Kripto Cinayətlərin Açılması

Hüquq-mühafizə Orqanları üçün Bələdçi

OSCE Organization for Security and Co-operation in Europe

Məsuliyyətdən imtina

Hazırki nəşr müəllifin təqdim etdiyi orijinal materialdan hazırlanmışdır. O, ATƏT-in redaksiya heyəti tərəfindən redaktə olunmayıb. İfadə olunan fikirlər müəllifin məsuliyyətidir və mütləq şəkildə nə ATƏT-in, nə Missiyaların, nə də onun iştirakçı dövlətlərinin fikirlərini əks etdirmir.

ATƏT, onun missiyaları və iştirakçı dövlətlər bu nəşrin istifadəsindən irəli gələ biləcək hər hansı nəticələrə görə məsuliyyət daşımır. Bu nəşr hər hansı bir şəxsin hərəkət və ya hərəkətsizliyinə görə hüquqi və ya digər məsuliyyətlə bağlı suallara toxunmur. Bu nəşrdə konkret ölkələrin və ya ərazilərin qeyd edilməsi və ya istinad edilməsi ATƏT-in onların hüquqi statusu, idarəetmə orqanları, təsisatları və ya sərhədlərinin müəyyən edilməsi ilə bağlı hər hansı mövqeyini ifadə etmir.

Kripto Cinayətlərin Açılması

Hüquq-mühafizə Orqanları üçün bələdçi

Organization for Security and Co-operation in Europe

Mündəricat

Akronimlər, qısaltmalar və izahı ilə əsas anlayışları

5-ci ÇPY (AML) Direktivası	Maliyyə sistemindən çirkli pulların yuyulması və ya terrorizmin maliyyələşdirilməsi məqsədləri üçün istifadəsinin qarşısının alınmasına dair (Aİ) 2015/849 sayı və və 2009/138/EC və 2013/36/EU Direktivlərinə dəyişiklik edən Avropa Parlamentinin və Şuranın 30 may 2018-ci il tarixli 2018/843 saylı Direktivi (Aİ), (EEA uyğunluğu olan mətn). Bu direktiv kripto aktivlərinin əhatə dairəsinə genişləndirdi. 10 yanvar 2020-ci ilə qədər Üzv Dövlətlər bu direktivə əməl etmək üçün tələb olunan qanun və qaydaları tətbiq etməlidirlər.
ÇPY (AML)	Çirkli pulların yuyulmasına qarşı mübarizə – Cinayətkarların qeyri-qanuni yolla əldə edilmiş vəsaitləri qanuni gəlir kimi gizlətməsinin qarşısını almaq məqsədi daşıyan qanunlara, qaydalaravə prosedurlara istinad edir.
KAXP (CASP)	Kripto aktivlərin xidmət təminatçıları – ictimaiyyətə kripto aktivləri ilə bağlı xidmətlər təklif edən qurumlar. Digərləri ilə birlikdə bu xidmətlər adı aşağıda keçən geniş spektrli fəaliyyətləri əhatə edə bilər: 1. Mübadilə Xidmətləri: FIAT pulları və ya digər kripto aktivləri üçün kripto aktivlərin alqı-satqısını asanlaşdırmaq. 2. Pul kisəi xidməti təminatçıları: Kripto aktivləri saxlamaq, idarə etmək və köçürmək üçün kastodial və ya qeyri-kastodial pul kisələri təklif edir. 3. Köçürmə Xidmətləri: Kripto aktivlərin bir ünvandan və ya hesabdan digərinə köçürülməsini təmin edir. 4. Maliyyə Məsləhəti: Kripto aktivlərin alınması, satışı və ya saxlanması ilə bağlı məsləhətlərin verilməsi. 5. Saxlama Xidmətləri: Müştərilər adından kripto aktivlərinin saxlanması və mühafizəsi. (Ətraflı məlumat üçün s. 20-ə baxın)
AŞ	Avropa Şurası – Avropada insan haqları, demokratiya və qanunun aliliyinin qorunmasına həsr olunmuş beynəlxalq təşkilat.
TMM (CTF)	Terrorçuluqla mübarizənin maliyyələşdirilməsi – Terror fəaliyyətinin maliyyələşdirilməsinin qarşısını almaq üçün siyasət və tədbirlər. O, həm qanuni, həm də qeyri-qanuni mənbələrdən terror aktları törətmək niyyətində olan qruplara pul axınını aşkar edib dayandırmağa çalışır.
ERC20 Tokens	20 Token üçün Ethereum sorğusu şərhi – Ethereum blokçeynində ağıllı müqavilələrin yaradılması və verilməsi üçün 2015-ci ildən tətbiq edilən texniki standartdır.
Aİ	Avropa İttifaqı – Avropada yerləşən 27 Avropa ölkəsinin siyasi və iqtisadi birliyidir.
EPE	Mütəxəssislər üçün Avropol (Europol) Platforması – Avropol hüquq-mühafizə orqanlarının ekspertlərinin cinayətlə bağlı bilikləri, qabaqcıl təcrübələri və şəxsi olmayan məlumatları bölüşmək üçün aparıcı məkandır.
AVROPOL (EUROPOL)	Avropa İttifaqının Hüquq Mühafizə Orqanları üzrə Əməkdaşlıq Agentliyi –Avropa İttifaqının üzv dövlətlərinə ciddi beynəlxalq cinayət və terrorizmlə mübarizədə kömək edən hüquq-mühafizə orqanı.
FATF	Maliyyə Fəaliyyəti üzrə İş Qrupu - çirkli pulların yuyulması və terrorizmin maliyyələşdirilməsi ilə mübarizə siyasətini inkişaf etdirmək üçün standartların inkişaf etdirilməsi üzrə hökumətlərarası orqan.

FinCEN	Maliyyə Cinayətləri ilə Mübarizə Şəbəkəsi – ABŞ Xəzinədarlıq Departamentinin maliyyə əməliyyatları haqqında məlumatları toplayan və təhlil edən bürosu.
MKB (FIU)	Maliyyə Kəşviyyat Bürosu - Çirkli pulların yuyulması və terrorizmin maliyyələşdirilməsində şübhəli bilinən fəaliyyətlərə dair maliyyə və kəşfiyyat məlumatlarının toplanması, təhlili və yayılmasına cavabdeh olan dövlət qurumu.
İP	İnternet protokolu – İnternet və ya digər şəbəkələr üzərindən göndərilən məlumatların formatını tənzimləyən qaydalar toplusu.
HMOM (LER)	Hüquq-mühafizə orqanlarına müraciət - Hüquq-mühafizə orqanları tərəfindən araşdırmalar üçün şirkətlərə və ya şəxslərə ünvanlanan edilən sorğu.
MiCA	Kriptoaktivlər bazarlarına dair Avropa Parlamentinin və Şurasının 31 may 2023-cü il tarixli 2023/1114 saylı Qaydası (Aİ) və 1093/2010 və (Aİ) № 1095/2010 və 2013/36/EU2 (319/EU) Direktivlərinə düzəlişlər. Bu, kripto aktivlərini tənzimləyən yeni AB Qaydasıdır. 30 dekabr 2024-cü il tarixindən qüvvəyə minəcək.
ÇPY	Çirkli pulların yuyulması – Cinayət fəaliyyəti nəticəsində əldə edilən külli miqdarda pulun qanuni mənbələrdən gəldiyi təsəvvürünü yaradan qeyri-qanuni proses.
MultiSig Wallet	Çox imzalı kriptovalyuta pul kisəsi – Əməliyyata icazə vermək üçün çoxlu şəxsi açar tələb edən kriptovalyuta pul kisəsinin növü.
OCEEA	ATƏT-in Avropada Təhlükəsizlik və Əməkdaşlıq Təşkilatının İqtisadi və Ətraf Mühitin Mühafizəsi üzrə Koordinator Ofisi
ATƏT	Avropada Təhlükəsizlik və Əməkdaşlıq Təşkilatı – Avropada hərbi, siyasi, ekoloji və iqtisadi sahələr üzrə dialoqun və hərtərəfli əməkdaşlığın təşviqinə yönələn regional təhlükəsizlik təşkilatı.
OSINT	Açıq mənbə kəşfiyyatı – İstintaq kontekstində istifadə edilən, açıq mənbələrdən toplanmış məlumatlar.
BK (OTC)	Birjadan kənar – Mərkəzi birja və ya brokeri olan və ya olmayan iki tərəf arasında virtual aktivlərin qiymətli kağızlarının ticarəti.
UNODC	Birləşmiş Millətlər Təşkilatının Narkotiklər və Cinayətkarlıqla Mübarizə İdarəsi - Narkotiklər və cinayətlər haqqında məlumatların istehsalı və yayılmasına cavabdeh olan Birləşmiş Millətlər Təşkilatının tərkibində fəaliyyət göstərən ofis.
VAXT (VASP)	Virtual Aktivlərin Xidmət Təminatçısı – FATF tərəfindən virtual aktivlər üçün fəaliyyət və ya əməliyyatlar həyata keçirən qurumu ifadə etmək üçün təqdim edilmiş termin. (Əlavə məlumat üçün səh. 20-ə baxın.)
VŞŞ (VPN)	Virtual şəxsi şəbəkə – Şəxsin kompüteri ilə internet arasında daha az qorunan şəbəkə üzərindən təhlükəsiz əlaqə yaratmağa imkan verən texnologiya, hər zaman olmasada, bəzən istifadəçinin yerini gizlətmək üçün istifadə olunur.

Giriş sözü

Hazırki bələdçinin məqsədi

Bu sənəd hüquq-mühafizə orqanlarının (HMO) əməkdaşları, o cümlədən polis, prokurorlar, müvafiq agentlər, həmçinin kriptovalyutalar və digər virtual aktivlərlə yeni tanış olan vergi və məhkəmə ekspertizası mütəxəssisləri üçün hərtərəfli bələdçi rolunu oynayır. Bu, qarşısında kripto aktivlərlə bağlı cinayətləri araşdırmaq tapşırığı olanlar üçün tərtib olunmuşdur

Bələdçi saxtakarlıq və fırıldaqçılıq davranışının ən geniş yayılmış növlərinə diqqət yetirir, məsul şəxslər üçün ən yaxşı təcrübələri izah edir, atılacaq addımları və potensial qurbanlardan, xüsusən də yerli polis bölmələrində ilkin sübutların toplanması prosesi zamanı hansı məlumatların toplana biləcəyini izah edir.

Hazırki sənəd HMO əməkdaşları üçün bələdçi olmaq üçün yazılmış və hazırlanmışdır. Sənəd məqsədyönlü şəkildə fərdi qurbanlarla bağlı polis işlərində əhəmiyyət kəsb etməyən kriptovalyuta sahələrini əhatə etmir.

Bələdçi həmçinin məqsədli şəkildə hüquq-mühafizə orqanları ilə fiziki şəxslər arasında qarşılıqlı əlaqələrə diqqət yetirir. Maliyyə institutları və ya maliyyə kəşfiyyatı bölmələri (və ya oxşar idarələr) tərəfindən istifadə edilən SƏH (Şübhəli Əməliyyat Hesabatları) və ya SFH (Şübhəli Fəaliyyət Hesabatları) haqqında məlumat nəzərə alınmayıb.

Günümüzdə kriptovalyuta cinayətlərin açılması üsulları ilə əlaqədar bir çox məsələlər artıq müəyyən edilmişdir. Məsələn, məlumatların natamam toplanması səbəbindən müstəntiqlər kriptovalyuta pul kisəsinin ünvanı kimi məlumat toplamaq üçün zərərçəkənlə əlaqə saxlamalı olduqlarını bildirdilər, çünki bu olmadan istintaq mümkün deyil. Müstəntiqlər toplanacaq məlumatların dəyərini bilmədirlər. Bu baxımdan, lüzumsuz məlumat çox vaxt ləngimələrlə nəticələnir, çünki zərərçəkənlərin özləri hansı məlumatın hüquq-mühafizə orqanlarına aid olduğunu tam başa düşməyə bilərlər.

Bəhs olunan məlumat boşluğu sadəcə narahatlığa səbəb olmur; kriptovalyuta ilə əlaqədar istintaq təcrübəsinin daha aşağı sürətlə inkişaf etməsi texnologiyanın ilk gündən üstünlükləri mənimsəyən cinayətkarlar tərəfindən qlobal səviyyədə məharətlə istifadə olunur. Artmaqda olan çağırışlara cavab olaraq, biz HMO istintaqlarında və kriptovalyuta ilə bağlı cinayət barədə məlumat verən potensial qurbanlara dəstəkləyici tədbirləri və hərəkətləri paylaşan bu bələdçini hazırladıq.

Mövzunun mürəkkəbliyini və ATƏT-in iştirakçısı olan dövlətlərdə hüquqi çərçivələrin və təcrübələrin müxtəlifliyini dərk edərək, məqsədimiz hərtərəfli bələdçi deyil, vətəndaşlardan məlumatı alan HMO əməkdaşları üçün xüsusi olaraq istifadə edə biləcələri praktiki bacarıqlar təklif etməkdir. Xüsusilə ölkənin qüvvədə olan normativ bazası kriptovalyutaları əhatə etmirsə, bələdçi ən yaxşı təcrübələrin inkişafı barədə müzakirələrə təkan vermək üçün nəzərdə tutulub. Ən çox yayılmış saxtakarlıq təcrübələri günümüzə uyğun ümumiləşdirilmiş və mövzunun daha dərindən başa düşülməsini asanlaşdırmaq üçün giriş materialı təqdim edilmişdir.

Bu bələdçi HMO ilə daim dəyişən virtual aktivlər dünyası arasındakı boşluğu aradan qaldırmaq üçün mühüm körpu rolunu oynayır. Kriptovalyutaların fəaliyyət göstərdiyi Web3 məkanının sürətlə inkişaf etdiyini və bu təlimatın əlavə biliklərlə tamamlanmasını tələb edə biləcəyini nəzərə almaq lazımdır.

Hazırki sənəd yalnız effektiv istintaq üçün lazım olan alətləri və strategiyaları vurğulamır, həm də peşəkarlar arasında əməkdaşlığı və davamlı öyrənməni təşviq etmək məqsədi daşıyır.
Son məqsəd kriptovalyuta ilə bağlı cinayətlərin yaratdığı unikal problemlərlə mübarizə aparmaq üçün hüquq-mühafizə orqanları əməkdaşlarını lazımi bilik və inamla təchiz etməkdir.

Bələdçinin strukturu

Bu bələdçinin əsas məqsədi virtual aktivlərlə əlaqədar cinayətlər sahəsində yeni olan hüquq-mühafizə orqanları əməkdaşlarını maarifləndirmək və bu cür cinayətlər barədə məlumat verən zərərçəkənlərə dəstək olmaqdı. Bu məqsədi nəzərə alaraq, bələdçi aşağıdakı kimi qurulmuşdur:

Birincisi, rəqəmsal aktivlərin qısa icmalı təqdim olunur. Rəqəmsal aktivlər, Bitkoin (Bitcoin) və Etereum (Ethereum) kimi kriptovalyutalar kimi subyektləri əhatə edən böyük bir çətir termini kimi düşünülə bilər. Onların nə olduğu və bir-biri ilə oxşar və ya fərqli xüsusiyyətlərinə dair izahat veriləcəkdir.

Onların fərqləri və oxşarlıqları aydın başa düşülməsi üçün araşdırılacaq. Bundan əlavə, kriptovalyutaların potensial istifadəsi və sui-istifadəsi və onları dəstəkləyən texnologiya müzakirə olunacaq.

Virtual aktivlər haqqında təməl anlayışı qurduqdan sonra bələdçi onlarla əlaqəli ümumi cinayətləri təqdim edir. Daha sonra bu cinayətlərlə məşğul olmaq üçün standart protokolları təsvir edir, və onlar arasında tez həll oluna bilən və daha ətraflı araşdırma tələb edənləri müəyyənləşdirir.

Bələdçi həmçinin hər bir cinayət üçün sübutların toplanması, qurbanlara veriləcək suallar, virtual aktiv xidmət təminatçıları ilə paylaşılacaq məlumatları və virtual aktiv mübadiləsindən əldə edilə bilən məlumatları əhatə edir.

Əlçatanlıq və dilin sadələşdirilməsi: Sahənin mürəkkəbliyinə görə müəlliflər bu hesabatı yeni başlayanlar üçün əlçatan etmək üçün sadələşdirilmiş, texniki olmayan dildən istifadə etmişlər. Jarqonun qarşısını almaqla məqsəd məzmunun bütün oxucular üçün aydın və başa düşülən olmasını təmin etməkdir. Nəhayət, bələdçi cinayət qurbanlarına dəstək resurslarını təklif və kriptovalyuta ilə bağlı cinayətlərin qarşısını almağa kömək edə biləcək müxtəlif təkliflər təqdim edir.

Tarixçə

Kriptovalyuta aktivləri ətrafında aparılan istintaqlar, xüsusən aktivlərin bərpasının çətinliyi ilə bağlı yanlış təsəvvürləri nəzərə alsaq, əvvəlcə qorxuducu görünə bilər. Milli valyutanın Bitkoin kimi kriptovalyutaya çevrilməsindən sonra vəsaitlərin geri qaytarıla bilməyəcək şəkildə itirilməsi, qurbanların köməksiz qalması və müstəntiqləri öz işlərini bağlamağa məcbur etməsi mifdir. Bu təsəvvür bir neçə il əvvələ qədər dəqiq idi, lakin zaman artıq dəyişib.

Texnologiyadakı bu irəliləyiş DNT yoxlamasının həll olunmamış işlərin yenidən açılmasına və həllinə necə imkan verdiyi kimi yeni qapılar açdı. İndi biz artıq əvvəllər bağlanmış kriptovalyuta işlərini yenidən açа bilərik.

Blokçeyn üzrə kriptovalyuta əməliyyatlarını aşkar etmək və nəzərdən keçirmək üçün müvafiq alətlərin getdikcə artan əlçatanlığı və beynəlxalq hüquqdakı dəyişikliklər kriptovalyuta ilə bağlı cinayətkarları aşkarlamağa imkan verir. Bu alətlər getdikcə daha çox istifadəçilər üçün rahat olur və geniş yayılır, istintaq sahəsində dəyişiklikdən xəbər verir.

Bütün bu vasitələrə baxmayaraq, biz hələ də yerli polis əməkdaşları tərəfindən aparılan bir çox istintaqların məhdud anlayış və biliyə görə vaxtından əvvəl bağlandığını görürük. Ümumi təsəvvürün əksinə olaraq, kriptovalyuta əməliyyatları izlənilə bilər. İlkin mərhələdə məlumatları dəqiq qeyd etməklə, əməliyyatları potensial şübhəli şəxslə əlaqələndirmək, virtual və maddi sübutları mükəmməl birləşdirmək ehtimalı artır.
Son illərdə bir sıra ATƏT-in iştirakçı dövlətləri Maliyyə Fəaliyyəti İşçi Qrupu (FATF) tərəfindən yenilənmiş standartlara uyğun olaraq kriptovalyutaları və digər virtual aktivləri çirkli pulların yuyulmasına qarşı milli qaydalarına inteqrasiya etməyə başlayıblar. Bu inkişaf o deməkdir ki, kriptovalyutalarla işləyən şirkətlər əvvəlcə ənənəvi bank institutları üçün nəzərdə tutulmuş proseslərə əməl etməlidirlər. Onlardan müştərilərinin şəxsiyyətini yoxlamaq, vəsaitlərin mənbələrini araşdırmaq və kriptovalyutaların hara göndərilməsinə nəzarət etmək tələb olunur.

Bu dəyişiklikləri nəzərə alaraq, ATƏT-in Virtual Aktiv üzrə Ekspert komandası yerli hüquq-mühafizə qurumlarının nümayəndələri üçün xüsusi olaraq hazırlanmış dəstək təlimatını işə salmaq qərarına gəlib. Bu bələdçi kriptovalyuta araşdırmalarında yeni imkanları işıqlandırmaqla yanaşı, həm də hüquq-mühafizə orqanları əməkdaşlarını bu mürəkkəb və inkişaf edən sahədə ədaləti təmin etmək üçün lazım olan bilik və alətlərlə gücləndirəcək.


30th OSCE MINISTERIAL COUNCIL
osce NORTH MACEDONIA 2023
IT'S ABOUT PEOPLE
30 NOVEMBER 1 DECEMBER 2023
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


Valiant Richey
OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings
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

ATƏT haqqında

ATƏT Avropada Təhlükəsizlik və Əməkdaşlıq Təşkilatıdır. O, dialoqu və əməkdaşlığı təşviq etmək məqsədi ilə regional təhlükəsizlik təşkilatı kimi fəaliyyət göstərir və hərbi və siyasidən başlayaraq ekoloji və iqtisadi sahələrə qədər geniş əhatəyə malik təhlükəsizliyə müfəssəl yanaşma sərgiləyir.

ATƏT 1975-ci ildə Soyuq Müharibə dövründə yaradılıb və hazırda 57 iştirakçı dövlətdən ibarətdir. Bu dövlətlər əsasən ATƏT-in fəaliyyətinin böyük hissəsinin cəmləşdiyi Avropadadır, lakin təşkilat eyni zamanda Şimali Amerikada Kanada və ABŞ, eləcə də Mərkəzi Asiyada Qazaxıstan, Qırğızıstan və Özbəkistan kimi ölkələri əhatə edir. Əsas fəaliyyət istiqamətlərinə hərbi, siyasi, iqtisadi, ekoloji və insan inkişafını əhatə edən hərtərəfli təhlükəsizlik prinsipləri daxildir.

Avropada ATƏT sabitliyin möhkəmləndirilməsi və təhlükəsizlik problemlərinin həlli üçün çalışır. Onun əsas məqsədi diplomatik danışıqlar, münaqişələrin həlli təşəbbüsləri və silahlara nəzarət sazişləri kimi mexanizmlər vasitəsilə münaqişələrin qarşısını almaq və regional əməkdaşlığı təşviq etməkdir. Bundan əlavə, ATƏT-in seçkilərin monitorinqi kimi demokratik və insan haqlarını dəstəkləmək üçün fəaliyyəti var

Maliyyə və kripto cinayəti mövzusuna gəldikdə, ATƏT transsərhəd məlumat axınının yaxşılaşdırılmasına çalışan iştirakçı dövlətlər arasında kəşfiyyat mübadiləsini və potensialın gücləndirilməsini asanlaşdırmaqla bu çağırışlarla mübarizə aparmağa kömək edir. Bu mühüm işdir, çünki kriptovalyuta cinayətləri təbiətcə tək bir ölkə və ya valyuta ilə məhdudlaşmır və buna görə də transsərhəd əməkdaşlıq həyati əhəmiyyət kəsb edir.

ATƏT həm ənənəvi çirkli pulların yuyulması, həm də terrorçuluğun maliyyələşdirilməsi ilə mübarizə aparmaq, eləcə də kriptovalyutalarla bağlı qeyri-qanuni fəaliyyətləri aşkarlamaq və qarşısını almaq məqsədilə hüquqi bazaların və güclü tənzimləyici tədbirlərin yaradılmasını təşviq edir.
Buraya iştirakçı dövlətlərin çirkli pulların yuyulmasına qarşı mübarizə (ÇPY/AML) və terrorçuluğun maliyyələşdirilməsilə mübarizə üzrə (TMM/CTF) beynəlxalq standartlarına riayət etmələrinin təmin edilməsi daxildir.

Maliyyə və kriptovalyuta cinayətləri ilə mübarizədə HOM-ların, maliyyə institutlarının və digər aidiyyəti subyektlərin təcrübələrini təkmilləşdirmək məqsədi ilə ATƏT tərəfindən təlim proqramları və seminarlar keçirilir. Bu səylər kibercinayətkarlıq və kriptovalyuta ilə bağlı cinayət fəaliyyətlərini aşkar etmək və onlarla mübarizə aparmaq üçün istintaq üsullarını və qabaqcıl texnologiyalardan istifadəni təkmilləşdirmək məqsədi daşıyır.

Bu nəşrin məqsədi ilə ATƏT konkret iştirakçı dövlətlərin cinayət məqsədləri və beynəlxalq sanksiyalardan yayınmaq üçün virtual aktivlərdən istifadənin yaratdığı riskləri aradan qaldırmaq ehtiyacına cavab verir. Riskin bu cür qarşısının alınması ATƏT-in İqtisadi və Ekoloji Fəaliyyətlər üzrə Koordinator Ofisi (OCEEA) tərəfindən həyata keçirilən "Virtual aktivlərin çirkli pulların yuyulması risklərinin azaldılması üçün innovativ siyasət həlləri" layihəsinin əsas məqsədidir

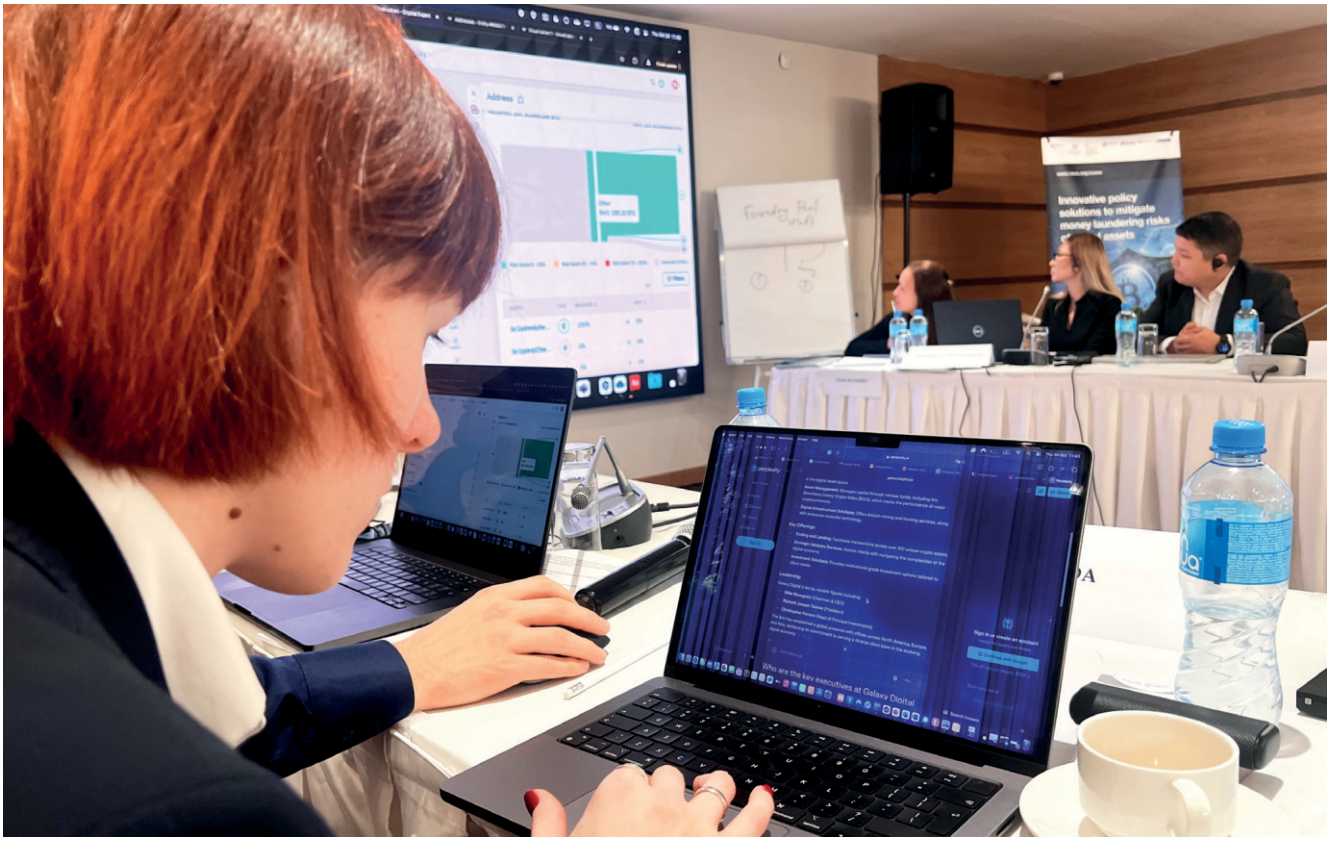
Bu layihənin son məqsədi bu virtual aktivlərə məxsus zəifliklərə qarşı mübarizə aparmaq üçün milli orqanların bacarıqlarını artırmaqdır.

Layihənin icrası boyu OCEEA, Birləşmiş Millətlər Təşkilatının Narkotiklər və Cinayətkarlıqla Mübarizə İdarəsinin Çirkli Pulların Yuyulmasına Qarşı Qlobal Proqramı (UNODC GPML) ilə birlikdə Şərqi Avropa və Qafqazın üç ölkəsinə - Gürcüstan, Moldova və Ukraynaya virtual aktivlərini (VA) və virtual aktivlərin xidmət təminatçıları (VAXT) ilə birlikdə tənzimləmə çərçivəsində yardım göstərməyə davam etdirir və üç ölkənin müvafiq hüquq-mühafizə orqanlarına potensialın gücləndirilməsi və texniki dəstək göstərir.

Layihənin səmərəliliyini artırmaq üçün ATƏT heyəti kriptovalyutalar, çirkli pulların yuyulması (ÇPY) və terrorçuluğun maliyyələşdirilməsi (TM) riskləri, təhqiqat, müsadirə, tənzimləmə və müştərilərin müvafiq qaydada yoxlanması üzrə daxili təcrübə və praktiki təlim proqramlarına töhfə verən UNODC təşkilatı ilə əməkdaşlıq edib. OCEEA mərkəzi banklar, əsas maliyyə institutlarının komplayns departamentləri, maliyyə kəşfiyyatı bölmələri, baş prokurorluqlar, ədliyyə və daxili işlər nazirlikləri kimi müvafiq orqanların şəxsi heyəti üçün normativ sənədlərin və təlimatların hazırlanmasına kömək etməklə, maarifləndirmə tədbirlərinin təşkilində və qurumlararası kriptovalyutalarla əlaqədar cinayətlərin təhqiqatında və beynəlxalq əməkdaşlıqda istifadənin aparılmasına kömək etməklə dəstəyini davam etdirir.

Bu nəşr Almaniya, İtaliya, Polşa, Rumıniya, Böyük Britaniya və ABŞ tərəfindən maliyyələşdirilən virtual aktiv layihələri çərçivəsində çirkli pulların yuyulması risklərini azaltmaq üçün innovativ siyasət həllərinin bir hissəsi kimi tərtib olunmuşdur.

OSCE Organization for Security and Co-operation in Europe



Qreta Barkauskienė, Qazaxıstanın Astana şəhərində müstəntiqlər üçün seminara rəhbərlik edir. ÇPY eksperti və Litvanın Çirkli Pulların Yuyulmasına Qarşı Mübarizə üzrə Mükəmməllik Mərkəzinin milli taktiki əməkdaşlıq qrupunun koordinatoru kimi geniş təcrübəsindən istifadə edərək, benefisiar ölkələrin nümayəndələrinin potensialını gücləndirmək üçün həm dövlət, həm də özəl maraqlı tərəflərin ən yaxşı təcrübələrini paylaşır.

Müstəntiqlərin Gürcüstanın Tbilisi şəhərində keçirilən seminarları kriptovalyuta aktivlərinin ələ keçirilməsinin əsas aspektlərinə, o cümlədən potensial müsadirə üçün təhlükəsiz obyektlərin hazırlanmasına yönəldilib. Bu seminarlar Blokçeyn-də kriptovalyuta aktivlərinin müəyyən edilməsi, ötürülməsi və bərpasında bacarıqların artırılmasına yönəlmiş növbəti məşqlə sıx bağlı idi. Foto: Mixal Qromek.

Rəqəmsal aktivlərin mahiyyəti: Sadələşdirilmiş bələdçi

Rəqəmsal aktivlərin mahiyyəti: Sadələşdirilmiş bələdçi

Bu fəsil müxtəlif rəqəmsal aktivlər, FIAT və kriptovalyutalar arasındakı fərqləri əhatə edəcək. Biz həmçinin müxtəlif növ kriptovalyutalar və onların ətrafındakı infrastruktur arasındakı fərqləri ayırd edəcəyik.

Rəqəmsal aktivlər, virtual aktivlər, kripto aktivlər və kriptovalyuta arasında fərqin nə olduğuna dair tez-tez çaşqınlıq yaranır

Sadə dildə **rəqəmsal aktiv** ən geniş termindir. Bu, rəqəmsal formada mövcud olan bir aktivdir. Buraya şəkillər, videolar, musiqi, məsələn, MP3 formatında, sənədlər və virtual valyutalar daxildir.

Virtual aktiv rəqəmsal aktivlərin daha kiçik həcmi dəstidir. FATF[1]-a əsasən, virtual aktivlər (kripto aktivlər) rəqəmsal olaraq alqı-satqı, köçürmə və ya ödəniş üçün istifadə edilə bilən hər hansı rəqəmsal dəyər daşıyıcısına aiddir. Buraya FIAT valyutalarının rəqəmsal sürəti daxil deyil.

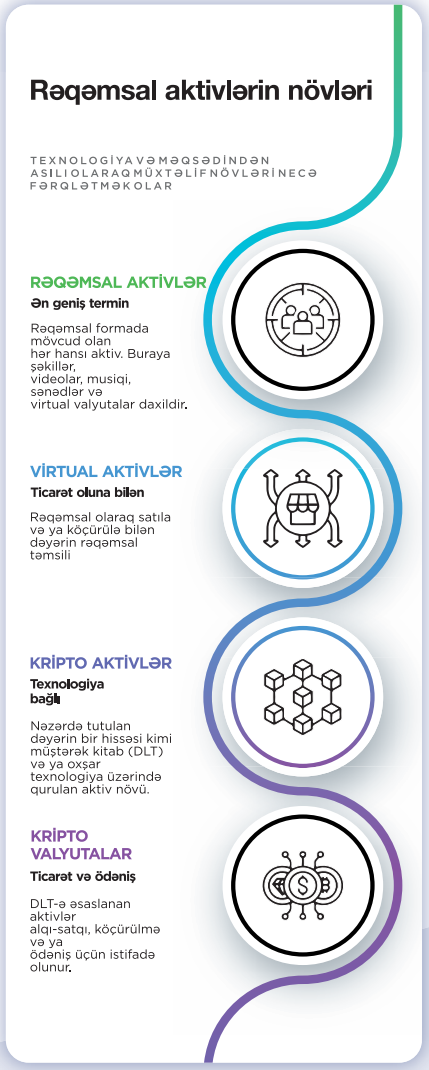
Bundan fərqli olaraq, **kriptovalyuta** daha da dar məfhumdur. Bu, dəyəri malik bir aktivdir, lakin müştərək kitab texnologiyası (DLT) ilə ötürülməlidir. Blokçeyn bir DLT növüdür. Siz kripto aktiv hesab olunmayan oyunda sikkə kimi virtual aktivə sahib ola bilərsiniz, və o, müştərək kitab texnologiyasından istifadə etmədən oyundakı oyunçular arasında ötürülür.

Blokçeyn hazırda müştərək kitab texnologiyasının ən tanınmış növüdür, lakin Hashgraph, Iota Tangle, R3 Corda və bir çox başqaları kimi digər DLT texnologiyaları da mövcuddur. Bu təlimatın məqsədi üçün blokçeyn əsaslı maliyyə alətlərinə diqqət yetiririk.

Rəqəmsal aktivlər arasında blokçeyn texnologiyasından istifadə edərək işləyən yeni valyuta növləri olan kriptovalyutalar və təsvirə əsaslanan aktivlər olan əvəzolunmayan tokenlər (NFTs) daxil olmaqla bir çox müxtəlif aktiv növləri var

Beləliklə, bir kripto alqı-satqı, köçürmə və ya ödəniş üçün istifadə edilmək üçün hazırlandıqdan sonra biz onu kriptovalyuta adlandıracağıq. Tez-tez kriptovalyuta ilə əvəzlənən virtual valyuta terminə də rast gələ bilərsiniz. Kriptovalyuta və virtual valyuta arasında fərqləndirici amil onların əsasında duran texnologiyadır. Kriptovalyutalar blokçeyndən istifadə edir, halbuki virtual valyutalar mütləq şəkildə blokçeyn üzərində qurulmur.

Bu bələdçi əsasən kriptovalyutaların istifadəsi ilə törədilən cinayətlərə diqqət yetirəcək.



Müəllifin icazəsi ilə (Aleksandra Andhov, Hesablama Qanunu, Karnov, 2022).

1 Maliyyə Fəaliyyəti üzrə İş Qrupu, mənbə: https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies (son baxış: 26.10.2023).

Kriptovalyutalarla FIAT-ın fərqi

"FIAT valyutası" kimi tanınan ənənəvi sikkələr və kağız pullar əsrlər boyu iqtisadiyyatlarımızın əsasını təşkil etmişdir. Lakin texnologiyanın inkişafı ilə maddi və virtual arasındakı sərhədləri bulanıq edən yeni pul formaları ortaya çıxıb. Fiziki şəxslər bir şəxsdən digərinə FIAT valyutasının elektron köçürmələrini həyata keçirərkən "elektron pul"dan istifadə edirlər. Elektron pul və ya e-pul, dəyərini dəyişmədən elektron əməliyyatları asanlaşdıraraq bizə tanış olan FIAT valyutamızı rəqəmsal formada təmsil edir. Elektron pul fiat valyutasının rəqəmsal əksidir.

FIAT-dan fərqli olaraq, kriptovalyutalar mərkəzləşdirilməmiş bir mühitdə fəaliyyət göstərir. Onlar heç bir hökumət və ya mərkəzi bankla bağlı deyillər və tələb, texnologiya və etibar da daxil olmaqla müxtəlif amillər onların dəyərini müəyyən edir. Bu sahədə ən tanınmış olan Bitkoin, dəyərini nəzərəçarpacaq dərəcədə yüksəltməklə bu valyutaların potensialını nümayiş etdirdi. 2021-ci ildə bir bitkoin üçün qiyməti 64.000 dollardan çox təşkil edirdi. Bitkoin və Tether kimi kriptovalyutalara heç bir hökumət və ya mərkəzi bank zəmanət vermir. FIAT valyutası qədər köhnə olmasa da, virtual valyutalar insanların çoxunun düşündüyü qədər yeni deyil. İlk virtual valyutalardan biri - E-Qızıl - artıq təxminən 30 il əvvəl, 1996-cı ildə təqdim edilmişdir.

E-Qızıl haqqında məlumat

İlk məşhur virtual valyutalardan biri "E-Qızıl" adlanırdı. İlk dəfə 1996-cı ildə Duqlas Cekson və Barri Dauni tərəfindən yaradılan E-Qızıl istifadəçilərə qızılın (və ya digər qiymətli metalların) qramında ifadə olunan dəyəri və digər E- Qızıl hesablarına ani dəyəri köçürmə imkanı olan hesab açmağa icazə verdi.

2005-ci ildə E-Qızıl-ın 2,5 milyon hesab sahibi var idi və gündəlik əməliyyatlar 6,3 milyon ABŞ dolları dəyərində idi. Aktiv səmərəliliyi, aşağı xidmət qiyməti və qlobal əlçatanlığı səbəbindən məşhur idi. Bununla belə, sərt qaydaların olmaması qeyri-qanuni fəaliyyətləri də cəlb edirdi. 2007-ci ildə E-Qızıl Birləşmiş Ştatlarda böyük münsiflər heyəti tərəfindən ittiham edildi, bununla da şirkət çirkli pulların yuyulması, sövdələşmə və lisenziyasız pul köçürmə biznesi ilə məşğul olmaqda ittiham edildi və nəticədə 2009-cu ildə ABŞ məhkəmələri E-Qızıl-ın bağlanmasına səbəb oldu və başqaları E-Qızıl, e-Bullion.com, Pecunix.com və sairləri kimi bir sıra nüsxələri yaratdı.[2]

Bu sahəni müzakirə edərkən konkret olmaq vacibdir, çünki pullar həm də kriptovalyutalara istinad edərəkə istifadə oluna bilər. Bu, əksər hallar çaşqınlıq yarada bilər. Bu təlimatda biz kriptovalyutalara diqqət yetiririk.

Əsas texnologiya: Blokçeyn

Blokçeyn müştərək kitab texnologiyasının (DLT) bir növüdür. Bu yeni texnologiya ilk dəfə 2008-ci ildə Satoşi Nakomoto tərəfindən nəşr olunan ağ kağız sənədində qeyd olunub.[3] Tək bir idarəetmə mərkəzi və ya məsul şəxs olmadığı üçün mərkəzləşdirilməmiş kimi təsnif edilir. Bunun əvəzinə, dəyişikliklər istənilən istifadəçi tərəfindən edilə bilər, lakin daimi olmaq üçün istifadəçilərin əksəriyyəti tərəfindən qəbul edilməlidir.

Müxtəlif blokçeynlər var. Blokçeyn sadəcə əsas texnologiyayanın adıdır. Hər blokçenini bir bina kimi təsəvvür edin. Hər birinin kənardan çox fərqli görünə biləcəyi və çox fərqli məqsədi ola bilsə də, altına baxdığınız zaman demək olar ki, bütün binalar kərpic və sementlə tikilmişdir.

Binalarda olduğu kimi, bəzi blokçeynlərə icazə tələb olunmadan hər kəs üçün açıqdı, digərlərinə isə qoşulmağa icazə verilməzdən əvvəl təsdiq tələb edir.

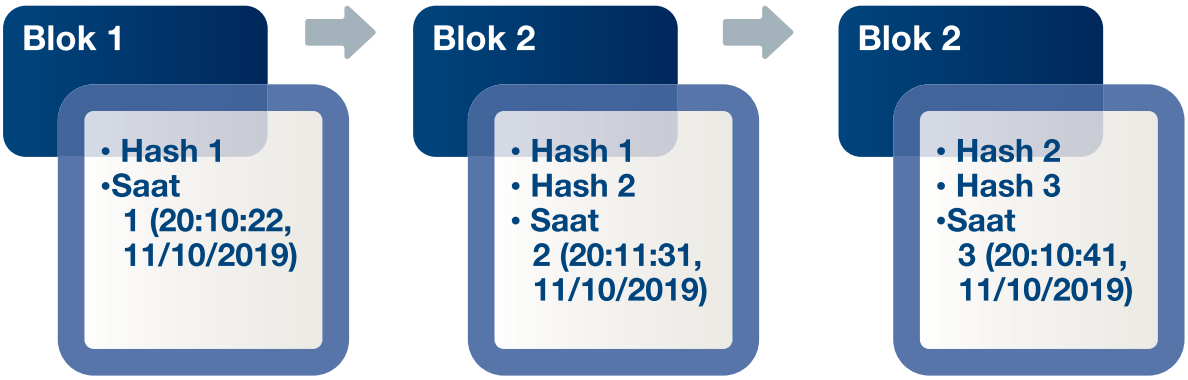
2 "E-Qızıl kiberfırıldaqçılara kömək etməkdə günahlandırır", NBC News, May 2007. (Mənbə: http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helpingcybercrooks (son giriş: 24 avqust 2023-cü il). "İnternet valyuta şirkəti çirkli pulların yuyulmasında günahkar olduğunu etiraf edir", The Industry Standard, iyul 2008-ci il. Mənbə: http://web.archive.org/web/20090414185759/http:// www.thestandard.com/news/2008/0 7/22/internet-currency-firm-pleads-guilty-money-laundering (son giriş: 24 avqust 2023-cü il). *Elektron qızıl əməliyyatlarının xülasəsi (1996) E-Gold*. Mənbə: http://www.e-gold.com/unsecure/synopsis.htm (accessed: 24 Aug. 2023).

3 Nakamoto, S. (2008) Mübadilə üçün elektron nağd sistemi Bitkoin. Mənbə: https://bitcoin.org/en/bitcoin-paper (son giriş: 26 avqust 2023-cü il).

Bu baxımdan biz ictimai və özəl blokçeynləri fərqləndiririk. İctimai blokçeynlər "icazəsiz" adlanır və daha az şəffaflıq və ya nəzarət tələb edir, "icazəli" blokçeynlər isə tez-tez müəssisə məqsədləri üçün istifadə olunur və qoşulmaq istəyən şəxsin təsdiqlənməsini tələb edir.

Blokçeyn adı istifadəçilər tərəfindən məlumatları "bloklar" əlavə etməsi və ya dəyişdirməsi və bu blokların xronoloji (zamanla) bir zəncirdə bir-birinə bağlı olması əsasın yaranıb. Bir istifadəçi yeni blok yaratdıqda və ya yüklədikdə (məsələn, Bitkoin ilə yeni əməliyyat), digər istifadəçilər "konsensus metodlarından" istifadə edərək yeni bloku təsdiqləməlidirlər (buna etibar etmək üçün kifayət qədər mürəkkəb riyazi tənliklər daxildir). Blokların hamısı bir-birinə bağlı olduğundan, əvvəlki bloka keçmək və onu dəyişmək demək olar ki, mümkün deyil. Bu o deməkdir ki, sistemə müdaxilə etmək olmaz. İstənilən yeni məlumat, o cümlədən köhnə məlumatların dəyişməsi yeni blokda qeyd olunur.

Blokçeyn həmin zəncirə qoşulmuş bütün istifadəçilərə zəncirin bütün tarixini ("kitabçasını") görməyə imkan verməklə işləyir. Buna görə də, Bitkoin Blokçeyn ilə istifadəçilər baş vermiş hər bir əməliyyatı görə bilərlər. Bu, müstəntiqlərə araşdırma aparmağa imkan verir. Blokçeyn kitabçasının hər bir istifadəçiyə paylanması səbəbindən blokçeyn "müştərək kitab texnologiyası" və ya DLT adlanır. Bu, hər kəsin əməkdaşlıq edə biləcəyi və əvvəlki versiyaları görə biləcəyi "google cədvəli" kimidir. Hər şey göründüyündən və hər kəs onu görmədən dəyişdirilə bilməyəcəyindən, yüksək şəffaflıq, etibar və təhlükəsizlik səviyyəsi var. Hücumlara qarşı yüksək dayanıqlıq səviyyəsi də mövcuddur: Çünki hər bir şəxs blokçeynin surətinə malikdir və mərkəzləşdirilmiş versiya yoxdur, hətta bir istifadəçi ("blokçeyn terminologiyasında düyün") hücuma məruz qalsa və yazı pozulsa belə, sistem hələ də işləyə bilər.



Müəllifin icazəsi ilə (Aleksandra Andhov, Hesablama Qanunu, Karnov, 2022).

Kriptovalyuta növləri

Kriptovalyutaları ayırd etməyin iki yolu var:

- **Konvertasiya oluna bilən, və ya olunmayan**
- **Mərkəzləşdirilmiş və ya təmərküzləşdirilmiş**

Fərqləndirici xüsusiyyətlər aşağıda daha ətraflı təsvir edilmişdir.

Konvertasiya olunan və olunmayan valyutalar

Konvertasiya olunan valyutalar FIAT valyutasında ekvivalent dəyərə malikdir
və onları "normal" pula dəyişdirmək olar. Kriptovalyutalar heç bir hökumət və ya qurum tərəfindən dəstəklənmədiyi üçün bu konvertasiyaya zəmanət verilmir.

Kriptovalyutanın FIAT valyutasına çevrilməsi bazara və qəbul edilən özəl təkliflərə əsaslanır.

Bu, ən çox cinayətlərin baş verdiyi kriptovalyuta növüdür. Konvertasiya olunan valyutalara misal olaraq Bitkoin və E-Gold daxildir.

Konvertasiya olunmayan valyutalar kompüter
oyununda olan qızıl sikkələr kimidir. Bunlarla
törədilən cinayət daha az ehtimal olunur, çünki onlar real dünyada dəyərə malik deyillər. Bununla belə, bəzi şəxslər onları mövcud oyunun hüdudlarından kənarda ticarət etmək üçün bir yol taparaq, oyun qaydalarına zidd olsa belə, onları oyundan kənarda dəyişdirilə bilər. Məsələn, kimsə

"toplanmış qızıl sikkələri" oyunda bir oyunçudan digər oyunçuya köçürə bilər, əməliyyat oflayn olaraq nağd şəkildə ödənilir.

Mərkəzləşdirilmiş və mərkəzləşdirilməmiş valyutalar

Mərkəzləşdirilmiş kriptovalyutalara valyuta buraxan, onun qaydalarını təyin edən, ödəniş kitabçasını aparan və onu dövriyyədən çıxarmaq səlahiyyətinə malik olan vahid orqan nəzarət edir. Mərkəzləşdirilmiş valyutalar konvertasiya olunan və ya olunmayan ola bilər.

Konvertasiya olunmayan valyutalar həmişə mərkəzləşdirilmişdir (çünki, məsələn, oyun valyutaya nəzarət etmədən oyun daxilində valyutaya sahib ola bilməz). Mərkəzləşdirilmiş konvertasiya olunan valyuta dəyişdirilərkən məzənnə bazar tələbi və təklifi və ya inzibatçı tərəfindən müəyyən edilir. Mərkəzləşdirilmiş valyutanın yaxşı nümunəsi E-Qızıldır.

Təmərküzləşdirilmiş valyutalar isə mərkəzi səlahiyyətə malik deyil və istifadəçilər şəbəkəsi əsasında fəaliyyət göstərir. İnternet kimi təmərküzləşdirilmiş bir sistem düşünün. Bütün internetə cavabdeh olan bir nəzarətçi olmadığı kimi, təmərküzləşdirilmiş sistemin bir əsas nəzarətçisi yoxdur. İnsanların əksəriyyəti internetdən gündəlik istifadə etsə də, ödənişi yığan bir sahib yoxdur; əvəzinə, müxtəlif provayderlərə müxtəlif xidmətlər üçün ödənilir. Bitkoin kimi kriptovalyutaların arxasında blokçeyn şəbəkə texnologiyası belə istifadə olunur. Əməliyyatlar şəbəkə vasitəsilə idarə olunur və heç bir orqan tərəfindən ayrı monitorinq yoxdur.

23 avqust 2023-cü il tarixinə ən böyük bazar dəyərinə malik on kriptovalyutanın seçimi aşağıdakı mənbəyə əsasən təqdim olunur.[4]

Ad	Simvol	Bazar dəyəri (23 avqust 2023-cü il)	Məcmu ÜDM-i ilə müqayisə oluna bilən ölkələr[5]
Bitkoin	BTC	$514,912,135,787	Sudan
Ethereum	ETH	$201,475,414,760	Haiti
Tether USDt	USDT	$82,835,552,223	Somali
BNB	BNB	$33,285,580,473	Andorra
XRP	XRP	$27,991,699,189	Kuraçao
USD Coin	USDC	$26,005,195,827	Lesoto
Cardano	ADA	$9,357,776,591	St. Vinsent və Qrenadin
Dogecoin	DOGE	$8,965,846,112	Şimali Mariana Adaları
Solana	SOL	$8,792,761,272	Samoa
TRON	TRX	$6,938,358,042	Amerika Samoası

Psevdo valyutalar və məxfilik sikkələri

Psevdo-anonim valyutalar təxəllüslərdən istifadə edən hesabları əhatə edir, yəni əməliyyatlar birbaşa fərdi şəxsiyyətlərlə əlaqəli olmasa da, bəzi identifikasiya məlumatları qalır. Məsələn, kriptovalyuta almaq üçün istifadə edilən ənənəvi FIAT valyuta bank hesabı müəyyən edilə bilən məlumatlarla əlaqələndirilir. Bu kateqoriyaya daxil olan sikkələrə Bitkoin və Ether daxildir. Əksinə, məxfilik sikkələri əməliyyat təfərrüatlarını və əlaqəli şəxsiyyətləri gizlətmək üçün qabaqcıl kriptoqrafik metodlardan istifadə etməklə daha çox anonimlik təklif edir və onları orijinal istifadəçiyə qədər izləməyi çətinləşdirir. Belə sikkələrə misal olaraq Monero və Zcash-ı göstərmək olar.

4 Bütün kriptovalyutalar (2023) CoinMarketCap. Bu ünvana baxın: https://coinmarketcap.com/all/views/all/ (son baxış: 24.08.2023).

5 Dünya Bankının ÜDM məlumatlarına (ABŞ dolları) əsasən, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false (son baxış: 23.08.2023).

Kripto pulqabıları

Kriptovalyuta pulqabıları kriptovalyutanın saxlandığı yerdir. Faydalı bir bənzətmə, bu gün dünyanın hər yerində pulun necə saxlanıldığını təsəvvür etməkdir.

Pul müxtəlif formalarda gəlir. Onun bir hissəsi böyük bankların yerləşdiyi qızıl külçələrdə saxlanılır, bir hissəsi kağız əskinaslar, onlayn bank köçürmələri və ya kriptovalyutalar şəklində dövriyyədədir. Kriptovalyuta pulqabıları da müxtəlif formalar da: telefondakı proqram, USB yaddaşa bənzəyən cihaz və ya sadəcə bir proqram hissəsi (e-poçt ünvanınıza bir qədər bənzəyir) və giriş və şifrənizi daxil etdikdən sonra daxil ola bilərsiniz. Müxtəlif növ kriptovalyuta pulqabları olsa da, eyni texnologiyadan istifadə edirlər. Əksəriyyətini açmaq üçün 12, 18 və ya 24 sözdən ibarət bərpa açar sözləri olur.

Kripto pulqabların ünvanları

Kriptovalyuta pulqablarının ünvanları bank hesab nömrəsinə bənzəyir. Kiminsə bank hesabı nömrəsinə sahib olmaq kiminsə puluna çıxışın olması demək deyil. Kripto pulqabılarının ünvanları çoxlu sayda hərf və rəqəmlərdən ibarət uzun, mürəkkəb ardıcıllığa malikdir. Bunun iki nümunəsinə baxın:

TRON valyutası üçün kriptovalyuta pul kisəsi
TYm3NTSyk85t9UHSd68DY4vGWQADHXpaXJ

Bitkoin üçün kriptovalyuta pul kisəsi
Bc1qu5z7kn0v2krhglsnan4c0m5f76xk69p53wjwgh

Ənənəvi bank hesabı nömrələri ilə kripto pul kisəsi ünvanları arasındakı fərq ondan ibarətdir ki, kripto pul kisəsi ünvanı ilə müqayisədə bank hesab nömrəsindən çoxlu məlumat toplana bilər. Hüquq-mühafizə orqanları asanlıqla IBAN nömrəsini deşifrə edə və müvafiq orqanla əlaqə saxlaya bilər.

IBAN beynəlxalq bank hesab nömrəsidir. 34-ə qədər hərf və rəqəm ola bilər. Bu, ölkənin kodu, iki rəqəmli təhlükəsizlik yoxlaması və sonra bank və hesab haqqında məlumatla başlayır. Bəzi ölkələrdə bu fərqli bank rekvizitləri forması mövcuddur. Məsələn:

IBAN:

- **LT44 3250047338696265**

  LT Litva Respublikası deməkdi,

  32500 Revolut Bank UAB-ı kodudur

  47338696265 istifadəçinin hesab nömrəsidir[6]

İstintaqda belə bir IBAN bank hesab nömrəsi çıxsa, müstəntiq Litvada Bank Revolut ilə əlaqə saxlaya biləcək. Bu məlumatı iban.com və ya https:// wise.com/gb/iban/checker kimi "IBAN validatorları" adlanan mənbələrdən əldə etmək olar. Bundan sonra hesab istifadəçisi haqqında şəxsi məlumatların əldə edilməsi prosesinə başlamaq olar.

Bitkoin kimi psevdoanonim kriptovalyutalar üçün heç bir hüquq-mühafizə orqanı hesab sahibi haqqında şəxsi məlumatları belə hesab nömrəsi əsasında müəyyən edə bilməyəcək: bc1qu5z7kn0v2krhglsnan4c0m5f76xk-69p53wjwgh.

Sahibinin identifikasiya məlumatlarını tapmaq üçün xüsusi proqram təminatı lazımdır, məsələn, **blokçeyn analitik provayderi.**

Blokçeyn analitika provayderləri istifadəçilərin identifikasiya məlumatlarını aşkar edə və oğurlanmış kriptovalyutalarla istifadə edilən ümumi taktika olan müxtəlif kriptovalyutalar üzrə əməliyyatları izləyə bilər.

6 IBAN və maliyyə qurumlarının kodları, Bank of Lithuania, https://www.lb.lt/en/iban-and-financial-institution-codes (son baxış 25.10.2023).

Bu cür provayderlərin hansı maliyyə institutlarının və ya kriptovalyuta birjalarının (VAXT – virtual aktiv xidməti təminatçıları) bu şəxsiyyət məlumatına malik olduğunu müəyyən etmək qabiliyyəti onların fəaliyyət göstərdiyi ölkənin qanunlarından asılıdır. Bu səbəbdən ATƏT kimi beynəlxalq təşkilatlar öz iştirakçı dövlətlərinə bu sahədə ən yaxşı beynəlxalq təcrübələri uyğunlaşdırmağa kömək edirlər.

Kripto pulqabıları üzrə axtarış sistemlər

İctimai blokçeynin aparıcı növləri hər kəs üçün açıq olduğundan, "kripto pulqabıları üzrə axtarış sistemi"ndən istifadə edərək pul kisəsində baş verən bütün əməliyyatları nəzərdən keçirmək olar.

Kripto pulqabıları axtarış sistemi, blokçeyn məlumatlarında naviqasiya etmək üçün xüsusi axtarış mühərrikidir. Bu, fərdi bloklar, əməliyyatlar və əlaqəli pulqabıları haqqında ətraflı məlumat verir. Blokçeyn əməliyyatlarını "Google" ilə müqayisə etmək olar.

Diqqətli olun:

Hər bir kriptovalyuta növü üçün fərqli pul kisəsi axtarış sisteminə ehtiyac ola bilər. Məlumat tapmaq üçün müvafiq kriptovalyutanın adını və aparıcı provayderləri haqqında ətraflı öyrənmək üçün axtarış sisteminə wallet explorer" və ya "Blokçeyn explorer" ifadəsini yazmağınız tövsiyə olunur. Bu cür xidmətlər ümumiyyətlə pulsuzdur.

Kripto pulqabıları axtarış sistemlərinin əsas istifadəsi:

- **Tranzaksiyaların yoxlanılması:** Axtarış sistemi istifadəçilərə əməliyyatın baş verdiyini yoxlamağa imkan verir. Kimsə kriptovalyuta göndərdiyini iddia etdikdə, axtarış sistemi identifikatoru və ya pul kisəsi ünvanından istifadə edərək əməliyyatı axtararaq bunu təsdiqləmək üçün istifadə edilə bilər.
- **Audit və uçotun aparılması:** Əməliyyatların qeydlərini aparmalı olan şəxslər və ya müəssisələr üçün axtarış sistemi əməliyyatın nə vaxt baş verdiyi, nə qədər göndərildiyi və iştirak edən ünvanlar haqqında ətraflı məlumat verə bilərlər.
- **Tədqiqat və təhlil:** Developerlər, tədqiqatçılar və analitiklər blokçeynin ümumi sabitliyini və fəaliyyətini öyrənmək üçün tez-tez pul kisəsi axtarış sistemlərində istifadə edirlər. Onlar nə qədər əməliyyatın baş verdiyini, əməliyyatların ölçüsünü və s. baş verdiyini görə bilərlər.
- **Balans:** Axtarış sistrminə pul kisəsinin ünvanını daxil etməklə, konkret kriptovalyuta pul kisəsinin balansına və onun əməliyyat tarixinə baxmaq olar.

Pulsuz axtarış sistemləri:

Sıravi axtarış sisteminə "best free XXX cryptocurrency wallet explorer" yazmaqla hər bir kriptovalyuta növü üçün kripto pul kisəsiləri üzrə axtarış sistemini tapmaq mümkündür.

Bu alətlərdən istifadə edərək, hər kəs kriptovalyutaya və ya texnologiya haqqında dərin biliyə malik olmasa belə, blokçeynlə əməliyyatları araşdıra və yoxlaya bilər. Eyni şəkildə biz internetdə ciddi axtarış vasitələri ilə axtarış etdiyimiz kimi, blokçeynlərdə də axtarış edə bilərik.

Kriptovalyutaların mübadiləsi

"Ənənəvi" pul kimi, bir növ kriptovalyutanı digərinə və ya FIAT valyutasına dəyişmək üçün xüsusi platformadan istifadə etmək lazımdır. Üç əsas platforma var: istifadəçilərarası mübadilə (P2P), mərkəzləşdirilmiş dəyişdiricilər (CEX) və mərkəz-ləşdirilməmiş dəyişdiricilər (DEX).

P2P **peer-to-peer** kimi oxunur və beləliklə, şəxsdən şəxsə və ya daha tez-tez istifadəçidən istifadəçiyə (hüquqi şəxslər öz aktivlərini sata və ya təklif edə bildiyi üçün) deməkdir. Burada istifadəçilər birjanın özündən deyil, digər istifadəçilərdən alırlar. Fəaliyyətini dayandıran belə bir P2P mübadiləsinə misal LocalBitkoin.com adlı Finlyadiyalı provayder ola bilər.

Bu cür mübadilə sistemləri öz virtual aktivlərini satırlar və istifadəçiləri bir-birinə qarşılaşdırmırlar.

Peer-to-peer mübadilə sistemləri ÇPY və TMM qaydalarına7 tabedir və ətraflı istifadəçi məlumatı tələb edir. Onlar da fəaliyyət göstərdikləri ölkələrdə müəyyən qaydalara əməl etməlidirlər.

Mərkəzləşdirilməmiş birjalar avtomatik fayl çeviriciləri kimi fəaliyyət göstərdiklərini iddia edirlər (məsələn, .doc-dan .pdf-ə). Onlar əsasən kripto-kripto əməliyyatları üçün, daha az FIAT-dan kriptovalyuta mübadiləsi üçün istifadə olunur. Mərkəzləşdirilməmiş mübadilələrdə iştirak edən fondlar izləmə üçün xüsusi dəstək tələb edir.

Bu, aysberqin yalnız görünən hissəsidir. Yuxarıda qeyd olunan OTC mübadilə sistemləri, mikserlər və tumblerlər kimi yeni birja növləri də mövcuddur. Bu, istifadəçilərin əməliyyatlarının izlərini gizlətmək məqsədi ilə hazırlanmış sürətlə inkişaf edən texnologiyadır. Bir çox ATƏT-ə üzv dövlətlər bu cür alətlərin istifadəsini məhdudlaşdırmaq üçün tədbirlər görürlər.

Mikserlər and tumblyorlar

Mikserlər və tumblyorlar kriptovalyuta əməliyyatlarının məxfiliyini və anonimliyi artırmaq üçün nəzərdə tutulmuş xidmətlərdir. Onların əsas funksiyası müxtəlif istifadəçilərin vəsaitlərini qarışdırmaq və bununla da vəsaitlərin ilkin mənbəyini gizlətməkdir

7 Bu, yalnız FATF-ın 15-ci tövsiyəsini yerinə yetirmiş ölkələrdə fəaliyyət göstərən kriptovalyuta birjalarına şamil edilir, hansı ki, ölkələrdən kriptovalyutalarla məşğul olan maliyyə qurumlarını öz ÇPY və TMMçərçivələrinə daxil etməyi tələb edir.

Mikserlər

Bunlar, mənşəyini gizlətmək üçün müxtəlif mənbələrdən kriptovalyuta fondlarını qarışdıran mərkəzləşdirilmiş və ya təmərküzləşdirmiş xidmətlərdir. İstifadəçilər öz kriptovalyutalarını (Bitkoin kimi) mikserə göndərirlər, xidmət isə onları digər istifadəçilər və ya öz sikkələri ilə qarışdırır. "Qarışdırma prosesi" başa çatdıqdan sonra xidmət pulların mənşəyini izləməyi çətinləşdirərək istifadəçinin müəyyən etdiyi ünvana rüsum çıxılmaqla bərabər miqdarda sikkə göndərir

Bununla belə, mərkəzləşdirilmiş qarışdırıcılar potensial olaraq əməliyyatları qeyd edə bilən vahid tərəfindən idarə olunur. Europol EC3 komandası demiksinq üzrə kurslar təklif edir, kurslar yalnız təsdiqlənmiş hüquq-mühafizə orqanları üçün keçərlidir

Ənənəvi bankçılıqda mikser kimi əlaqəli xidmətlər

Mikserlər vəsaitlərin yatırıldığı və çıxarıldığı ənənəvi banklara bənzər şəkildə işləyir. Müxtəlif şəxslərin pul yatırdığı böyük bir maliyyə institutunu təxmin edin. Əgər bank bütün bu əmanətləri birləşdirsə və sonra hər bir dolların mənşəyini göstərmədən onları hesab sahiblərinə paylasa, bu, qarışdırma (mixing) prosesinə bənzəyəcək. Fondlara mərkəzləşdirilmiş mikser kimi tanınan bir qurum nəzarət edir və içəri daxil olduqdan sonra bu vəsaitlər başqaları ilə qarışır. Blokçeyn üzrə aparıcı analitika provayderləri tanınmış mikserlərin əksəriyyəti üçün avtomatik və ya əl ilə "demiksləmə" xidmətləri təklif etdiklərini iddia edir və bu provayderlərə bu cür xidmətlər üzrə əməliyyatları nəzərdən keçirməyə imkan verir.[8]

Tumblyorlar

Tumblyorlar mikserlərə bənzəyir və bir çox kontekstdə terminlər bir-birini əvəz edir. Tumbler-in əsas məqsədi həm də əməliyyat məxfiliyini gücləndirməkdir. Bəziləri tumblerləri mikserlərin daha mürəkkəb versiyaları hesab edirlər. Onlar qarışıq sikkələrin orijinal mənbələrinə bağlanmamasını təmin etmək üçün qabaqcıl alqoritmlərdən istifadə edirlər.

Ənənəvi bankçılıqda tumber kimi əlaqəli xidmətlər

Tumblerləri vergi cənnətləri kimi müəyyən edilən ölkələrdəki bank hesabları və ya gücləndirilmiş məxfilik və konfindensiallıq təklif etdiyi üçün ofşor banklarla müqayisə etmək olar. Belə banklar adətən məxfilik və aktivlərin qorunması üçün hazırlanmış mürəkkəb strukturlardan və xidmətlərdən istifadə edirlər. Kriptovalyuta sahəsində tumblerlər əməliyyatların anonimliyini qorumaq üçün ən müasir riyazi alqoritmlərdən istifadə edir və standart mikserlərə nisbətən daha təkmil gizlətmə səviyyəsini təmin edir. Tumbler üzərində əməliyyatı izləmək mürəkkəb və vaxt aparan işdir, lakin qeyri-mümkün deyil.

Fərqlər və oxşarlıqlar

Həm mikserlər, həm də tumblerlər əməliyyat məxfiliyini artırmaq üçün eyni məqsədə xidmət etsə də, aralarındakı xüsusiyyətlər metodlarına və mükəmməllik səviyyəsinə görə azalır.

Bu, ənənəvi veb brauzerləri təkmil məxfilik xüsusiyyətləri təklif edənlərlə müqayisə etmək kimidir. Hər ikisi internetdə axtarış etməyə imkan verir, lakin biri anonimliyi qorumaq üçün daha təkmil alətlər təklif edir

VAXT-lar və KAXT-lar

Virtual aktiv xidmət təminatçısı (VAXT) aşağıdakı fəaliyyətləri həyata keçirir

- Virtual aktivlər və FIAT valyutaları arasında mübadilənin asanlaşdırılması;
- Virtual aktivlərin bir və ya bir neçə forması arasında mübadilənin asanlaşdırılması;
- Virtual aktivlərin bir pul kisəsindən digərinə köçürülməsini asanlaşdırmaq,
- Virtual aktivlərin satışı ilə bağlı maliyyə xidmətlərinin göstərilməsi.

VAXT-lara gəldikdə, bir-birini əvəz edən bir sıra terminlər var. "VAXT"-ən adı Maliyyə Fəaliyyət İşçi Qrupu (FATF) tərəfindən qəbul olunub. Bununla belə, kriptovalyuta xidməti təminatçısı olan "KAXT" Al-da VAXT əvəzinə adətən istifadə olunur. KAXT-larda müəyyən edilmiş xidmətlərin sayı VAXT-lardan daha genişdir. Bəzən "birjalar" və "brokerlər" terminləri də istifadə olunur, lakin onlar VAXT və ya KAXT-ın bir çox növlərindən yalnız birini təmsil edir.

8 Müəllif bu nəşrin redaksiya müddətindən əvvəl həmin iddiaları təsdiq və ya təkzib edə bilməyib.

Rəqəmsal aktivlərlə bağlı cinayətlərin araşdırılması protokolu

Rəqəmsal aktivlərlə bağlı cinayətlərin araşdırması protokolu

Toplamaq üçün ən vacib dörd məlumat

Potensial zərərçəkən polis bölməsinə gələndə və kriptovalyuta fırıldaqçılığına məruz qaldığını iddia etdikdə, toplanması lazım olan dörd mühüm məlumat var.

Kriptovalyuta əməliyyatları geri dönməzdir – onlar tamamlandıqdan və blokçeynə daxil olduqdan sonra həmin vəsaitləri zərərçəkənə qaytarmaq üçün xeyli səy tələb olunacaq. Və buna baxmayaraq, əhəmiyyətli səy göstərilsə də, qaytarmaq mümkün deyil.

Vaxt

Birinci əsas element vaxtdır. Kriptovalyuta əməliyyatları həmişə blokçeynə dərhal daxil olmur. Blokçeyndə qeyd edilmədən əvvəl vəsaitlər müəyyən müddət bankda və ya lisenziyalı kriptovalyuta brokerində saxlanılır. Bunun belə olub-olmadığını müəyyən etmək ilk və ən vacib sualdır, çünki bu, hələ də əməliyyatı geri qaytarmaq şansı verir.

Maliyyə institutları

Növbəti ən vacib sual zərərçəkəndən FIAT valyutası köçürülərkən hansı kriptovalyuta brokerindən və ya maliyyə qurumundan istifadə edildiyini soruşmaqdır.

Köçürmə maliyyə institutlarında çirkli pulların yuyulmasına qarşı qaydaları tətbiq edən aşağı riskli ölkədə brokerlər arasında aparılıbsa, əməliyyatın dayandırıla bilinməsi ehtimalı artır.

Həcm

Üçüncü ən vacib sual əməliyyatın həcmidir, çünki çirkli pulların yuyulmasına qarşı təyin olunan həddi aşan külli miqdarda vəsait VAXT və ya KAXT tərəfindən yoxlanılır. Zərərçəkən lisenziyalı birjaya böyük məbləğdə köçürmə edibsə, bu birja ilə əlaqə saxlamaq və köçürmənin kriptovalyutalara dəyişdirilməsini dayandırmaq mümkün ola bilər.

Kriptovalyutanın növü

Nəhayət, sonuncu əsas sual hansı növ kriptovalyutanın və ya virtual aktivin alındığıdır. Bitkoin kimi bəzi növləri asanlıqla izlənilə bilər. Monero və ZCash adlı məxfilik sikkələri kimi tanınan kriptovalyutanın digər növləri izləmə və araşdırmaları çətinləşdirmək üçün hazırlanmışdır, lakin hətta bəzi hallarda və səylərlə onları da izləmək mümkündür.

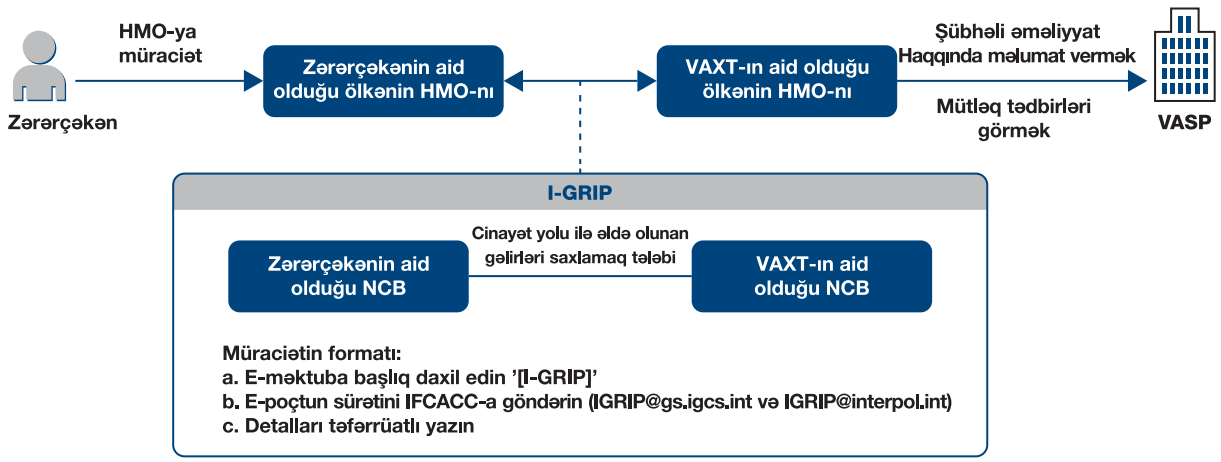
Zərərçəkən şəxsin bank hesabından əməliyyat qısa müddət əvvəl həyata keçirilibsə, bütün səylər onun blokçeynə daxil olmasını dayandırmağa yönəldilməlidir. Yerinizdə belə bir işi qəbul etmək və onu yalnız günlər sonra qəbul edə biləcək digər həmkarlarına təhqiqatdan əvvəl ötürmək uğur ehtimalını əhəmiyyətli dərəcədə azalda bilər.

Bu konsepsiyaya səciyyəvi olan və onu təsvir edən üç nümunəyə baxaq

Nümunə 1: Potensial zərərçəkənlə bağlı FIAT-ın beynəlxalq bankdan köçürülməsi, məsələn, cümə günü axşam başlayır və bu hal barədə məlumat hüquq-mühafizə orqanlarına şənbə günü səhər verilir, o zaman hələ də bankla əlaqə saxlamaq və əməliyyatı dayandırmaq mümkündür. Zərərçəkən bankla əlaqə saxlamayıbsa, dərhal bunu etməlidir. (INTERPOLUN IGrip həlli, səh. 23)

Nümunə 2: Zərərçəkən öz bank hesabından kriptovalyuta brokerinə daha böyük məbləğ köçürsə və köçürmə artıq birincinin hesabını tərk etsə belə, müştərinin bank hesabında köçürmənin göndərildiyi VAXT/KASP-ın adını göstərən məlumat ola bilər. Bu halda köçürmə Binance kimi daha böyük brokerlərdən birinə göndərilibsə, müştəri dərhal çat vasitəsilə müştəri xidməti ilə əlaqə saxlamalı və ya belə başlıqlı e-məktub göndərməlidir: **"Təcili: Mübadiləni dayandırın – fırıldaqçılıq".** Göndəriləcək ünvanlar fraud@nameofthebroker.domain və ya compliance@nameofthebroker.domain Məktubda müəyyən bir həcmdə və müddət ərzində müəyyən IBAN-dan gələn köçürmə haqqında məlumat təqdim olunacaq.

Hüquq-mühafizə orqanlarının əməkdaşları, məsələn, Binance sisteminə Hüquq Mühafizəsi Sorğusu vasitəsilə də vəsaitin dayandırılmasını tələb edə bilərlər: https://www.binance.com/en/support/law-enforcement.
Daha iri brokerlər və ya birjalar və digər VAXT-lar adətən qərarların icraçılarına köçürmənin yerini tapmağa və dayandırmağa kömək edə biləcək bir prosesə malikdirlər. Sektordakı şirkətlərin əksəriyyətinin təcili hallar barədə məlumat vermək üçün istifadə edilə bilən compliance@name-of-the-broker.com və ya fraud@name-on-of-the-broker.com kimi e-poçt ünvanları olacaq.



Mənbə: INTERPOL

Eyni zamanda, zərərçəkənin aid olduğug yurisdiksiyasının HMO-nı **Qlobal Rapid Intervention of Payment** (I-GRIP) (Ödənişlər üzrə Qlobal Çevik Müdaxilə) adlı alətlə INTERPOL vasitəsilə ödənişin dayandırılması tələbi verə bilər. Bu, VAXT-ın yerləşdiyi yurisdiksiyanın HMO ilə ünsiyyət kanalıdır. INTERPOL aktivlərin bərpasının ilkin mərhələlərini həyata keçirmək məqsədilə beynəlxalq əməkdaşlığı kifayət qədər sürətli etmək üçün I-GRIP-i işə salıb.

VAXT-ının yerləşdiyi yurisdiksiyanın HMO-nı I-GRIP sorğusunu aldıqdan sonra, onlar öz milli qanunvericiliklərinə uyğun olaraq cinayətdən əldə olunan gəlirlərin daha sonra emal edilməməsi üçün lazımi tədbirlər görə bilərlər. Tələb olunan tədbirlər müxtəlif ola bilər. Onlar sadəcə olaraq şübhəli əməliyyat haqqında alıcıya VAXT-dan məlumat verə bilərlər, beləliklə, VAXT şübhəli hesabı dayandırmaq və ya hətta əməliyyatları geri çağırmaq üçün öz mülahizəsinə əsasən qərar verə bilər. Həmçinin, HMO-lar şübhəli hesabı dayandırmaq üçün VAXT-a mandat vermək üçün öz səlahiyyətlərindən istifadə edə bilərlər. Əlavə olaraq, HMO yurisdiksiyaları tələb edən I-GRIP tərəfindən aparılan istintaqa paralel olaraq öz daxili cinayət təhqiqatını açа və şübhəli hesaba qarşı müsadirəsi əmri verə bilər

Əgər ATƏT-in iştirakçısı olan dövlətin hüquqi bazası buna imkan verirsə, başqa bir ehtimal potensial zərərçəkənin verdiyi məlumat əsasında işin dərhal açılması ola bilər, çünki zaman kriptovalyuta istintaqlarında ən vacib amillərdən biridir.

Nümunə 3: Potensial zərərçəkən vəsaitin hansı kriptovalyuta brokerinə göndərildiyinə tam əmin deyilsə və köçürmə detallarında buna bənzər hərf və rəqəmlərin abreviaturaları varsa:

`1C5Eu4UpeK5djG3QiKwhcLELtFwHT146dG`

bu, vəsaitlərin kriptovalyuta pul kisəsində dəyişdirildiyini və ya dəyişdiriləcəyini göstərə bilər. Belə pulqablarını bank hesabları və ya vəsaitlərin saxlandığı elektron poçt qutusu ilə müqayisə etmək olar. Bir az bacarıqla belə bir pul kisəsindəki vəsaiti bərpa etmək və ya dondurmaq olar.

Hərflərin və rəqəmlərin belə sırası kriptovalyuta ilə tanış olmayan şəxslər üçün qeyri-adi görünsə də, təcrübəli müstəntiqlər üçün bu birləşmə kredit kartı nömrəsinə bənzər məlumat verir. Kriptovalyuta pul kisəsi ünvanına sahib olmaq kredit kartı nömrəsinə bənzəyir, lakin ad və ya emitent bank kimi şəxsi məlumatlar daxil edilmir. Kredit kartı nömrəsi kartın emitentini və kartın növünü göstərir. Eynilə, kriptovalyuta pul kisəsinin ünvanı zərərçəkən tərəfindən hüquq-mühafizə orqanlarına bildirildikdən sonra, xarici alətlərin köməyi ilə pul kisəsinin ünvanını müəyyən kriptovalyutaya və ya konkret VAXT və ya maliyyə vasitəçiləri ilə əlaqələndirmək (hər zaman uğurlu olmur) mövcuddur.

(Ətraflı məlumat üçün "Virtual aktivlərdə cinayətlərin araşdırılması üçün əlavə alətlər" bölməsinə baxın, səh. 47.)

9 INTERPOL, Virtual aktivlərin müsadirəsi üçün təlimatlar (oktyabr 2023), səh. 40.

Hər bir əməliyyat növü üzrə qabaqcıl təcrübə nümunələri

Müstəntiqlərin bilməsi vacib olan blokçeynlərdə üç növ əməliyyat var, çünki onlara aid virtual aktiv xidməti təminatçıları ilə (VAXT) əməkdaşlığın təmin olunmasına ehtiyac yarana bilər.

Əməliyyatın növü	Təsviri	İstintaqa təsiri
FIAT valyutasından kriptovalyutaya	Zərərçəkən bank köçürməsi, kart ödənişi, mobil ödəniş və ya milli valyutada nağd pulla vəsaiti kriptovalyutalara mübadilə edən VAXT-da ödənişi tamamlayıb.	**Qabaqcıl təcrübə 1** **Mümkün olduqda, kriptovalyuta brokerinə köçürməni dayandırmağa və ya geri qaytarmağa çalışın.** Fırıldaqçılıq haqqında məlumat verildikdə ən böyük uğursuzluq şübhəli cinayətin qeydə alınması və ilkin istintaqın aparılması üçün polis idarsində məsul şəxsin təyin edilməsidir. Bu, zərərçəkənlər ilkin əlaqəni gecikdirir. Əgər gecikmə olmazsa, əməliyyat potensial olaraq hələ də dayandırıla bilər. Əgər əməliyyat bank iş saatlarından əvvəl/sonra və ya həftə sonu icra olunubsa, bəzi banklar növbəti iş günü bank köçürmələrini emal etdiyi üçün bank köçürməsini dayandırmaq hələ də mümkün ola bilər. Əgər əməliyyat kart ödənişi ilə tamamlanıbsa, ödənişin qaytarılması və ya köçürülməsini dayandırmaq üçün kart emitenti ilə əlaqə saxlamaq mümkün ola bilər. Əsas məqam bank köçürməsini hansı maliyyə qurumunun həyata keçirdiyini öyrənməkdir. Bu, bank **Qabaqcıl təcrübə 2** **Əgər köçürməni dayandırmaq alınmırsa, onun hansı VAXT-a göndərildiyini müəyyən etməyə çalışın, məqsəd onların əməliyyatı dayandırması və mümkün olduqda vəsaiti dondurmaısıdır.** Əgər kriptovalyuta brokeri kriptovalyuta aktivləri üçün ÇPY/TMM qaydalarını tətbiq edən aşağı riskli ölkədə fəaliyyət göstərirsə, o zaman gecikmədən brokerlə əlaqə saxlamaq və vəsaitin, əgər onlar artıq dəyişdirilməyibsə, dondurulmasını və ya geri qaytarılmasını tələb etmək mümkündür. Bir sıra hallarda prosess zərərçəkən tərəfindən də başlana bilər. Brokerlər vəsaitlərin mübadiləsini dayandıra bilər, çünki ÇPY qanunları yalnız vəsaitlərin mənbəyi və təyinat hesab məlum olduğu halda onların köçürülməsinə icazə verir. Kriptovalyuta pulqabısının təyinatının fırıldaq olduğunu VAXT-a bildirmək onları pul yuyulmasının qarşısını almaq üzrə tədbir görməyə məcbur edəcək.

Əməliyyatın növü	Təsviri	İstintaqa təsiri
		Bu, VAXT-ın daxili komplayns siyasətindən asılı olsa da, bir neçə iş günü ərzində vəsaitin müvəqqəti dondurulması hüquq-mühafizə orqanlarına və ya prokurorlara vəsaitlərin geri qaytarılması üçün rəsmi sorğu ilə müraciət etməyə imkan verəcək. Bu, çevik addımlar atılarsa və kriptovalyuta brokeri cavab verərsə, mümkündür. Hər iki proses uğursuz olarsa, üçüncü ehtimal müəyyən edilmiş VAXT ilə əlaqə saxlayıb məlumat bazalarından istifadəçi hesabı yaratmış istifadəçinin kimliyi (çünki bu, fırıldaqçı və ya saxta şəxsiyyət ola bilər), onların identifikasiya məlumatları və əməliyyat heşi ilə bağlı bütün sübutları tələb etməkdir.
Kriptovalyutadan kriptovalyutaya	Zərərçəkən, FIAT valyutalarını emal edən ənənəvi maliyyə institutları ilə əlaqəsi olmayan, yalnız blokçeyn texnologiyası daxilində olan fırıldaqçılıq barədə məlumat verir. Məsələn, istifadəçinin başqa kriptovalyuta məhsulu (NFT, Staking və s. kimi) alması üçün aldadıldığı və maliyyə itkiləri ilə nəticələnən fırıldaqçılıq baş veribÇPY qanunları yalnız vəsaitlərin mənbəyi və	**Qabaqcıl təcrübə 1** **Mübadilədə iştirak etmiş "mərkəzləşdirilmiş birjalar" adlanan potensial lisenziyalı maliyyə vasitəçilərini axtarın. Əgər onlar tapılarsa, bu vasitəçi üzərindən iştirakçı tərəflər haqqında şəxsiyyət məlumatlarını toplamaq mümkün ola bilər.** **Qabaqcıl təcrübə 2** **Əksər hallarda zərərçəkən sosial şəbəkələr və ya proqramlar üzərindən fırıldaqçılığa məruz qalırlar ki, bu da əhəmiyyətli sayda kibertəhlükəsizlik izləri qoyur. Məsələn, şübhəlilər tez-tez zərərçəkənlərdən uzaqdan idarəetmə proqramları, e-poçtlar, telefon zəngləri, ilkin bank köçürmələri, sms və ya çat vasitəsilə onlarla əlaqə saxlamağı xahiş edirlər.** Bu halda zərərçəkənlər adətən Blokçeyn əsaslı maliyyə fırıldağı ilə üzləşirlər. İlkin vəzifə ən dəqiq və yenilənmiş köçürmə məlumatlarını toplamaqdır: əməliyyat vaxtları, zərərçəkənin istifadə etdiyi valyuta növləri, kriptovalyuta pulqabları, qəbzlər, e-poçtlar, sms təsdiqləri və digər məlumat növləri. (Ətraflı təfərrüatları növbəti "Sübutların toplanması" bölməsində, səh. 27-də tapa bilərsiniz).

Əməliyyatın növü	Təsviri	İstintaqa təsiri
Kriptovalyutadan FIAT valyutasına	Zərərçəkən pulun oğurlanması və ya itirilməsi barədə məlumat verir	Bu halda zərərçəkənin artıq kriptovalyuta birjasına göndərilmiş və daha sonra bank köçürməsi və ya fiziki ofisdə nağd şəkildə ödənilməsi üçün milli valyutaya dəyişdirilmiş kriptovalyutaları var idi. FIAT-dan kriptovalyutaya köçürmələrə bənzər şəkildə, burada milli valyuta ilə mübadilə aparan və bank köçürməsinə başlayan maliyyə vasitəçisinin tapılmasına ehtiyac var. Böyük məbləğ cəlb olunursa və maliyyə institutu aşağı riskli yurisdiksiyada yerləşirsə, bu qurum vəsaitlərin haradan gəldiyini nəzərdən keçirməlidir - bu addım komplayns əməkdaşları tərəfindən həyata keçirilir. Əgər belə bir yoxlama nəzərdə tutulubsa, o, adətən əməliyyat anından 24 saat ilə bir neçə iş günü arasında baş verir. Mümkünsə, kriptovalyuta pul kisəsinin ünvanını blokcheyn-pul kisəsi-axtarış sisteminə daxil edərək onu yoxlamaq və əlaqə saxlamaq mümkün olan maliyyə vasitəçisinə qoşulub-qoşulmadığını nəzərdən keçirin (ətraflı məlumat üçün “Virtual cinayət müstəntiqlri üçün əlavə alətlər” bölməsinə baxın, səh. 40). Əgər belə bir axtarış uğursuz olarsa, o zaman ünvanın tanınmış maliyyə institutuna qoşulub-qoşulmadığını göstərən xüsusi proqram təminatından (blokçeyn analitika provayderi) istifadə edilməlidir.

Sübutların toplanması

Sübutların toplanması

Məlumatların fərdlərdən toplanılması

İstintaq üçün əhəmiyyətli olan 10 məlumat

- **Aktivin təbiəti:** adı, rəmzi və əsas texnologiyanın xüsusiyyətləri daxil olmaqla hansı kriptovalyuta layihəsi və ya NFT iştirak etmişdir.
- **Əməliyyat təfərrüatları:** Zərərçəkənin etdiyi əməliyyatlar haqqında məlumat, məsələn, tarix, vaxt, məbləğ, valyuta və əməliyyat identifikatorları (məsələn, VAXT-dan daxilolmalar).
- **Pul kisəsi ünvanları:** Həm zərərçəkənin, həm də potensial fırıldaqçının cəlb olunan kriptovalyuta pul kisəsi ünvanlarının detalları.
- **Ünsiyyət qeydləri:** Zərərçəkənin ehtimal edilən fırıldaqçılarla, istər e-poçt, sosial media, çat proqramları, telefon zəngləri və ya forumlar vasitəsilə apardığı hər hansı ünsiyyətin qeydləri.
- **Təşviqat materialı:** Zərərçəkən tərəfindən virtual aktivlərlə bağlı qəbul olunan hər hansı reklamlar, onlayn yazılar və ya digər tanıtım materialları. E-məktubların nüsxələri ilə bərabər hiperlinklərin USB yaddaş cihazında göndərilməsində əmin olun. Xəbərdarlıq! Bu cür materialı nəzərə alarkən elektron materialda təqdim olunan heç bir hiperlinkə kliklәməyin, çünki onlar saxta və viruslu ola bilər.
- **Platformanın təfərrüatları:** Zərərçəkənin kriptovalyuta aktivini aldığı VAXT ("VAXTlar və KAXTlar" bölməsinə baxın, səh. 20) platforması və ya birjasının hər hansı təfərrüatları. VAXT-lardan məlumatların sorğulanması haqqında prosedurla tanış olmaq üçün aşağıdakı bölməyə baxın, "VAXT-lardan məlumatların sorğulanması," səh. 29. Birjaların adlarına çox vaxt əməliyyat qəbzlərində rast gəlmək olar.
- **İstinad məlumatı:** Zərərçəkənin aktiv barəsində öyrənməsinə səbəb olan məlumat, müraciət, onlayn reklam, və ya söz və s.
- **Kodlaşdırma anomaliyaları:** Olduğu təqdirdə, satışın qarşısını alan hər hansı manipulyasiya kodu sübutu və ya hər hansı digər qeyri-adi hallar. Cinayətə yardımçı olan vebsaytlara hər hansı hiperlinklər və yurisdiksiyadan asılı olaraq, zərərçəkən öz maliyyə məlumatlarını ayırdıqda, hüquq-mühafizə orqanlarına proqram təminatını başa düşməsinə kömək edəcək hər hansı giriş məlumatları
- **Maliyyə qeydləri:** Bank çıxarışları, kredit kartı çıxarışları və ya investisiya ilə bağlı vəsaitlərin köçürülməsini göstərən digər maliyyə sənədləri.
- **Şəxsiyyəti təsdiq edən məlumatlar:** İstifadəçi adları, sosial media profilləri, e-poçt ünvanları və ya zərərçəkənin kompüterində zərərçəkənlə qarşılıqlı əlaqə zamanı istifadə edilmiş hər hansı digər əlaqə məlumatı kimi fırıldaqçının müəyyən edilməsinə kömək edə biləcək hər hansı təfərrüatlar.
- **Texnoloji uyğunsuzluqlar:** Zərərçəkən aldadılma prosesi zamanı hər hansı proqram təminatı quraşdırıbmı? Bu proqram silinib, yoxsa hələ də kompüterdədir? Proqram təminatının mənbəyini və ya mənşəyini müəyyən etmək mümkündürmü?

Kriptovalyuta əməliyyatı dayandırılmayıbsa, vəsaitlərin göndərildiyi və ya alındığı kriptovalyuta pul kisəsinin ünvanını əldə etmək çox vacibdir.

Kriptovalyuta pulqabların ünvanlarının tapılması

Blokçeyn üzrə araşdırma üçün lazım olan ən vacib məlumat hansılardır?

Əməliyyat təfərrüatları: Kriptovalyuta pul kisəsinin ünvanı və Heş nömrələri

Ümumi səhv müvafiq kriptovalyuta pul kisəsinin ünvanlarının səhv qeyd edilməsidir, çünki bunlar uzun rəqəmlər və hərflər sətirlərini əhatə edir.

Nümunə 4: Kriptovalyuta pul kisəsinin ünvanını və s. qeyd edərkən sıfır rəqəmi "0" asanlıqla O hərfi ilə və ya q hərfi ilə g ilə qarışdırıla bilər Ən yaxşı təcrübə qeyd edilmiş kriptovalyuta pul kisəsinin ünvanını Google və ya Bing kimi internet axtarış sisteminə yazmaq və onun müəyyən edilib-edilmədiyini görməkdir. Ünvan dərhal görünməzsə, pul kisəsi axtarışı alətindən istifadə edilə bilər.

(Həmçinin "Virtual aktivlər üzrə istintaq üçün əlavə alətlər" bölməsinə baxın, səh. 47)

Kriptovalyuta pul kisəsinin ünvanı düzgündürsə, aşağıdakı məlumatları əldə etməyə imkan verən ani məlumat göstərilir:

Bitkoin üzrə:

- **Əməliyyatın məbləği:** Siz hər bir əməliyyatda göndərilən və ya alınan Bitkoin məbləğini görə bilərsiniz.
- **Əməliyyatın vaxtı:** Əməliyyatın bloka nə vaxt daxil edildiyini göstərən dəqiq vaxtı göstərir.
- **Kriptovalyuta pul kisəsinin cari balansı:** Hal-hazırda pul kisəsində olan Bitkoin-in ümumi məbləğinə baxa bilərsiniz.
- **Əməliyyatın Haşi:** Bu, hər bir əməliyyat üçün unikal identifikatordur, məsələn, ödəniş xidməti təminatçıları tərəfindən onun "barmaq izi" kimi istifadə edilən əməliyyat ID-si.

  Bəzi məhsullar üzrə mövcuddur, lakin hamısında deyil:
- **Əməliyyatın həcmi:** Bəzi xidmətlər tez-tez ABŞ dolları və ya Avro aparıcı FIAT valyutalarında mübadilə edilən əməliyyatın həcmi haqqında təfərrüatları təqdim edir.
- **Saat qurşağının fərdiləşdirilməsi:** Bəzi platformalar bir qayda olaraq UTC saat qurşağını dəyişmək imkanı təklif edir. Məsələn, istifadəçilər sübutların toplanmasına kömək edərək onu yerli saat qurşağına uyğunlaşdıra bilərlər.

Bir kriptovalyuta pul kisəsi ünvanında müxtəlif növ kriptovalyutaları saxlamaq mümkündürmü?

İstifadəçinin eyni şəxsi məlumatdan istifadə edərək müxtəlif virtual aktivlərə daxil olmaq üçün vahid proqramdan istifadə etməsi potensialı çoximzalı (MultiSig) pul kisəsində mümkün olur. MultiSig eyni məlumata malik müxtəlif virtual aktivləri idarə etmək üçün vahid bir proqramdan istifadə edir, və bununla müxtəlif kriptovalyutalarla işləmə prosesini asanlaşdırır.

Bankların müxtəlif valyutalar üçün (biri ABŞ dolları, digəri Avro üçün) unikal hesab nömrələrini təyin etdiyi kimi Bitkoin və Tron kimi müxtəlif blokçeyn texnologiyalarına əsaslanan kriptovalyutalar üçün də unikal pul kisəsi ünvanları tələb olunur.

MultiSig pulqabıları heç də mütləq şəkildə bir neçə fərdi məlumat tələb etmir; əvəzinə, onlar çoxlu özəl əməliyyata icazə vermək üçün çoxlu şəxsi açarların istifadəsinə əsaslanırlar. Bir şəxs birdən çox şəxsi açara sahib ola bilər və ya hər birinin öz şəxsi açarı olan bir neçə şəxs aktivlərin idarə edilməsində iştirak edə bilər.

Bu konsepsiyanın vizuallaşdırılması smartfon növləri ilə onların dəstəklədiyi əməliyyat sistemləri və ya proqramlar arasındakı fərqə bənzədilə bilər. Bəzi proqramlar yalnız Apple-ın iOS sistemi üçün nəzərdə tutulub və iPhone üzərindən işləyir, digərləri isə Android üçün uyğunlaşdırılıb və Apple cihazlarında işləməyəcək. Bununla belə, müxtəlif proqramçılar tərəfindən hazırlanmış müxtəlif proqramlar Android platformasında işləyə və Google Play Store-dan əldə edilə bilər. Eynilə, Ethereum blokçeynində qurulmuş ERC20 tokenləri kimi ümumi texnologiya ilə birləşdirilən kriptovalyutalar tək Ethereum əsaslı pul kisəsi ünvanı daxilində idarə oluna bilər.

Bu, bir proqram dükanından eyni platforma üzərində hazırlanmış çoxsaylı proqramların endirilməsini necə asanlaşdırdığını əks etdirir. Eyni şəkildə, Ethereum kimi eyni blokçeyndə hazırlanmış kriptovalyutalar, daha sadələşdirilmiş istifadəçi təcrübəsi üçün tək Ethereum əsaslı pul kisəsi ünvanında birləşdirilə bilər.

VAXT-dan məlumat sorğusu

Zərərçəkən pulun hansı virtual aktiv xidməti təminatçısına (VAXT) göndərildiyini bilmirsə, pul qabının ünvanlarını göstərən qəbzdə bu məlumat tapıla bilər. Əks halda, bu məlumatlar blokçeyn analitik provayder proqramından istifadə etməklə görünə bilər. Bu cür provayderlər qanunların virtual aktivlərin çirkli pulların yuyulması ilə mübarizə qaydalarına əməl etməli olduğunu açıq şəkildə bildirdiyi ölkələrdə qeydiyyata alınır. Bu qaydalara uyğun olaraq, VAXT-lar istifadəçilərinin şəxsiyyətini yoxlamalı və əməliyyatları qeyd etməlidir. Məsələn, Avropa İttifaqı daxilində, Beşinci Aİ ÇPY Direktivinə əsasən, Aİ daxilində fəaliyyət göstərən VAXT-lar üzv dövlətlərdə qeydiyyatdan keçməli və çirkli pulların yuyulmasına qarşı müxtəlif öhdəliklərə əməl etməlidirlər.

Əgər zərərçəkən vəsaitin hansı VAXT-a göndərildiyini və ya ondan gəldiyini bilirsə və hələ də sistemə giriş imkanı varsa (və ya bərpa edə bilər), onda ilk addım mübadilədən bütün köçürmə məlumatlarını çıxarmaqdır. Bu köçürmə məlumatına aparılan əməliyyatlar, göndərilən kriptovalyutalar və onların kriptovalyuta pul kisəsi ünvanları daxil olacaq.

Zərərçəkən pulun hara köçürüldüyünə və ya haradan göndərildiyinə əmin deyilsə, VAXT-ın adı bəzən zərərçəkənin bank və ya kart çıxarışında tapıla bilər.

Virtual aktivlərin və ya mübadilələrin bəzi adlarına PanCake Swap (https://pancakeswap.finance/) daxildir; Wasabi Pul kisəsi (https://wasabiwallet.io); Doge Coin (https://dogecoin.com/); və Bok Sikkə (https://www.investopedia.com/terms/s/shitcoin.asp). Bunlar kriptovalyuta dünyası ilə maraqlananlara dərhal tanış olmasa da, çox vaxt istifadə olunur.

Hətta Uniswap kimi tam təmərküzləşdirilmiş olduğunu iddia edən platformalar da .csv-də istifadəçilər üçün araşdırmaya kömək edə biləcək əməliyyat tarixçəsi imkanı təklif edir.

Dünyada icra olunan yüzlərlə mübadilə fonunda yalnız bir neçə şirkət adı geniş ictimaiyyət və ya hüquq-mühafizə orqanları tərəfindən asanlıqla tanınır.

Əgər istifadəçi VAXT-da öz hesabına giriş əldə edə bilmirsə, kömək üçün mərkəzləşdirilmiş VAXT və ya kriptovalyuta pul kisəsinə (xidmət təminatçısına) müraciət etmək imkanı qalır.

Ən yaxşı təcrübələrdən irəli gələrək VAXT-lar adətən telefonla heç bir məlumat verməyəcəklər, buna görə də zərərçəkənə məxsus vəsaitlərin mübadiləsini həyata keçirən VAXT və ya digər maliyyə institutlarına Hüquq Mühafizə Sorğusunun (HMS) göndərilməsi tələb olunur. HMS-in VAXT məqsədləri üçün doldurulması prosesi səhifə 22-də təsvir edilmişdir.

Mərkəzləşdirilmiş VAXT-dan ala biləcəyiniz məlumat aşağıdakılardır:

- Ad
- Soyad
- Doğum tarixi
- Şəxsiyyəti təsdiq edən sənədlərin surətləri[10]
- Tamamlanmış əməliyyatların həcmi
- Əməliyyatların dəqiq vaxtı[11]
- Əməliyyatın FIAT və kriptovalyutası[12]
- Agentin komissiyasının həcmi
- Sanksiya yoxlamasının və siyasi baxımdan əhəmiyyətli şəxslərin (PEP) yoxlanmasının təsdiq müddəti, həmçinin istifadə olunmuş izləmə siyahılarının növləri.
- Əməliyyatlar və valyutalar sayı çox olduqda, kriptovalyuta pul kisəsinin ünvanı və ya ünvanları
- Aparılmış əməliyyatlara əməliyyat hashləri

Aşağıdakı məlumatları almaq ehtimalı azdır, lakin yenə də mümkündür:

- Agentdə qeydə alınmış müştəri nömrəsi və ya şəxsiyyət vəsiqəsi
- Müştərinin elan edilmiş yaşayış ünvanı[13]
- Müştərinin qeydiyyat ünvanı[14]
- Platformanın qeydiyyatdan keçdiyi ölkədən asılı olaraq sosial müdafiə nömrəsi
- Agent (VAXT/KAXT) və müştəri arasında qarşılıqlı əlaqə (çox vaxt PDF formatında olur, çünki müştəri xidməti tez-tez Intercom və ya ZenDesk kimi kınar proqram təminatçıları ilə aparılır)
- Vəsaitləri sübut edən bütün sənədlər – istifadəçi tərəfindən yüklənmiş və göndərilən
- IP ünvanı (istifadəçilər VPN-lərdən istifadə etdikləri üçün bu, aldadıcı ola bilər)
- Mobil telefon və ya masaüstü kompüter kimi daxil olmaq üçün istifadə edilən cihaz
- Brauzer və xidmətə daxil olmaq üçün istifadə olunan versiya: Opera, Chrome, Safari, Internet Explorer və ya oxşar
- Açıq Mənbə Məlumatı (OSINT)[15] ilə həyata keçirilən müştəri haqqında məlumat yoxlanışı
- VAXT işçilərinin konkret istifadəçi və ya onun əməliyyatları ilə bağlı şərhləri
- VAXT əməkdaşları tərəfindən istifadəçi və ya onun əməliyyatları üzərində aparılan istənilən blokçeyn analitik araşdırmaları
- Digər hüquq-mühafizə orqanlarından və ya maliyyə institutlarından konkret istifadəçi haqqında hər hansı sorğular
- İstifadəçi tərəfindən başlanmış, lakin tamamlanmamış istənilən əməliyyat
- Fiziki ofislər və ya bankomatlar üçün binalardan istifadə edən şəxslərin video qeydi ola bilər
- İstifadəçilərin yüklədiyi bütün sənədləri (o cümlədən vəsaitin və ya gəlirin mənbəyinin sübutu), eləcə də müştəri xidməti ilə bütün qarşılıqlı əlaqəni tələb edin

Polis əməkdaşları zərərçəkəndən bank hesablarının təfərrüatları haqqında daha çox məlumat toplaya bilər ki, bu da VAXT-lardan toplanmış məlumatları filtrləməyə kömək edir. Bu məlumat yalnız FIAT-dan kriptovalyuta əməliyyatları üçün əlçatan olacaq (kripto-FIAT əməliyyatları üçün deyil).

- VAXT hesabına köçürmə həyata keçirmək üçün istifadə edilən zərərçəkənin bank hesab nömrəsi.

10 Bura pasport, şəxsiyyət vəsiqəsi və ya e-identifikasiya daxil ola bilər. Bununla belə, bu proses həqiqi şəxsiyyət sənədlərini təqlid edən saxta və ya kolleksiya əşyalarının istifadəsi (məsələn, dokumencik.pl kimi internet saytlarında mövcud olan "yığım sənədləri") kimi ənənəvi kibercinayətkarlıqla eyni məsələlərə qarşı həssasdır.

11 Vaxt hansı saat qurşağına aid olduğunu müəyyən etmək üçün vacibdir. Məsələn, bütün Bitcoin Blokçeyn əməliyyatları istifadəçinin haradan gəldiyindən asılı olmayaraq UTC (London vaxtı) ilə qeydə alınır. Yanlış əməliyyat vaxt digər sübutlarla əlaqələndirilməsi problemi bir sıra hallarda həlledici olmuşdur.

12 Həm virtual aktivlər, həm də nağd pul (FIAT).

13 Qanunlarla icazə verildiyi halda, platformada eyni ünvanda qeydiyyatdan keçmiş və əməliyyatlar aparmış digər müştərilərin olub-olmadığını yoxlamaq mümkündür.

14 Platformanın bu cür məlumatları ictimai məlumat bazasından çıxarıb-çıxarmaması.

15 Platformanın komplayns işçiləri tərəfindən çıxarıla bilən cinayət qeydləri və ya xüsusi müəssisələrin UBO haqqında məlumat kimi ictimaiyyət üçün açıq olan məlumat mənbələrindən çıxarışlar daxil ola bilər.

- Telefon nömrəsi: Bəzi istifadəçilər telefonlarının ödəniş sistemindən istifadə edirlər

- Əməliyyat üçün istifadə edilmiş kredit, debet və ya əvvəlcədən ödənilmiş kartdan kart məlumatları. Provayderin hesabında mobil bank proqramı və ya 3D təhlükəsiz adlı SMS xidməti vasitəsilə ikinci səviyyəli təsdiq kimi əlavə məlumat ola bilər.

- "Açıq bankçılıqdan" istifadə edən ölkələr üçün bu əməliyyatları həyata keçirən ödəniş xidməti təminatçılarından əlavə məlumat əldə edilə bilər (əgər bu əməliyyatlar açıq bankçılıqdan istifadə etməklə tamamlanıbsa)

VAXT sorğular üçün məlumat formatı

Optimal səmərəlilik üçün hüquq-mühafizə sistemlərinə birbaşa inteqrasiyanı asanlaşdıran ".csv" formatında tələb olunan əməliyyat məlumatlarını əldə etmək məsləhətdir. Adatən Hüquq-Mühafizə Sorğularına (HMS) cavablar iki formatda təqdim olunur:

- Virtual Aktiv Təminatçısı Hüquq-Mühafizə Orqanları (HMO) tərəfindən edilən sorğulara birbaşa cavabları əks etdirən ".pdf" faylı

- Tranzaksiya məlumatlarından ibarət ".csv" faylı

Çox vaxt VAXT-lar müştəriyə dair məlumatları vahid bir qovluqda saxlayır. Bu qovluğa vəsaitin sübutu (POF) və digər yüklənmiş fayllar kimi mühüm sənədlər daxildir. Böyük VAXT-lar adətən HMO sorğularına cavab vermək üçün müəyyən qaydaya malikdirlər. Kiçik qurumlarla qarşılıqlı əlaqədə olarkən HMO tələb olunan məlumatı almaq üçün öz üstünlük verdiyi məlumat formatını müəyyən edə bilər.

Bununla belə, müştərinin şəxsiyyətini təsdiq edən sənəd ".pdf" və ya ".jpeg" faylda və ya ".avi" və ya ".mov" kimi formatlarda video kimi saxlanılar bilər

VAXT-lardan ".xml" və ya ".xls" faylları tələb etməkdən çəkinmək tövsiyə olunur. Xüsusilə, ".xlsx" fayllarının istifadəsi kibertəhlükəsizliyə görə tövsiyə edilmir. VAXT-lar tərəfindən ".xlsx" formatında təqdim edilən məlumatların, xüsusən də fayla daxil edilmiş makrolarda virusları saxlaya bilməsi riski var ki, bu da HMO kompüter sistemlərinin təhlükəsizliyini poza bilər.

Əldə edilmiş İP ünvanların etibarlılığı

İnternet Protokolu (IP) çox vaxt hüquq-mühafizə orqanlarının sorğu prosesi vasitəsilə VAXT-dan əldə edilə bilər. IP ünvanı internet şəbəkəsində smartfon və ya noutbuk kimi cihazın unikal identifikatorudur. IP ünvanını telefon nömrəsi kimi unikal nömrələr dəsti kimi düşünün. Məsələn, 193.46.242.201, Stokholm, İsveç. Ancaq bir stasionar telefon nömrəsi bir evdə bir neçə ailə üzvü tərəfindən paylaşıldığı kimi, NAT (Şəbəkə Ünvanının Şərhi) adlı texnologiya sayəsində birdən çox cihaz eyni IP ünvanından istifadə edə bilər.

VAXT-lar adətən istifadəçilərin giriş prosesi zamanı qeydə alınan IP ünvanlarını tapa bildiklərini iddia edirlər, lakin bu məlumatların araşdırmalar üçün etibarlılığı şübhə altına alınmalıdır. IP ünvanları yalnız kimin istifadə etdiyini deyil, hansı cihazın internetə daxil olduğunu göstərir. Onlar virtual şəxsi şəbəkələrdən (VPN) istifadə edən fırıldaqçılar tərəfindən maskalana bilər və buna görə də yalnız istifadəçinin İP-si potensial cinayət fəaliyyəti ilə əlaqələndirə biləcək digər sübutların olduğu hallarda istifadə edilməlidir.

İstifadəçilərin evlərinə internet təmin edən şirkətlər (internet xidməti təminatçıları, "İSP"lər) adətən müəyyən bir zamanda müəyyən bir IP ünvanından kimin istifadə etdiyini müəyyən edə bilərlər.

Araşdırma zamanı bu cür şirkətlərdən xidmətləri üçün müqavilə bağlamış xüsusi istifadəçilərə ünvanı qoşmaq tələb oluna bilər. Təəssüf ki, istifadəçi VPN-dən istifadə etməsə belə, bu məlumat heç də həmişə etibarlı olmur. İstifadəçilər WIFI şəbəkələrini parolsuz təmin edə bildiyi üçün başqasının IP ünvanından istifadə olunduğu vaxtlar ola bilər.

Tək bir IP ünvanını bilmək heç də hər zaman onlayn kimin konkret hərəkət etdiyi barədə dəqiq məlumat vermir. Dövlət idarələri, məktəblər və ya iş yerləri kimi mühitlərdə birdən çox fərd eyni internet bağlantısını paylaşa bilər ki, bu da onlayn hərəkətlərin konkret şəxsə aid edilməsini daha da çətinləşdirir.

Nəhayət, VPN-lər əlaqənin fərqli bir yerdən yarandığı görünüşü proyeksiya edərək istifadəçinin faktiki IP ünvanını gizlətmək üçün hazırlanmışdır. Bununla bərabər, VPN ilə belə, müəyyən bir istifadəçi hərəkətlərini müəyyən bir müddət ərzində müəyyən bir IP ilə əlaqələndirərək, müəyyən veb-saytlara baxmasını əlaqələndirmək imkanı ola bilər. Bu o deməkdir ki, VPN-lər istifadəçinin anonimliyini artırsa da, onlayn hərəkətləri tamamilə izlənilməz etmir. Fərqli qurumlar hələ də müəyyən şərtlər daxilində onlayn fəaliyyətləri fərdi istifadəçilərlə əlaqələndirə bilər.iyini müəyyən edə bilərlər.

İP ünvanların toplanması

Lehinə arqumentlər

- **İzlənmə qabiliyyəti:** İP ünvanları potensial şübhəliləri izləmək və ya şübhəli fəaliyyətlərin mənşəyini müəyyən etmək üçün başlanğıc nöqtəsi kimi xidmət edə bilər. Onların başqa araşdırmalara əlaqə ehtimalı ola bilər.

- **Profilaktika:** IP ünvanlarına nəzarət edildiyini bilmək potensial cinayətkarları qanunsuz fəaliyyətlər üçün öz şəbəkələrindən istifadə etməkdən çəkindirə bilər.

- **Collaborative evidence:** Digər sübutlarlar birlikdə İP ünvanları şübhəlilərə qarşı daha əsaslı ittihamın qurulmasına kömək edə bilər.

Roman Bieda Qazaxıstanda müstəntiqlər üçün praktiki seminar keçirir. Blokçeyn təhlili alətinin sabiq məhsul sahibi və Avropa və ABŞ-da məhkəmələrdə ekspert şahidi kimi o, təkcə bilikləri deyil, həm də sübutların toplanması prosesi zamanı üzləşdiyi çətinliklərlə bağlı ən yaxşı təcrübələri və fikirləri paylaşmağa diqqət yetirir. ATƏT-in seminarlarının məqsədi bir iştirakçı dövlətdə yaşanan problemlərin digərlərində təkrarlanmasına ehtiyac qalmamasını təmin etməkdir.

Əleyhinə arqumentlər:

- **Qeyri-dəqiqlik:** Birdən çox cihaz bir IP ünvanını paylaşa, habelə VPN-lər və digər çaşdırıcı üsullardan istifadə oluna bilindiyəndən, yalnız IP ünvanlarına etibar etmək yanlış identifikasiyaya səbəb ola bilər.

- **Məxfiliklə bağlı problemlər:** Xüsusən də müvafiq əsaslandırma olmadan İP ünvanlarının kütləvi şəkildə toplanması fərdlərin məxfilik hüquqlarını poza bilər.

- **Resurslara ehtiyac:** IP ünvanlarını izləmək və yoxlamaq, xüsusən VPN-lər və ya digər maskalama alətləri cəlb edildikdə, vaxt apara və resursları digər mühüm istintaq fəaliyyətlərindən yayındıra bilər.

Nəticədə, IP ünvanları müəyyən bir zamanda cihazın fəaliyyəti və müəyyən bir cihazın yeri haqqında əlavə məlumat verə bilsə də, fərdi istifadəçiləri heç bir halda müəyyən etmir. IP ünvanlarına əsaslanan araşdırmalar yalnız ehtiyatla yanaşdıqda və daha böyük alətlər dəstinin bir hissəsi kimi baxdıqda faydalıdır.

Digər mühüm sənədlər

ATƏT-in bir sıra iştirakçı dövlətlərində virtual aktivlərlə (məsələn, kriptovalyutalar) məşğul şirkətlər "tənzimlənən maliyyə institutları" və ya vasitəçilər hesab edilir. Bu o deməkdir ki, onlar mütəmadi olaraq müştərilərinin fəaliyyətinə nəzarət etməlidirlər. Onlardan potensial risk mənbələrini müəyyən etmək üçün blokçeyn analitika alətlərindən istifadə edərək şübhəli davranış nümayiş etdirən müştəriləri və əməliyyatları nəzərdən keçirmələri tələb olunur. Bu yoxlamalar aparıldıqdan və sənədləşdirildikdən sonra hüquq-mühafizə orqanları onlarla tanış olmaq üçün müraciət edə bilər.

Məsələn, Gürcüstan Respublikasında Gürcüstan Milli Bankında qeydiyyatdan keçmiş mübadilə xidmətləri göstərən şirkətlər blokçeyn əməliyyatlarını təhlil etmək üçün xüsusi alətləri istifadə etmək məsuliyyəti daşıyır. **Bu, virtual aktivlərin axınının monitorinqində şəffaflıq və təhlükəsizlik səviyyəsini təmin edir.**

HMO-ların sözügedən blokçeyn analitik alətlərinə çıxışı yoxdursa, onlar VAXT-dan təhqiqat üçün təfərrüatlı məlumatı paylaşmağı tələb edə bilərlər. Bu məlumat PDF və ya şəkil faylı kimi əlçatan və redaktə edilə bilən formatda ola bilər.

Digər sözlə, alətlər əməliyyatların bütövlüyünün qorunmasında və qeyri-qanuni fəaliyyətlərin müəyyən edilməsində mühüm rol oynasa da, bu alətlərdən əldə edilən məlumatların paylaşılması zamanı nəzərə alınmalı olan prosedur və hüquqi mülahizələr var. Məsələn, çoxsaylı blokçeyn təhlili və uyğunluq həlləri təminatçıları əvvəlcədən razılıq olmadan hətta hüquq-mühafizə orqanları ilə belə həssas və ya redaktə edilə bilən məlumatların paylaşılmasını məhdudlaşdıran xüsusi protokollara və razılaşmalara malik ola bilər.

Bu, etibarlı məlumatı açıqlamağa hazır olan VAXT-lar üçün müqavilə şərtlərinə əsasən sübutları məhdudlaşdırmaq məsuliyyəti arasında ziddiyət yarada bilər.

İşlərin məhkəməyə çıxarılması

İşlərin məhkəməyə çıxarılması

Virtual aktiv işləri üzrə prokurorlar

Prokurorların işləmək üçün tutarlı əsaslara malik olmasını təmin etmək məqsədilə HMO əməkdaşları çirkli pulların yuyulmasına qarşı mübarizə (ÇPY) fəaliyyətləri ilə bağlı sübutların toplanması, xüsusən də virtual aktivlərin və kriptovalyutaların sürətlə artan sahəsini yaxşı bilməlidirlər.

Araşdırma mərhələsi

- **Rəqəmsal sübut axtarın:** Blokçeyn texnologiyası və müştərək kitablar üzrə əməliyyatları öyrənin və izləyin.
- **Məlumatı təhlil edin:** Kriptovalyuta birjalarında sürətli və yüksək həcmli əməliyyatlar kimi çirkli pulların yuyulmasını təklif edə biləcək nümunələri ayırd edin.
- **Rəqəmsal axınları izləyin:** Lazım gəldikdə, xüsusi proqramlardan istifadə edərək, çoxsaylı virtual pulqabıları və platformalar üzrə aktivlərin axınını izləyin.
- **VAXT-lardan alınan bütün qəbul edilmiş şəxsiyyət məlumatlarının etibarlılığını qiymətləndirin** ("Şəxsiyyət sənədlərinin surətləri" ilə bağlı problemlərə baxın, səh. 30)

Məhkəmə və ya istintaqa hazırlıq

a. İşin ümumi təsviri:

- Kripto pul kisələrinə, IP ünvanlarına, əməliyyatların dəqiq vaxtına və rəqəmsal sahədə mübadilə edilən məbləğlərə diqqət yetirilməlidir.
- İlk məqsəd virtual aktivlərin əmlak və ya mallar kimi maddi aktivlərə çevrilməsini anlamaq və onların mənşəyini izləmək olmalıdır.

b. Cinayət növünün müəyyən edilməsi:

- Kriptovalyutanın pulların yuyulması üçün vəsaitlərin mənbəyini gizlətmək məqsədi daşıyan "sxemlər (tumbling)" və ya "qarışdırma (mixing)" xidmətləri vasitəsilə istifadə edilməsinin əlamətlərini müəyyən edin. Bəzi aparıcı blokçeyn analitika təminatçıları mikser vasitəsilə emal olunan əməliyyatları ayırd edə bildiklərini iddia edən "demiksinq xidmətləri" təklif edirlər. Əgər iş ciddi əhəmiyyət kəsb edirsə, həm blokçeyn analitika təminatçıları tərəfindən təklif olunan demiksinq xidmətləri, həm də Europol kimi HMO tərəfindən təklif olunan demiksinq kurslarına müraciət edin.
- Cinayətin elementlərini sübut etmək üçün blokçeyn əməliyyatlarının reyestrindən istifadə edin.

c. Cinayət fəaliyyətinin aktivlərlə əlaqələndirilməsi:

- Kriptovalyuta pulqablarının maddi və ya digər virtual aktivlərin alınmasına qədər istənilən hərəkətlərini izləyin. Bu, kriptovalyutanın birjadan şəxsi pul kisəsinə, sonra isə başqa bir quruma və ya xidmətə yönəldilməsini araşdırmağı əhatə edə bilər.
- İstifadə olunan hər hansı anonimləşdirmə xidmətlərini və ya üsullarını müəyyən edin və çətinliklərə baxmayaraq, aktivləri izləməyə çalışın.
- Böyük miqdarda kriptovalyutanın çoxsaylı pulqablarına paylanması və ya Monero və ya Zcash adlı məxfilik sikkələrinin istifadəsi kimi çirkli pulların yuyulması kimi cinayət niyyətini göstərə bilən nümunələrin fərqində olun.

Sübutların təqdimatı:

- Kriptovalyutaların və blokçeynin necə işlədiyini aydın şəkildə izah edin, çünki bir çox məhkəmə əməkdaşı bu texnologiyadan məlumatsız ola bilər.
- Qeyri-qanuni vəsaitlərin mənbəyindən onların son təyinat yerinə qədər çirkli pulların yuyulması prosesinin aydın və qısa rəqəmsal izini təqdim edin. Sübut təqdim edərkən əyani rekvizitlər yaratmaq və asan, texniki olmayan dildən istifadə etmək tövsiyə olunur, çünki bir çox prokuror və ya hakim kriptovalyutaların mürəkkəbliyi ilə hələ tam tanış olmaya bilər.

Əlavə sübutlar:

- Kriptovalyuta ilə əməliyyat qeydləri: Bunlar istifadəçi fəaliyyəti təfərrüatları, pul kisəsinin ünvanları, IP qeydləri, əməliyyat məbləğləri və tarixləri təmin edə bilər.
- Blokçeyn təhlil proqramı: Bu, rəqəmsal valyutaların axınını vizuallaşdıra bilər.
- Rəqəmsal pulqabıların təhlili: Aparat, mobil və masaüstü pulqabları araşdırın. Onların faydalı ola biləcək qeydləri, əməliyyat tarixçəsi və ya metadatası ola bilər.
- IP ünvanının izlənməsi: Şübhəli şəxslərin coğrafi yerini tapmaq üçün əməliyyatlarla əlaqəli IP ünvanlarını izləyin. (IP ünvanlarının məhdudiyyətləri üçün s. 31-ə baxın)

- Beynəlxalq agentliklərlə əməkdaşlıq: Kriptovalyutaların mərkəzləşdirilməmiş təbiətinə görə, beynəlxalq əməkdaşlıq transsərhəd əməliyyatları izləmək üçün mühüm əhəmiyyət kəsb edə bilər. Bununla belə, bu cür əməkdaşlıq adətən sonrakı mərhələdə baş müstəntiq tərəfindən başlanır.[16]

Kriptovalyuta əməliyyatları və fəaliyyətləri ilə bağlı hərtərəfli sübutlar toplayaraq, polis əməkdaşları istintaq həmkarlarına, eləcə də prokurorlara işi ətraflı araşdırmaq və günahkarların məsuliyyətə cəlb olunmasını təmin etmək üçün möhkəm baza təmin edə bilər.

16 Egmont Group ilə birlikdə işləyən Maliyyə Kəşfiyyat Bölmələri buradan əldə edilə bilən mübadilə sistemi mexanizmini işləyib hazırlayıblar: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf 16(son baxış 15 fevral 2024-cü il)

Mürəkkəb hallar üçün tövsiyələr və əlaqə məlumatı

Mürəkkəb hallar üçün tövsiyələr və əlaqə məlumatı

Xüsusi qruplar və təcrübə

Blokçeyn təhlili üzrə aparıcı təminatçılar tez-tez həm kriptovalyuta, həm də istintaq proseslərində ekspertlərdən ibarət xüsusi qruplar yaradırlar. Bu qruplar hüquq-mühafizə orqanlarına blokçeyn analitikasının incəliklərini dərindən başa düşməkdə kömək, alətlərin maksimum potensialından istifadə olunmasını təmin etmək üzrə ixtisaslaşırlar. Hansı şöbələrin blokçeyn əsaslı təhlil proqram təminatından artıq istifadə etdiyini öyrənmək üçün qurumun intranetini yoxlamaq tövsiyə olunur, çünki həmin şöbədəki həmkarlar bu məsələ ilə bağlı daha çox məlumata sahib ola bilərlər.

Təlim və sertifikatlaşdırma

Blokçeyn texnologiyalarının mürəkkəbliyini və ciddi biliklərin idarə edilməsinin vacibliyini dərk edərək, bir çox blokçeyn təhlili üzrə proqram təminatçıları da sistemli təlim proqramları təklif edir.

Bu proqramlar adətən müxtəlif səviyyələrdə sertifikatlaşdırma ilə başa çatır ki, bu da təkcə HMO işçilərinin bacarıqlarını təsdiqləmir, həm də blokçeynlə əlaqəli araşdırmaları idarə etməkdə onların səmərəliliyini artırır. Bəzi xidmətlər məsləhət dəstəyi çərçivəsində ödəniş tələb edə bilsə də, daha ciddi istintaq imkanları baxımından uzunmüddətli faydası da əhəmiyyətli ola bilər.

Müfəssəl araşdırmalar üçün kənar dəstək

Daxili komandalar və təlimlərdən əlavə, blokçeyndə kriptovalyuta əməliyyatlarının hərtərəfli araşdırmalarını aparmağa qadir geniş sayda xarici kommersiya təminatçıları fəaliyyət göstərir. Bu qurumlar HMO-na öz ixtisas bacarıqlarını təklif edərək podratçı kimi çıxış edirlər. Xüsusən də dərin təhlil və çoxşaxəli istintaq üsullarının tələb olunduğu mürəkkəb hallarda onları təcrübəsi əvəzolunmaz ola bilər. INTERPOL və ya Europol kimi HMO-lar müstəntiqlər üçün xüsusi dəstək və təlim təklif edir (“Rəqəmsal aktivlər üzrə ekspertlərlə əməkdaşlıq” bölməsi, səh. 51-ə baxın). Qrupunuz təlim tədbirlərinə qoşulmaq istədiyi halda əlavə məlumat almaq üçün VirtualAssets@osce.org ilə əlaqə saxlayın.

Ehtiyatla davranın

Bununla belə, xarici təminatçıların təklif etdiyi üstünlüklərin çox olmasına, istifadəçi qurumlar potensial çətinliklərin fərqində olmalıdırlar. Məsləhət agentlikləri və ya blokçeyn əsaslı təhlil təminatçıları kimi xarici qurumları həssas araşdırmalara cəlb etmək işin icraatında çətinliklər yarada bilər. Məlumat təhlükəsizliyinin həssas məqamlarını da unutmayaq. Məlumatların bütövlüyünün qorunub saxlanmasını və məxfi məlumatın təsadüfən sızmaması üçün həssas məlumatların üçüncü tərəflərə ötürülməsinə son dərəcə ehtiyatla yanaşmaq lazımdır.

Maçiej Szulç ATƏT-in iştirakçısı olan dövlətlərin siyasətçilərinin mürəkkəb işlərin həlli və milli maraqlı tərəflərə köməklik göstərilməsi üçün ən yaxşı təcrübələri paylaşdıqları Qdanskda təlimçi-təlimçi seminar aparır. Diqqət məzmun keyfiyyətindən başlayaraq idarəetmə üsullarına qədər əhatə edir.

Zərərçəkənlərə dəstək

Zərərçəkənlərə dəstək

Zərərçəkənlərin fərqində olmalı olduğu çətinliklər

Kriptovalyuta fırıldaqının qurbanları asanlıqla digər cinayətin də qurbanına çevrilə bilər. Mütəşəkkil fırıldaqçılar sadəcə bir cəbhədən vurmur, əksinə qurbanlarını təkrar-təkrar və strateji olaraq hədəfə alırlar. Aşağıda ikinci dərəcəli fırıldaqların ümumi təfərrüatları təqdim olunur:

- "Xilaskar" oyunu: Bir şəxsin fırıldaq şəbəkəsi ilə ilkin təmasından sonra, eyni qrupun fərqli bir qanadı itirilmiş sərmayələrini geri qaytarmağa kömək edə biləcək bir peşəkar kimi özünü təqdim edib kömək təklifini edir. Bu ilk baxışdan səxavətli təklifin də öz qiyməti var və zərərçəkən şəxsdən itirilmiş vəsaiti bərpa etmək üçün xidmət pulunu ödəməsi gözlənilir. Əksər hallarda vəsaitlər köçürüldükdən sonra "xilaskar" da itirilmiş vəsaitlərlə birlikdə yoxa çıxır.

"Xəbərçi" tələsi: Digər hallarda fırıldaqçılar fırıldaqçı şirkətin narazı sabiq işçiləri kimi davrana və qurbanlara aktivlərini geri qaytarmağa kömək edə biləcək daxili biliklərə sahib insanlar kimi hərəkət edə bilərlər. Proses "xilaskar" oyununa bənzərdir – əvvəlcədən xidmət haqqı ödənilməlidir və sonra bu şəxsdə dərhal əlaqəni kəsir.

- Hüquqi prosesin saxta görüntüsü: Bunlar, xüsusilə VAXT-lar istifadə olunduqda, pulu geri almağı vəd edən hüquq mütəxəssisinin qurbanlara müraciət etdiyi ssenarilərdir. Zərərçəkən saat-hesabı tariflə razılaşdıqdan sonra, bu "vəkillər" geniş iş apardıqların iddia edir və bəzən 40 səhifədən çox sənəd tərtib edirlər. Bu kimi sənədlər çirkli pulların yuyulmasının (ÇPY) əleyhinə və terroçuluğun maliyyələşdirilməsi (TM) ilə mübarizə aparan qanunvericiliyinin əsas təməl prinsiplərinin təfərrüatlarına, lakin məhdud hüquqi dəyəri malik olurlar. Təəssüf ki, istifadə edilən sənədlər əsasən ümumi sözlərdən ibarətdir və onların 99%-i oxşar məzmunludur, buna görə də VAXT kiçik fərqləri olan oxşar sənədlərlə doludur. Zərərçəkənlərdən bu kimi saysız-hesabsız lüzumsuz şeylər üçün həddindən artıq yüksək pul alınır. Əksər VAXT-lardan istifadə etməklə edilən əməliyyatların geri dönməz olduğunu başa düşmək vacibdir. "Kredit kartı üzərindən ödənişlərin geri qaytarılması" iddiasının müvəffəqiyyət şansı azdır. Beləliklə, bu cür hüquqi fəaliyyət cəhdləri adətən aşağı dəyərə malikdir və zərərçəkənin vəsaitlərini havaya sovudur.

ATƏT-in Virtual Aktiv Eksperti və Europol Maliyyə Kəşfiyyatının Dövlət-Özəl Tərəfdaşlığının (EFIPPP) Kripto-Aktivlər İş Qrupunun həm-sədri Olqa de Truxis virtual aktivlər və virtual aktiv xidməti təminatçıları ilə bağlı maliyyə cinayəti risklərinin idarə edilməsində ənənəvi maliyyə təminatçıları üçün ən yaxşı təcrübələrə dair sessiyaya rəhbərlik edir. Latviya Milli Bankının (Latvijas Banka) binasında keçirilən seminarda ATƏT-in əlavə dörd iştirakçı dövlətinin nümayəndələri də iştirak ediblər.

Kriptovalyutalarla bağlı törədilmiş cinayətlərin seçilmiş növləri

Kriptovalyutalarla bağlı törədilmiş cinayətlərin bir neçə nümunəsi

Aşağıda kriptovalyutalar ilə törədilən ən çox yayılmış cinayət növləri haqqında ətraflı məlumat verilmişdir. Siyahı cinayətlərin tam çeşidini əhatə etməsə də, ən azından bu növ cinayətlər haqqında məlumatlı olmaq lazımdır.

Kriptovalyuta investisiya sxemləri

Təsviri

Kriptovalyuta ilə investisiya fırıldaqları saxtakarlıq sxemlərinin ən çox yayılmış növlərindən biridir. Əvvəlcə bu fırıldaqçılıq yüksək gəlirli ölkələrdəki varlı və yaşlı vətəndaşları hədəf alırdı. Bununla belə, taktikalar inkişaf edir, birja investorları və təqaüdə yaxınlaşanlar getdikcə daha çox hədəfə alınır. Gələcəkdə bu fırıldaqçılığın yeni növlərinə diqqət yetirmək və uyğun tədbirlər görmək çox vacibdir.

Bu sxem varlı şəxslərlə əlaqə saxlayaraq onlara gəlirli investisiya imkanları təqdim edən fırıldaqçılar tərəfindən tətbiq olunur. Adətən bir fırıldaqçı özünü təcrübəli kripto investoru kimi təqdim edərək, ciddi sərvətə malik və bu sahədən bixəbər şəxsləri hədəf alır.

Bu fırıldaqçılığın müxtəlif növləri

Qurulan müxtəlif tələ növləri:

- **Avans rüsüm ödənişi:** Fırıldaqçılar yatırılacaq investisiyaların yüksək gəlir gətirməsi vədi ilə insanları cəlb edirlər. Bununla belə, Bununla belə, prosesi başlamaq üçün onlar adətən bu diapazonun aşağı həddindən, yəni 250 avrodan 1000 avroya (və ya müvafiq milli valyutada ekvivalenti) qədər ilkin ödəniş istəyirlər. Bu ilkin ödənişi aldıqdan sonra fırıldaqçı sadəcə olaraq ödənişdən sonra yoxa çıxır və qurbana heç bir perspektivli sərmayə göstərmədən maddi cəhətdən zərər vurmuş olur.

- Daha mürəkkəb bir üsul isə prosesin canlı video zənglə aparılmasıdır ki, bu müddət ərzində fırıldaqçı ciddi pul axını əldə edəcək potensial qurbana məxsus olduğu iddia edilən "maliyyə hesabı" nümayiş etdirir. Bu hesablar həqiqi görünmək üçün nəzərdə tutulsa da, onlar əslində saxta nüsxələridir və ənənəvi maliyyə institutları ilə heç bir əlaqəsi yoxdur.

- Bəzən qurbanı daha çox ödəməyə sövq etmək üçün, ona 50-100 avro kimi "ilkin vəsait" köçürürlər və fırıldaqçılar bunu güya investisiyaların gətirdiyi faiz kimi təqdim edirlər.

- **Şəxsiyyət oğurluğu:** Həqiqilik illüziyası yaratmaq üçün fırıldaqçılar pul köçürmələri və ya depozitlər üçün qurbanın şəxsi identifikasiya məlumatlarını tələb edirlər. Bununla belə, investisiyaya kömək etmək əvəzinə, qurbanın şəxsi və maliyyə detallarına icazəsiz giriş əldə edirlər. Zərərçəkənlər maliyyə təşkilatında şəxsiyyətlərini təsdiq edən sənədləri bloklamağı unudur və ya hətta bu məlumatların surətlərini fırıldaqçıya göndərirlər.

Problemi necə həll etməli

- **Əlavə köçürmə müraciətlərini rədd edin.** Adətən fırıldaqçılar kiçik köçürmə xərcləri və ya fırıldağın ümumi məbləği ilə müqayisədə çox kiçik görünən ödəmə xərcləri haqqında danışırlar. Misal: 60.000 avro fırıldaq üçün 600 avro rüsum.

- **Qurban ünsiyyəti kəsməməlidir.** Adətən zərərçəkən HMO-a müraciət edənə qədər onların fırıldaqçı ilə əlaqəsi artıq kəsilir. Amma əlaqə kəsilməyibsə, bu istifadə olunan kibercinayətkarlıq alətlərinin axtarışını təmin etməkdə istintaqa kömək edə bilər.

İnvestisiya, maliyyə və ya onlayn alətlərdən istifadədə daha az təcrübəli insanlar üçün fırıldaqçılar tez-tez məsafədən (uzaqdan) müdaxilə proqramı quraşdırırlar.

Bu cür proqramlar ilk növbədə uzaqdan giriş, nəzarət və dəstək üçün nəzərdə tutulmuşdur. O, istifadəçilərə istənilən yerdən öz masaüstü və ya noutbuk və serverlərinə məsafədən daxil olmaq və onları idarə etmək imkanı verir. Zərərçəkən adətən belə bir proqramı fırıldaqçının köməyi ilə quraşdırır. Bağlantı qurulduqdan sonra qurbanlar proqramı silməyi unudurlar. Proqramın yaddaşında qalan izlər düzgün saxlanıldığı halda, onlar hüquq-mühafizə orqanlarının araşdırması üçün faydalı ola bilər.

Proqram təminatının növündən asılı olaraq, müxtəlif funksiyalar mövcuddur:

- **Məsafədən idarəetmə:** İstifadəçilər kompüteri sanki onun qarşısında oturmuş kimi başqa yerdən idarə edə bilərlər. Bu, problemləri həll etmək, uzaqdan dəstək göstərmək və ya fayllara daxil olmaq üçün faydalıdır.
- **Fayl göndərilməsi:** İstifadəçilərə kompüterlər arasında faylları göndərməyə imkan verən proqram. Bu, bəzən istifadəçinin yazdığı hər şeyi izləyən və kompüterə quraşdırıldıqdan sonra illər ərzində onu fırıldaqçılarla paylaşa bilən bir növ "keylogger"in tətbiqinə gətirib çıxarır.
- **Məsafədən giriş:** Bu, fırıldaqçılara qurbanın kompüterinə və ya serverinə uzaqdan daxil olmaq və faylları dəyişdirmək, proqramlar quraşdırmaq və ya əlaqə yaratmağa imkan verir.
- **Mobil giriş:** Bu, smartfon və planşetlərdən cihazları uzaqdan idarə etməyə imkan verir.

- **Qurbanlar öz cihazlarında** yerləşdirilmiş proqram təminatını silməməlidirlər, çünki bu, istintaq üçün faydalı kibertəhlükəsizlik izlərinə malik ola bilər. Bununla belə, qurban onun cihazında nə yazdığını izləyən və ya kameranı açıq saxlayan proqram təminatının olması ehtimalından xəbərdar olmalıdır. Bu halda cinayət qurbanı öz cihazından istifadəni məhdudlaşdırmalıdır.
- **Paylaşılan şəxsi məlumatları nəzərdən keçirmək.** Mümkün olduqda, bank hesabına giriş məlumatlarını dəyişin və belə alətlərdən istifadə edildiyi təqdirdə e-identifikasiya alətləri üçün yeni parollar sifariş edin.
- Yuxarıda səh. 38-də **İkinci dərəcəli fırıldaqçılar bölməsini nəzərdən keçirin.**
- **Atılacaq müvafiq addımlar qurbanın konkret vəziyyətindən asılıdır.** Əlavə məlumat üçün "Hər bir əməliyyat növü üçün ən yaxşı təcrübə" bölməsinə baxın, səh. 24.

Bu kimi fırıldaqçılığın digər fəndi saxta məşhur şəxslərin paylaşımlarından istifadədir. Fırıldaqçılar həqiqi fotoları ələ keçirir və onları uydurma hesablar və ya reklam materialları ilə birləşdirərək, sanki tanınmış şəxsiyyətlərin sxemə zəmanət verməsi kimi təqdim edir.

Məcburetmə və cinsi şantaj

Məcburetmə hallarında, fərdlər adətən hakerin qurbanın kompüterinə giriş əldə etməsi və noutbuk və ya smartfonun kamerasına qoşula bilməsi barədə yalan məlumat verən mürəkkəb e-poçt məktubu alır. Cinsi şantajdən isə adətən hakerin qurbanı masturbasiya hərəkəti zamanı lentə almasıdır

Bu necə baş verə bilər?

İstifadəçi fırıldaqçıdan e-poçt alır. Bu e-poçtda deyilir ki, güya fırıldaqçı qurbanın kompüterini və ya smartfonunu qırıb və kameraya giriş əldə edib. Cinsi şantaj hallarında isə fırıldaqçılar daha sonra iddia edir ki, onlar qurbanın masturbasiya aktı zamanı çəkilişlərini lentə alıblar və qurban onlara kriptovalyuta ilə pul ödəməsə, videonu dərc edəcəklər.

Qurbandan, hakerin cihazda tapdığını iddia etdiyi bu cür saxta görüntülərin işgüzar və şəxsi əlaqələrə yayılmasının qarşısını almaq üçün müəyyən müddət ərzində müəyyən edilmiş kriptovalyuta pul kisəsinə vəsait köçürməsi təklif edilir.

İddialarına "sübut" olaraq haker adətən müxtəlif veb-saytlarla əlaqəli istifadəçi adlarının və parolların siyahısını təqdim edir, bu da qurbanın böyüklər üçün olan çoxsaylı saytlarda eyni etimadnamələrdən istifadə etdiyini təxmin edir.

Bu məktubun alan şəxsə göndərilən həqiqi e-poçt mesajı

Mövzu: Məndə sənin videoyazın var - (burada fırıldaqçı tapdığı parolu paylaşır)
Tarix: 2023-06-22 3:32
Göndərən: “Save Your Life “ <xxxxxxxxxf@xxxx.ga>
Məktubu alan: XXXXXX@xxxx.com

Salam, mən xaker və proqramçıyam və sizin parollarınızdan birinin aşağıdakı kimi olduğunu bilirəm: (parol sızması sistemindən götürülən istifadəçinin açar sözü)

Brauzerin yenilənməməsi və ya qorunmaması səbəbindən kompüterinizi mənə məxsus zərərli proqram yoluxdurmuşam. Bu halda mənə məxsus iframe-in yerləşdirildiyi istənilən vebsayta daxil olmağınız kifayətdir ki, kompüterinizə virus düşsün. Ətraflı məlumat üçün Google: “Drive-by exploit” səhifəsinə baxın.

Zərərli proqram mənə bütün hesablarınıza sərbəst giriş imkanı verib (yuxarıdakı açar sözə baxın). Bundan əlavə kompüterinizə veb-kameranızdakı sizi izləyən proqram vasitəsilə tam nəzarəti ələ keçirmişəm.

Sizin bütün şəxsi məlumatlarınızı əldə edib, sizin bir neçə videonuzu (veb-kameranız vasitəsilə) lentə aldım və ÖZÜNÜZLƏ ƏYLƏNDİYİNİZ VİDEOLAR DA MƏNDƏDİ!!!

Sizin bütün şəxsi məlumatlarınızı istənilən resursda, o cümlədən bədniyyətli insanların olduğu darknet də videolarınızı dərc edə, kontaktlarınıza göndərə və sosial şəbəkələrdə yerləşdirə bilərəm!

Mənə bundan yalnız siz çəkindirə bilərsiniz və yalnız mən sizə kömək edə bilərəm. İşimi bitirdikdən sonra zərərli proqramı sildiyimdə heç bir iz qalmır və nəzərə alın ki, bu e-məktub (lar) müdaxilə olunmuş server üzərindən göndərilib…

Məni dayandırmağın yeganə yolu 400$ Bitkoin (BTC) göndərməkdir.
Ödəmək istəməsəniz, inanın ki, düşəcəyiniz bütün DƏHŞƏTLİ vəziyyətlə müqayisədə bu, çox yaxşı təklifdir!

Siz Bitkoinları www.xxxxxxx.com, www.xxxxx.com , www.xxxxxx.com səhifələrindən asanlıqla əldə edə bilərsiniz. Və ya yaxınlıqdakı Bitkoin bankomatına gedin və ya digər mübadilə üsulları üçün Google-da Siz Bitkoin-i birbaşa pul kisəsmə göndərə və ya əvvəlcə burada öz pul kisənizi yarada bilərsiniz:

www.login.xxxxx.com/en/#/signup/, Bundan sonra şərtləri qəbul edib mənim hesabıma göndərin.
Mənim Bitkoin pul kisəm: **17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG**
Kopyalayın və daxil edin: (cAsE-sEnSEtiVE).
3 gün vaxtınız var

Bu e-poçt hesabına giriş əldə etdiyim üçün bu e-poçtun tərəfininizdən oxunub-oxunmadığını biləcəyəm.

Bu məktubu bir neçə dəfə alsanız, bu onu oxuduğunuzdan əmin olmaq üçündür. Mənim poçt skriptim belə konfiqurasiya edilib və ödənişdən sonra məktubları silə bilərsiz.

Ödənişi aldıqdan sonra bütün məlumatlarınızı silirəm və siz əvvəlki kimi rahat yaşaya bilərsiniz. Növbəti dəfə internetə girəndən əvvəl brauzerinizi yeniləyin!

Nina-Louz Şidler, Riqa şəhərində virtual aktivlərin tənzimlənməsi ilə bağlı dəyirmi masaların fikirlərini bölüşən beş iştirakçı dövlətin siyasətçiləri üçün seminara rəhbərlik edir. Sessiya tənzimləyici sahəsində çatışmazlıqları müəyyən etmək və iştirakçı dövlətlər üçün aktual olan yeni inkişafları nümayiş etdirmək məqsədi daşıyan virtual aktivlərlə bağlı ümumavropa qanunvericiliyinə diqqət yetirib.

Problemi necə həll etməli

Məcburetmə hallarına dair məlumat verən qurbanlara dəstək üçün qabaqcıl təcrübələr.

- **Təmkinli olun:** Əgər istifadəçi cinsi şantaj məzmunlu e-məktub alıbsa, ilk əvvəl təmkinli olmalıdır. Yuxarıdakı məktub nümunəsi göstərir ki, cinayətkarlar qorxu aşılamaq, təşviş yaratmaq, utandırmaq və panikaya salmaq məqsədi ilə təsirli sifət sözlərdən istifadə edirlər.

- **Zərərçəkən məktub müəllifi ilə heç bir təmasa keçməməli**
  Cinsi şantaj məzmunlu e-məktublar adətən sübut kimi heç nə göndərmir və ya qoşmasız olur. E-poçtla göndərilən hər hansı bir istinad varsa, istifadəçi onları açmamalıdır.
- İstifadəçiyə FIAT-ı kriptovalyuta ilə dəyişmək və onu şübhəli kriptovalyuta pul kisəsinə köçürmək qadağan edilməlidir.

- **Kriptovalyuta pul kisəsini yoxlayın:** Kriptovalyuta pul kisəsinin ünvanının həqiqiliyini yoxlamağın bir yolu adətən "pul kisəsi tədqiqatçıları" adlandırılan alətlərdir. Məsələn, sözügedən kriptovalyuta pul kisəsini aşağıdakı linkdən istifadə etməklə yoxlamaq olar: https://www.blockchain.com/explorer/addresses/btc/17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG

- Ödənişsiz və 10 saniyədən az vaxt aparan ilkin araşdırma zamanı məlum olur ki, bu pul kisəsi üzərində çoxlu əməliyyatlar aparılıb. Bu, tez-tez hakerin bunun unikal və tək istifadə olunan kriptovalyuta pul kisəsi ünvanı olduğu iddiasına ziddir. Çoxsaylı əməliyyatlar göstərir ki, bir neçə şəxs ona pul köçürmüş ola bilər.

- **Oğurlanmış hesab məlumatları bazarından qurbanların xeyrinə istifadə:** Zərərçəkənlər aşağıdakı kimi pulsuz xidmətlərdən istifadə edə bilərlər: https://haveibeenpwned.com, Bu xidmət onlara milyardlarla sızdırılmış hesab təfərrüatlarını araşdıraraq özünə məxsus məlumatların müdaxiləyə məruz qalıb-qalmadığını yoxlamağa imkan verir. E-poçt və ya istifadəçi adlarını daxil etməklə istifadəçilər məlumatlarının hər hansı məlum pozuntularda görünüb-görünmədiyini tapa bilərlər. Müdaxilə etmək istəyən şəxs istifadə edilən parolu nümayiş etdirirsə, onu işlətdiyiniz bütün platformalarda dərhal dəyişdirin.

Məcburetmədə şübhəli bilinən şəxsləri araşdırarkən onların kriptovalyuta pulqablarına ödənişləri izləmək vacibdir.

Bununla, hər hansı pulqablarının rəsmi maliyyə platformalarına bağlı olub-olmadığını görə bilərsiniz ki, bu da hüquq-mühafizə orqanlarına şübhəli şəxsə kimin pul göndərdiyini müəyyən etməyə kömək edə bilər. Cinayətkərin pul kisəsinə pul ödəmək cinayət olmasa da, bunu edənlər müvafiq məlumata malik ola və ya eyni şəxs tərəfindən oxşar təhdidlərlə üzləşə bilər ki, bu da istintaq üçün faydalı ola bilər.

ATƏT-in Vyana Katibliyində ukraynalı nümayəndələr üçün mərkəzləşdirilməmiş mübadilələrə diqqət yetirməklə virtual aktivlərdə tənzimləmə boşluqlarına həsr olunmuş təlim keçirilir.

"Rug Pull" fırıldağı

Çıxış fırıldaqları, pump-and-dump sxemləri və ya "xalça çəkmə" fırıldaqları ("xalçanı kiminsə ayaq altından çıxarmaq" metaforası) fırıldaqçının yeni rəqəmsal aktivlərdən istifadə etməklə böyük həvəslə yaratdığı sxemlərdir. Əslində yalnız yeni kriptovalyuta deyil, istənilən rəqəmsal aktiv növü ola bilər. Bu sxemlər layihələr və əvəzolunmayan tokenlər (NFTs) ilə aparılmışdır. Fırıldaqçılar daha sonra sərmayəçilərin pullarını oğurlayaraq və rəqəmsal aktivi dəyərsiz edərək layihəni tez tərk edirlər.

Təsviri

Bu cür fırıldaqların məqsədi yeni rəqəmsal aktiv üçün mümkün qədər çox alıcı və ya investor tapmaq və onun qəbul edilən dəyərini mümkün qədər yüksək etmək üçün süni şəkildə artırmaqdır. Fırıldaqçılar kifayət qədər pul topladıqdan sonra yoxa çıxırlar (çıxış fırıldaqının "çıxışı") və pulları götürürlər. Bu əməliyyət sürətli baş verə, hər kəs birdən yoxa çıxa bilər və ya zaman keçdikcə pul yavaş-yavaş silənəcək və fırıldaqçılar məqsədli şəkildə aktivi daha da çox dəyərdən salırlar. Sonuncu halda, bəzən əsl "xalça çəkmə" fırıldağı və ya sadəcə pis idarə olunan, uğursuz layihə arasında fərq qoymaq çətin ola bilər.

Hər iki halda, fırıldaqçıların aktivi tərk etməsi aktivin saxta və dəyərsiz olduğunun göstəricisidir. Qurbanlar alıcı tapa bilsələr belə, onların əlində ödədiklərinin cuzi bir hissəsi dəyərinə bərabət sikkələr və ya tokenlər qalır, ya da rəqəmsal aktivdə aktivin ümumiyyətlə satıla bilməyəcəyini göstərən kod görsənir.

Fişinq sxemləri

Fişinq sxemləri internetin bir çox sahələri üçün ümumi olan fırıldaq növüdür. Bu, həm də rəqəmsal aktivlərlə əlaqəli ümumi və təsirli bir fırıldaqdır

Təsviri

Fırıldaqçılar sıravi görünən veb səhifə və ya şirkət sənədləri ilə rəsmi biznesi təmsil edirlər və veb-saytın saxta versiyasına aparan keçidi əks etdirən minlərlə e-məktub və ismarış göndərirlər. Bu vebsayta daxil olmaq çox asandır və hər bir ziyarətçinin şəxsi məlumatlarını, eləcə də yazdıqları bütün kripto ünvanlarını və parollarını ("kripto pulqabları açarları" adlanır) saxlamaq üçün yaradılmışdır. Bu yanaşma kripto cinayəti üçün xüsusilə vacibdir, çünki digər hesab növlərindən fərqli olaraq, kripto pulqabların şəxsi açarı oğurlandıqda, hesabı geri almaq demək olar ki, mümkün deyil. Bu, pul kisəsindəki vəsaitlərin əbədi olaraq itirilməsi deməkdir.

Bu fırıldağın müxtəlif növləri

Bir blokçeyn təhlili üzrə təminatçısının hesabatına görə,[17] fişinq fırıldaqçılığının yeni növü qurbanları NFT almaq ümidi ilə yanlış hesaba pul göndərməyə məcbur və yeni kripto investorların "FOMO" (imkanı qaçırmaq qorxusundan) istifadə edir. Bu o demək idi ki, qurbanlar bütün vəsaiti deyil, yalnız yanlış hesaba göndərdiklərini itirirlər.

17 Qanunsuz Kripto Ekosistemi Hesabatı. (2023), mənbə: https://www.trmlabs.com/report (son baxış: avqust 2023-cü il).

Populyarlıq qazanan fırıldaq sxemlərinin başqa bir növü "ünvanların viruslanması"dir ki, burada fırıldaqçı hədəf seçilən qurbanın əvvəllər pul göndərdiyi ünvana bənzəyən saxta ünvan yaradır. Daha sonra fırıldaqçı hədəf ünvana kiçik miqdarda kriptovalyuta göndərir ki, gələcəkdə digər istifadəçilər fərqində olmadan nəzərdə tutulan alıcının əvəzinə oxşar görsənən saxta ünvana ödəniş etsinlər.

Bunu necə həll etmək və ya qarşısını necə almaq olar?

İnsanlar saxta fişinq keçidlərdən xəbərdar olmalı və onları yoxlamalıdırlar.

Ünvanları iki dəfə yoxlayın:

- Xüsusən də böyük məbləğlərlə işləyərkən pulun göndərildiyi ünvanı iki dəfə yoxlayın. Yalnız mübadilə buferi funksiyalarına ("kopyala-yapışdırmaq" funksiyası) etibar etməyin, çünki zərərli proqramlar istifadəçinin kopyaladığını düşündüyündən başqa kriptovalyuta pul kisəsinin ünvanını daxil etmək üçün onları manipulyasiya edə bilər.

- Tez-tez ziyarət edilən kripto saytları üçün sürətli keçidlərdən istifadə edin ki, səhv yazmaq və ya oxşar görünən fişinq saytına girmək riskinin qarşısını almaq mümkün olsun.

Əlavə təhlükəsizlik tədbirlərini aktivləşdirin:

- Mümkün olduqda iki mərhələli autentifikasiyadan (2FA) istifadə etmək tövsiyə olunur. Bu, fırıldaqçıların hesablara daxil olmasını çətinləşdirən əlavə təhlükəsizlik qatını əlavə edir.

- Cihazınızdakı potensial təhlükələri aşkar etmək və aradan qaldırmaq üçün zərərli proqram əleyhinə proqram təminatını müntəzəm olaraq yeniləyin və işlədin. Bəzi zərərli proqram qalıqları kriptovalyuta əməliyyatlarını izləmək və ya bufer məlumatlarını dəyişdirmək üçün nəzərdə tutulub.

Açar sözü menecerlərindən istifadə edin: Açar sözü menecerləri açar sözləri saxlamaq, idarə etmək və avtomatik doldurmaq üçün nəzərdə tutulmuş proqram alətləridir. Onlar həmçinin tez-tez istifadəçilərə müxtəlif onlayn hesablar üçün kriptovalyuta pul kisəsindən nömrələrini təhlükəsiz saxlaya bilən qorunan qeydlər yaratmağa imkan verir.

Vasitəçi üzərindən hücumlar

Təsviri

Bu kimi əməllərdə fırıldaqçılar birbaşa qurbanı hədəf almırlar, əksinə, kimsə ictimai və ya təhlükəsiz Wi-Fi şəbəkəsində kriptovalyuta hesabına daxil olduqda, yəni vebsaytlara baxdıqda və kompüterdən vebsayta göndərilən məlumatın şəxsi olmadığı zaman məlumat ötürülməsinə müdaxilə edirlər. Fırıldaqçılar kripto pul kisəsinin ünvanını məlumatlarını və pul kisəsinin açarlarını toplayır və sonra hesabı ələ keçirmək üçün bundan istifadə edirlər

Bunu necə həll etmək və ya qarşısını necə almaq olar?

Virtual şəxsi şəbəkədən (VPN) istifadə etməklə bu cür fırıldaqların qarşısını almaq olar. Bunlar kifayət qədər ucuzdur, adətən ayda cəmi 3-4 avro. VPN-lər istifadəçinin internet bağlantısını şifrələyir, bu da icazəsiz şəxslərin hansı veb-saytlara girdiyini və ya nəyin yazıldığını görməsini çətinləşdirir. O, həmçinin istifadəçinin orijinal IP ünvanını gizlədir, anonim şəkildə baxmağa imkan verir və istifadəçinin faktiki coğrafi yerini aşkarlanmasının qarşısını alır. Bu, istifadəçilərə təşkilatlarının resurslarına uzaqdan daxil olmaq və ya senzuradan yan keçmək imkanı verir.
("IP ünvanlarının toplanması" bölməsində daha çox baxın, səh. 31.)

Kriptovalyuta birjalarını təqlid edən saxta saytlar

Təsviri

Saxta kriptovalyuta yaratmaq əvəzinə, fırıldaqçı kriptovalyuta birjalarına bənzəyən veb saytlar yaradır. Qurban öz kriptovalyutasını fərqli bir növə və ya FIAT valyutasına dəyişmək üçün bu vebsayta daxil olduqda, fırıldaqçılar onların məlumatlarını və yatırılan kriptovalyutanı oğurlayırlar.

Bunu necə həll etmək və ya qarşısını necə almaq olar?

Təhlükəsizliyi gücləndirmək üçün birjaya daxil olarkən həmişə iki mərhələli autentifikasiyadan (2FA) istifadə edin. Bu əlavə yoxlama pilləsi giriş zamanı daxil etməli olduğunuz SMS və ya e-poçt vasitəsilə birdəfəlik kodun alınmasını nəzərdə tuta bilər. Alternativ olaraq, ATƏT-in iştirakçı dövlətlərdən biri elektron identifikasiya həllini təklif edərsə, sistemə giriş zamanı əlavə qorunma tədbiri üçün ondan istifadə etməyi nəzərdən keçirin.

İkinci dərəcəli fırıldaqçılıq

Qurbanın bir dəfə aldadılmasından sonra baş verən ikinci dərəcəli fırıldaqlar da var. Daha ətraflı: "Zərərçəkənlərə dəstək", fəslinə, səh. 37-ə baxın.

Soldan sağa: Marçin Zarakovski, Mixal Qromek, Anna Pajevska və seminara rəhbərlik edən Nina-Luis Şiedler, Ukrayna nümayəndə heyəti üçün virtual aktiv xidməti təminatçılarına (VAXT) nəzarətin çətinlikləri və üstünlükləri haqqında biliklərini paylaşırlar. Sessiyaya Ukrayna Milli Bankı (MBU), Ukrayna Dövlət Maliyyə Monitorinqi Xidməti (SFMS), Rəqəmsal Transformasiya Nazirliyi və Qiymətli Kağızlar və Fond Bazarı üzrə Milli Komissiyası (NSSMC) kimi əsas Ukrayna qurumlarının nümayəndələrin iştirakı ilə təşkil olunmuşdu. Seminar Polşa Maliyyə Nazirliyində keçirilib ki, qurum Ukrayna nümayəndələrinin üçün bir sıra təlimləri üçün öz imkanlarını pulsuz təklif etməyə davam edir.

Virtual aktivlər üzrə cinayətlərin araşdırılması üçün əlavə alətlər

Virtual aktivlər üzrə cinayətlərinin araşdırılması üçün əlavə alətlər

Blokçeyn təhlili üzrə alətlər

Blokçeyn üzrə təhlil üçün keyfiyyətli alət və ya pul kisəsi tədqiqatçısı o deməkdir ki, polis əməkdaşı VAXT-lardan gec daxil olan və ya natamam məlumatlardan asılı olmadan öz araşdırmasının bir hissəsini apara bilər. Bundan əlavə, hələ də bütün VAXT-lar blokçeyn təhlili üzrə alətlərdən istifadə etmir.

Əhəmiyyəti:

HMO-lar tez-tez VAXT-lardan xüsusi kriptovalyuta pulqanı ünvanlarının cari balansı haqqında məlumat tələb edirlər. VAXT-ın komplayns qruplarının cavab üçün bacarıqlı olmasına baxmayaraq, bu sorğular üçün bunu etmək əhəmiyyətli bir inzibati prosesə çevrilir. Daha səmərəli alternativ, kriptovalyuta pul kisəsinin ünvanını pul kisəsiləri üzrə axtarış sisteminə daxil etməkdir ki, bu da bütün aparıcı kriptovalyutalar üçün deyil, əksəriyyət üçün lazım olan məlumatları tez bir zamanda təmin edir.

Pul kisəsi axtarış sistemlərinin məlumatları:

- Kriptovalyuta və əsas FIAT valyutalarında cari balans;
- Kriptovalyuta pul kisəsinə edilən ümumi mədaxil.
- Kriptovalyuta pul kisəsindən göndərilən ümumi vəsait.
- Əməliyyatların dəqiq vaxtı. (Qeyd: əməliyyat vaxtı kriptovalyutanın vaxt zonasına görə dəyişə bilər).
- Blokçeyn-də rüsumlar.
- Mənbə kriptovalyuta pul kisəsinin ünvanları (vəsaitlərinin köçürüldüyü mənbə).
- Təyinat kriptovalyutası pul kisəsinin ünvanları (vəsaitlərin göndərildiyi yerlər).

Blokçeyn təhlili ilə tanış olmayanlar üçün bu məlumatlar səthi görünə bilər. Bununla belə, istintaq məqsədləri üçün o, daha kiçik sürətlə gedən əməliyyatlarla birləşən çoxlu kiçik saylı daxil olan əməliyyatların nümunəsini göstərmək kimi dəyərli ipucları təqdim edə bilər. Bu kimi nümunələr narkotik satıcısının əməliyyatlarına bənzəyə bilər.

Təcrübədən nümunələr:

Aşağıdakı pulqablarının cinayət əməllərində istifadə olunduğu aşkarlanıb:

- Cinsi şantaj işi ilə əlaqəli kriptovalyuta pul kisəsi: Blokçeyn Explorer
- Twitter Hack ilə əlaqəli kriptovalyuta pul kisəsi

istifadəçilərdən rəy toplayan axtarış sistemi və Zəncirdən sui-istifadə

Bütün açıq mənbə araşdırma mənbələri kimi, bu cür axtarış sistemlərindən əldə edilən hər hansı məlumata şübhə ilə yanaşmalı və nəticə çıxarandan əvvəl yoxlanılmalıdır.

Blokçeyn təhlili üzrə pulsuz alətlərinin nümunələri:

- Block Explorer: Bu, Bitkoin blokları, ünvanları və əməliyyatları haqqında ətraflı məlumat verən sadə alətdir. Yeni başlayanlar üçün yaxşı bir başlanğıc nöqtəsidir.
- Etherscan: Bu alət xüsusi olaraq Ethereum blokçeyninə aiddir və ətraflı əməliyyat və ünvan analitikası təklif edə bilər.
- Blockchair: Bu alət Bitkoin-dən Ethereum-a qədər bir çox blokçeynləri əhatə edir və onu müxtəlif şəbəkələri təhlil etmək istəyənlər üçün çox yönlü edir.

Olqa de Trukis və Qreta Barkauskiené, ATƏT-in Virtual Aktiv Ekspertləri və Europol Maliyyə Kəşfiyyatının Dövlət-Özəl Tərəfdaşlığının (EFIPPP) Kripto-Aktivlər İş qrupunun həm-rəhbərləri Avropol-un Haaqadakı mənzil-qərargahında EFIPPP-in 2024-cü il aprel plenar iclasında iştirak edirlər. Birlikdə onlar müxtəlif ölkələrdən, o cümlədən ATƏT-in benefisiar ölkələrindən olan iştirakçıların virtual aktivlər məkanında mütəşəkkil cinayətkarlığın yaranmaqda olan əməliyyat üsullarını araşdırdıqları və müzakirə etdikləri bilik mübadiləsi sessiyalarını təşkil etdilər.

Blokçeyn təhlili təminatçıları

Blokçeyn təhlili təminatçıları pulqabları üzrə axtarış sistemlərinin kommersiya tərəfdaşlarıdır.

Onlar blokçeyn şəbəkələrində fəaliyyətləri izləmək, təhlil etmək və vizuallaşdırmaq üçün nəzərdə tutulmuş xüsusi proqram təminatından istifadə edirlər. Bu alətlər müstəntiqlərə tendensiyalar aşkar etməyə, əməliyyatları izləməyə və blokçeynin geniş və mürəkkəb dünyası haqqında fikirlər əldə etməyə kömək edir.

Pul kisəsi üzrə axtarış sistemlərindən istifadə etməklə mövcud olan məlumatlardan əlavə, blokçeyn təhlili üzrə təminatçıları həmçinin aşağıdakı imkanları təklif edir:

- **İzləmə və təqib:** Əksər analitik alətlər kriptovalyuta əməliyyatının mənbədən təyinat yerinə qədər səyahətini izləyə və təqib edə bilər. Bu, vəsaitlərin hərəkətini başa düşmək və hər hansı potensial qeyri-qanuni fəaliyyətləri müəyyən etmək üçün çox vacibdir.
- **Vizualizasiya:** Adətən bu alətlər böyük həcmdə məlumatların mənimsənilməsini asanlaşdıran və kriptovalyuta pul kisələrini maliyyə institutları ilə birləşdirməyə və ya əməliyyatları və ya pul kisəsi təminatçılarını əlaqələndirməyə imkan verən vizual qrafiklər və diaqramlar təqdim edir.
- **Riskin qiymətləndirilməsi:** Əməliyyat nümunələrini təhlil edərək, bəzi alətlər maliyyə institutları və tənzimləyicilər üçün dəyərli fikirlər təqdim edərək, xüsusi pul kisələri və ya əməliyyatlarla bağlı riski qiymətləndirə bilər.
- **Müfəssəl məlumat:** Bu alətlər müxtəlif blokçeynlərdən məlumatları götürə və birləşdirə bilər ki, bu da istifadəçilərə kriptovalyuta aləminin vahid mənzərəsini verir ki, bu da daha geniş istintaq üçün faydalı ola bilər.
- **Demikser xidməti:** Bəzi təminatçılar iddia edirlər ki, onların xidmətləri kriptovalyuta əməliyyatlarının məxfiliyini və anonimliyini artırmaq üçün nəzərdə tutulmuş xidmətlər olan mikserlər və tumblyorlar arasında əməliyyatları göstərə bilir. (Ətraflı məlumat üçün "Qarışdırıcılar və tumblyorlar" fəslinə, səh. 19-a, həmçinin "İşlərin məhkəmə qarşısında çıxarılması" fəslində demiksinq xidmətlərinin müzakirəsinə, səh. 34-ə baxın).

Müstəntiqlər bu alətlərdən istifadə etməklə blokçeyn dünyasının mürəkkəb dinamikasını daha yaxşı başa düşərək, məlumatlı qərarlar qəbul edə və bu inqilabi texnologiyanın daha dərindən qavranılmasını təmin edə bilərlər.

Gürcüstan Milli Bankının baş ofisində Virtual Aktiv Qrupu son iki il ərzində ATƏT-in Virtual Aktiv Ekspertlərindən mühüm dəstək alıb. Nəticədə, Gürcüstanın MONEYVAL üzrə indeksi FATF-ın 15 saylı Tövsiyəsinə əsasən "Əsasən Uyğundur" səviyyəsinə qədər yüksəlib.

Rəqəmsal aktivlər üzrə mütəxəssislərlə əməkdaşlıq

Rəqəmsal aktivlər üzrə mütəxəssislərlə əməkdaşlıq

Rəqəmsal aktivlər və onlarla əlaqəli məlumatları araşdırdıqda Hüquq-mühafizə orqanlarının (HMO) xarici qurumlarla əməkdaşlıq etmələri vacibdir. Bu siyahıya beynəlxalq polis təşkilatları, banklar və müəyyən ölkələr daxilində ixtisaslaşmış bölmələr daxildir. Onların təcrübəsi istintaqın effektiv idarə olunmasına kömək edir.

Yerli ekspertizanın müəyyən edilməsi

Virtual aktivlərlə işləmək təcrübəsi olan HMO-ların yerli əməkdaşlarını müəyyən etmək xüsusilə əhəmiyyətlidir. Onların əlaqə məlumatlarını toplamaq aşağıdakı səbəblərdən faydalı ola bilər:

- **Məqsəd:** Hesabat prosesində suallar vermək və fikir əldə etmək.
- **Nümunə:** Böyük Britaniyanın Cinayətkarıqla Mübarizə üzrə Milli Agentliyi (NCA) mürəkkəb işlər üzrə məsləhət vermək üçün xüsusi kriptovalyuta qrupu yaratmışdır. Virtual aktivlərlə bağlı HMO-da araşdırmalar necə təşkil olunmasına dair maraqlı fikirləri Avropa Şurası tərəfindən tərtib edilmiş 2023 Tipologiyalar Hesabatında tapmaq olar[18]

Beynəlxalq dəstək

Mütəxəssislər üçün Avropol Platforması (EPE):

- **Təsviri :** Bu, HMO nümayəndələri üçün virtual aktivlər üzrə praktiki yardım üzrə pulsuz platformadır.
- **Uyğunluq:** EPE-yə uyğun olmaq üçün (https://epe.europol.europa.eu/), ölkə Avropa İttifaqının üzvü və ya əməliyyat sazişinin bir hissəsi olmalıdır.[19]
- **Faydaları:** EPE virtual aktivlərin araşdırılması üzrə ən yaxşı təcrübələri təklif edir. Habelə vebinarlara girişi maraqlı tərəflər, konfranslar və digər öyrənmə resursları ilə əlaqə məlumatlarını təmin edir.
- **Qoşulma qaydası:** ATƏT-in iştirakçı dövləti Budapeşt Memorandumunun əməliyyat sazişinin[20] üzvü olduqda (siyahı ayrıca verilir), qoşulmaq üçün müraciət edə Bilər. Proses belədir:
  - Rəsmi e-poçt ünvanından istifadə edərək o3 (at) europol.europa.eu using ünvanı vasitəsilə səlahiyyətli qurumla əlaqə saxlayın və sizi virtual aktivlərlə təcrübənizi və biliklərinizin başqalarına necə fayda verəcəyini göstərin.
  - Xüsusilə virtual aktivlərlə bağlı qoşulma səbəbinin aydın şəkildə göstərilməsi.
- **Kim qoşula bilər:** Platforma, ilk növbədə, HMO əməkdaşları üçün nəzərdə tutulsa da, sistemə həm dövlət, həm də özəl mütəxəssislər də

18 "İş toplularına" diqqət yetirin -Tipologiyalar Hesabatı 2023 - Virtual Aktivlər Dünyasında Çirkli Pulların Yuyulması və Terrorçuluğun Maliyyələşdirilməsi Riskləri, Moneyval, Avropa Şurası https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 (son baxış 25.02.2024).

19 Ölkələrlə Sazişlər və İş Razılaşmaları. Avropol https://www.europol.europa.eu/partners-collaboration/agreements (son baxış 26.11.2023).

20 Ölkələrlə Sazişlər və İş Razılaşmaları. Avropol https://www.europol.europa.eu/partners-collaboration/agreements (son baxış 26.11.2023).

müraciət edə bilərlər. Bununla belə, məlumatın detalları HMO əməkdaşı olmayan mütəxəssislər üçün məhdudlaşdırıla bilər

- **Xərci:** Ödənişsizdir. Giriş təmamilə pulsuzdur.

2019-cu ilin oktyabrında Europol "Kriptopol" adlı iki təhsil oyununa start verib. Oyun bir neçə dəfə yenilənib və çoxsaylı kriptovalyutaları əhatə edir. Onlar Aİ Üzv Dövlətlərinin nümayəndələri üçün pulsuz təmin olunur. Bax: o3@europol.europa.eu.

INTERPOL-un Maliyyə Cinayətləri və Korrupsiyaya Qarşı Mübarizə Mərkəzi (IFCACC)

INTERPOL-un Maliyyə Cinayətləri və Korrupsiyaya Qarşı Mübarizə Mərkəzi (IFCACC): Bu, qlobal maliyyə sistemlərini qorumaq üçün transmilli maliyyə cinayətlərinə qarşı mübarizəyə yönəldilmiş mərkəzdir.

Uyğunluq: Maliyyə cinayətlərinin qloballaşması ilə bağlı artan narahatlıqlara cavab olaraq, INTERPOL bu problemlərlə birgə mübarizəyə kömək etmək üçün IFCACC-ni təqdim etdi. Bu, HMO-larla bərabər beynəlxalq qurumlar və maraqlı tərəflər üçün də mühüm təşəbbüsdür.

Faydaları: Proseslərin asanlaşdırılması:

- HMO-dan dələduzluq, ödəniş sistemləri üzərindən cinayətlər və transsərhəd sorğularına dəstək.
- Çirkli pulların yuyulmasına qarşı mübarizə, aktivlərin bərpası və virtual aktivlərin anlaşılmasında yardım.
- Korrupsiyaya qarşı mübarizə təcrübələrinə nəzarət: idmanla bağlı məsələlərdən tutmuş yüksək səviyyəli siyasi mübahisələrə qədər.

Qoşulma prosesi: IFCACC çoxtərəfli agentlik modeli əsasında fəaliyyət göstərdiyindən, potensial əməkdaşlıqlar aşağıdakıları əhatə edir:

- INTERPOL Baş Katibliyi və ya adətən Ədliyyə Nazirliyi və məhkəmə polisi nəznində fəaliyyət göstərən I NTERPOL Milli Mərkəzi Bürosu ilə əlaqə.
- Maliyyə cinayətlərinə və korrupsiyaya qarşı məqsədlər arasında aydın əlaqələnin nümayiş etdirilməsi.
- Potensial əməkdaşlıq sahələrinin və ya ehtiyacların ifadə edilməsi.

Kim qoşula bilər: HMO-dan əlavə, maliyyə institutları, beynəlxalq qurumlar və özəl sektor nümayəndələri.

Bununla belə, əməkdaşlığın xasiyyəti təşkilatın mahiyyəti və məqsədindən asılı olaraq dəyişə bilər.

Xərci: INTERPOL-un beynəlxalq təşkilat olması səbəbindən onun Baş Katibliyi ilə əlaqə saxlamaq üçün heç bir xərc tələb olunmur.

IFCACC və I-GRIP haqqında əlavə məlumat üçün mənbələr:

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

Virtual aktivlərin texniki xüsusiyyətləri ilə bağlı əlavə məlumat üçün hüquq-mühafizə orqanlarının nümayəndələri innovation@interpol.int **ünvanına e-məktub göndərə bilərlər.**

Əlavə resurs: HMO nümayəndələri INTERPOL-un Virtual Aktivlərin Müsadirəsinə dair Təlimatlarını əldə edə bilərlər: vaguidelines@interpol.int

UNODC təşkilatının kibercinayətkarlığa və çirkli pulların yuyulmasına qarşı virtual aktivlər proqramları və araşdırma seminarları

Ümumi məlumat:
Birləşmiş Millətlər Təşkilatının Narkotiklər və Cinayətkarlıqla Mübarizə İdarəsinin (UNODC) komandası tərəfindən idarə olunan bu müfəssəl seminarlar silsiləsi virtual aktivlərin, maliyyə cinayətlərinin və uyğunluğun əsas istiqamətlərinin dərindən araşdırılmasını təklif edir.

Proqram təlimçilərin təlimi kimi müəyyən edilən əsas, təkmil və kaskad sessiyalar şəklində qurulub və sahənin ən yaxşı təcrübələrinin təbliğini təşviq edir. Seminarlar ciddi nəzəri konsepsiyaları praktiki məşğələlərlə birləşdirir, hüquq-mühafizə orqanlarının iştirakçılarını virtual aktivlərin izlənilməsi, tədqiqi və effektiv idarə edilməsində əvəzolunmaz bacarıqlarla təchiz edir.

Uyğunluq:
Bu ixtisaslaşdırılmış təlim HMO, maliyyə institutları, texnoloji müəssisələri və təhsil sahələri kimi müxtəlif sektorları əhatə edən peşəkarlar üçün nəzərdə tutulur. Kurs siyasətçilər, tənzimləyicilər, müstəntiqlər və virtual aktivlərin mürəkkəbliklərini, blokçeyn dinamikasını və maliyyə cinayətlərinin azaldılması üsullarını deşifrə etmək niyyətində olan bütün peşəkarlar üçün əvəzolunmaz mənbə rolunu oynayır.

Əsas istiqamətləri:

- **Virtual aktivlərin əsasları:** Daim inkişaf edən virtual aktivlərin mənşəyinə, təkamülünə və mürəkkəbliklərinə və onları dəstəkləyən texnologiyaların daha dərin araşdırılması.
- **Əməliyyat dinamikası:** Blokçeyn əməliyyatlarının prosesini əvvəldən sona qədər deşifrə edin.
- **Blokçeyn haqqında təfərrüatlar:** Blokçeyn-də tranzaksiyaların qeydə alındığı, ratifikasiya edildiyi və arxivləşdirildiyi prosesləri tədqiq edin.
- **Blokçeyn üzrə kriminalistika:** Real vaxt rejimində əməliyyatlara nəzarət və şəxsiyyətlərini gizlətmək üçün cinayətkar tərəfindən istifadə olunan üsulları öyrənin.
- **ÇPY/TMM taktikası:** Virtual aktivlərin dəyişkən mənzərəsinə uyğunlaşmaq üçün çirkli pulların yuyulmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə protokollarının təfərrüatları öyrənin.

- **Risklərin idarə edilməsi:** İştirakçıların virtual aktivlərə bağlı fərqli risklərin azaldılmasında qızıl standartları ilə tanış olmaq
- **Aktivlərə nəzarət :** İstintaq zamanı virtual aktivlərin düzgün müsadirəsi və idarə olunması ilə bağlı ən yaxşı təcrübələri iştirakçılara təqdim etmək.

Qoşulma addımları:
Potensial iştirakçılar:
- Qarşıdan gələn seminarın cədvəlini nəzərdən keçirib və özlərinə uyğun vaxt seçə bilərlər.
- Şablon əsasında fəaliyyət sahəsinə uyğun ödəniş güzəştlərini müəyyə edə bilərlər.

Bazel İdarəetmə İnstitutu

Bazel İdarəetmə İnstitutu:
Bu, idarəçiliyin təkmilləşdirilməsinə və qlobal miqyasda maliyyə cinayətlərinə qarşı mübarizəyə yönəlmiş müstəqil, qeyri-kommersiya təşkilatıdır. Bazel şəhərində yerləşən institut Bazel Universiteti ilə sıx əməkdaşlıq edir və Afrika qitəsinin müxtəlif ölkələrində fəaliyyət göstərir.
Bazel İnstitutunun kriptovalyuta seminarı: Bazel İnstitutunun kriptovalyuta seminarı: Kriptovalyutalar, maliyyə cinayətləri və ÇPY komplyans əsaslarına həsr olunan dörd günlük müfəssəl virtual təlim təklif edir. Kurs, qeyri-qanuni fəaliyyətlər üçün blokçeyn əməliyyatlarını izləməklə iştirakçılara çirkli pulların yuyulması üzrə praktiki ssenariləri əhatə edir.

İştirakçılar: HMO-dan, maliyyə sektorlarından, biznes nümayəndələri və hətta tələbələrdən də daxil olmaqla peşəkarlar üçün açıqdır. Proqram siyasətçilər, tənzimləyici orqanlar, araşdırmaçı jurnalistlər və virtual aktivlər, blokçeyn və maliyyə cinayətlərinin

Maliyyə cinayətləri (FinCrim) ilə mübarizə Fondu

Maliyyə Cinayətləri ilə Mübarizə üzrə Qlobal Koalisiyasının Rəqəmsal Aktiv İşçi Qrupunun mütəxəssisləri tərəfindən yaradılan və Stokholmda yerləşən fonddur. Əsas məqsədi blokçeyn əsaslı maliyyə və Web 3 ilə əlaqəli məsələlərə dair sürətli və istinad-əsaslı cavablar

- Hərtərəfli nəzərdən keçirə və açıq təlim şərtlərini qəbul edə bilərlər. engagement.

Hədəf auditoriyası:
Seminarlar müstəntiqləri, hüquq sahəsinin peşəkarları, maliyyə tənzimləyici qurumunun heyətini, texnoloji sahənin qabaqcıl nümayəndələri, jurnalistləri və digərlərini əhatə edən müxtəlif auditoriya üçün uyğun olmaq üçün hazırlanmışdır. Seminarlar həm dövlət, həm də özəl sektora xidmət edir, və diqqəti virtual aktivlər və əlaqəli fiskal normalarla maraqlananlara xidmət edir.

Ödəniş strukturu: Təlim sessiyası üçün ödənişlər 10,000 – 20,000 ABŞ dolları

qarşının alınması ilə maraqlananlar üçün hazırlanmışdır.

Faydaları: Bazel İnstitutunun seminarı aşağıdakılara dair biliklər təqdim edir:
- **Kriptovalyutanın əsasları:** Virtual aktivlərin əsasını, yaranmasını və əhatə dairəsini, müştərək kitab texnologiyasını və s.

- **Tranzaksiyalar:** Bitkoin şəbəkəsinin, kriptoqrafiya və əməliyyatların idarəedilməsinin iş üslubları.
- **Blokçeyn və mayninq:** Tranzaksiyaların blokçeyndə necə qorunduğunun, saxlandığının və yoxlanıldığının öyrənilməsi.
- **Blokçeyn təhlili:** Real vaxt rejimində əməliyyatların monitorinqi üsulları, cinayətkarların anonimlikdən necə yan keçməsi və alətlərdən istifadə etməsi.
- **Hüquqi ekspertiza:** ÇPY/TMM proqramlarının yeni ödəniş rejimlərinə uyğunlaşdırılması.
- **Risklərin idarə edilməsi:** Virtual aktivlərin risklərini idarə etmək üçün ən yaxşı təcrübələr və mənbələr.

Blokçeyn əsaslı maliyyə və Web 3 ilə əlaqəlidi

almaq olub. Fond yalnız dövlət və özəl maliyyə cinayətləri ilə mübarizə aparanlara yönəlmiş generativ Süni Zəka köməkçisinə pulsuz token hovuzu təqdim edir. Heyət daim ən yeni hesabatları, o cümlədən

arasında dəyişir. Güzəştli qiymətlər potensial olaraq dövlət sektorunun nümayəndələri, alimlər, qeyri-kommersiya təşkilatları və media işçiləri üçün əlçatandır. Təlimin əhatə dairəsi ilə bağlı əlavə məlumatı UNODC-nin Virtual Aktivlərin Təlim Şöbəsi ilə e-poçt vasitəsilə əlaqə saxlamaqla əldə etmək olar: cryptocurrency@unodc.org

Əlavə xüsusiyyətlər:
UNODC-nin elektron tədris platforması ilə aşağıdakı linkdən tanış olmaq olar: https://www.unodc.org/elearning/en/courses/course-catalogue.html

- **Aktivlərin müsadirəsi:** Kripto aktivlərin müsadirəsi, pul qabların idarə edilməsi və s. ilə bağlı prosedurlar və əsas amillər.

Kim qoşula bilər: Kurs müstəntiqlər, hüquqşünaslar, ÇPY/TMM mütəxəssisləri, maliyyə kəşfiyyatı bölmələrinin üzvləri, FinTech təcrübələri, jurnalistlər və s. üçün nəzərdə tutulub. O, virtual aktivlər və maliyyə cinayətləri dünyasında işləmək istəyən həm dövlət, həm də özəl sektor mütəxəssisləri üçün nəzərdə tutulub.

Xərci: Dövlət sektorunun nümayəndələri, alimlər, qeyri-kommersiya təşkilatları və jurnalistlər kimi xüsusi üzvlər üçün 300 CHF endirimlə adambaşı 750 CHF.

Əlavə məlumat üçün:
info@baselgovernance.org

Kursun təfərrüatları və mövcud tarixlər üçün qeydiyyat linkləri Bazel İnstitutunun sosial media platformalarında tapıla bilər.

ATƏT-in ictimaiyyətə açıqlanmış materiallarını yükləyir və nəzərdən keçirir. Qaydalar Chat GPT kimi sistemdən istifadə etməklə axtarıla bilər ki, bu da mütəxəssislərə gündəlik olaraq qaydalardakı dəyişikliklərdən xəbərdar olmağa kömək edir

https://www. fncrimefi ghters.com/

Hüquq-mühafizə orqanlarının hesabatlarına dair tövsiyələr

Hüquq-mühafizə orqanlarının hesabatlarına dair tövsiyələr

- **Dərhal dəstək göstərmək:** Qurbanlara onların qalan rəqəmsal aktivlərini qorumaq və əlavə maliyyə itkisi riskini azaltmaq barədə dərhal təlimat verildiyinə əmin olun. Bu, parolların dəyişdirilməsi, pul kisəsinin təhlükəsizliyi və ya aktivlərin daha təhlükəsiz platformaya köçürülməsi ilə bağlı təlimatları əhatə edə bilər.

- **Financial counselling:** Qurbanları öz itkilərini, potensial vergi nəticələrini və zamanla itkiləri bərpa etmək və ya azaltmaq üçün strategiyaları mənimsəməyə kömək edə biləcək maliyyə məsləhət xidmətlərinə yönəldin.

- **Maarifləndirmə:** Bu cür fırıldaqlarla bağlı ictimaiyyəti məlumatlandırma kampaniyalarına və seminarlara başlayın. İctimaiyyət nə qədər çox məlumatlı olsa, fırıldaqçılar üçün potensial investorları aldatmaq bir o qədər çətinləşir.

- **Birjalarla əməkdaşlıq edin:** Fırıldaqçıların aktivlərini izləmək və potensial dondurmaq üçün kriptovalyuta birjaları ilə sıx əməkdaşlıq edin. Bununla onların qanunsuz qazanclarını nağdlaşdırmalarını çətinləşdirə bilərsiz.

- **Ölkələrarası əməkdaşlıq:** Rəqəmsal fırıldaqlar tez-tez sərhədləri aşdığı üçün günahkarları izləmək, tutmaq və mühakimə etmək məqsədilə beynəlxalq hüquq-mühafizə orqanları ilə əməkdaşlıq edin.

Mariam Qriqalaşvili Yerevanda kriptovalyuta vergisi və onun ÇPY və TMM siyasətləri ilə əlaqəsinə həsr olunmuş seminar zamanı Ermənistan Mərkəzi Bankından olan həmkarları ilə öz ölkəsinin və Gürcüstan Milli Bankının təcrübəsini paylaşır.

ATƏT ilə əməkdaşlığın xülasəsi və prinsipləri

ATƏT ilə əməkdaşlığın xülasəsi və prinsipləri

ATƏT-in Virtual Aktivlərə Dəstək Təşəbbüsü

Biz kimik

ATƏT-in Virtual Aktiv Ekspert Qrupu virtual aktivlər üzrə siyasəti formalaşdıranlara və HMO-lara dəyişkən çağırışlara cavab vermək üçün unikal potensiala malikdir. Texniki təcrübənin təmin edilməsində təxminən əlli illik mükəmməl tarixçəmizə əsasən biz müvafiq qurumlara ATƏT-in 57 iştirakçı dövləti daxilində virtual aktivlərin mürəkkəb dünyasında prosesləri idarə etməkdə kömək edirik.

HMO və siyasəti formalaşdıranlar üçün yaratdığımız dəyər

- **Qabaqcıl biliklər:** Təlimlərimiz HMO və siyasəti formalaşdıranları virtual aktivlər sahəsinə xas olan problemləri həll etmək üçün uyğun və ən müasir anlayışlar və strategiyalarla təchiz edir.

- **Əməliyyat səmərəliliyi:** Təcrübəli təlimlə bərabər biz təşkilatı məsələlər, yerin seçilməsini təmin, ATƏT-in iştirakçı dövlətlərindən virtual aktivlər üzrə sınanmış ekspertləri dəvət edir, habelə gündəliyi formalaşdırır və təlim məqsədlərini uyğunlaşdırırıq.

- **Təlim və təcrübənin inkişafı:** Biz virtual aktivlər üzrə hərtərəfli təlim proqramları təklif edirik. Siyasəti formalaşdıranlar, HMO, ənənəvi bankların komplyans şöbələrinin və WEB3 şirkətlərinin nümayəndələrindən ibarət komandamız məhdud, lakin tutarlı nəzəri komponentlə praktiki təlimə üstünlük verir. Əsas diqqət real dünyada tətbiqi təmin edən praktiki məşğələlərə yönəldilmişdir. Qeyd edək ki, keçmiş iştirakçıların bir qismi mürəkkəb ÇPY hallarının uğurlu araşdırılması da daxil olmaqla təlimdəki biliklərdən istifadə etməklə konkret nəticələr əldə etmişlər.

- **Resurs təminatı:** Biz aparıcı blokçeyn ekspertləri ilə əməkdaşlıq edirik. Peşəkar alətlərlə bərabər bu təcrübə iştirakçılara öyrəndiklərini dərindən sınaq zamanı və seminarlarda effektiv şəkildə həyata keçirməyə imkan verir ki, bu da daha mürəkkəb hallar üzərində məşq keçməyə imkan açır.

- **Halların təhlili:** Təlimimiz adətən real vaxt rejimində halları araşdırılmasını və problemləri real həyatda baş verməmişdən əvvəl həll etməyimizi təmin etmək üçün davamlı inkişafları vizuallaşdıran qanunverici dəstəyi əhatə edir.

- **Daha geniş tətbiq və davamlılıq** Bizim kaskad tipli təlim sistemimizə "təlimçilərin təlimi" modeli daxildir və biz bu bilikləri daha da geniş yaymaq üçün ekspertləri öz ölkələrinə qayıtdıqda bilikləri paylaşmağa sövq edirik. Bu, onların öz ölkələrində təcrübənin inkişafında daha geniş əhatəsini və davamlılığı təmin edir.

- **Daha təhlükəsiz rəqəmsal mühitin yaradılması:**Siyasəti formaladıran-ların və HMO-ların virtual aktivlərlə məşğul olmaq üçün biliklərlə təchiz olunmasını təmin etməklə, biz daha təhlükəsiz və şəffaf rəqəmsal maliyyə mühitinin yaradılmasına əhəmiyyətli töhfə veririk.

Kibertəhlükəsizliyin gələcəyini formalaşdırmaqda və hamı üçün daha təhlükəsiz, daha şəffaf rəqəmsal məkanını təmin etməkdə bizə qoşulun.

Bizimlə əlaqə:
VirtualAssets@osce.org

Mövzu üzrə əlavə mənbələr

Mövzu üzrə əlavə mənbələr

BMT-nin Narkotiklər və Cinayətkarlıq üzrə İdarəsi (UNODC)

Virtual Valyutalardan İstifadə etməklə Cinayət Gəlirlərinin Yuyulmasının Aşkarlanması və Araşdırılması üzrə Əsas Təlimat (2014)

UNODC tərəfindən on ildən çox əvvəl, 2014-cü ildə nəşr olunmasına baxmayaraq, 200 səhifəlik bu müfəssəl bələdçi müxtəlif terminləri dərindən araşdırır və hazırkı icmalda təsvir edilən terminlər üçün kontekst təmin edir. Bələdçi həmçinin ətraflı özünüqiymətləndirmə anketlərini təqdim edir:

https://www.unodc.org/documents/middleeastandnorthafrica/money-laundering/FULL10-UNODCVirtualCurrencies-final.pdf.pdf

Avropada Təhlükəsizlik və Əməkdaşlıq Təşkilatı (ATƏT)

Cinayət Təqibində Virtual Valyutalarla Mübarizə üzrə Təlimat Kitabı (2022)

https://www.osce.org/files/f/documents/2/0/522754.pdf

AbŞ Ədliyyə Nazirliyi

Rəqəmsal Aktivlərlə Əlaqədar Cinayət Fəaliyyətinin Müəyyən edilməsi, Araşdırılması və Mühakimə olunmasında Hüquq Mühafizə Orqanlarının Rolu (2022)

https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf

ABŞ Ədliyyə Nazirliyi tərəfindən nəşr olunan hesabat Beynəlxalq Hüquq Mühafizə Orqanları üzrə Əməkdaşlıq Hesabatının köməkçi vəsaiti kimi xidmət edir və Kriptovalyuta sahəsində Qanunların Tətbiqi Çərçivəsini yeniləyir. O, gələcək istinad üçün hərtərəfli icmal təqdim edir.

Müəllif haqqında

Qarşınızdakı bələdçi ATƏT-in İqtisadi və Ətraf Mühit Fəaliyyətləri (OCEEA) üzrə Koordinatorunun Ofisində aparılan virtual aktivlər və kriptovalyutalarla bağlı çirkli pulların yuyulması risklərinin azaldılmasına yönəlmiş ATƏT layihəsinin aparıcı virtual aktiv eksperti Mixal Qromek tərəfindən tərtib olunmuşdur. Qromek, Stokholmda yerləşən Nasdaq-la ticarət edilən VAXT Safello şirkətinin keçmiş Baş Komplyans Direktorudur

O, Avropol, Dünya İqtisadi Forumu və London Fond Birjası arasında Risk Həllləri üzrə yaradılmış Maliyyə Cinayətləri ilə Mübarizə Qlobal Koalisiyası çərçivəsində Rəqəmsal Aktiv İşçi Qrupuna sədrlik edir. Müəllif həm də Maliyyə Cinayətləri ilə Mübarizə Qlobal Koalisiyasının icraçı qrupunun üzvüdür.
O, hökumətlər və hüquq-mühafizə orqanları üçün təlimlər keçməyə davam edir, ATƏT-in iştirakçısı olan dövlətlərin üzləşdiyi problemlərin qarşısını almaq üçün qanunvericiliyin hazırlanmasına dəstək verir. O, öz təcrübəsini FinTech icraçı direktoru və Stokholm İqtisadiyyat Məktəbində İcraçı Təhsil şöbəsinin proqram direktoru kimi keçmiş rolları vasitəsilə əldə edib. On ildən artıqdır Mixal Qromek, Fintech və Virtual Assets Compliance ilə əməkdaşlıq edib. Onun məqalələri Forbes.com saytında, eləcə də bir sıra kitab və jurnallarda dərc olunub.

Minnətdarlıq

Hazırki bələdçinin daha təkmil olmasi üçün doktor Aleksandra Andhovun apardığı araşdırmaların və verdiyi töhfələrin xüsusi əhəmiyyəti var. Onun hüquq sahəsində təcrübəsi və bilikləri təqdim olunan məzmunun dəqiqliyini, aktuallığını və dərinliyini kifayət qədər artırıb. Kopenhagen Universitetinin Hüquq Fakültəsinin dosenti kimi o, bu sənədin yazılmasında əvəzsiz qiymətləndirmələr və tövsiyələr verib. Dr. Andhov, hüquq və texnologiyanın kəsişdiyi sahələr üzrə təcrübəyə malikdir və Maliyyə Cinayətləri ilə Mübarizə Təşkilatının həmtəsisçisi və baş hüquq əməkdaşı qismində sözügedən istiqamət üzrə böyük sayda layihələrə töhfə verir.

Mümkün olan ən yüksək oxunaqlılığı və keyfiyyəti təmin etmək üçün sənədin dili bir neçə şəxs, əsasən Qreys Marşall tərəfindən redaktə edilib və bu, nəşrin aydın dilini və ahəngliyi təmin edilib. Maliyyə Cinayətləri ilə Mübarizə üzrə Qlobal Koalisiyasının Baş Katibi kimi o, məlumatın oxucular üçün uyğunlaşdırılmasına dəstək olub.

Xanım Marşallı ilə bərabər Deniss Rudiç, sənədin qiymətləndirilməsi və redaktə edilməsində geniş dəstək göstərərək, öz təcrübəsi əsasında əhəmiyyətli töhfə verib. Onun nəşrin məzmununa və dilinə dair fikirləri əvəzolunmaz rol oynayıb.

Əlavə redaksiya dəstəyi Qreta Barkauskienė, Emilia Paçomov, Sangyong Kanq və Vinsent Danjin tərəfindən verilmişdir. Əlavə araşdırma və redaktə təklifləri INTERPOL Maliyyə Cinayətləri və Korrupsiyaya Qarşı Mübarizə Mərkəzi (IFCACC), xüsusən Mona Hessein, habelə Avropa Kibercinayətkarlıq Mərkəzinin (EC3) nümayəndələri, xüsusilə də Qert Yan van Hardeveld tərəfindən irəli sürülüb.

ATƏT-in OCEEA heyəti sözügedən geniş dəstəyə bütün həmkarlara minnətdarlığını ifadə edir.

Virtual aktivlər mövzusunda Baltikyanı ölkələrə öyrənmə səfəri üçün ekosistem liderlərinin müəyyən edilməsində və seçilməsində mühüm rola görə Latviya Maliyyə Kəşfiyyatı Bölməsinə səmimi təşəkkürümüzü bildiririk. Biz həmçinin Polşa Maliyyə Nazirliyinə təlim imkanlarının təmin edilməsində göstərdiyi davamlı dəstəyə görə minnətdarıq. Bundan əlavə, layihənin uğurlu getməsi ilə əlaqədar töhfələri olan müxtəlif sektorlardan olan çoxsaylı qurumlara və şəxslərə dərin minnətdarlığımızı bildiririk.

Qeydlər

ATƏT Katibliyi
ATƏT-in İqtisadi və Ətraf Mühit
Fəaliyyəti Koordinatorunun Ofisi
İqtisadi İdarəetmə Bölməsi
Volnerştrasse 6
1010 Vyana, Avstriya
E-poçt: virtualassets@osce.org
www.osce.org/eea

Organization for Security and
Co-operation in Europe