნის (LER) გაგზავნა VASP-ში ან სხვა ფინანსურ ინსტიტუტებში, რომლებმაც მსხვერპლის თანხების გადაცვლა აწარმოეს. VASP-ისთვის LER-ის შევსების პროცესი აღწერილია 22-ე გვერდზე.

სავარაუდოდ, ცენტრალიზებული VASP-ისგან შემდეგ ინფორმაციას მიიღებთ:

- სახელი
- გვარი
- დაბადების თარიღი
- პირადობის მოწმობის ქსეროასლები[10]
- დასრულებული ტრანზაქციების მოცულობა
- ტრანზაქციების დროის ნიშნული/შტამპი[11]
- ტრანზაქციის ფიატ და კრიპტოვალუტა[12]
- აგენტის საკომისიო
- სანქციების სკრინინგისა და პოლიტიკურად აქტიური პირების სკრინინგის დადასტურების დრო და გამოყენებული სიების ტიპები
- კრიპტოვალუტის საფულის მისამართი ან მისამართები, რამდენიმე ტრანზაქციის და ვალუტის შემთხვევაში
- ტრანზაქციის ჰეშები ჩატარებული ტრანზაქციებისთვის

ნაკლებად სავარაუდოა, მაგრამ შემდეგი ინფორმაციის მიღება მაინც შესაძლებელია:

- მომხმარებლის ნომერი ან ID, რომელიც აგენტთან ინახება.
- მომხმარებლის დეკლარირებული საცხოვრებელი მისამართი.[13]
- მომხმარებლის რეგისტრირებული მისამართი.[14]
- სოციალური დაზღვევის ნომერი, იმის მიხედვით, თუ პლატფორმა რომელ ქვეყანაშია რეგისტრირებული.
- აგენტს (VASP/CASP) და მომხმარებელს შორის ურთიერთქმედების ჩანაწერები (ხშირად PDF-ის სახით, რადგან მომხმარებლის მომსახურება ხშირად პროგრამული უზრუნველყოფის გარე მიმწოდებლებთან ტარდება, როგორიცაა Intercom ან ZenDesk).
- მომხმარებლის მიერ ატვირთული ფულადი სახსრების წარმომავლობის დამადასტურებელი ყველა დოკუმენტი.
- მომხმარებლის IP მისამართი (რასაც შეცდომაში შეყვანა შეუძლია, რადგან ჩვეულებრივ, მომხმარებლები VPN-ებს იყენებენ).
- მოწყობილობა, რომელიც სისტემაში შესვლისთვის გამოიყენება (მაგალითად, მობილური ტელეფონი, ან კომპიუტერი).
- ბრაუზერი და სერვისზე წვდომისთვის გამოყენებული ვერსია: Opera, Chrome, Safari, Internet Explorer ან მსგავსი.
- მომხმარებლის ბიოგრაფიის შემოწმება, რომელიც ღია წყაროების მოკვლევით (OSINT)[15] დგინდება.
- VASP-ის თანამშრომლების კომენტარები კონკრეტულ მომხმარებელთან, ან მის ტრანზაქციებთან დაკავშირებით.
- ბლოკჩეინის ნებისმიერი ანალიტიკური გამოკვლევა, რომლებსაც VASP-ის თანამშრომლები მომხმარებელზე ან მის ტრანზაქციებზე ატარებენ.
- ნებისმიერი შეკითხვა სხვა სამართალდამცავი ორგანოებიდან ან ფინანსური ინსტიტუტებიდან, კონკრეტული მომხმარებლის შესახებ.
- ნებისმიერი ტრანზაქცია, რომელიც მომხმარებლის მიერ არის დაწყებული, მაგრამ არ დასრულებულა.
- შესაძლოა იმ პირების ვიდეოჩანაწერი, რომლებიც ოფისებში იღებენ მომსახურებას ან თვითმომსახურების აპარატებით სარგებლობენ.
- მომხმარებელთა მიერ ატვირთული ყველა დოკუმენტის (მათ შორის, დაფინანსების წყაროს და დაგროვილი ქონების წარმომავლობის) დამადასტურებელი მტკიცებულება, ასევე მომხმარებელთა დახმარებასთან დაკავშირებული ყველა ურთიერთქმედება.

პოლიციის ოფიცრებს შეუძლიათ მსხვერპლისგან მისი საბანკო ანგარიშის დეტალების შესახებ მეტი ინფორმაცია შეაგროვონ, რაც VASP-ისგან შეგროვებული ინფორმაციის გაფილტვრას უწყობს ხელს. ეს ინფორმაცია ხელმისაწვდომი მხოლოდ ფიატის კრიპტოვალუტაზე ურთიერთგადაცვლის ტრანზაქციებისთვის იქნება.

- დაზარალებულის საბანკო ანგარიშის ნომერი, რომელიც VASP ანგარიშზე და ანგარიშიდან გადარიცხვისთვის გამოიყენებოდა.
- ტელეფონის ნომერი: ზოგიერთი

---

10 ეს შეიძლება მოიცავდეს პასპორტს, პირადობის მოწმობას ან ელექტრონულ იდენტიფიკაციას. თუმცა პროცესი ხშირად ტრადიციული კიბერდანაშაულის მსგავსად (მაგ, ყალბი ან "საკოლექციო" დოკუმენტების გამოყენება) რეალური იდენტობის იმიტაციას ახდენს (dokumencik.pl).

11 მნიშვნელოვანია განისაზღვროს, დროის ნიშნული რომელ საათობრივ სარტყელშია. მაგალითად, ბიტკოინის ბლოკჩეინის ყველა ტრანზაქცია UTC-ით (ლონდონის დროით) რეგისტრირდება, იმის მიუხედავად, საიდანაა მომხმარებელი. ტრანზაქციის არასწორი დროითი ნიშნულების სხვა მტკიცებულებებთან დაკავშირების პრობლემა ზოგჯერ კრიტიკულია.

12 როგორც ვირტუალური აქტივები, ასევე ფიატური ვალუტა.

13 თუ იურისდიქციით დაშვებულია, შესაძლებელია შემოწმდეს, პლატფორმას ჰყავს თუ არა იმავე მისამართზე რეგისტრირებული სხვა მომხმარებლები, რომლებმაც ტრანზაქციები განახორციელეს.

14 იღებს თუ არა პლატფორმა ასეთ ინფორმაციას საჯარო მონაცემთა ბაზიდან.

15 Open Source Intelligence (OSINT) ეს შეიძლება მოიცავდეს ამონაწერებს მონაცემთა საჯაროდ ხელმისაწვდომი წყაროებიდან, როგორიცაა ნასამართლეობის ცნობა, ან ინფორმაცია კონკრეტული საწარმოების UBO-ს შესახებ, რომელიც შესაძლოა მოპოვებული ყოფილიყო პლატფორმის შესაბამისი თანამშრომლების მიერ.

მომხმარებელი თავისი მობილური ოპერატორის გადახდის სისტემას იყენებს.

- ბარათის ინფორმაცია საკრედიტო, სადებეტო ან წინასწარ გადახდის ბარათიდან, რომელიც ტრანზაქციისთვის იყო გამოყენებული. პროვაიდერის ანგარიშზე წვდომისთვის შეიძლება გამოიყენებოდეს დადასტურების მეორე დონე მობაილ ბანკის აპლიკაციის, ან SMS მომსახურება 3D secure-ს საშუალებით, რომლის ამოღებაც შესაძლებელია.

- ქვეყნებში, სადაც „ღია ბანკინგი“ გამოიყენება, დამატებითი ინფორმაციის მიღება შეიძლება გადახდის მომსახურების პროვაიდერისგან, რომლებიც ამ ტრანზაქციებს (თუ ეს ტრანზაქციები ღია ბანკინგის გამოყენებით შესრულდა) ახორციელებენ.

ინფორმაცია VASP მონაცემების ფორმატზე

ოპტიმალური ეფექტურობისათვის ტრანზაქციების მონაცემთა მიღება „.csv“ ფორმატშია სასურველი. ეს ხელს უწყობს სამართალდამცავ სისტემებში მარტივ ინტეგრაციას. როგორც წესი, სამართალდამცავი ორგანოების მოთხოვნას (LER) პასუხი ორი ფორმატით მიეწოდება:

- „.pdf“, სადაც ვირტუალური აქტივების პროვაიდერი სამართალდამცავი სააგენტოს (LEA) მიერ დასმულ შეკითხვებზე პირდაპირ პასუხებს იძლევა.

- .csv“ ფაილი, რომელიც ტრანზაქციის მონაცემებს შეიცავს.

ხშირად, VASP-ები კონსოლიდირებული მომხმარებლის მონაცემების შემცველ საქაღალდეს ინახავენ. ეს საქაღალდე მნიშვნელოვან დოკუმენტებს შეიცავს, როგორიცაა ფულადი სახსრების დამადასტურებელი საბუთი (proof of funds - POF) და სხვა ატვირთული ფაილები.

მსხვილ VASP-ებს ჩვეულებრივ, სამართალდამცავი ორგანოების მოთხოვნებზე რეაგირების დადგენილი წესი აქვთ. მცირე დაწესებულებებთან ურთიერთობისას სამართალდამცავ ორგანოებს საჭირო ინფორმაციის მისაღებად, სასურველი ინფორმაციის ფორმატის დაზუსტება შეუძლიათ. თუმცა, მომხმარებლის ვინაობის აღრიცხვა ზოგჯერ სხვადასხვა ფორმატშია შესაძლებელი. მაგალითად, პირადობის დამადასტურებელი დოკუმენტის „.pdf“ ან „.jpeg“ ფორმატში ან ვიდეოში, რომელიც „.avi“ ან „.mov“ ფორმატებში არსებობს.

რეკომენდებულია თავი შეიკავოთ VASP-ებიდან „.xml“ ან „.xls“ ფაილების მოთხოვნაზე. კერძოდ, „.xlsx“ ფაილების გამოყენება კიბერუსაფრთხოების თვალსაზრისით არ არის მიზანშეწონილი. არსებობს რისკი, რომ VASP-ების მიერ „.xlsx“ ფორმატში მოწოდებული მონაცემები, განსაკუთრებით ფაილში „ჩაშენებული“ მაკროსები, ვირუსებს შეიცავს. ამან კი შეიძლება საფრთხე შეუქმნას სამართალდამცავი უწყებების (LEA) კომპიუტერული სისტემების უსაფრთხოებას.

მიღებული (obtained) IP მისამართების სანდოობა

VASP-დან ინტერნეტ პროტოკოლის (IP) მიღება ხშირად სამართალდამცავი ორგანოების მოთხოვნის საფუძველზე წარმოებს. IP მისამართი უნიკალური იდენტიფიკატორია, რომელიც ინტერნეტქსელთან დაკავშირებულ მოწყობილობას, მაგალითად, სმარტფონს ან ლეპტოპს, ენიჭება. ტელეფონის ნომრის მსგავსად IP მისამართიც ციფრების უნიკალური ნაკრებია. მაგალითად: IP მისამართი 193.46.242.201 შვედეთზე, სტოკჰოლმზე მიუთითებს. თუმცა, ისევე როგორც ერთი სახლის ტელეფონის ნომრით სარგებლობს რამდენიმე ოჯახის წევრი, ტექნოლოგია NAT-ის (ქსელური მისამართების გარდაქმნა) საშუალებით რამდენიმე მოწყობილობა ერთსა და იმავე IP მისამართს იყენებს.

VASP-ები ხშირად აცხადებენ, რომ შეუძლიათ მომხმარებლების ინტერნეტ ქსელში შესვლის პროცესში დაფიქსირებული IP მისამართების ექსპორტი. თუმცა, გამოძიებისათვის ამ ინფორმაციის სანდოობა საეჭვოა. IP მისამართები მხოლოდ ინტერნეტში შესულ მოწყობილობას და არა მოწყობილობის კონკრეტულ მომხმარებელს აჩვენებს. თაღლითების მიერ ვირტუალური კერძო ქსელების (VPN) გამოყენებით შესაძლებელია მისამართების შენიღბვაც. შესაბამისად, ზემოაღნიშნული ინფორმაცია გამოსადეგია მხოლოდ იმ შემთხვევებში, როცა არსებობს მომხმარებლის IP მისამართის პოტენციურ კრიმინალურ საქმიანობასთან კავშირის მტკიცებულება.

მომხმარებლისათვის სახლებში ინტერნეტის მიმწოდებელ კომპანიებს (ინტერნეტ სერვისის პროვაიდერებს „ISP“) შეუძლიათ გაარკვიონ თუ ვინ და კონკრეტულად რა დროს გამოიყენა IP მისამართი. გამოძიებისას ასეთ კომპანიებს შეიძლება მოსთხოვონ მომსახურების კონტრაქტზე ხელმომწერი კონკრეტული მომხმარებლისა და IP მისამართის კავშირის იდენტიფიცირება. თუმცა ეს ინფორმაცია ყოველთვის სანდო არ არის — მაშინაც კი, თუ მომხმარებელი VPN-ს არ იყენებს: Wi-Fi ქსელი შეიძლება პაროლის გარეშე იყოს ხელმისაწვდომი და შესაძლოა IP მისამართი სხვა პირმაც გამოიყენოს.

ინტერნეტ-სივრცეში კონკრეტული ქმედების შემსრულებელის იდენტიფიცირებას მხოლოდ IP მისამართის ცოდნა ვერ უზრუნველყოფს. ისეთ ადგილებში, როგორიცაა სკოლები, ოფისები, სამსახურები და სხვ. ერთსა და იმავე ინტერნეტ-კავშირს შეიძლება რამდენიმე პირი იყენებდეს. ეს გარემოება კიდევ უფრო ართულებს ონლაინ ქმედებების კონკრეტულ პირთან დაკავშირებას.

VPN-ები სპეციალურად შექმნილია იმისთვის, რომ დამალონ მომხმარებლის რეალური IP მისამართი და შექმნან შთაბეჭდილება, თითქოს ინტერნეტკავშირი სხვა ადგილმდებარეობას უკავშირდება. თუმცა, VPN-ის გამოყენების შემთხვევაშიც კი, გარკვეულ ვითარებაში შესაძლებელია მომხმარებლის ქცევა და კონკრეტულ ვებგვერდებზე ვიზიტები ასოცირდეს კონკრეტულ IP მისამართთან კონკრეტულ დროის მონაკვეთში. მიუხედავად იმისა, რომ VPN ზრდის ანონიმურობას, ის არ ხდის ონლაინ ქმედებებს სრულად დაფარულს. გამოცდილ უწყებებს გარკვეულ პირობებში შეუძლიათ ონლაინ აქტივობების კონკრეტულ მომხმარებლებთან დაკავშირება.

IP მისამართების შეგროვება

არგუმენტები:

- **მიკვლევადობისთვის:** IP მისამართები შეიძლება გამოყენებული იქნეს პოტენციური ეჭვმიტანილების მოსაძებნად, ან საეჭვო აქტივობების წარმომავლობის დასადგენად საწყის ეტაპზე. შესაძლებელია მათი სხვა გამოძიებებთან დაკავშირებაც.
- **შეკავება:** ცოდნა იმის შესახებ, რომ IP მისამართები კონტროლდება, შესაძლოა პოტენციური დამნაშავეებისთვის საკუთარი ქსელების უკანონო საქმიანობისთვის გამოყენებისგან შემაკავებელ ფაქტორად მოქმედებდეს.
- **ერთობლივი მტკიცებულება:** სხვა მტკიცებულებებთან ერთად, IP მისამართების დახმარებით, ეჭვმიტანილთა წინააღმდეგ უფრო დამაჯერებელი ბრალდების ფორმულირებაა შესაძლებელი.

რომან ბიედა ყაზახეთში გამომძიებლებისთვის პრაქტიკულ სემინარს ატარებს. როგორც ბლოკჩეინის ანალიზის ინსტრუმენტის პროდუქტის ყოფილი მფლობელი და ევროპისა და შეერთებული შტატების სასამართლოების მოწმე-ექსპერტი, არა მხოლოდ ცოდნის, არამედ მტკიცებულებების შეგროვების პროცესში არსებული გამოწვევების შესახებ, საუკეთესო პრაქტიკისა და შეხედულებების გაზიარებას ემსახურება. ეუთო-ს სემინარების მიზანია უზრუნველყოს, რომ ერთ წევრ სახელმწიფოში არსებული გამოწვევები სხვა სახელმწიფოებში აღარ განმეორდეს.

საწინააღმდეგო არგუმენტები:

- **უზუსტობა:** იმის გამო, რომ ერთ IP მისამართს ხშირად რამდენიმე მოწყობილობა იყენებს და შესაძლებელია VPN-ებისა თუ სხვა შემნიღბავი საშუალებების გამოყენება, მხოლოდ IP მისამართზე დაყრდნობა გამოძიებისას შესაძლოა არასწორი იდენტიფიკაციის მიზეზი გახდეს.
- **კონფიდენციალურობის საკითხები:** IP მისამართების მასობრივი შეგროვებით შესაძლოა დაირღვეს პირადი მონაცემების დაცვის უფლება, განსაკუთრებით მაშინ, თუ ეს ხდება სათანადო სამართლებრივი საფუძვლის გარეშე.
- **რესურსების საჭიროება:** VPN-ის ან სხვა შესანიღბი ინსტრუმენტების გამოყენების შემთხვევაში IP მისამართების მოკვლევა დიდ დროს მოითხოვს, რამაც შესაძლოა სხვა მნიშვნელოვანი გამოძიებისათვის საჭირო რესურსები თავისკენ მიიზიდოს.

დასასრულს, მიუხედავად იმისა, რომ IP მისამართებით შეიძლება კონკრეტულ დროში მოწყობილობის აქტივობისა და მისი მდებარეობის დადგენა, ისინი ინდივიდუალური მომხმარებლის იდენტიფიცირებას ერთმნიშვნელოვნად ვერ უზრუნველყოფს. IP მისამართებზე დაფუძნებული გამოძიებები შედეგიანია მხოლოდ განსაკუთრებული სიფრთხილით წარმოებისას, თუ იგი განიხილება როგორც მტკიცებულებების შეგროვების ფართო სტრატეგიის შემადგენელი ნაწილი.

სხვა მოსათხოვნი დოკუმენტები

ეუთო-ს წევრ ზოგიერთ სახელმწიფოში ვირტუალურ აქტივებთან (მაგ. კრიპტოვალუტები) მომუშავე კომპანიები „ფინანსურად ვალდებულ დაწესებულებებად“, ან შუამავლებად კვალიფიცირდება. აქედან გამომდინარე, რისკების პოტენციური წარმომავლობის დასადგენად ამ კომპანიებმა რეგულარულად უნდა აკონტროლონ და თვალი ადევნონ მომხმარებლების ქმედებებს - ბლოკჩეინის ინსტრუმენტების გამოყენებით განხორციელებულ საეჭვო ტრანზაქციებს. მსგავსი რევიზიის შედეგები დოკუმენტირდება და მოთხოვნის შემთხვევაში გადაეცემა სამართალდამცავებს.

მაგალითად, საქართველოში, საქართველოს ეროვნულ ბანკში რეგისტრირებულ კომპანიებს ბლოკჩეინ ტრანზაქციების გასაანალიზებლად სპეციალიზებული ინსტრუმენტების გამოყენების ვალდებულება გააჩნიათ. ეს ვირტუალური აქტივების ნაკადის მონიტორინგის გამჭვირვალობისა და უსაფრთხოების დონეს უზრუნველყოფს. თუ სამართალდამცავ ორგანოებს არ აქვთ წვდომა ასეთ ბლოკჩეინ ანალიტიკურ ინსტრუმენტებზე, შეუძლიათ მოითხოვონ VASP-ისგან გამოძიებისთვის დეტალების გაზიარება. ეს ინფორმაცია შეიძლება იყოს ხელმისაწვდომი და რედაქტირებადი ფორმატით, მაგ. PDF ან სურათის ფაილი.

ეს ნიშნავს, რომ მიუხედავად იმისა, რომ ინსტრუმენტები მნიშვნელოვან როლს ასრულებს ტრანზაქციების მთლიანობის შენარჩუნებასა და უკანონო საქმიანობის იდენტიფიცირებაში, არსებობს პროცედურული და სამართლებრივი საკითხები, რომლებიც უნდა იქნას დაცული ამ ინსტრუმენტებიდან მიღებული ინფორმაციის გაზიარებისას. მაგალითად, რამდენიმე ბლოკჩეინის ანალიზის და შესაბამისობის განმსაზღვრელ პროვაიდერს შეიძლება ჰქონდეს კონკრეტული პროტოკოლები და შეთანხმებები, რომლებიც წინასწარი ავტორიზაციის გარეშე მნიშვნელოვანი, ან რედაქტირებადი ინფორმაციის გაზიარებას სამართალდამცავ ორგანოებთანაც კი ზღუდავს. ამან შეიძლება პრობლემები შეუქმნას VASP-ებს, როცა მტკიცებულებების შეზღუდვის შეთანხმების ვალდებულების მიუხედავად თანახმანი არიან გაამჟღავნონ სანდო ინფორმაცია.

საქმეთა წარდგენა სასამართლოში

საქმეთა წარგენა სასამართლოში

ვირტუალური აქტივების საქმეთა პროკურორები

პროკურორთა საქმიანობის მტკიცე საფუძვლის უზრუნველსაყოფად სამართალდამცავი ორგანოების თანამშრომლები კარგად უნდა ერკვეოდნენ ფულის გათეთრების წინააღმდეგ ბრძოლასთან დაკავშირებული მტკიცებულებების შეგროვების საკითხებში. განსაკუთრებით საყურადღებოა ვირტუალური აქტივებისა და კრიპტოვალუტების დინამიურად მზარდი სფერო.

გამოძიების ეტაპი:

- **მოიძიეთ ციფრული მტკიცებულებები:** გაერკვიეთ და თვალი ადევნეთ ტრანზაქციებს ბლოკჩეინ ტექნოლოგიასა და განაწილებულ რეესტრებზე.
- **გააანალიზეთ ინფორმაცია:** ამოიცანით კანონზომიერებანი, რომლებიც შეიძლება ფულის გათეთრებაზე მიუთითებდეს. მაგალითად, სწრაფი და მასშტაბური ტრანზაქციები კრიპტოვალუტის ბირჟებზე.
- **მიჰყევით ციფრულ კვალს:** თვალყური ადევნეთ აქტივების ნაკადს სხვადასხვა ვირტუალურ საფულესა და პლატფორმაზე, საჭიროების შემთხვევაში სპეციალური პროგრამული უზრუნველყოფის გამოყენებით.
- **შეაფასეთ VASP-ებისგან მიღებული ყველა საიდენტიფიკაციო ინფორმაციის სანდოობა** (იხილეთ „პირადობის დამადასტურებელი დოკუმენტების ასლებთან“ დაკავშირებული პრობლემები, გვ. 30).

სასამართლო პროცესის, ან გამოძიების მომზადება

ა.საქმის მიმოხილვა:

- ყურადღება უნდა გამახვილდეს კრიპტო საფულეებზე, IP მისამართებზე, ტრანზაქციის დროით ნიშნულებსა და ტრანზაქციაში მონაწილე თანხის მოცულობაზე ციფრულ სივრცეში.
- პირველ რიგში უნდა გაიაზროთ თუ როგორ გარდაიქმნება ვირტუალური აქტივები მატერიალურ აქტივებად, როგორიცაა ქონება ან საქონელი, და მათ წარმოშობას მიადევნოთ თვალი.

ბ. დანაშაულის ტიპის განსაზღვრა:

- გამოავლინეთ ფულის გათეთრებისათვის კრიპტოვალუტის გამოყენების ნიშნები. მაგ. „შერევის“ ან „გადამუშავების“ სერვისები, რომლებიც თანხების წარმომავლობის დაფარვას ემსახურება. ბლოკჩეინ ანალიტიკის წამყვანი პროვაიდერები ხშირად სთავაზობენ ე.წ. „დემიქსინგ“ მომსახურებას და აცხადებენ, რომ შეუძლიათ „მიქსერის“ საშუალებით დამუშავებული ტრანზაქციების დაშლა. თუ საქმე განსაკუთრებული მნიშვნელობისაა, არსებობს დემიქსინგის სერვისები, რომლებსაც სთავაზობენ როგორც ბლოკჩეინ ანალიტიკის პროვაიდერები, ასევე სამართალდამცავი ორგანოების მაგ. ევროპოლის დემიქსინგის კურსები.
- დანაშაულის ელემენტების დასამტკიცებლად გამოიყენეთ ბლოკჩეინზე ტრანზაქციების ჩანაწერები.

გ. აქტივებთან კრიმინალური საქმიანობის დაკავშირება:

- თვალყური ადევნეთ ნებისმიერ მოძრაობას კრიპტოვალუტის საფულეებიდან მატერიალური, ან სხვა ვირტუალური აქტივების შეძენამდე. ეს შეიძლება მოიცავდეს კრიპტოვალუტის გადაადგილებას ბირჟიდან კერძო საფულეში და შემდეგ სხვა ობიექტზე, ან მომსახურებაზე.
- განსაზღვრეთ ანონიმიზაციის რომელი მომსახურება, ან ტექნიკა გამოიყენებოდა და ამ გამოწვევების მიუხედავად, შეეცადეთ თვალყური ადევნოთ აქტივებს.
- ამოიცანით პატერნები, რომლებიც შეიძლება დანაშაულებრივ განზრახვაზე მიუთითებდეს, როგორიცაა ფულის გათეთრება, დიდი რაოდენობით კრიპტოვალუტის რამდენიმე საფულეზე განაწილება, ან ისეთი ანონიმური კრიპტო აქტივების გამოყენება, როგორებიცაა მონერო ან ზეროქეში.

მტკიცებულებების წარდგენა:

- ნათლად განმარტეთ, თუ როგორ მუშაობს კრიპტოვალუტები და ბლოკჩეინი, რადგან სასამართლოს ბევრი თანამშრომლისთვის შესაძლოა ეს ტექნოლოგია უცნობი იყოს.
- წარადგინეთ ფულის გათეთრების პროცესის მკაფიო და მოკლედ აღწერილი ციფრული კვალი, უკანონო თანხების წყაროდან მათ საბოლოო დანიშნულებამდე. მტკიცებულებების წარდგენისას რეკომენდებულია ვიზუალური მასალის შექმნა და მარტივი არატექნიკური ენის გამოყენება, რადგან ბევრი პროკურორი ან მოსამართლე, შესაძლოა, კრიპტოვალუტის სირთულეებს ბოლომდე არ იცნობდეს.

დამატებითი მტკიცებულება:

- კრიპტოგადაცვლების ჩანაწერები: მათში მომხმარებლის მოქმედების მონაცემების, საფულის მისამართების, IP ლოგების, ტრანზაქციის თანხების და თარიღების ნახვაა შესაძლებელი.
- ბლოკჩეინის ანალიზის პროგრამა: ასეთ პროგრამას ციფრული ვალუტების ნაკადის ვიზუალიზაცია შეუძლია.
- ციფრული საფულეების შემოწმება: გამოიკვლიეთ ე.წ. ჰარდვეარ ანუ მყარი საფულეები, მობილური საფულეები და დესკტოპის საფულეები. მათში შეიძლება იყოს ჩანაწერები, ტრანზაქციის ისტორია, ან მეტამონაცემები, რომლებიც შეიძლება სასარგებლო აღმოჩნდეს.
- IP მისამართისთვის თვალყურის დევნება: ეჭვმიტანილთა გეოგრაფიული მდებარეობის დასადგენად თვალყური ადევნეთ ტრანზაქციებთან დაკავშირებულ IP მისამართებს (იხ. გვ. 31 IP მისამართების შეზღუდვა).
- საერთაშორისო სააგენტოებთან თანამშრომლობა: კრიპტოვალუტების დეცენტრალიზებული ბუნების გამო, საერთაშორისო თანამშრომლობა ტრანსსასაზღვრო ტრანზაქციების თვალყურის დევნებისთვის, შეიძლება გადამწყვეტი გამოდგეს. თუმცა, ასეთი თანამშრომლობა ჩვეულებრივ, გვიან ეტაპზე იწყება წამყვანი გამომძიებლის მიერ.[16]

კრიპტოვალუტის ტრანზაქციებთან და აქტივობებთან დაკავშირებული ყოვლისმომცველი მტკიცებულებების შეგროვებით, პოლიციის ოფიცრებს შეუძლიათ თავიანთ გამომძიებელ კოლეგებს და პროკურორებს, საქმის გასამყარებლად მტკიცე ბაზა მიაწოდონ და უზრუნველყონ დამნაშავეებისთვის პასუხისმგებლობის დაკისრება.

16 ფინანსური დაზვერვის 16-მა ერთეულმა, Egmont Group-თან თანამშრომლობით, შეიმუშავა გაცვლის სისტემის მექანიზმი. იხილეთ ბმული: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (შემოწმდა15 თებ. 2024).

რეკომენდაციები და კონტაქტები რთული შემთხვევებისთვის

რეკომენდაციები და კონტაქტები რთული შემთხვევებისთვის

სპეციალიზებული გუნდები და ექსპერტიზა

ბლოკჩეინ ანალიტიკის პროგრამული უზრუნველყოფის წამყვანი პროვაიდერები ხშირად ქმნიან სპეციალურ გუნდებს, რომლებიც როგორც კრიპტოვალუტის, ასევე საგამოძიებო პროცესების სფეროს ექსპერტებისგან არიან დაკომპლექტებულნი. ეს გუნდები სამართალდამცავ ორგანოებს ბლოკჩეინ ანალიტიკის სირთულეების დაძლევაში ეხმარებიან, რაც ინსტრუმენტების მაქსიმალურ გამოყენებას უზრუნველყოფს. იმის სანახავად, თუ რომელი დეპარტამენტი იყენებს უკვე ბლოკჩეინზე დაფუძნებულ ანალიტიკურ პროგრამულ უზრუნველყოფას. რეკომენდებულია თქვენი სააგენტოს ინტრანეტის შემოწმება. სავარაუდოდ, ყველაზე უკეთესი წარმოდგენა ამ საკითხზე თავად დეპარტამენტის თანამშრომლებს გააჩნიათ.

ტრენინგი და სერტიფიცირება

ბლოკჩეინ ტექნოლოგიების სირთულეებისა და ცოდნის მართვის მნიშვნელობის გაცნობიერებით, ბლოკჩეინ ანალიტიკური პროგრამული უზრუნველყოფის მრავალი პროვაიდერი სტრუქტურირებულ სასწავლო პროგრამებს გვთავაზობს. ეს პროგრამები ხშირად სხვადასხვა დონის სერტიფიცირებით მთავრდება, რაც არა მხოლოდ ადასტურებს სამართალდამცავი პერსონალის უნარებს, არამედ ზრდის მათ ეფექტურობას ბლოკჩეინთან დაკავშირებული საქმეების გამოძიებებში. მიუხედავად იმისა, რომ ზოგიერთ მომსახურებას, როგორიცაა საკონსულტაციო მხარდაჭერა, შესაძლოა დამატებითი დაფინანსება დასჭირდეს, გრძელვადიანი უკუგება მნიშვნელოვანია საგამოძიებო შესაძლებლობების გაფართოების თვალსაზრისით.

გარე მხარდაჭერა სიღრმისეული გამოძიებებისთვის

საკუთარი გუნდების და სწავლებების გარდა, არსებობს გარე კომერციული მიმწოდებლების გაფართოებული სპექტრი, რომლებსაც ბლოკჩეინზე შესრულებული კრიპტოვალუტის ტრანზაქციების ამომწურავი გამოძიებების ჩატარება შეუძლიათ. ეს ორგანიზაციები მოქმედებენ როგორც კონტრაქტორები და თავიანთ სპეციალიზებულ უნარებს სამართალდამცავ ორგანოებს სთავაზობენ. მათი გამოცდილება შეიძლება ფასდაუდებელი იყოს, განსაკუთრებით რთულ შემთხვევებში, როდესაც სიღრმისეული ანალიზი და მრავალმხრივი საგამოძიებო ტექნიკაა საჭირო. სამართალდამცავი უწყებები, როგორიცაა ინტერპოლი ან ევროპოლი, გამომძიებლებს სპეციალურ მხარდაჭერას და სწავლებას სთავაზობენ (იხ. ნაწილი „თანამშრომლობა ციფრული აქტივების ექსპერტებთან“, გვ. 51). თუ თქვენს გუნდს სურს სწავლების ღონისძიებებს შეუერთდეს, დამატებითი ინფორმაციისთვის გთხოვთ დაუკავშირდეთ VirtualAssets@osce.org.

ფრთხილად გააგრძელეთ

თუმცა, გარე მიმწოდებლების მრავალი უპირატესობის მიუხედავად, სააგენტოებს პოტენციური გამოწვევებიც უნდა ახსოვდეთ. სენსიტიურ გამოძიებებში გარე ორგანიზაციების ჩართვამ, როგორებიცაა კონსალტინგური სააგენტოები, ან ბლოკჩეინზე დაფუძნებული ანალიტიკის მიმწოდებლები, შეიძლება საქმის წარმოებაში გართულებები გამოიწვიოს. ასევე კრიტიკულად მნიშვნელოვანი საკითხია მონაცემთა დაცვა. სენსიტიური ინფორმაციის გარე მხარეებისთვის გადაცემას განსაკუთრებული სიფრთხილით უნდა მივუდგეთ, რათა უზრუნველყოფილი იყოს მონაცემთა მთლიანობის შენარჩუნება და გამოირიცხოს კონფიდენციალური ინფორმაციის უნებლიე გაჟონვა.

მაცეი შულცი უძღვება ინსქტუქტორთა მომზადების სემინარს გდანსკში, სადაც ეუთო-ს წევრი ქვეყნების რეგულატორები ერთმანეთს მოწინავე გამოცდილებას უზიარებენ, რთული შემთხვევების გადაჭრასა და დაინტერესებული მხარეების დახმარებაში. ყურადღება ექცევა არამხოლოდ კონტენტის ხარისხს, არამედ მიწოდების ეფექტურ მეთოდებსაც.

მსხვერპლთა მხარდაჭერა

მსხვერპლთა მხარდაჭერა

გამოწვევები, რომელთა შესახებ მსხვერპლი უნდა გავაფრთხილოთ

ერთი კრიპტოვალუტური თაღლითობის მსხვერპლნი, მეორედაც ადვილად ებმებიან თაღლითობის ხაფანგში. ორგანიზებული თაღლითური დაჯგუფებები არ ჯერდებიან მხოლოდ ერთჯერად თავდასხმას და მსხვერპლებს განმეორებით და სტრატეგიულად იღებენ მიზანში. ქვემოთ გავრცელებული მეორადი თაღლითობის დეტალებია მოცემული:

- „მხსნელის“ სიცრუე: თაღლითურ ქსელში მხვერპლის თავდაპირველი ჩათრევის შემდეგ, იმავე სინდიკატის სხვა ფრთა თავს პროფესიონალად წარმოაჩენს და მას დაკარგული ინვესტიციების დასაბრუნებლად დახმარებას სთავაზობს. ამ ერთი შეხედვით გულუხვ შეთავაზებას თავისი ფასი აქვს: მსხვერპლმა დაკარგული თანხების დასაბრუნებლად მომსახურების კომპანიას გასამრჯელო უნდა გადაუხადოს. თანხების გადარიცხვის შემდეგ, „მხსნელი“ ხშირად დაკარგულ თანხებთან ერთად ქრება.
- "მამხილებლის“ ხრიკი: განსხვავებულ სცენარში თაღლითმა შეიძლება საკუთარი თავი თაღლითური კომპანიის ყოფილ უკმაყოფილო თანამშრომლად წარმოაჩინოს და მსხვერპლს არწმუნებდეს, რომ შიდა ინფორმაციის საშუალებით დაეხმარება თანხების დაბრუნებაში. პროცესი „მხსნელის“ შემთხვევის მსგავსია - თანხა წინასწარ უნდა იქნეს გადახდილი. როგორც წესი, საკონტაქტო პირი ამის მერე უჩინარდება.
- სამართლებრივი დახმარების მითი: ეს არის სცენარი, სადაც იურისტი მსხვერპლს ფულის დაბრუნების პირობით მიმართავს. ეს განსაკუთრებით იმ შემთხვევაში ხდება, როდესაც საქმეში VASP-ები ფიგურირებენ. მსხვერპლთან საათობრივ ტარიფზე შეთანხმების შემდეგ, იურისტები ქმნიან და მსხვერპლებს სთავაზობენ ვრცელ დოკუმენტებს (ზოგჯერ 40 გვერდი და მეტი), რომლებშიც დეტალურად აღწერენ ფულის გათეთრების საწინააღმდეგო (AML) და ტერორიზმის დაფინანსების საწინააღმდეგო (CTF) კანონმდებლობის ძირითად საფუძვლებს, მაგრამ აქვთ შეზღუდული იურიდიული ღირებულება. სამწუხაროდ, გამოყენებული დოკუმენტები ძირითადად ზოგადი ხასიათისაა და მათი 99% უცვლელი რჩება, შედეგად VASP-ები გადატვირთულია მცირედ განსხვავებული იმავე დოკუმენტებით. მსხვერპლები იხდიან გაუმართლებლად მაღალ ფასებს ამ ძირითადად ზედმეტი და უსარგებლო ძალისხმევისთვის. აუცილებელია გავითვალისწინოთ, რომ ძირითადად, უკვე შესრულებული VASP ტრანზაქციები უკუქცევადია. საკრედიტო ბარათით გადახდების დაბრუნების (Chargeback) მოთხოვნას წარმატების მცირე შანსი აქვს.

ამგვარად, ასეთი სამართლებრივი ქმედების ეფექტურობა, როგორც წესი, უმნიშვნელოა და საგრძნობლად აცარიელებს მსხვერპლის საფულეს.

ოლგა დე ტრუში, ეუთოს ვირტუალური აქტივების ექსპერტი და ევროპოლის ფინანსური დაზვერვის საჯარო და კერძო პარტნიორობის (EFIPPP) კრიპტო აქტივების სამუშაო ჯგუფის თანათავმჯდომარე. იგი უძღვებოდა ტრადიციული ფინანსური პროვაიდერების, ასევე ვირტუალურ აქტივებთან და ვირტუალური აქტივების სერვის-პროვაიდერებთან დაკავშირებული ფინანსური დანაშაულის ჯგუფების მოწინავე მეთოდების და რისკების მართვის შესახებ სემინარს. სემინარი რომელიც ლატვიის ეროვნული ბანკის (Latvijas Banka) შენობაში ჩატარდა და მასში მონაწილეობა ეუთო-ს კიდევ ოთხი წევრი სახელმწიფოს წარმომადგენლებმა მიიღეს.

კროპტოვალუტების გამოყენებით ჩადენილი დანაშაულების ცალკეული ტიპები

კროპტოვალუტების გამოყენებით ჩადენილი დანაშაულების ცალკეული ტიპები

ქვემოთ მოცემულია კრიპტოვალუტასთან დაკავშირებული ყველაზე გავრცელებული დანაშაულების ტიპების აღწერა. როგორც მინიმუმ, უნდა იცოდეთ ამ ტიპის დანაშაულების არსებობის შესახებ, თუმცა გახსოვდეთ, რომ ეს სია ამომწურავი არ არის.

კრიპტოვალუტაში ინვესტირების სქემები

რა არის ეს?

კრიპტოვალუტაში ინვესტირების თაღლითობა ერთ-ერთი ყველაზე გავრცელებული თაღლითური სქემაა. თავდაპირველად, სამიზნეს მაღალშემოსავლიანი ქვეყნების მდიდარი მოხუცები წარმოადგენდნენ. თუმცა, ტაქტიკა განვითარდა და თავდასხმის ობიექტებად, სულ უფრო ხშირად, საფონდო ბირჟის ინვესტორები და საპენსიო ასაკს მიახლოებული ადამიანები გვევლინებიან. სიფხიზლის შენარჩუნება და მომავალში ამ ტიპის თაღლითობის განვითარების თვალის მიდევნება მნიშვნელოვანია.

მოქმედების მექანიზმი ასეთია: თაღლითები უკავშირდებიან ფინანსურად შეძლებულ ადამიანებს და თითქოსდა მომგებიან საინვესტიციო შესაძლებლობას სთავაზობენ. ისინი როგორც წესი თავს გამოცდილ კრიპტოინვესტორად აცხადებენ და უკავშირდებიან გულუბრყვილო პირებს, რომლებიც დაუფარავად აჩვენებენ სიმდიდრეს.

ასეთი თაღლითობების სხვადასხვა ტიპები

ჩვეულებრივ, განსხვავებული ტიპის პრეტენზიები არსებობს:

წინასწარი გადახდები: თაღლითები პირებს ინვესტიციებიდან მაღალი შემოსავლის მიღების დაპირებით აცდუნებენ. პროცესის დასაწყებად, როგორც წესი, საწყის - 250 ევროდან 1000 ევრომდე (ან ეკვივალენტს ეროვნულ ვალუტაში) დიაპაზონის ქვედა ზღვარზე თანხის გადახდას ავალდებულებენ. საწყისი გადახდის მიღების შემდეგ თაღლითი უბრალოდ ქრება. შედეგი: მსხვერპლი ფინანსურად დაზარალებულია და არანაირი პოტენციური ინვესტიცია არ აქვს.

- უფრო რთული სქემით პროცესის დროს გამოიყენება ვიდეოზარი. ვიდეოზარის ფარგლებში თაღლითი მომავალ მსხვერპლს „ფინანსურ ანგარიშს“ წარუდგენს. თაღლითის რწმუნებით ეს ანგარიში მსხვერპლს ეკუთვნის და მასში ფულადი შემოსავლის მნიშვნელოვანი შემოდინება განხორციელდება. ეს ანგარიშები ისეა შექმნილი, რომ კანონიერად გამოიყურებიან. თუმცა, სინამდვილეში დიზაინის ასლებია და ტრადიციულ ფინანსურ ინსტიტუტებთან კავშირი არ გააჩნიათ.

- ზოგჯერ მსხვერპლი „პირველ გაცემას“, მაგალითად, 50-დან 100 ევრომდე იღებს. თაღლითები აცხადებენ, რომ ეს მათი ინვესტიციების პროცენტია, რათა მსხვერპლი შეიტყუონ და უფრო მეტი გადაახდევინონ.

- **პირადი მონაცემების ქურდობა:** კანონიერების ილუზიის შესაქმნელად თაღლითებმა შეიძლება მოითხოვონ მსხვერპლის პირადი საიდენტიფიკაციო მონაცემები, ვითომ სახსრების გადმორიცხვის, ან ანგარიშზე შემოსატანად. თუმცა, ინვესტიციაში დახმარების ნაცვლად, ისინი მსხვერპლის პირად და ფინანსურ დეტალებზე უნებართვო წვდომას იღებენ. მსხვერპლს ფინანსურ ინსტიტუტში თავისი პირადობის დამადასტურებელი დოკუმენტების დაბლოკვა ავიწყდება და თაღლითს ამ ინფორმაციის ასლებსაც კი უგზავნის.

როგორ ვიმოქმედოთ?

რაიმე დამატებითი გადარიცხვები არ შეასრულოთ. ხშირად თაღლითები საუბრობენ გადარიცხვის, ან გადახდის მცირე ფასზე, რომლებიც თაღლითობის მთლიან ოდენობასთან შედარებით ძალიან მცირედ მოჩანს. მაგალითი: 60 000 ევროს თაღლითობისთვის, 600 ევროს საკომისიო.

- **მსხვერპლმა არ უნდა შეწყვიტოს ურთიერთობა.** როგორც წესი, სამართალდამცავ ორგანოებთან დაკავშირების მომენტისათვის მსხვერპლის და თაღლითის ურთიერთობა დამთავრებულია. თუმცა, თუ ეს ასე არაა, ურთიერთობის შენარჩუნება გამოძიებას გამოყენებული კიბერდანაშაულის ინსტრუმენტების ძიებაში შეიძლება დაეხმაროს.

- **მსხვერპლმა არ უნდა** წაშალოს არცერთი პროგრამული უზრუნველყოფა, რომელიც მის მოწყობილობაზეა განთავსებული, რადგან ისინი კიბერუსაფრთხოების კვალს ტოვებენ, რომელიც გამოძიებისთვის სასარგებლოა. თუმცა, მსხვერპლმა უნდა იცოდეს, რომ შეიძლება მის მოწყობილობაზე პროგრამული უზრუნველყოფაა დაყენებული, რომელიც თვალყურს

მომხმარებლებისთვის, რომლებსაც ინვესტირების, ფინანსების ან ონლაინ ინსტრუმენტების გამოყენების მცირე გამოცდილება აქვთ, თაღლითები ხშირად დისტანციური წვდომის პროგრამულ უზრუნველყოფას აინსტალირებენ.

ეს პროგრამა განკუთვნილია დისტანციური წვდომისა და მართვისთვის და საშუალებას აძლევს მომხმარებლებს ნებისმიერი ადგილიდან მართონ კომპიუტერი ან სერვერი. მსხვერპლი ხშირად თავად აყენებს ასეთ პროგრამას თაღლითის „დახმარებით“. კავშირის დამყარების შემდეგ, მსხვერპლს ხშირ შემთხვევაში ავიწყდება პროგრამის წაშლა. ასეთ პროგრამაში დარჩენილი კვალი სწორად დაცვის შემთხვევაში, შეიძლება გამოსადეგი იყოს სამართალდამცავი ორგანოებისთვის გამოძიების პროცესში.

პროგრამას ტიპის მიხედვით, შესაძლებელია გააჩნდეს სხვადასხვა ფუნქცია, მათ შორის:

- დისტანციური მართვა: მომხმარებლებს კომპიუტერის მართვა შეუძლიათ სხვადასხვა ადგილიდან ისე, თითქოს ისინი თავისი კომპიუტერების წინ სხედან. ეს სასარგებლოა ტექნიკური პრობლემების მოსაგვარებლად, დისტანციური მხარდაჭერისთვის, ან ფაილებზე წვდომის მოსაპოვებლად.
- ფაილების გადაცემა: პროგრამული უზრუნველყოფა, რომელიც მომხმარებლებს ფაილების კომპიუტერებს შორის გადატანის საშუალებას აძლევს. ეს ზოგჯერ ჯაშუშური პროგრამის ტიპის - „keylogger“-ის ინსტალაციას იწვევს. ეს პროგრამა აკონტროლებს ყველაფერს, რასაც მომხმარებელი აკრეფს და მას მერე რაც კომპიუტერზე დაინსტალირდება, შეუძლია თაღლითებთან წლების განმავლობაში გააზიაროს აკრეფილი.
- დისტანციური წვდომა: თაღლითებს ეს მსხვერპლის კომპიუტერზე ან სერვერზე, დისტანციურად შესვლის, ფაილების შეცვლის, პროგრამების დაინსტალირების და კავშირების დაწყების საშუალებას აძლევს.
- მობილური წვდომა: ეს სმარტფონებით და პლანშეტებით, მოწყობილობების დისტანციურად მართვის საშუალებას იძლევა.

ადევნებს - რას ბეჭდავს, ან თუ იგი კამერას ჩართულს ტოვებს და ა.შ. ამიტომ მან თავისი მოწყობილობის მოხმარება უნდა შეზღუდოს

- **გადახედეთ, რა პერსონალური ინფორმაცია გამოქვეყნდა.** თუ შესაძლებელია, შეცვალეთ ბანკის სისტემაში შესვლის მონაცემები და ელექტრონული იდენტიფიკაციის ხელსაწყოებისთვის, თუ ასეთი ინსტრუმენტები გამოიყენება, ახალი პაროლები შეუკვეთეთ.
- **გადახედეთ განყოფილებას მეორადი თაღლითობის შესახებ,** რომლის ნახვაც ზემოთ შეგიძლიათ გვ. 38-ზე
- **საჭირო ნაბიჯების გადადგმა, მსხვერპლის სპეციფიკურ სიტუაციაზეა დამოკიდებული.** დამატებითი დეტალებისთვის იხილეთ ნაწილი „საუკეთესო პრაქტიკა თითოეული ტიპის ტრანზაქციისთვის“, გვ. 24.
- ასეთი თაღლითობის ერთ-ერთი თავისებურება, ცნობილი ადამიანების ყალბი მოწონებების გამოყენებაა. თაღლითები რეალურ ფოტოებს ითვისებენ და მათ შეთითხნილ ანგარიშებთან ან სარეკლამო მასალებთან აერთიანებენ, რითაც იმის შთაბეჭდილებას ქმნიან, თითქოს სქემის გარანტად ცნობილი პიროვნებები გამოდიან.

გამოძალვა და სექსუალური შანტაჟი

გამოძალვის შემთხვევებში, პიროვნებას ეგზავნება ელ.წერილი. წერილი შეიცავს ცრუ ინფორმაციას, თითქოს ჰაკერმა მოიპოვა წვდომა მსხვერპლის კომპიუტერზე და შეუძლია დაუკავშირდეს ლეპტოპის ან სმარტფონის კამერას. სექსუალურ საფუძველზე გამოძალვის დროს, როგორც წესი, მსხვერპლს არწმუნებენ, რომ ჰაკერმა იგი მასტურბაციის დროს გადაიღო.

რა არის ეს?

ინდივიდი თაღლითისგან ელ.წერილს იღებს. ამ ელ.წერილში ნათქვამია, რომ თაღლითმა მსხვერპლის კომპიუტერი ან სმარტფონი გატეხა და კამერაზე წვდომა მიიღო. სექსუალური შანტაჟის შემთხვევაში, თაღლითი ამტკიცებს, რომ ჩაწერა მსხვერპლის კადრები მასტურბაციის დროს და გამოაქვეყნებს ვიდეოს, თუ მსხვერპლი კრიპტოვალუტით არ გადაუხდის.

მსხვერპლს სთავაზობენ, კრიპტოვალუტის მითითებულ საფულეზე თანხები მჭიდრო ვადაში გადარიცხოს, რათა თავიდან აიცილოს ასეთი ვითომ გადაღებული კადრების ბიზნეს და კერძო კონტაქტებისთვის გაზიარება, რომლებიც ჰაკერის მტკიცებით, მან მოწყობილობაზე იპოვა.

მისი მოთხოვნის „მტკიცებულების“ სახით, ჰაკერი ჩვეულებრივ, მომხმარებლის სახელებისა და პაროლების ჩამონათვალს აწვდის, რომლებიც დაკავშირებულია სხვადასხვა ვებსაიტთან, რადგან ვარაუდობს, რომ მსხვერპლი იდენტურ მონაცემებს, ზრდასრულთათვის განკუთვნილი შინაარსის მქონე რამდენიმე საიტზე იყენებდა.
.

წინამდებარე პუბლიკაციის ავტორისთვის გაგზავნილი ელ.ფოსტით მიღებული შეტყობინების დედანი:

თემა: მე ჩაგწერე *(აქ თაღლითი გადასცემს პაროლს, რომელიც ნაპოვნია გატეხვისას)*
თარიღი: 22/06/23 03:32
გამგზავნი: „გადაარჩინე შენი სიცოცხლე“ <xxxxxxxxxf@xxxx.ga>
მიმღები: XXXXXX@xxxx.com

გამარჯობა, მე ვარ ჰაკერი და პროგრამისტი, ვიცი, რომ შენი ერთ-ერთი პაროლია: (*მომხმარებლის პაროლი, რომელიც პაროლის გაჟონვით არის მიღებული)*

შენი კომპიუტერი ჩემი პირადი მალვეარით (მავნე პროგრამით) დაინფიცირდა, რადგან ბრაუზერი არ იყო განახლებული/“პაჩით” დაცული(patched). ასეთ შემთხვევაში საკმარისია უბრალოდ ეწვიო ვებსაიტს, სადაც ჩემი ფრეიმ-ჩარჩო (iframe)-ია განთავსებული, და ავტომატურად დაინფიცირდები. თუ გინდა მეტი გაიგო, დაგუგლე: “Drive-by exploit”.

ჩემმა მალვეარმა უზრუნველყო სრული წვდომა შენს ყველა ანგარიშზე (იხილეთ პაროლი ზემოთ), შენი კომპიუტერის მთლიანი კონტროლი და ასევე მომცა შესაძლებლობა შენთვის ვებ-კამერის საშუალებით მეთვალთვალა .

შევაგროვე შენი ყველა პირადი მონაცემი, ჩავწერე რამდენიმე ვიდეო (ვებ-კამერის მეშვეობით) და ასევე ჩავწერე თუ როგორ იკმაყოფილებდი საკუთარ თავს!!!

შემიძლია გავავრცელო შენი ნებისმიერი პირადი ინფორმაცია ყველგან — მათ შორის darknet-ზე, სადაც ძალიან ავადმყოფი ადამიანები არიან, ასევე შემიძლია შენი ვიდეოები გავუგზავნო შენს საკონტაქტო პირებს და გამოვაქვეყნო სოციალურ ქსელებში და ყველა სხვა ნებისმიერ პლატფორმაზე!

მხოლოდ შენ შეგიძლია ხელი შემიშალო და არ გამაკეთებინო ეს და მხოლოდ მე შემიძლია დაგეხმარო. არანაირი კვალი არ დარჩა, რადგან სამუშაოს დასრულების შემდეგ მალვეარი წავშალე. ეს ელ.წერილი(ები) სხვა გატეხილი სერვერიდან გამოიგზავნა.

ჩემი შეჩერების ერთადერთი გზა, ზუსტად 400$-ის გადახდაა ბიტკოინებში (BTC).
ეს ძალიან კარგი შეთავაზებაა, იმ საშინელებასთან შედარებით, რაც მოხდება, თუ არ გადაიხდი!
ბიტკოინის ყიდვა მარტივად აქ შეგიძლია: www.xxxxxxx.com, www.xxxxx.com , www.xxxxxx.com ან ნახე შენს მახლობლად ბიტკოინის ბანკომატი, ან Google-ში სხვა ბირჟები მოძებნე.
შენ შეგიძლია, ბიტკოინი პირდაპირ ჩემს საფულეზე ჩარიცხო, ან შექმნა საკუთარი საფულე ჯერ აქ: www.login.xxxxx.com/en/#/signup/, შემდეგ მიიღე და გამოაზავნე ჩემთან.
ჩემი ბიტკოინის საფულეა: 17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG
დააკოპირე და ჩასვი; ეს არის (cAsE-sEnSEtiVE).
შენ 3 დღე გაქვს.

რადგან ელ.ფოსტის ანგარიშზე წვდომა მივიღე, ადვილად გავიგებ, ეს ელ.წერილი წაკითხულია თუ არა.

თუ ამ ელფოსტას რამდენჯერმე მიიღებ, ეს იმისთვისაა, რომ დავრწმუნდე, რომ ის წაიკითხე, ჩემი გაგზავნების სკრიპტი ასეა კონფიგურირებული და გადახდის შემდეგ მისი იგნორირება შეგიძლია.

თანხის მიღების შემდეგ შენს ყველა მონაცემს წავშლი და შეგიძლია, როგორც აქამდე, მშვიდად იცხოვრო. ინტერნეტში მომდევნო შესვლამდე განაახლე შენი ბრაუზერი!

ნინა-ლუიზა ზიდლერი რიგაში, ხუთი წევრი სახელმწიფოს რეგულაციების (პოლიტიკის) შემმუშავებელთათვის გამართულ სემინარს ხელმძღვანელობს და მათ ვირტუალური აქტივების რეგულატორებთან შეხვედრების შედეგებს/დასკვნებს უზიარებს. სესიაზე ძირითადად ვირტუალურ აქტივებთან დაკავშირებული საერთოევროპული კანონმდებლობა განიხილებოდა. მისი მიზანი არსებული რეგულატორების ხარვეზების იდენტიფიცირება და წევრი სახელმწიფოებისთვის ახალი, მათთვის აქტულური მიდგომების წარმოჩენა იყო.

როგორ ვიმოქმდოთ?

საუკეთესო გამოცდილება იმ მსხვერპლთა მხარდასაჭერად, რომლებიც გამოძალვის წერილებს ასაჯაროებენ.

- **შეინარჩუნეთ სიმშვიდე:** სექსუალური გამოძალვის ელ-წერილის მიღების შემთხვევაში მომხმარებელმა სიმშვიდე უნდა შეინარჩუნოს. ზემოთ წარმოდგენილი ელ-წერილში ჩანს, რომ კრიმინალი ემოციურ ეპითეტებს გადაუდებელი საქმის ვითარების შესაქმნელად და შიშის, სირცხვილისა და პანიკის დასათესად იყენებს.
- **მსხვერპლმა გამომგზავნთან** არანაირი ურთიერთობა არ უნდა დაამყაროს: სექსუალური გამოძალვის ელ.ფოსტა, როგორც წესი, არანაირ მტკიცებულებას, ან ჩანართებს არ შეიცავს. თუ ელ.წერილში ბმულებია, მომხმარებელმა ისინი არ უნდა გახსნას.
- მომხმარებელს უნდა აეკრძალოს ფიატური ფულის კრიპტოვალუტაზე გადაცვლა და საეჭვო კრიპტოვალუტის საფულეში მისი გადატანა.
- **შეამოწმეთ კრიპტოვალუტის საფულე:** კრიპტოვალუტის საფულის მისამართის ავთენტურობის შესაფასებლად ერთ-ერთი საშუალება იმ ინსტრუმენტების გამოყენებაა, რომლებსაც ჩვეულებრივ უწოდებენ „საფულის ექსპლორერს“. მაგალითად, ნახსენები კრიპტოვალუტის საფულის შემოწმება შესაძლებელია შემდეგი ბმულის გამოყენებით:

  https://www.blockchain.com/explorer/addresses/btc/17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG

- წინასწარი გამოძიებით, რომელიც უფასოა და 10 წამზე ნაკლებს გრძელდება, ცხადი ხდება, რომ ამ საფულეზე ბევრი ტრანზაქცია განხორციელდა. ეს ხშირად ეწინააღმდეგება ჰაკერის მტკიცებას, თითქოს ეს არის უნიკალური და ერთჯერადად გამოყენებული კრიპტოვალუტის საფულის მისამართი. მრავალი ტრანზაქცია მიუთითებს, რომ შესაძლოა რამდენიმე პირმა მასზე თანხები გადარიცხა.
- **მოპარული ანგარიშის მონაცემების ბაზრის გამოყენება მსხვერპლთა სასარგებლოდ:** მსხვერპლს შეუძლია გამოიყენოს უფასო სერვისები (https://haveibeenpwned.com). ეს მომსახურება საშუალებას იძლევა შემოწმდეს, მსხვერპლის მონაცემები, მონაცემთა დარღვევის მსხვერპლთა მილიარდობით გაჟონილი ანგარიშის დეტალების შესწავლით ხომ არ გამჟღავნდა. ელექტრონული ფოსტის მისამართით, ან მომხმარებლის სახელის შეყვანით, მომხმარებლებს შეუძლიათ ნახონ, ჩანს თუ არა მათი ინფორმაცია რომელიმე ცნობილი გაჟონვის ფარგლებში. თუ თავდამსხმელი გამოყენებულ პაროლს გამოავლენს, დაუყოვნებლივ შეცვალეთ იგი ყველა პლატფორმაზე, სადაც კი გამოიყენება.

გამოძალვის საქმეების გამოძიებისას, მნიშვნელოვანია მიაკვლიოთ ეჭვმიტანილი პირების საფულეებს .

ამგვარი ქმედებით გამოჩნდება დაკავშირებულია თუ არა რომელიმე საფულე ოფიციალურ ფინანსურ პლატფორმებთან. ეს დაეხმარება სამართალდამცავ ორგანოებს გაარკვიონ, თუ ვინ გაუგზავნა ფული ეჭვმიტანილს. გამომძალველის საფულეში გადახდა არ არის დანაშაული, მაგრამ მნიშვნელოვანია, რომ გადამხდელს შეიძლება თაღლითის შესახებ ინფორმაცია გააჩნდეს ან იგივე თაღლითი მას ისევ დაემუქროს. ეს კი დაეხმარება გამოძიებას.

ვენაში, ეუთო-ს სამდივნოში, უკრაინელი პოლიტიკოსებისათვის ტარდება ტრენინგი ვირტუალური აქტივების მარეგულირებელი კანონმდებლობის ხარვეზების შესახებ. ყურადღება გამახვილებულია დეცენტრალიზებულ ბირჟებზე.

"რაგ პული" ("Rug Pull" - "ხალიჩის გამოქაჩვა") თაღლითობა

ე.წ. „საქმიდან გასვლა“, „გადაქაჩვა და გადაგდება“ ან „ხალიჩის გამოქაჩვა“ (შემდეგში „რაგ პული“) იდიომატური გამოთქმაა, რაც „ვინმეს ფეხქვეშ ხალიჩის გამოცლას“ გულისხმობს. თაღლითობის სქემებია, რომლის დროსაც თაღლითები ახალი ციფრული აქტივების ირგვლივ დიდ აჟიოტაჟს ქმნიან. ეს შეიძლება ეხებოდეს არა მხოლოდ კრიპტოვალუტას, არამედ ნებისმიერ ციფრულ აქტივს. მსგავსი მაქინაციები პროექტებსა და არაჩანაცვლებად ტოკენებთან (NFT) მიმართებითაც განხორციელებულა. თაღლითები პროექტს სასწრაფოდ ეთიშებიან, იპარავენ ინვესტორის ფულს და ციფრულ აქტივს ღირებულების გარეშე, სრულიად გამოუსადეგარს ტოვებენ.

რა არის ეს?

ამ ტიპის თაღლითობის მიზანი, ახალი ციფრული აქტივისთვის რაც შეიძლება მეტი მყიდველის ან ინვესტორის მიზიდვა და მისი სავარაუდო ფასის მაქსიმალურად შესაძლებელ დონემდე ხელოვნურად გაბერვაა. როგორც კი თაღლითები საკმარის ფულს შეაგროვებენ, ისინი ქრებიან (გასვლით თაღლითობა) და ფული თან მიაქვთ. ეს გასვლა შეიძლება სწრაფად მოხდეს. ამ დროს ყველა მოულოდნელად, ან დროთა განმავლობაში ქრება, ფული კი ნელ-ნელა გააქვთ. ამ დროს შემმუშავებლები აქტივს განზრახ სულ უფრო ნაკლებად ავითარებენ. ამ უკანასკნელის შემთხვევაში, ზოგჯერ ძნელია, ნამდვილი "რაგ პულ" თაღლითობა უბრალოდ წარუმატებელი პროექტისგან განასხვავო.

თითოეულ შემთხვევაში, თაღლითების გასვლა ნიშნავს, რომ აქტივი ყალბია და ფასი არ გააჩნია. მსხვერპლი რამდენიმე მონეტისა და ტოკენის ამარა რჩება, რაც გადახდილი თანხის მხოლოდ მცირე ნაწილს შეადგენს. ასევე ,ამ ციფრულ აქტივს აქვს კოდი, რომელიც მიუთითებს, რომ მისი გაყიდვა შეუძლებელია, იმ შემთხვევაშიც კი თუ მსხვერპლი მყიდველს იპოვის.

ფიშინგ (Phising) თაღლითობები

ფიშინგ თაღლითობები ინტერნეტის მრავალ სფეროშია გავრცელებული. ეს ასევე გავრცელებული და ეფექტური თაღლითური სქემაა ციფრულ აქტივებთან მიმართებითაც.

რა არის ეს?

თაღლითები თავს ლეგიტიმური კონფიგურაციის ვებსაიტების ან ოფიციალური კომპანიების დოკუმენტაციის მქონე პირებად ასაღებენ. ათასობით ელ-წერილებს და შეტყობინებებს აგზავნიან ბმულებთან ერთად. ბმულების მეშვეობით მსხვერპლი თაღლითების ვებსაიტის ყალბ ვერსიამდე მიდის. ვებსაიტი შექმნილია იმისათვის, რომ დაუშვას სისტემაზე წვდომა და ყველა ვიზიტორის მიერ შეყვანილი პირადი ინფორმაცია, ყველა კრიპტო მისამართი და პაროლი (ე.წ. „კრიპტო საფულის გასაღებები“) შეინახოს. ეს განსაკუთრებით საყურადღებოა კრიპტოდანაშაულთან მიმართებით, რადგანაც თუ კრიპტო საფულის პირადული გასაღები იქნა მოპარული, ასეთი ანგარიშის აღდგენა პრაქტიკულად შეუძლებელია. ეს ნიშნავს რომ საფულეში არსებული თანხები სამუდამოდ დაიკარგა.

ასეთი თაღლითობის სხვადასხვა ტიპები

ბლოკჩეინ ანალიტიკის ერთ-ერთი პროვაიდერის მიერ გამოქვეყნებული მოხსენების თანახმად[17] ფიშინგით ახალი ტიპის თაღლითობა გულისხმობს ახალ კრიპტო-ინვესტორებში „FOMO“-ზე (Fear of Missing Out - ხელიდან გაშვების შიშის) თამაშს, რომლის დროსაც, NFT-ის შეძენის დაპირებით, მსხვერპლს ფულს არასწორ ანგარიშზე აგზავნინებენ. ეს ნიშნავს, რომ დაზარალებულები მხოლოდ არასწორ ანგარიშზე გაგზავნილ თანხას

17 უკანონო კრიპტო ეკოსისტემის ანგარიში. (2023): https://www.trmlabs.com/report (შემოწმდა: 2023 წლის აგვისტოს).

კარგავენ და არა მთელ საფულეს. თაღლითობის კიდევ ერთი სახეობა სახელად „მისამართის მოწამლვა“ მეტ პოპულარობას იძენს. სქემა ასეთია: თაღლითი იმ მისამართის მსგავს მისამართს ქმნის, რომელზეც შერჩეულმა მსხვერპლმა ადრე გააგზავნა თანხა. ამის შემდეგ თაღლითი მცირე ოდენობის კრიპტოვალუტას იმ იმედით აგზავნის, რომ მსხვერპლიც დაგეგმილი მიმღების ნაცვლად მომავალ გადახდას იმავე თაღლითურ მისამართზე დაუფიქრებლად განახორციელებს.

როგორ ავირიდოთ თავიდან?

უნდა იცოდეთ ყალბი ფიშინგის ბმულების შესახებ და ყველა ბმული შეამოწმოთ.

გადაამოწმეთ მისამართები

- ყოველთვის გადაამოწმეთ მისამართი, რომელზეც თანხას აგზავნით, განსაკუთრებით დიდი თანხების შემთხვევაში. ნუ დაეყრდნობით ბუფერულ ფუნქციებს (ე.წ. კოპირება-ჩასმის ფუნქცია), რადგან მავნე პროგრამას შეუძლია მათი საშუალებით მანიპულირება: მსხვერპლის მიერ მონიშნული მისამართი მან შესაძლოა სხვა კრიპტოვალუტის საფულის მისამართით შეცვალოს.
- კრიპტოსაიტებისთვის, რომლებზეც ხშირად შედიხართ, გამოიყენეთ სანიშნეები. ეს თავიდან აგაცილებთ არასწორად აკრეფის ან ვიზუალურად მსგავს ფიშინგ საიტზე მოხვედრის რისკს.

გამოიყენეთ დამატებითი უსაფრთხოების ზომები

- ყველგან, სადაც ეს შესაძლებელია, ორფაქტორიანი ავთენტიფიკაციის (2FA) გამოყენებაა რეკომენდებული. ეს ზრდის უსაფრთხოების დონეს, რაც თაღლითებს ანგარიშებზე წვდომას ურთულებს.
- რეგულარულად განაახლეთ და გაუშვით მავნე პროგრამების საწინააღმდეგო პროგრამები, რათა თქვენს მოწყობილობაზე პოტენციური საფრთხეები აღმოაჩინოთ და წაშალოთ. ზოგიერთი მავნე პროგრამის განშტოება კრიპტო ტრანზაქციების მონიტორინგისთვის, ან “Clipboard”-ის მონაცემების შესაცვლელად არის შექმნილი.

გამოიყენეთ პაროლების მენეჯერები (Password Managers)

პაროლების მენეჯერები მათ შესანახად, სამართავად და ავტომატურად შევსებისთვის შექმნილი პროგრამებია. ისინი მომხმარებელს ჩანაწერების უსაფრთხოდ შექმნის და მისი შენახვის საშუალებას აძლევენ და კრიპტოვალუტის საფულის ნომრებს სხვადასხვა ონლაინ ანგარიშებისთვის საიმედოდ ინახავენ.

"შუამავალი"(Man-in-the-Middle) იერიშები

რა არის ეს?

ამ ტიპის თაღლითობისას, თაღლითები არ ესხმიან თავს მსხვერპლს პირდაპირ, არამედ დააფიქსირებენ და მოიპარავენ მონაცემებს იმ დროს, როცა ვინმე შედის თავის კრიპტოვალუტის ანგარიშზე საჯარო ან დაუცველი Wi-Fi ქსელის მეშვეობით — ანუ ისეთ გარემოში, სადაც მონახულებული ვებსაიტები და კომპიუტერიდან საიტზე გაგზავნილი ინფორმაცია არ არის დაცული. თაღლითები აგროვებენ კრიპტოსაფულის მისამართს, ავტორიზაციის მონაცემებსა და საფულის გასაღებებს, შემდეგ კი იყენებენ ამ ინფორმაციას ანგარიშზე კონტროლის მოსაპოვებლად.

როგორ ავირიდოთ თავიდან?

ამ ტიპის თაღლითობის თავიდან აცილება შესაძლებელია ვირტუალური კერძო ქსელის (VPN) გამოყენებით. იგი საკმაოდ იაფია — ჩვეულებრივ მხოლოდ 3-4 ევრო თვეში. VPN იცავს მომხმარებლის კავშირს ინტერნეტთან — დაშიფვრავს მას, რაც არაავტორიზებული პირებისთვის ართულებს იმის ნახვას, თუ რომელ ვებსაიტებს სტუმრობენ ან რა ინფორმაცია შეჰყავთ კლავიატურით. ასევე, VPN მალავს მომხმარებლის რეალურ IP მისამართს, რაც უზრუნველყოფს ანონიმურ დათვალიერებას და ფარავს მომხმარებლის გეოგრაფიულ მდებარეობას. ეს მომხმარებელს აძლევს შესაძლებლობას დისტანციურად ჰქონდეს წვდომა საკუთარი ორგანიზაციის რესურსებზე ან გვერდი აუაროს ცენზურას. (დამატებითი ინფორმაციისთვის იხილეთ განყოფილება „IP მისამართების შეგროვება“, გვ. 31.)

კრიპტოვალუტის ბირჟების იმიტატორი ყალბი ვებ-გვერდები

რა არის ეს?

ყალბი კრიპტოვალუტის შექმნის ნაცვლად, თაღლითი ვებსაიტებს ქმნის, რომლებიც კრიპტოვალუტის ბირჟებს ჰგავს. როდესაც მსხვერპლი აკითხავს ამ ვებსაიტს, რათა თავისი კრიპტოვალუტა სხვა ტიპის კრიპტოზე, ან ფიატურ ვალუტაზე გაცვალოს, თაღლითები მის დეტალებს და შეტანილ კრიპტოვალუტას იპარავენ.

როგორ ავირიდოთ თავიდან?

უსაფრთხოების გასაძლიერებლად, თქვენს ბირჟაზე შესვლისას, ყოველთვის გამოიყენეთ ორფაქტორიანი ავთენტიფიკაცია (2FA). ეს შეიძლება მოიცავდეს ერთჯერადი კოდის მიღებას SMS-ით, ან ელექტრონული ფოსტით, რომელიც უნდა შეიყვანოთ სისტემაში შესვლის პროცესში როგორც დადასტურების დამატებითი საფეხური. თუ ეუთო-ს წევრი ქვეყანა გთავაზობთ ელექტრონული იდენტიფიკაციის სერვისს (e-identification), გაითვალისწინეთ მისი გამოყენება ავტორიზაციის დროს — როგორც დამატებითი დაცვა.

მეორადი თაღლითობები

არსებობს მეორადი თაღლითობის შემთხვევებიც, რომლებიც ხდება მას შემდეგ, რაც მსხვერპლი ერთხელ უკვე მოტყუვდა. აღნიშნულ საკითხს განიხილავს სექცია „მსხვერპლთა მხარდაჭერა“ (გვ. 37).

მარცხნიდან მარჯვნივ: მარსინ ზარაკოვსკიმ, მიხალ გრომეკმა, ანა პაჟევსკამ და ნინა-ლუიზ ზიდლერმა, უკრაინის დელეგაციისთვის დამოუკიდებელი სემინარი ჩაატარეს, რომელიც ვირტუალური აქტივების მომსახურების პროვაიდერებზე (VASP) ზედამხედველობის გამოწვევებს და უპირატესობებს მიეძღვნა. სესიაში მონაწილეობდნენ უკრაინის ძირითადი ინსტიტუტების წარმომადგენლები, როგორიცაა უკრაინის ეროვნული ბანკი (NBU), უკრაინის სახელმწიფო ფინანსური მონიტორინგის სამსახური (SFMS), ციფრული ტრანსფორმაციის სამინისტრო და ფასიანი ქაღალდებისა და საფონდო ბაზრის ეროვნული კომისია (NSSMC).
სემინარი პოლონეთის ფინანსთა სამინისტროში გაიმართა, რომელიც თავის ობიექტებზე უკრაინელი დელეგატებისთვის სწავლებების სერიის უსასყიდლოდ მასპინძლობას აგრძელებს.

ვირტუალური აქტივების სფეროში დანაშაულის გამოძიების დამატებითი ინსტრუმენტები

ვირტუალური აქტივების სფეროში დანაშაულის გამოძიების დამატებითი ინსტრუმენტები.

ბლოკჩეინ ანალიტიკის ინსტრუმენტები

ბლოკჩეინ ანალიტიკის კარგი ინსტრუმენტი ან საფულის ექსპლორერი პოლიციის ოფიცრებს საშუალებას აძლევს გამოძიების თავიანთი ნაწილი VASP-ების ინფორმაციის გათვალისწინების გარეშე აწარმოონ. ეს პროცესი შესაძლებელია არასრული და ხანგრძლივი იყოს. გარდა ამისა ყველა VASP ჯერაც არ იყენებს ბლოკჩეინ ანალიტიკის ინსტრუმენტებს.

სამართალდამცავი უწყებები ხშირად ითხოვენ VASP-ებისგან კონკრეტული კრიპტოვალუტის საფულის მისამართების მიმდინარე ბალანსთან დაკავშირებულ ინფორმაციას. მიუხედავად იმისა, რომ VASP-ების შესაბამისობის ჯგუფებს შეუძლიათ ასეთ მოთხოვნებზე რეაგირება, ეს პროცესი ხშირ შემთხვევაში დიდ ადმინისტრაციულ რესურსს მოითხოვს.

უფრო ეფექტური ალტერნატივა კრიპტოსაფულის მისამართის შესაბამის საფულის ექსპლორერში შეყვანაა, რომელიც მეტწილად სწრაფად გასცემს წამყვანი კრიპტოვალუტის შესახებ საჭირო ინფორმაციას — თუმცა არა ყოველთვის.

საფულეების ექსპლორერის მიერ მოწოდებული ინფორმაცია:

- კრიპტოვალუტის მიმდინარე ბალანსი და ძირითადი FIAT ვალუტები, მაგ. აშშ დოლარი (USD).
- კრიპტოვალუტის საფულით მიღებული თანხების ჯამური ოდენობა.
- კრიპტოვალუტის საფულედან გაგზავნილი თანხების ჯამური ოდენობა.
- ტრანზაქციების დროის ნიშნულები/შტამპები. (შენიშვნა: ტრანზაქციების დრო შეიძლება განსხვავდებოდეს კრიპტოვალუტის დროის სარტყლის მიხედვით).
- ბლოკჩეინზე დარიცხული საკომისიოები.
- კრიპტოვალუტის მისამართების წყარო (საიდანაც თანხები გადაირიცხა).
- კრიპტოვალუტის საფულის მისამართების დანიშნულების ადგილი (სადაც თანხები გაიგზავნა).

მან, ვინც ბლოკჩეინ ანალიტიკას არ იცნობს, შეიძლება ზემოთ ჩამოთვლილი მონაცემები ზედაპირულად ჩათვალოს. თუმცა საპირისპიროდ, ეს მონაცემები ხშირად გამოძიებისთვის ძალიან ღირებულ ინფორმაციას შეიცავს. მაგალითად, შეიძლება გამოიკვეთოს მცირე თანხების მრავალი შემომავალი ტრანზაქციებისა და შედარებით მცირე რაოდენობის, მაგრამ დიდი მოცულობის გამავალი ტრანზაქციების ტენდენცია. ასეთი პატერნი გამოძიებას ნარკოტიკებით მოვაჭრის მსგავს/შესაძლო საქმიანობაზე მიანიშნებს,

რეალური მაგალითები:

კრიმინალურ საქმეებში გამოყენებული საფულეების მაგალითები:

- კრიპტოვალუტის საფულე, რომელიც დაკავშირებულია სექსუალური შანტაჟის საქმესთან — იდენტიფიცირებულია Blockchain Explorer-ის მეშვეობით.
- კრიპტოვალუტის საფულე, რომელიც ასოცირდება Twitter Hack-თან — იდენტიფიცირებულია საფულის ექსპლორერის, მომხმარებელთა გამოხმაურებებისა და Chain Abuse პლატფორმაზე დაფიქსირებული მონაცემების საფუძველზე.

ყველა სადაზვერვო ღია წყაროს მსგავსად, ასეთი ექსპლორერებისაგან მიღებულ ნებისმიერ მონაცემს სკეპტიკურად უნდა მივუდგეთ და დასკვნების გამოტანამდე გადავამოწმოთ.

უფასო ბლოკჩეინ ანალიტიკური ინსტრუმენტების მაგალითები:

- Block Explorer: ეს არის მარტივი ინსტრუმენტი, რომელიც დეტალურ ინფორმაციას გვაწვდის ბიტკოინის ბლოკების, მისამართების და ტრანზაქციების შესახებ. ეს ინსტრუმენტი დამწყებთათვის კარგი საწყისი წერტილია.
- Etherscan: ეს ინსტრუმენტი სპეციალურად ეთერიუმის ბლოკჩეინისთვის არის განკუთვნილი და ტრანზაქციისა და მისამართების დეტალური ანალიტიკის შეთავაზება შეუძლია.
- Blockchair: ეს ინსტრუმენტი მოიცავს მრავალ ბლოკჩეინს - ბიტკოინიდან ეთერიუმამდე და სხვადასხვა ქსელის ანალიზის მსურველთათვის მრავალმხრივად გამოყენებადია.

ეუთოს ვირტუალური აქტივების ექსპერტებმა და ევროპოლის ფინანსური დაზვერვის საჯარო და კერძო თანამშრომლობის სააგენტოს (EFIPPP) კრიპტოაქტივების სამუშაო მიმართულების თანათავმჯდომარეებმა - ოლგა დე ტრუჩისმა და გრეტა ბარკაუსკიენემ მონაწილეობა მიიღეს EFIPPP-ის 2024 წლის აპრილის პლენარულ სხდომაში, რომელიც ჰააგაში, ევროპოლის შტაბ-ბინაში გაიმართა.
ერთობლივად უზრუნველყვეს ცოდნის გაზიარების სესიები, რომლებზეც სხვადასხვა ქვეყნის, მათ შორის ეუთო-ს ბენეფიციარი ქვეყნების მონაწილეებმა შეისწავლეს და განიხილეს ორგანიზებული დანაშაულის ახალი მოქმედების მეთოდები ვირტუალური აქტივების სივრცეში.

ბლოკჩეინ ანალიტიკის პროვაიდერები

ბლოკჩეინ ანალიტიკის პროვაიდერები საფულის ექსპლორერის კომერციულ ანალოგებს წარმოადგენენ.

ისინი ბლოკჩეინ ქსელებში აქტივობების მონიტორინგის, ანალიზისა და ვიზუალიზაციისთვის შექმნილ სპეციალიზებულ პროგრამულ უზრუნველყოფას იყენებენ. ეს ინსტრუმენტები გამომძიებლებს კანონზომიერების გამოვლენაში, ტრანზაქციების მეთვალყურეობასა და ბლოკჩეინის უზარმაზარი და რთული სამყაროს შესახებ ცოდნის მიღებაში ეხმარება.

საფულის ექსპლორერის მეშვეობით ხელმისაწვდომი მონაცემების გარდა, ბლოკჩეინ ანალიტიკის პროვაიდერები გვთავაზობენ:

- **დაკვირვებას და მიკვლევას:** ანალიტიკური ინსტრუმენტების უმეტესობას შეუძლია თვალყური ადევნოს და დააკვირდეს კრიპტოვალუტის ტრანზაქციას მისი წყაროდან დანიშნულების ადგილამდე. ეს სასიცოცხლოდ მნიშვნელოვანია სახსრების ნაკადის გასაგებად და ნებისმიერი პოტენციური უკანონო ქმედებების გამოსავლენად.
- **ვიზუალიზაციას:** ეს ხელსაწყოები ხშირად გვთავაზობენ ვიზუალურ სქემებსა და გრაფიკებს, რათა დიდი მოცულობის მონაცემების ერთი შეხედვით აღქმა გააადვილონ და კრიპტოვალუტის საფულეები ფინანსურ ინსტიტუტებთან, ან ტრანზაქციებთან, ან საფულის პროვაიდერები ერთმანეთს დაუკავშირონ.
- **რისკების შეფასება**: ტრანზაქციების მოდელების ანალიზის მეშვეობით ზოგიერთ ინსტრუმენტს კონკრეტულ საფულეებთან და ტრანზაქციებთან დაკავშირებული რისკების შეფასება შეუძლია. აქედან გამომდინარე, ფინანსურ ინსტიტუტებსა და მარეგულირებლებს ღირებულ ინფორმაციას სთავაზობს.
- **ყოვლისმომცველი მონაცემები:** ამ ინსტრუმენტებს სხვადასხვა ბლოკჩეინიდან მონაცემების ამოღება და ინტეგრირება შეუძლიათ. ეს მომხმარებლებს კრიპტოვალუტის ლანდშაფტის ერთიანი წარმოდგენის საშუალებას აძლევს, რაც შეიძლება სასარგებლო იყოს მრავალი გამოძიებისათვის.
- **დემიქსინგის მომსახურება:** ზოგი პროვაიდერი აცხადებს, რომ მათ სერვისებს შეუძლია მიქსერებსა და ტამბლერებს შორის ტრანზაქციების ჩვენება. ეს მომსახურება კრიპტოვალუტის ტრანზაქციების კონფიდენციალურობისა და ანონიმურობის გასაძლიერებლად შეიქმნა. (დამატებითი ინფორმაციისათვის იხილეთ გვ.19, „მიქსერები და ტამბლერები“, ასევე გვ.34 დემიქსინგის სერვისების განხილვა სექციაში „საქმეების სასამართლოში წარდგენა“).

ამ ინსტრუმენტების გამოყენება გამომძიებლებს ბლოკჩეინ სამყაროს რთული დინამიკის უკეთ გაგებაში, გააზრებული გადაწყვეტილებების მიღებასა და რევოლუციური ტექნოლოგიის საფუძვლიან გარკვევაში ეხმარება.

საქართველოს ეროვნული ბანკის შტაბ-ბინაში ბოლო ორი წლის განმავლობაში, ვირტუალური აქტივების გუნდმა მნიშვნელოვანი მხარდაჭერა მიიღო ეუთო-ს ვირტუალური აქტივების ექსპერტებისგან.

ციფრული აქტივების ექსპერტებთან თანამშრომლობა

ციფრული აქტივების ექსპერტებთან თანამშრომლობა

ციფრული აქტივებისა და მათთან დაკავშირებული ანგარიშების დამუშავების პროცესში აუცილებელია სამართალდამცავი ორგანოების (LEA) გარე ძალებთან თანამშრომლობა. ესენია: საერთაშორისო საპოლიციო სტრუქტურები, ბანკები და სპეციალიზებული დანაყოფები. მათი ექსპერტული დასკვნები გამოძიების ეფექტურობას შეუწყობს ხელს.

ადგილობრივი ექსპერტების იდენტიფიცირება

ვირტუალური აქტივების მართვის გამოცდილების მქონე სამართალდამცავი ორგანოების ადგილობრივი წევრების გამოვლენა ფასდაუდებელია. მათი საკონტაქტო დეტალების ფლობა სასარგებლო შეიძლება იყოს რიგი მიზეზების გამო:

- **მიზანი:** კითხვების დასმა და ინფორმაციის მოპოვება ანგარიშგების მომზადების პროცესში.
- **მაგალითი:** გაერთიანებული სამეფოს დანაშაულის წინააღმდეგ ბრძოლის ეროვნულმა სააგენტომ (NCA) სპეციალური კრიპტო ქვედანაყოფი შექმნა, რომელიც უზრუნველყოფს რთულ საქმეებზე კონსულტაციებს. ასევე სამართალდამცავ სტრუქტურებში ვირტუალური აქტივების საკითხებზე შიდა ორგანიზაციული თანამშრომლობის ჩამოყალიბებისთვის შთაგონების წყარო შეიძლება იყოს ევროსაბჭოს მიერ, 2023 წელს მომზადებული „ტიპოლოგიების ანგარიში“.[18]

საერთაშორისო მხარდაჭერა

ევროპოლის პლატფორმა ექსპერტებისთვის (Europol Platform For Experts - EPE):

- **აღწერა:** ეს არის უფასო პლატფორმა LEA-ს წევრებისთვის ვირტუალურ აქტივებზე მუშაობისას, პრაქტიკული დახმარების მისაღებად.
- **მოთხოვნებთან შესაბამისობა:** EPE-ში მონაწილეობის უფლების მოსაპოვებლად (https://epe.europol.europa.eu/), ქვეყანა ევროკავშირის წევრი, ან ე.წ. ოპერატიული შეთანხმების ნაწილი უნდა იყოს.[19]
- **უპირატესობები:** ვირტუალური აქტივების გამოძიებისათვის EPE საუკეთესო პრაქტიკას გთავაზობთ. ის უზრუნველყოფს წვდომას ვებინარებზე, ასევე დაინტერესებული მხარეების საკონტაქტო ინფორმაციასა, კონფერენციებსა თუ სხვა სასწავლო რესურსებზე.
- **შეერთების პროცესი:** თუ ეუთო-ს წევრი სახელმწიფო, ბუდაპეშტის მემორანდუმის საოპერაციო შეთანხმების[20] მონაწილეა (სია მოცემულია ცალკე), მას შეუძლია გააკეთოს წვდომაზე განაცხადი.
- **პროცესში ჩართვა:** სამუშაოს ელ.ფოსტის მისამართის გამოყენებით დაუკავშირდით უფლებამოსილ ორგანოს მისამართზე o3@ europol.europa.eu
  - მიუთითეთ, თუ რა გაკავშირებთ ვირტუალურ აქტივებთან და რა სარგებელს მოუტანს თქვენი ცოდნა სხვებს.
  - ნათლად მიუთითეთ გაწევრიანების კონკრეტული , ვირტუალურ აქტივებთან დაკავშირებული მიზეზი.
- **ვინ შეიძლება შეუერთდეს:** მიუხედავად იმისა, რომ პლატფორმა პირველ რიგში სამართალდამცავი უწყებების წარმომადგენლებისთვის არის განკუთვნილი, მასში გაწევრიანებაზე განაცხადის შეტანა შეუძლიათ ამ წრის გარეთ მყოფ ექსპერტებსაც — როგორც საჯარო, ისე კერძო სექტორიდან. თუმცა, არასამართალდამცავი

18 გადახედეთ „საქმეთა ბოქსების“ (Case Boxes) ევროპის საბჭოს MONEYVAL-ის მიერ 2023 წელს გამოქვეყნებულ ანგარიშს — „ტიპოლოგიების ანგარიში: ფულის გათეთრებისა და ტერორიზმის დაფინანსების რისკები ვირტუალურ აქტივებთან დაკავშირებულ სამყაროში“ https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 (შემოწმდა 25 თებ. 2024).

19 ხელშეკრულებები/სამუშაო შეთანხმებები. ევროპოლი. https://www.europol.europa.eu/partners-collaboration/agreements (შემოწმდა 26 ნოემბ. 2023).

20 ხელშეკრულებები/სამუშაო შეთანხმებები. ევროპოლი. https://www.europol.europa.eu/partners-collaboration/agreements (შემოწმდა 26 ნოემბ. 2023).

პროფესიონალებისთვის ხელმისაწვდომი ინფორმაციის მოცულობა შეიძლება შეზღუდული იყოს.

- ღირებულება: წვდომა სრულიად უფასოა.

- 2019 წლის ოქტომბერში ევროპოლმა ორი საგანმანათლებლო თამაში, სახელწოდებით „კრიპტოპოლი“ წამოიწყო. ისინი რამდენჯერმე განახლდა და მოიცავს სხვადასხვა კრიპტოვალუტას. ევროკავშირის წევრი ქვეყნების სამართალდამცავი უწყებების წარმომადგენლებისთვის ისინი დღემდე უფასოა. იხილეთ: o3@europol.europa.eu.

ინტერპოლის ფინანსური დანაშაულის და ანტიკორუფციული ცენტრი (IFCACC)

ინტერპოლის ფინანსური დანაშაულის და ანტიკორუფციული ცენტრი (IFCACC): ეს არის ცენტრი, რომელიც გლობალური ფინანსური სისტემების დაცვის მიზნით ტრანსნაციონალური ფინანსური დანაშაულის წინააღმდეგ ბრძოლას ემსახურება.

მოთხოვნებთან შესაბამისობა: გლობალიზებული ფინანსური დანაშაულების მზარდი საფრთხის საპასუხოდ, INTERPOL-მა შექმნა IFCACC — ერთიანი მექანიზმი ამ გამოწვევებთან ბრძოლის მხარდასაჭერად. ინიციატივა სცდება მხოლოდ სამართალდამცავი უწყებების ჩართულობას და ასევე აქტუალურია საერთაშორისო ორგანიზაციებისა და სხვა დაინტერესებული მხარეებისთვის.

სარგებელი: IFCACC ხელშეწყობით ხორციელდება:

- თაღლითობის, გადახდის დანაშაულისა და საზღვრისპირა საქმეების გამოძიებაში სამართალდამცავი ორგანოების მხარდაჭერა.
- ანტიკორუფციული პრაქტიკის ზედამხედველობა — სპორტთან დაკავშირებული საქმეებიდან დაწყებული, მაღალი დონის პოლიტიკური უთანხმოებებით დამთავრებული.

შეერთების პროცესი: ვინაიდან, IFCACC ფუნქციონირებს უწყებათაშორისი თანამშრომლობის მოდელზე დაყრდნობით, პოტენციური თანამშრომლობა მოიცავს შემდეგს:

- კონტაქტის დამყარება ინტერპოლის გენერალურ სამდივნოს, ან ინტერპოლის ეროვნულ ცენტრალურ ბიუროსთან, რომელიც სახელმწიფოს იუსტიციის სამინისტროს და მის სასამართლო პოლიციას ექვემდებარება.
- ფინანსურ დანაშაულთან და კორუფციასთან ბრძოლის მიზნების მკაფიო თანხვედრის დემონსტრირება
- თანამშრომლობის ან საჭიროებების პოტენციური სფეროების გამოკვეთა.

ვის შეუძლია შეერთდეს: სამართალდამცავ ორგანოებს, დამატებით - ფინანსურ ინსტიტუტებს, საერთაშორისო ორგანიზაციებს და კერძო სექტორის წარმომადგენლებს. თუმცა, თანამშრომლობის დონე შეიძლება ასოციაციის ხასიათისა და მიზნის შესაბამისად განსხვავდებოდეს.

ღირებულება: რადგან ინტერპოლი საერთაშორისო ორგანიზაციაა, მის გენერალურ სამდივნოსთან თანამშრომლობა უფასოა.

IFCACC-ისა და I-GRIP-ის შესახებ დამატებით მიმართეთ:

- IFCACC@interpol.int
- IGRIP@interpol.int

დამატებით, ვირტუალური აქტივების ტექნიკურ საკითხებზე, სამართალდამცავი ორგანოების წარმომადგენლებს შეუძლიათ მიმართონ მისამართზე: innovation@interpol.int

დამატებითი რესურსი: სამართალდამცავი ორგანოების წარმომადგენლებს შეუძლიათ მოითხოვონ ინტერპოლის სახელმძღვანელო ვირტუალური აქტივების ჩამორთმევის შესახებ: vaguidelines@interpol.int

ვირტუალური აქტივების გამოყენებით ჩადენილი კიბერდანაშაულისა და ფულის გათეთრების წინააღმდეგ ბრძოლის UNODC-ის პროგრამები და გამოძიების სემინარები

მიმოხილვა:

გაეროს ნარკოტიკებისა და დანაშაულის ოფისის (UNODC) ჯგუფის ხელმძღვანელობით, ეს ყოვლისმომცველი სემინარების სერია ვირტუალური აქტივების, ფინანსური დანაშაულისა და შესაბამისობის ძირითადი სფეროს სიღრმისეულ შესწავლას გთავაზობთ. სასწავლო პროგრამა დაყოფილია საბაზისო, ძირითად და კასკადურ სესიებად, და მოიაზრება როგორც „ტრენერთა მომზადება“, რომელიც მიზნად ისახავს ინდუსტრიის საუკეთესო გამოცდილებების გავრცელებას. სემინარები აერთიანებს ღრმა თეორიულ საფუძველსა და პრაქტიკულ დავალებებს. საბოლოოდ სამართალდამცავი უწყებების წარმომადგენლები ვირტუალური აქტივების თვალთვალის, გამოძიებისა და ოსტატურად მართვის ეფექტური უნარებით აღიჭურვებიან.

მოთხოვნებთან შესაბამისობა: ეს სპეციალიზებული სწავლება განკუთვნილია სხვადასხვა სექტორის პროფესიონალებისთვის, როგორიცაა სამართალდამცავი ორგანოები, ფინანსური ინსტიტუტები, ტექნოლოგიური საწარმოები და საგანმანათლებლო სფეროები. ის წარმოადგენს ფასდაუდებელ რესურსს მარეგულირებლებისთვის, გამომძიებლებისა და ყველა პროფესიონალისთვის, რომლებსაც სურთ, ვირტუალური აქტივების სირთულეებში, ბლოკჩეინის დინამიკასა და ფინანსურ დანაშაულთან ბრძოლის ხელოვნებაში გაერკვნენ.

ძირითადი მიმართულებები:

- ვირტუალური აქტივების საფუძვლები: ჩაუღრმავდით მუდმივად განვითარებადი ვირტუალური აქტივებისა და მათი საყრდენი ტექნოლოგიების გენეზისს, ევოლუციას და რთულ ასპექტებს.
- **ტრანზაქციის დინამიკა:** გაშიფრეთ ბლოკჩეინში ტრანზაქციების სასიცოცხლო ციკლი, დაწყებიდან კულმინაციამდე.
- **ბლოკჩეინი სიღრმისეულად:** გამოავლინეთ ბლოკჩეინზე ტრანზაქციების აღრიცხვის, რატიფიცირებისა და დაარქივების პროცესები
- **ბლოკჩეინ კრიმინალისტიკა:** შეიძინეთ კვალიფიციური ცოდნა რეალურ დროში ტრანზაქციების თვალთვალისა თუ ბოროტმოქმედების მიერ საკუთარი ვინაობის დასაფარად გამოყენებული სქემების შესახებ.
- **AML/CTF ტაქტიკა:** შეისწავლეთ, როგორ დააკორექტიროთ ფულის გათეთრებისა და ტერორიზმის დაფინანსების საწინააღმდეგო პროტოკოლები ვირტუალური აქტივების დინამიურად ცვალებად რეალობასთან შესაბამისობაში.

- **რისკების მართვა:** მონაწილეებისთვის ვირტუალურ აქტივებთან დაკავშირებული სპეციფიკური რისკების შემცირების ოქროს სტანდარტების გაცნობა.
- **აქტივების ზედამხედველობა:** მონაწილეებისთვის ვირტუალური აქტივების მოკვლევის პროცესში კონფისკაციისა და მართვის სწორი მეთოდების საუკეთესო გამოცდილების გაზიარება

სწავლებაზე მიღების ნაბიჯები:

პოტენციურ მონაწილეებს შეუძლიათ:

- გაეცნონ მომავალი სემინარების განრიგს და დროულად დაჯავშნონ ადგილი.
- მითითებული ფორმის საშუალებით გადაამოწმონ პროფესიული სტატუსიდან გამომდინარე სწავლის საფასურზე შეღავათის მიღების შესაძლებლობა.
- ყურადღებით გაეცნონ და დაეთანხმონ ტრენინგში მონაწილეობის პირობებს.

მიზნობრივი აუდიტორია:

სემინარები მრავალფეროვანი აუდიტორიისთვის შემუშავდა: გამომძიებლები, იურისტები, ფინანსური რეგულირების ორგანოების პერსონალი, ტექნოლოგიური პიონერები, ჟურნალისტები და სხვა. განსაზღვრულია როგორც საჯარო, ასევე კერძო სექტორებისათვის - მათთვის, ვინც ვირტუალური აქტივებითა და მასთან დაკავშირებული ფისკალური ნორმებით არის დაინტერესებული.

მოსაკრებლის სტრუქტურა: მონაწილეთა რაოდენობის შესაბამისად, სასწავლო სესიის საფასური 10 000 აშშ დოლარიდან 20 000 აშშ დოლარამდე მერყეობს.

საჯარო სექტორის პირებისთვის, აკადემიური წრეებისთვის, არაკომერციული ორგანიზაციების და მედიის პერსონალისთვის, ხელმისაწვდომია შეღავათიანი ფასები.

ტრენინგის შინაარსის შესახებ დამატებითი ინფორმაციისთვის მიმართეთ UNODC-ის ვირტუალური აქტივების სწავლების სამმართველოს მისამართზე:cryptocurrency@unodc.org

დამატებითი შესაძლებლობები:
UNODC-ის ელექტრონული სწავლების პლატფორმა ნახეთ ბმულზე: https://www.unodc.org/elearning/en/courses/course-catalogue.html

ბაზელის მმართველობის ინსტიტუტი

ბაზელის მმართველობის ინსტიტუტი: ეს არის დამოუკიდებელი, არაკომერციული ორგანიზაცია, რომელიც ორიენტირებულია მმართველობის გაძლიერებასა და ფინანსური დანაშაულების წინააღმდეგ ბრძოლაზე მთელ მსოფლიოში. მისი სათაო ოფისი მდებარეობს ბაზელში, შვეიცარია. ასევე ოპერირებს სხვადასხვა აფრიკულ ქვეყანაში და მჭიდროდ თანამშრომლობს ბაზელის უნივერსიტეტთან.

ბაზელის ინსტიტუტის კრიპტოვალუტის სემინარი: გთავაზობთ ყოლისმომცველ 4-დღიან ვირტუალურ ტრენინგს, რომელიც განიხილავს კრიპტოვალუტების რაობას, ფინანსურ დანაშაულსა და ფულის გათეთრების საწინააღმდეგო (AML) რეგულაციებს. კურსი მოიცავს ფულის გათეთრების პრაქტიკულ სცენარს და მონაწილეებს აჩვენებს, თუ როგორ ხდება ბლოკჩეინ ტრანზაქციების თვალთვალი უკანონო აქტივობების გამოსავლენად.

მოთხოვნებთან შესაბამისობა: ღიაა სხვადასხვა სფეროს პროფესიონალებისთვის — სამართალდამცავი ორგანოების წარმომადგენლებისთვის, ფინანსური სექტორის სპეციალისტებისთვის, ბიზნესის წარმომადგენლებისთვის და სტუდენტებისთვისაც კი. სემინარის შინაარსი მორგებულია პოლიტიკის შემმუშავებლებისთვის, რეგულატორებისთვის, საგამოძიებო ჟურნალისტებისთვის და ყველა იმ პირისთვის, ვინც დაინტერესებულია ვირტუალური აქტივებით, ბლოკჩეინ ტექნოლოგიითა და ფინანსური დანაშაულის პრევენციით.

უპირატესობები: ბაზელის ინსტიტუტის სემინარი გვთავაზობს გაეცნოთ:

- **კრიპტოვალუტის საფუძვლები:** ვირტუალური აქტივების საფუძვლის, წარმოქმნის და მასშტაბის გააზრება, განაწილებული აღრიცხვის ტექნოლოგია და სხვა.
- **ტრანზაქციების მექანიკა:** ბიტკოინის ქსელის ფუნქციონირების მექანიზმი, კრიპტოგრაფია და ტრანზაქციების მართვა.
- **ბლოკჩეინი და მაინინგი:** ბლოკჩეინში ტრანზაქციების დაცვა, შენახვა და დადასტურება.
- **ბლოკჩეინის ანალიზი:** ტრანზაქციის რეალურ დროში მონიტორინგის, კრიმინალების მიერ ანონიმურობის თავიდან აცილების და ხელსაწყოების გამოყენების ტექნიკა.
- **კომპლექსური შეფასება:** გადახდის ახალ რეჟიმებთან AML/CTF პროგრამების ადაპტაცია.
- **რისკების მართვა:** ვირტუალური აქტივების რისკების მართვის საუკეთესო გამოცდილება და წყაროები.
- **აქტივების ჩამორთმევა:** კრიპტო აქტივების კონფისკაციის, საფულეების მართვის და ა.შ. პროცედურები და ნიუანსები.

ვის შეუძლია შეერთდეს:
კურსი გამომძიებლებისთვის, იურისტებისთვის, AML/CTF პროფესიონალებისთვის, ფინანსური დაზვერვის განყოფილების წევრებისთვის, FinTech პრაქტიკოსებისთვის, ჟურნალისტებისთვის და სხვ. არის განკუთვნილი. როგორც საჯარო, ისე კერძო სექტორის პირებისთვის, რომლებიც ვირტუალური აქტივებისა და ფინანსური დანაშაულის სამყაროში ნავიგაციით არიან დაინტერესებულნი.

ღირებულება: 750 შვეიცარიული ფრანკი ერთ მონაწილეზე. საჯარო სექტორის წარმომადგენლებისთვის, აკადემიური წრეების წევრებისთვის, არასამთავრობო ორგანიზაციებისა და ჟურნალისტებისთვის მოქმედებს შეღავათიანი ტარიფი – 300 შვეიცარიული ფრანკი.

დამატებითი ინფორმაციისთვის მიმართეთ : info@baselgovernance.org
კურსის დეტალები, რეგისტრაციის ბმულები და თარიღები გამოქვეყნებულია ბაზელის ინსტიტუტის სოციალური მედიის პლატფორმებზე.

ფინანსურ დანაშაულებთან მებრძოლთა გუნდი

სტოკჰოლმში დაფუძნებული ორგანიზაციაა. შეიქმნა გლობალური კოალიციის Digital Asset Task Force-ის ექსპერტების მიერ ფინანსურ დანაშაულთან ბრძოლის მიზნით. ფონდის მიზანია უზრუნველყოს სწრაფი და წყაროებზე დაყრდნობილი პასუხები ბლოკჩეინზე დაფუძნებული ფინანსებისა და Web3-თან დაკავშირებულ საკითხებზე. ფონდი გთავაზობთ უფასო ტოკენის რესურსს გენერაციული AI ასისტენტისთვის, რომელიც განკუთვნილია მხოლოდ საჯარო და კერძო სექტორში მომუშავე ფინანსური დანაშაულის წინააღმდეგ მებრძოლი პირებისთვის. გუნდი მუდმივად განაახლებს ანგარიშებს, მათ შორის საჯაროდ ხელმისაწვდომ მასალებს, რომლებიც ეუთო-ს მიერ არის გამოქვეყნებული. ახალი სამართლებრივი ცვლილებების შესახებ რეგულაციების ძებნა შესაძლებელია ChatGPT-ს მსგავსი ინტერფეისის მეშვეობით:

https://www.fincrimefighters.com/

შეტყობინების შემდგომი რეკომენდაციები სამართალდამცავებისთვის

რეკომენდაციები სამართალდამცავი ორგანოებისთვის ფინანსურ დანაშაულზე შეტყობინების შემდგომი რეაგირების მიზნით

- **დაუყოვნებელი მხარდაჭერა:** დარწმუნდით, რომ დაზარალებულებს დაუყოვნებლივ განემარტათ თუ როგორ დაიცვან დარჩენილი ციფრული აქტივები და შეამცირონ შემდგომი ფინანსური დანაკარგების რისკი. ეს შეიძლება მოიცავდეს რეკომენდაციებს, თუ როგორ შეცვალონ პაროლები, დაიცვან საფულეები ან გადაიტანონ აქტივები უფრო უსაფრთხო პლატფორმაზე.
- **ფინანსური კონსულტაცია:** დააკავშირეთ მსხვერპლები ფინანსური კონსულტაციის სერვისებთან, რომლებიც მათ დანაკარგების, სავარაუდო საგადასახადო შედეგებისა და დროთა განმავლობაში დანაკარგების აღდგენის ან შემცირების სტრატეგიების გააზრებაში დაეხმარება.
- **სწავლება:** ჩაატარეთ საინფორმაციო კამპანიები და სამუშაო სემინარები მსგავსი თაღლითობების შესახებ. რაც უფრო ინფორმირებულია საზოგადოება, მით უფრო რთული ხდება თაღლითებისთვის პოტენციური ინვესტორების მოტყუება.
- **ბირჟებთან თანამშრომლობა:** მჭირდოდ ითანამშრომეთ კრიპტოვალუტის ბირჟებთან თაღლითური აქტივების გამოვლენისა და მათი შესაძლო გაყინვის უზრუნველსაყოფად. ეს მნიშვნელოვნად გაართულებს უკანონო შემოსავლების განაღდების პროცესს.
- **საერთაშორისო თანამშრომლობა სხვადასხვა იურისდიქციებთან:** ციფრული თაღლითობების გლობალური ხასიათიდან გამომდინარე, ითანამშრომლეთ უცხოურ სამართალდამცავ ორგანოებთან დანაშაულის კვალის დასადგენად, დამნაშავეთა დასაკავებლად და სამართლებრივი რეაგირების უზრუნველსაყოფად.

მარიამ გრიგალაშვილი ერევანში გამართული სემინარის ფარგლებში საქართველოსა და საქართველოს ეროვნული ბანკის გამოცდილებასა და ცოდნას უზიარებს სომხეთის ეროვნული ბანკის თანამშრომლებს. სემინარზე განიხილებოდა კრიპტოვალუტის დაბეგვრისა და ფულის გათეთრებისა და ტერორიზმის წინააღმდეგ ბრძოლის პოლიტიკასთან მისი ურთიერთკავშირის საკითხები.

შეჯამება და ეუთო-სთან თანამშრომლობის პრინციპები

შეჯამება და ეუთო-სთან თანამშრომლობის პრინციპები

ეუთო-ს ინიციატივა ვირტუალური აქტივების მხარდაჭერისთვის

ვინ ვართ ჩვენ?

ეუთო-ს ვირტუალური აქტივების ექსპერტთა ჯგუფს გააჩნია უნიკალური შესაძლებლობა პასუხი გასცეს პოლიტიკოსებსა და სამართალდამცავ ორგანოებს ვირტუალური აქტივების მზარდი გამოწვევების შესახებ. ტექნიკური ექსპერტიზის სფეროში თითქმის ორმოცდაათწლიან გამოცდილებაზე დაყრდნობით, ეუთო-ს 57 წევრი ქვეყნის პოლიტიკოსებსა და სამართალდამცავ ორგანოებს ვეხმარებით ვირტუალურ აქტივებთან დაკავშირებული სირთულეების მართვაში.

ღირებულება, რომელსაც ვქმნით სამართალდამცავი უწყებებისა და პოლიტიკის შემმუშავებლებისთვის:

- **ინოვაციური ცოდნა:** ჩვენი ტრენინგები სამართალდამცავ ორგანოებსა და პოლიტიკოსებს უახლესი ცოდნითა და სტრატეგიებით აიარაღებს, რომლებიც ვირტუალური აქტივების სფეროს უნიკალური გამოწვევების გადასაწყვეტადაა შემუშავებული.
- **მუშაობის ეფექტურობა:** პრაქტიკული სწავლების პარალელურად, ჩვენ ვუზრუნველყოფთ ლოგისტიკურ მხარდაჭერას: ვჯავშნით ადგილებს, ვიწვევთ ეუთო-ს წევრი ქვეყნებიდან ვირტუალური აქტივების სფეროს წინასწარ შერჩეულ ექსპერტებს, ვამზადებთ დღის წესრიგს და სასწავლო მიზნებს.
- **სწავლება და კვალიფიკაციის ამაღლება:** ჩვენ გთავაზობთ ვირტუალური აქტივების ყოვლისმომცველ სასწავლო პროგრამებს. ჩვენი გუნდი შედგება პოლიტიკის შემმუშავებლებისგან, სამართალდამცავი უწყებების წარმომადგენლებისგან, ტრადიციული ბანკების შესაბამისობის სპეციალისტებისა და WEB3 სექტორის პროფესიონალებისგან. გუნდი აქცენტს აკეთებს პრაქტიკულ სწავლებაზე — შეზღუდული, მაგრამ შინაარსიანი თეორიული კომპონენტის თანხლებით. ძირითადი ყურადღება ეთმობა პრაქტიკულ სავარჯიშოებს, რაც უზრუნველყოფს ცოდნის რეალურ გარემოში გამოყენებას. აღსანიშნავია, რომ წარსულში ტრენინგის მონაწილეებმა მიაღწიეს რეალურ შედეგებს — მათ შორის, წარმატებით გამოიძიეს ფულის გათეთრების რთული საქმეები.
- **რესურსებით უზრუნველყოფა**: ჩვენ ვთანამშრომლობთ ბლოკჩეინის სფეროს წამყვან ექსპერტებთან, რათა მონაწილეებს ჰქონდეთ წვდომა პროფესიულ ინსტრუმენტებზე დაფუძნებულ პრაქტიკულ გამოცდილებაზე. ეს ხელს უწყობს ცოდნის ეფექტურ დანერგვას სიღრმისეულ სესიებსა და სამუშაო სემინარებში, სადაც რთულ ტექნოლოგიურ პროცესებს სავარჯიშოების სახეს ვაძლევთ.
- **საქმეების ანალიზი**: ჩვენი ტრენინგი ხშირად მოიცავს რეალურ დროში მიმდინარე კონკრეტული შემთხვევების ანალიზსა და შესაბამის საკანონმდებლო მხარდაჭერას. ეს მეთოდი თვალნათლივ წარმოაჩენს მიმდინარე მოვლენებს, რაც უზრუნველყოფს პრობლემების მოგვარებას მანამდე, სანამ ისინი რეალურად მოხდება.
- **მასშტაბურობა და მდგრადობა:** ჩვენი კასკადური ტრენინგის სისტემა მოიცავს „ტრენერთა ტრენინგის“ მოდელს, რომლის ფარგლებშიც ექსპერტები იძენენ ცოდნასა და უნარებს, რათა თავიანთ იურისდიქციებში ცოდნის გავრცელება დამოუკიდებლად გააგრძელონ. ეს უზრუნველყოფს ცოდნის ფართო გავრცელებასა და კვალიფიკაციის განვითარების მდგრადობას ადგილობრივ დონეზე.
- **უსაფრთხო ციფრული გარემოს შექმნა:** პოლიტიკის შემქმნელების და სამართალდამცავების ვირტუალურ აქტივებთან მუშაობის უნარების გაძლიერებით, ჩვენ მნიშვნელოვანი წვლილი შეგვაქვს უსაფრთხო და გამჭვირვალე ციფრული საფინანსო ეკოსისტემის ჩამოყალიბებაში.

შემოგვიერთდით კიბერუსაფრთხოების მომავლის ფორმირებასა და ყველასთვის უსაფრთხო, უფრო გამჭვირვალე ციფრული სივრცის უზრუნველსაყოფად.
დაგვიკავშირდით მისამართზე:
VirtualAssets@osce.org

დამატებითი საკითხავის მოკლე ჩამონათვალი

დამატებითი საკითხავის მცირე ჩამონათვალი

გაეროს ნარკოტიკებისა და დანაშაულის წინააღმდეგ ბრძოლის ოფისი (UNODC)

ვირტუალური ვალუტების გამოყენებით ჩადენილი დანაშაულის შედეგად მიღებული შემოსავლების გათეთრების გამოვლენისა და გამოძიების ძირითადი სახელმძღვანელო (2014)

მიუხედავად იმისა, რომ ეს დოკუმენტი UNODC-ის მიერ ათზე მეტი წლის წინ, 2014 წელს გამოქვეყნდა, ის კვლავაც წარმოადგენს ღრმა და საფუძვლიან ანალიზს. 200-გვერდიანი მასალა დეტალურად განიხილავს სხვადასხვა ტერმინს და სთავაზობს მკითხველს კონტექსტს ამ მიმოხილვაში ნახსენები ცნებების გასაგებად. დოკუმენტში ასევე მოცემულია თვითშეფასების დეტალური კითხვარები.
https://www.unodc.org/documents/middleeastandnorthafrica/money-laundering/FULL10-UNODCVirtualCurrencies-final.pdf.pdf

ევროპის უსაფრთხოებისა და თანამშრომლობის ორგანიზაცია (OSCE)

სისხლისსამართლებრივ პროცესში ვირტუალურ ვალუტებთან ურთიერთობის სახელმძღვანელო (2022)
https://www.osce.org/files/f/documents/2/0/522754.pdf

აშშ-ს იუსტიციის დეპარტამენტი (U.S. Department of Justice)

სამართალდამცავი ორგანოების როლი ციფრულ აქტივებთან დაკავშირებული დანაშაულებრივი საქმიანობის გამოვლენაში, გამოძიებასა და სისხლისსამართლებრივი დევნის განხორციელებაში (2022)
https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf

ეს ანგარიში გამოქვეყნებულია აშშ-ს იუსტიციის დეპარტამენტის მიერ და წარმოადგენს დამატებას ანგარიშზე „საერთაშორისო სამართალდამცავი თანამშრომლობა“ (International Law Enforcement Cooperation Report). პარალელურად განაახლებს „კრიპტოვალუტის სამართალდამცავ ჩარჩოს“ (Cryptocurrency Enforcement Framework). დოკუმენტი გთავაზობთ ყოვლისმომცველ მიმოხილვას და განკუთვნილია შემდგომი გამოყენებისთვის.

ავტორის შესახებ

ეს მიმოხილვა მომზადებულია ვირტუალური აქტივების წამყვანი ექსპერტის მიხალ გრომეკის მიერ. ის მონაწილეობს ეუთო-ს პროექტში, რომელიც მიზნად ისახავს ვირტუალურ აქტივებსა და კრიპტოვალუტებთან დაკავშირებული ფულის გათეთრების რისკების შემცირებას. აღნიშნული ინიციატივა ხორციელდება ეუთო-ს ეკონომიკური და გარემოსდაცვითი საქმიანობის კოორდინატორის ოფისის (OCEEA) ფარგლებში.

გრომეკი არის სტოკჰოლმში დაფუძნებული, ვირტუალური აქტივების მომსახურების პროვაიდერის (VASP) — Safello-ს (ეს არის პროვაიდერი, Nasdaq-ზე ვაჭრობის უფლებით) — ყოფილი შესაბამისობის ხელმძღვანელი (Chief Compliance Officer).

ის ციფრული აქტივების ფინანსურ დანაშაულთან ბრძოლისთვის შექმნილი გლობალური კოალიციის სამუშაო ჯგუფს თავმჯდომარეობს— ეს კოალიცია Europol-ის, მსოფლიო ეკონომიკური ფორუმისა და ლონდონის საფონდო ბირჟის საფრთხეების ანალიტიკის განყოფილების ერთობლივი ინიციატივით შეიქმნა. გრომეკი ამავე კოალიციის აღმასრულებელი გუნდის წევრიცაა.

გარდა ამისა, ის აგრძელებს ტრენინგების ჩატარებას სახელმწიფო სტრუქტურებისა და სამართალდამცავი უწყებებისათვის, მონაწილეობს საკანონმდებლო ჩარჩოების ჩამოყალიბებაში, რათა ეუთო-ს წევრმა ქვეყნებმა არსებულ გამოწვევებზე დროული რეაგირება შეძლონ.

გრომეკმა გამოცდილება შეიძინა ფინტექ სექტორში ხელმძღვანელ პოზიციებზე მუშაობით, ასევე — როგორც სტოკჰოლმის ეკონომიკის სკოლის Executive Education განყოფილების პროგრამის დირექტორმა. ის ათ წელზე მეტია საქმიანობს ფინტექისა და ვირტუალური აქტივების შესაბამისობის (compliance) მიმართულებით. მისი ნაშრომები გამოქვეყნებულია Forbes.com-ზე, ასევე არაერთ წიგნსა და სამეცნიერო ჟურნალში.

მადლიერება

ამ სახელმძღვანელოს მნიშვნელოვანი გაუმჯობესება შესაძლებელი გახდა დოქტორ ალექსანდრა ანდჰოვის მიერ განხორციელებული რეცენზირებისა და შეტანილი წვლილის შედეგად. მისმა იურიდიულმა კომპეტენციამ და ხედვებმა მნიშვნელოვნად გააუმჯობესა სახელმძღვანელოს შინაარსის სიზუსტე, აქტუალობა და სიღრმე. კოპენჰაგენის უნივერსიტეტის იურიდიული ფაკულტეტის ასოცირებული პროფესორის გამოცდილებაზე დაყრდნობით, დოქტორმა ანდჰოვმა დოკუმენტზე მუშაობის პროცესში უზრუნველყო ფასდაუდებელი შეფასებები და რეკომენდაციები. ის გამოირჩევა სამართლისა და ტექნოლოგიის სფეროების ერთობლივი კომპეტენციით და ჩართულია არაერთ მნიშვნელოვან პროექტში, განსაკუთრებით Financial Crime Fighters-ის თანადამფუძნებლისა და იურიდიული დირექტორის რანგში.

დოკუმენტის წაკითხვადობისა და ხარისხის მაქსიმალურად უზრუნველსაყოფად, ტექსტის რედაქტირებაში მონაწილეობა მიიღო რამდენიმე ადამიანმა, მათ შორის წამყვანი როლი შეასრულა გრეის მარშალმა, რომელმაც უზრუნველყო სიცხადე და შინაარსობრივი თანმიმდევრობა მთელ პუბლიკაციაში. როგორც გლობალური კოალიციის ფინანსურ დანაშაულთან ბრძოლის გენერალური მდივანმა, მან შეითავსა ინფორმაციის ფართო აუდიტორიაზე მორგების პასუხისმგებლობა.

გრეის მარშალის გარდა, დოკუმენტის შეფასებასა და რედაქტირებას დიდი დრო დაუთმო და პროცესში თავისი ფართო პროფესიული გამოცდილება გამოიყენა დენის რუდიჩმა. მისი ხედვები შინაარსსა და ენობრივ ფორმულირებებზე უმნიშვნელოვანესი აღმოჩნდა.

დამატებითი სარედაქციო მხარდაჭერა უზრუნველყვეს გრეტა ბარკაუსკიენემ, ემილია პახომოვმა, სუნგიონგ კანგმა და ვენსან დანჟანმა. ასევე, ტექსტის დამატებითი გადახედვა და რედაქციული რეკომენდაციები მომზადდა ინტერპოლის ფინანსური დანაშაულისა და კორუფციის საწინააღმდეგო ცენტრის (IFCACC) მხრიდან, განსაკუთრებით — მონა ჰესეინის მიერ, და ევროპის კიბერდანაშაულის ცენტრის (EC3) წევრების მხრიდან, კერძოდ — გერტ იან ვან ჰარდეველდის მიერ.

ეუთო-ს ეკონომიკური და გარემოსდაცვითი საქმიანობის ოფისი (OCEEA) ყველა მონაწილეს მადლობას უხდის მხარდაჭერისთვის.

დიდ მადლობას ვუცხადებთ ლატვიის საფინანსო დაზვერვის სამსახურს ვირტუალური აქტივების თემატიკაზე ბალტიისპირეთში შემსწავლელი ვიზიტის ფარგლებში ეკოსისტემის ლიდერების იდენტიფიცირებასა და შერჩევაში გადამწყვეტი როლის შესრულებისთვის. ასევე განსაკუთრებულ მადლობას ვუხდით პოლონეთის ფინანსთა სამინისტროს, რომელმაც შეუფერხებლად უზრუნველყო ტრენინგის ინფრასტრუქტურული მხარდაჭერა. დამატებით, ღრმა მადლიერებას გამოვთქვამთ იმ მრავალფეროვანი სექტორების წარმომადგენელი ინსტიტუტებისა და პირების მიმართ, რომელთა წვლილიც ფასდაუდებელი იყო პროექტის წარმატებით მიმდინარეობისთვის.

შენიშვნები

ევროპის უსაფრთხოებისა და
თანამშრომლობის ოფისი

OSCE-ს სამდივნო
ეუთო-ს ეკონომიკური და
გარემოსდაცვითი საქმიანობის
კოორდინატორის ოფისი
ეკონომიკური მართვის განყოფილება
Wallnerstrasse 6
1010 Vienna, Austria
ელ-ფოსტა: virtualassets@osce.org
www.osce.org/eea