Կրիպտոհանգա-
գործությունների
վերլուծություն

Ուղեցույց իրավապահ
մարմինների համար

OSCE Organization for Security and Co-operation in Europe

Պատասխանատվությունից հրաժարում

Սույն փաստաթուղթը պատրաստվել է հեղինակի կողմից ի սկզբանե ներկայացված նյութի հիման վրա: Այն ԵԱՀԿ-ի խմբագրակազմի կողմից չի խմբագրվել: Այստեղ արտահայտված տեսակետների համար պատասխանատվությունը կրում է բացառապես հեղինակը, և պարտադիր չէ, որ դրանք ներկայացնեն ԵԱՀԿ-ի, նրա ներկայացուցչությունների կամ մասնակից պետությունների տեսակետները:

ԵԱՀԿ-ն, նրա ներկայացուցչությունները և մասնակից պետությունները հրաժարվում են սույն փաստաթղթի օգտագործման հետևանքով առաջացող ցանկացած պատասխանատվությունից: Սույն ուղեցույցը չի անդրադառնում որևէ անձի գործողությունների կամ բացթողումների համար պատասխանատվության, իրավական կամ այլ հարցերին: Այս հրապարակման մեջ կոնկրետ երկրների կամ տարածքների հիշատակումը կամ վկայակոչումը չի նշանակում ԵԱՀԿ-ի որևէ դիրքորոշում նրանց իրավական կարգավիճակի, կառավարման մարմինների, հաստատությունների կամ նրանց սահմանների սահմանազատման վերաբերյալ:

Կրիպտոհանցագործությունների վերլուծություն

Ուղեցույց իրավապահ մարմինների համար

OSCE Organization for Security and Co-operation in Europe

Բովանդակություն

Շապավումներ, կրճատումներ և հիմնական տերմիններ՝ բացատրություններով

ՓԼՊ 5-րդ դիրեկտիվ	Եվրոպական խորհրդարանի և խորհրդի 2018 թվականի մայիսի 30-ի թիվ 2018/843 (ԵՄ) դիրեկտիվ «Փողերի լվացման կամ ահաբեկչության ֆինանսավորման նպատակով ֆինանսական համակարգի օգտագործումը կանխելու մասին» թիվ 2015/849 (ԵՄ) դիրեկտիվում և թիվ 2013/36/ԵՄ դիրեկտիվում (տեքստը վերաբերում է Եվրոպական տնտեսական տարածքին) փոփոխություններ կատարելու մասին։ Սույն դիրեկտիվի առարկայում ներառվել են կրիպտոակտիվները։ Մինչև 2020թ. հունվարի 10-ը անդամ պետությունները պետք է ներդնեն անհրաժեշտ օրենքներ և կանոնակարգեր՝ այս դիրեկտիվի պահանջները կատարելու համար։
ՓԼՊ	Փողերի լվացման դեմ պայքար. Վերաբերում է օրենքներին, կանոնակարգերին և ընթացակարգերին, որոնք նպատակ ունեն կանխել հանցագործների կողմից ապօրինի ձեռք բերված միջոցները որպես օրինական եկամուտ ներկայացնելը։
ԿԱԾՄ (CASP)	Կրիպտոակտիվների ծառայություններ մատուցողներ. Շանրությանը կրիպտոակտիվների հետ կապված ծառայություններ առաջարկող կազմակերպություններ։ Այս ծառայությունները կարող են ընդգրկել գործունեության լայն շրջանակ, ներառյալ, բայց չսահմանափակվելով՝ 1. Փոխանակման ծառայություններ. օգնում են ֆիատ փողերով կամ այլ կրիպտոակտիվներով իրականացնել կրիպտոակտիվների առք ու վաճառք ։ 2. Դրամապանակներ առաջարկող մատակարարներ. առաջարկում են պահառուական կամ ոչ պահառուական դրամապանակներ կրիպտոակտիվները պահելու, կառավարելու և փոխանցելու համար։ 3. Փոխանցման ծառայություններ. տալիս են կրիպտոակտիվները մի հասցեից կամ հաշվից մյուսին փոխանցելու հնարավորություն։ 4. Ֆինանսական խորհրդատվություն. տրամադրում են խորհրդատվություն կրիպտոակտիվների գնման, վաճառքի կամ պահպանման վերաբերյալ։ 5. Պահառության ծառայություններ. Շաճախորդների անունից կրիպտոակտիվների պահում և պաշտպանություն։ (Լրացուցիչ տեղեկությունների համար տե՛ս էջ 20)
ԵԽ	Եվրոպայի խորհուրդ. միջազգային կազմակերպություն, որը զբաղվում է Եվրոպայում մարդու իրավունքների, ժողովրդավարության և օրենքի գերակայության պաշտպանությամբ։

ԱՖՊ	Ահաբեկչության ֆինանսավորման դեմ պայքար. վերաբերում է ահաբեկչական գործունեության ֆինանսավորումը կանխարգելող քաղաքականությանը և գործողություններին: Այն նպատակ ունի բացահայտել և կանխել ահաբեկչական գործողություններ իրականացնելու մտադրություն ունեցող խմբերին ուղղված ֆինանսական հոսքերն ինչպես օրինական, այնպես էլ անօրինական աղբյուրներից:
ERC20 ժետոններ	«Ethereum request for comment 20 ժետոններ (թոքեններ)». 2015 թվականին ներդրված ստանդարտ, որն օգտագործվում է Ethereum բլոկչեյնում խելացի պայմանագրերի ստեղծման և թողարկման համար
ԵՄ	Եվրոպական միություն. Եվրոպայի տարածքում գտնվող 27 եվրոպական երկրներ միավորող քաղաքական և տնտեսական կազմակերպություն:
ԵՓԶ (EPE)	Եվրոպոլի փորձագետների հարթակ. Եվրոպոլի կողմից ղեկավարվող հարթակ, որը հնարավորություն է տալիս իրավապահ մարմինների փորձագետներին փոխանակվել հանցագործությունների վերաբերյալ գիտելիքներով, լավագույն մեթոդներով և ոչ անձնական բնույթի տվյալներով:
ԵՎՐՈՊՈԼ	Եվրոպական միության իրավապահ մարմինների համագործակցության գործակալություն. Եվրոպական միության իրավապահ մարմին, որն օգնում է անդամ պետություններին միջազգային լուրջ հանցագործությունների և ահաբեկչության դեմ պայքարում:
ՖԳԱԽ (FATF)	Ֆինանսական գործողությունների հատուկ աշխատանքային խումբ. Միջկառավարական ստանդարտներ սահմանող մարմին, որը հիմնադրվել է փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարելու քաղաքականություն մշակելու նպատակով:
ՖՇՊՑ (FinCEN)	Ֆինանսական հանցագործությունների դեմ պայքարի ցանց. ԱՄՆ գանձապետարանի (ֆինանսների նախարարության) ստորաբաժանում, որը հավաքագրում և վերլուծում է ֆինանսական գործարքների վերաբերյալ տեղեկատվությունը:

ՖՀՄ (FIU)	Ֆինանսական հետախուզության ստորաբաժանում. Ենթադրյալ փողերի լվացման և ահաբեկչության ֆինանսավորման գործունեության վերաբերյալ ֆինանսական տեղեկատվության և հետախուզական տվյալների հավաքագրմամբ, վերլուծությամբ և տարածմամբ զբաղվող պետական մարմին:
IP	Ինտերնետ պրոտոկոլ. Համացանցով կամ այլ ցանցերով փոխանցվող տվյալների ձևաչափը կարգավորող կանոնների համակարգ:
ԻՄՀ (LER)	Իրավապահ մարմինների հարցում. Իրավապահ մարմինների կողմից կազմակերպություններին կամ ֆիզիկական անձանց ուղղված հարցում՝ հետաքննությունների համար տեղեկատվություն ստանալու նպատակով:
MiCA	Եվրոպական խորհրդարանի և խորհրդի 2023թ. մայիսի 31-ի թիվ 2023/1114 (ԵՄ) կանոնակարգ կրիպտոակտիվների շուկաների վերաբերյալ և ԵՄ թիվ 1093/2010 և 1095/2010 կանոնակարգերում և թիվ 2013/36/ԵՄ և (ԵՄ) 2019/1937 դիրեկտիվում փոփոխություններ կատարելու մասին: Սա ԵՄ-ի նոր կանոնակարգ է, որը կարգավորում է կրիպտոակտիվները: Այն ուժի մեջ կմտնի 2024թ. դեկտեմբերի 30-ից:
ՓԼ	Փողերի լվացում. Ձանցավոր գործունեության արդյունքում ստացված մեծ գումարները որպես օրինական աղբյուրներից ստացված ներկայացնելու ապօրինի գործընթաց:
MultiSig Wallet	Բազմակի ստորագրությամբ կրիպտոարժույթի դրամապանակ. Կրիպտոարժույթի դրամապանակի տեսակ, որի միջոցով գործարք կատարելու համար պահանջվում է մի քանի գաղտնի բանալի:
ՏԲՀԳ (OCEEA)	ԵԱՀԿ-ի տնտեսական և բնապահպանական գործունեության համակարգողի գրասենյակ
ԵԱՀԿ	Եվրոպայի անվտանգության և համագործակցության կազմակերպություն. տարածաշրջանային անվտանգության կազմակերպություն Եվրոպայում, որի գործունեությունն ուղղված է ռազմական, քաղաքական, բնապահպանական և տնտեսական ոլորտներում երկխոսության և համապարփակ համագործակցության խթանմանը:

ԲԱՕՀ (OSINT)	Բաց աղբյուրների օգտագործման մեթոդով իրականացվող հետախուզություն. Հետաքննությունների նպատակով օգտագործվող՝ հանրամատչելի աղբյուրներից ստացված տեղեկատվություն։
ՕՏՀ	Արտաբորսայական. վիրտուալ ակտիվների, արժեթղթերի առքուվաճառք, որն իրականացվում է երկու կողմերի միջև կենտրոնական բորսայի կամ բրոքերի միջոցով կամ առանց դրա։
ՄԱԹՀԳ (UNODC)	ՄԱԿ-ի թմրամիջոցների և հանցավորության դեմ պայքարի գրասենյակ. Միավորված ազգերի կազմակերպության շրջանակներում գործող գրասենյակ, որը զբաղվում է թմրամիջոցների և հանցավորության վերաբերյալ տվյալների հավաքագրմամբ և տարածմամբ։
ՎԱՅՄ (VASP)	Վիրտուալ ակտիվների ծառայություն մատուցող. ՖԳԱԽ-ի կողմից ներմուծված տերմին, որը վերաբերում է վիրտուալ ակտիվների հետ կապված գործունեություն կամ գործողություններ իրականացնող կազմակերպություններին։ : (Լրացուցիչ տեղեկությունների համար տե՛ս էջ 20)
ՎՄՑ (VPN)	Վիրտուալ մասնավոր ցանց. Տեխնոլոգիա, որը թույլ է տալիս ստեղծել ապահով կապ ավելի քիչ պաշտպանված ցանցի միջոցով՝ անհատի համակարգչի և ինտերնետի միջև՝ երբեմն, բայց ոչ միշտ, օգտագործողի գտնվելու վայրը թաքցնելու համար:

Ներածություն

Ուղեցույցի նպատակը

Սույն փաստաթուղթը ծառայում է որպես համապարփակ ուղեցույց իրավապահ մարմինների աշխատակիցների, այդ թվում՝ ոստիկանների, դատախազների, պետական և դաշնային գործակալների, ինչպես նաև հարկային և դատական փորձագետների համար, ովքեր նոր են ծանոթանում կրպիտոարժույթներին և այլ վիրտուալ ակտիվներին: Այն նախատեսված է կրիպտոակտիվների հետ կապված հանցագործությունների հետաքննությամբ ավելի հաճախ զբաղվող անձանց համար:

Այն շեշտը դնում է խարդախությունների և խաբեությունների ամենատարածված ձևերի վրա, ներկայացնում է իրավապահ մարմինների համար լավագույն մոտեցումները, անհրաժեշտ գործողությունները և հնարավոր տուժողներից հավաքվող տեղեկությունների տեսակները, հատկապես ոստիկանական բաժանմունքներում նախնական ապացույցների հավաքման գործընթացում:

Սույն ուղեցույցը գրվել և մշակվել է որպես ձեռնարկ իրավապահ մարմինների աշխատակիցների համար: Այն նպատակաուղղված չի անդրադառնում կրիպտոարժույթի հետ կապված այն ոլորտներին, որոնք դժվար թե կարևոր նշանակություն ունենան առանձին տուժողների հետ կապված՝ ոստիկանությունում քննվող գործերի համար:

Ուղեցույցում նաև հատուկ ուշադրություն է դարձվում իրավապահ մարմինների և ֆիզիկական անձանց փոխգործակցությանը: Ֆինանսական հաստատությունների և ֆինանսական հետախուզության հետախուզական ստորաբաժանումների (կամ դրանց համարժեք մարմինների) կողմից օգտագործվող կասկածելի գործարքների մասին կամ կասկածելի գործունեության մասին հաղորդումների վերաբերյալ տեղեկությունները հաշվի չեն առնվել:

Կրիպտոարժույթների հետ կապված գործերի քննության ներկայիս մոտեցումներում մի շարք խնդիրներ են վեր հանվել. օրինակ՝ հետաքննիչները հայտնել են, որ տվյալների ոչ լիարժեք հավաքագրման պատճառով իրենք ստիպված են եղել կապ հաստատել խարդախության զոհ դարձած անձանց հետ՝ ստանալու այնպիսի տեղեկություններ, ինչպիսիք են կիպտոդրամապանակի հասցեն, առանց որի հետաքննությունն անհնար է: Աշխատակիցները պետք է հասկանան, թե որ տեղեկատվությունն է կարևոր հավաքագրել և որը՝ ոչ: Նման սխալ հաղորդակցության հետևանքով գործերի քննությունը հաճախ օրերով ձգձգվում է, քանի որ տուժողները կարող են լիովին չպատկերացնել, թե որ տվյալներն են կարևոր իրավապահ մարմինների համար:

Գիտելիքների այս բացը պարզապես անհարմարություն չէ. այն շահարկվում է հանցագործների կողմից, ովքեր գիտակցում են, որ տեխնոլոգիաներն ամբողջ աշխարհում հասանելի են առաջին իսկ օրվանից, մինչդեռ կրիպտոարժույթների հետաքննության լավագույն մեթոդները դեռևս հետ են մնում: Մեծացող այս խնդրին արձագանքելու համար մենք ստեղծել ենք այս ուղեցույցը, որը ներկայացնում է, թե ինչպես պետք է գործեն իրավապահ մարմինները հետաքննությունների ընթացքում և ինչպես օգնեն կրիպտոարժույթների հետ կապված հանցագործությունների մասին հայտնող հնարավոր տուժողներին:

Հաշվի առնելով թեմայի բարդությունը, ինչպես նաև ԵԱՀԿ մասնակից տարբեր պետություններում իրավական իրավիճակների և գործելաոճի բազմազանությունը՝ մեր նպատակն է ոչ թե ներկայացնել համապարփակ ուղեցույց, այլ ավելի շուտ գործնական ձեռնարկ, որը կարող է հատուկ նպատակներով օգտագործվել առաջին գծի իրավապահների կողմից, ովքեր ստանում են քաղաքացիների հաղորդումները: Այն կոչված է խթանելու քննարկումների անցկացումը, թե ինչպես բարելավել ներքին աշխատանքային գործելաոճը, հատկապես եթե առկա ուղեցույցները չեն անդրադառնում կրիպտոարժույթների հետ կապված խնդիրներին:
Հակիրճ նկարագրված են այսօր խարդախության ամենատարածված գործողությունները, և ներկայացվել է ներածական նյութ, որը նպաստում է թեմայի ավելի խորը ընկալմանը:

Սույն ուղեցույցը ծառայում է որպես կարևոր քայլ իրավապահ մարմինների և վիրտուալ ակտիվների մշտապես փոփոխվող աշխարհի միջև եղած բացը լրացնելու համար: Պետք է ընդունել, որ «Web3» ոլորտը, որտեղ գործում են կրիպտոարժույթները, շարունակում է արագ զարգանալ, ուստի կարող է անհրաժեշտություն առաջանալ լրացնել այս ուղեցույցը լրացուցիչ գիտելիքներով:

Ուղեցույցում շեշտը դրվում է ոչ միայն արդյունավետ հետաքննությունների համար անհրաժեշտ գործիքների և ռազմավարությունների վրա, այլև այն նպաստում է համայնքում համագործակցության և շարունակական ուսուցման մշակույթի ձևավորմանը:
Գլխավոր նպատակն է զինել իրավապահ մարմինների աշխատակիցներին այնպիսի գիտելիքներով և ինքնավստահությամբ, որոնք կօգնեն հաղթահարել կրիպտոարժույթների հետ կապված հանցագործությունների յուրահատուկ մարտահրավերները:

Ուղեցույցի կառուցվածքը

Սույն ուղեցույցի հիմնական նպատակն է վերապատրաստել վիրտուալ ակտիվների հետ կապված հանցագործությունների հետաքննություններում նոր ներգրավված իրավապահ մարմինների աշխատակիցներին, ինչպես նաև աջակցել այդպիսի հանցագործությունների մասին հաղորդող տուժողներին: Այս նպատակով ուղեցույցը կառուցված է հետևյալ կերպ.

Նախ, ներկայացվում են թվային ակտիվների վերաբերյալ ընդհանուր տեղեկություններ:Թվային ակտիվները կարող են դիտվել որպես ընդարձակ տերմին, որը ներառում է այնպիսի հասկացություններ, ինչպիսիք են Bitcoin և Ethereum կրիպտոարժույթները:

Կներկայացվի դրանց բնույթի և դրանց տարբերությունների և նմանությունների վերաբերյալ պարզաբանում: Դրանց տարբերություններն ու նմանությունները կուսումնասիրվեն հստակ պատկերացում կազմելու համար: Բացի այդ, կքննարկվեն կրիպտոարժույթների և դրանց հիմքում ընկած տեխնոլոգիայի հնարավոր կիրառություններն ու չարաշահումները:

Վիրտուալ ակտիվների մասին հիմնական պատկերացում ձևավորելուց հետո ուղեցույցում ներկայացվում է դրանց հետ կապված տարածված հանցագործությունները:
Այնուհետև նկարագրվում են այդ հանցագործությունների դեպքում ձեռնարկվող ստանդարտ գործողությունները՝ առանձնացնելով այն դեպքերը, որոնք կարելի է արագ լուծել, և նրանք, որոնք պահանջում են մանրակրկիտ հետաքննություն:

Ուղեցույցում ներկայացվում են նաև ապացույցների հավաքագրման մեթոդները, տուժողներին ուղղվող հիմնական հարցերը, վիրտուալ ակտիվների ծառայություններ մատուցողներին փոխանցվող տվյալները և վիրտուալ ակտիվների փոխանակման հարթակներից (բորսաներից) ստացվող տեղեկատվությունը:

Մատչելիություն և լեզվի պարզեցում. Հաշվի առնելով ոլորտի բարդությունը՝ հեղինակներն օգտագործել են պարզ, ոչ տեխնիկական լեզու՝ սույն զեկույցը սկսնակների համար մատչելի դարձնելու համար: Մասնագիտական լեզվից խուսափելով՝ ձգտում ենք ապահովել, որ բովանդակությունը հստակ և հասկանալի լինի բոլոր ընթերցողների համար: Ի վերջո, ուղեցույցն առաջարկում է ռեսուրսներ տուժողներին աջակցելու համար և ներկայացնում է տարբեր առաջարկներ կրիպտոարժույթների հետ կապված հանցագործությունների կանխարգելման համար:

Ընհանուր տեղեկություններ

Կրիպտոակտիվների հետ կապված հետաքննություններն առաջին հայացքից կարող են վախեցնող թվալ՝ հատկապես հաշվի առնելով ակտիվների վերականգնման դժվարության վերաբերյալ առկա սխալ պատկերացումները: Առասպել է այն, թե երբ ազգային արժույթը փոխարկվում է որևէ կրիպտոարժույթի, օրինակ՝ Bitcoin-ի, միջոցներն անդառնալիորեն կորչում են՝ զոհերին թողնելով անօգնական և ստիպելով հետաքննիչներին փակել իրենց գործերը: Մի քանի տարի առաջ այս ընկալումը ճիշտ էր, սակայն ժամանակները փոխվել են:

Տեխնոլոգիաների զարգացումն այսօր նոր հնարավորություններ է ստեղծել, ինչպես, օրինակ, ԴՆԹ-ի ստուգումը թույլ տվեց վերաբացել և լուծել վաղուց չբացահայտված գործերը: Մենք այժմ կարող ենք վերաբացել նախկինում փակված կրիպտոարժույթների հետ կապված գործերը: Բլոկչեյնում կրիպտոարժույթների գործարքների վերլուծության համար նախատեսված գործիքների շարունակաբար աճող հասանելիությունը և միջազգային օրենսդրական փոփոխությունները թույլ են տալիս բացահայտել կրիպտոարժույթների հետ կապված հանցագործություններ կատարողներին: Այս գործիքները գնալով ավելի հարմար են դառնում օգտագործման համար և լայն տարածում են գտնում՝ փոփոխություններ մտցնելով հետաքննությունների ոլորտում:

Չնայած այս բոլոր գործիքների առկայությանը՝ դեռևս նկատում ենք, որ տեղական ոստիկանության ծառայողների կողմից իրականացվող հետաքննություններից շատերը վաղաժամ փակվում են սահմանափակ պատկերացումների և գիտելիքների պատճառով: Շակառակ տարածված կարծիքի՝ կրիպտոարժույթային գործարքները կարելի է հետևել: Ի սկզբանե ճիշտ արձանագրելով տվյալները՝ մեծանում է գործարքները հնարավոր կասկածյալի հետ կապելու հավանականությունը՝ համադրելով վիրտուալ և նյութական ապացույցները:

Վերջին տարիներին ԵԱՀԿ մասնակից մի շարք պետություններ սկսել են կրիպտոարժույթներն ու այլ վիրտուալ ակտիվները ներառել փողերի լվացման դեմ պայքարի իրենց իրավական ակտերում՝ Ֆինանսական գործողությունների հատուկ աշխատանքային խմբի կողմից մշակված նոր չափանիշների համաձայն: Այս զարգացումը նշանակում է, որ կրիպտոարժույթներով աշխատող ընկերություններն այժմ պետք է հավատարիմ մնան ավանդական բանկային հաստատությունների համար ի սկզբանե նախատեսված գործընթացներին: Նրանցից պահանջվում է ստուգել իրենց հաճախորդների ինքնությունը, մանրակրկիտ ուսումնասիրել ֆինանսական միջոցների աղբյուրները և հետևել, թե ուր են ուղարկվում կրիպտոարժույթները:

Հաշվի առնելով այս փոփոխությունները՝ ԵԱՀԿ-ի Վիրտուալ ակտիվների փորձագիտական խումբը որոշել է ստեղծել տեղական իրավապահ մարմինների աշխատակիցների համար հատուկ մշակված օժանդակ ուղեցույց, որը ոչ միայն կբացահայտի կրիպտոարժույթների գործով հետաքննությունների նոր հնարավորությունները, այլև իրավապահ մարմինների աշխատակիցներին կզինի գիտելիքներով և գործիքներով, որոնք անհրաժեշտ են արդարադատություն իրականացնելու համար այս բարդ և զարգացող ոլորտում:


30th OSCE MINISTERIAL COUNCIL
osce NORTH MACEDONIA 2023
IT'S ABOUT PEOPLE
SKOPJE
Interpretation Languages
CH 0 - Floor
CH 1 - ENG
CH 2 - FRA
CH 3 - GER
CH 4 - SPA
CH 5 - RUS
CH 6 - ITA
CH 7 - ALB
CH 8 - MKD


OSCE
Valiant Richey
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

ԵԱՀԿ-ի մասին

ԵԱՀԿ-ն Եվրոպայում անվտանգության և համագործակցության կազմակերպությունն է: Այն գործում է որպես տարածաշրջանային անվտանգության կազմակերպություն՝ նպատակ ունենալով խթանել երկխոսությունն ու համագործակցությունը, և ունի անվտանգության համապարփակ տեսլական, որն ընդգրկում է բոլոր ուղղությունները՝ սկսած ռազմական և քաղաքական ոլորտներից մինչև բնապահպանական և տնտեսական ոլորտները:

ԵԱՀԿ-ն հիմնադրվել է Սառը պատերազմի ժամանակ՝ 1975 թվականին, և ներկայումս բաղկացած է 57 մասնակից պետություններից: Այս պետությունները հիմնականում գտնվում են Եվրոպայում, որտեղ կենտրոնացած է ԵԱՀԿ-ի գործունեության մեծ մասը, սակայն մասնակից երկրների շարքում են նաև Չյուսիսային Ամերիկայի երկրները՝ Կանադան և Միացյալ Նահանգները, ինչպես նաև Կենտրոնական Ասիայի երկրները, այդ թվում՝ Ղազախստանը, Ղրղզստանը և Ուզբեկստանը: ԵԱՀԿ-ն գործում է համապարփակ անվտանգության սկզբունքներով՝ ներառելով ռազմական, քաղաքական, տնտեսական, բնապահպանական և մարդասիրական ոլորտները:

Եվրոպայում ԵԱՀԿ-ն աշխատում է կայունության ամրապնդման և անվտանգության խնդիրների լուծման ուղղությամբ: Դրա հիմնական նպատակն է կանխել հակամարտությունները և խթանել տարածաշրջանային համագործակցությունը այնպիսի մեխանիզմների միջոցով, ինչպիսիք են դիվանագիտական բանակցությունները, հակամարտությունների կարգավորման նախաձեռնությունները և սպառազինությունների վերահսկման համաձայնագրերը: Բացի այդ, ԵԱՀԿ-ն որոշակի աշխատանքներ է իրականացնում ժողովրդավարության և մարդու իրավունքների պաշտպանության հարցերում աջակցության ուղղությամբ, օրինակ՝ ընտրությունների դիտարկումը:

Ֆինանսական հանցագործությունների և կրիպտոհանցագործությունների համատեքստում ԵԱՀԿ-ն օգնում է պայքարել այս մարտահրավերների դեմ՝ նպաստելով իր մասնակից պետությունների միջև հետախուզական տվյալների փոխանակմանը և կարողությունների զարգացմանը, ինչը նպաստում է անդրսահմանային տեղեկատվության հոսքի բարելավմանը:

Սա կարևոր աշխատանք է, քանի որ կրիպտոհանցագործություններն իրենց բնույթով չեն սահմանափակվում մեկ երկրով կամ արժույթով, ուստի միջպետական համագործակցությունը կենսական նշանակություն ունի:

ԵԱՀԿ-ն խրախուսում է նաև իրավական հիմքերի և կարգավորման արդյունավետ միջոցների ստեղծումը ինչպես դասական փողերի լվացման, այնպես էլ ահաբեկչության ֆինանսավորման դեմ պայքարելու, ինչպես նաև կրիպտոարժույթների հետ կապված ապօրինի գործողությունների հայտնաբերման և կանխարգելման միջոցառումների իրականացման համար: Սա ներառում է փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի միջազգային չափանիշներին մասնակից պետությունների համապատասխանության ապահովումը:

Այս նպատակով ԵԱՀԿ-ն իրականացնում է վերապատրաստման ծրագրեր և աշխատաժողովներ՝ իրավապահ մարմինների, ֆինանսական հաստատությունների և ֆինանսական ու կրիպտոհանցագործությունների դեմ պայքարում ներգրավված համապատասխան այլ դերակատարների փորձագիտական գիտելիքները բարելավելու նպատակով: Այս նախաձեռնությունները միտված են հետաքննության մեթոդների կատարելագործմանը և նորագույն տեխնոլոգիաների կիրառման ընդլայնմանը՝ կիբերհանցագործությունները և կրիպտոարժույթի հետ կապված հանցավոր գործունեությունը բացահայտելու և դրանց դեմ պայքարելու համար: Սույն ուղեցույցի շրջանակներում ԵԱՀԿ-ն արձագանքում է որոշ մասնակից պետությունների՝ հանցավոր նպատակներով և միջազգային պատժամիջոցները շրջանցելու համար վիրտուալ ակտիվների օգտագործման հետ կապված ռիսկերը վերացնելու կարիքին: Այս ռիսկերի վերացումը «Վիրտուալ ակտիվների հետ կապված փողերի լվացման ռիսկերը մեղմելու

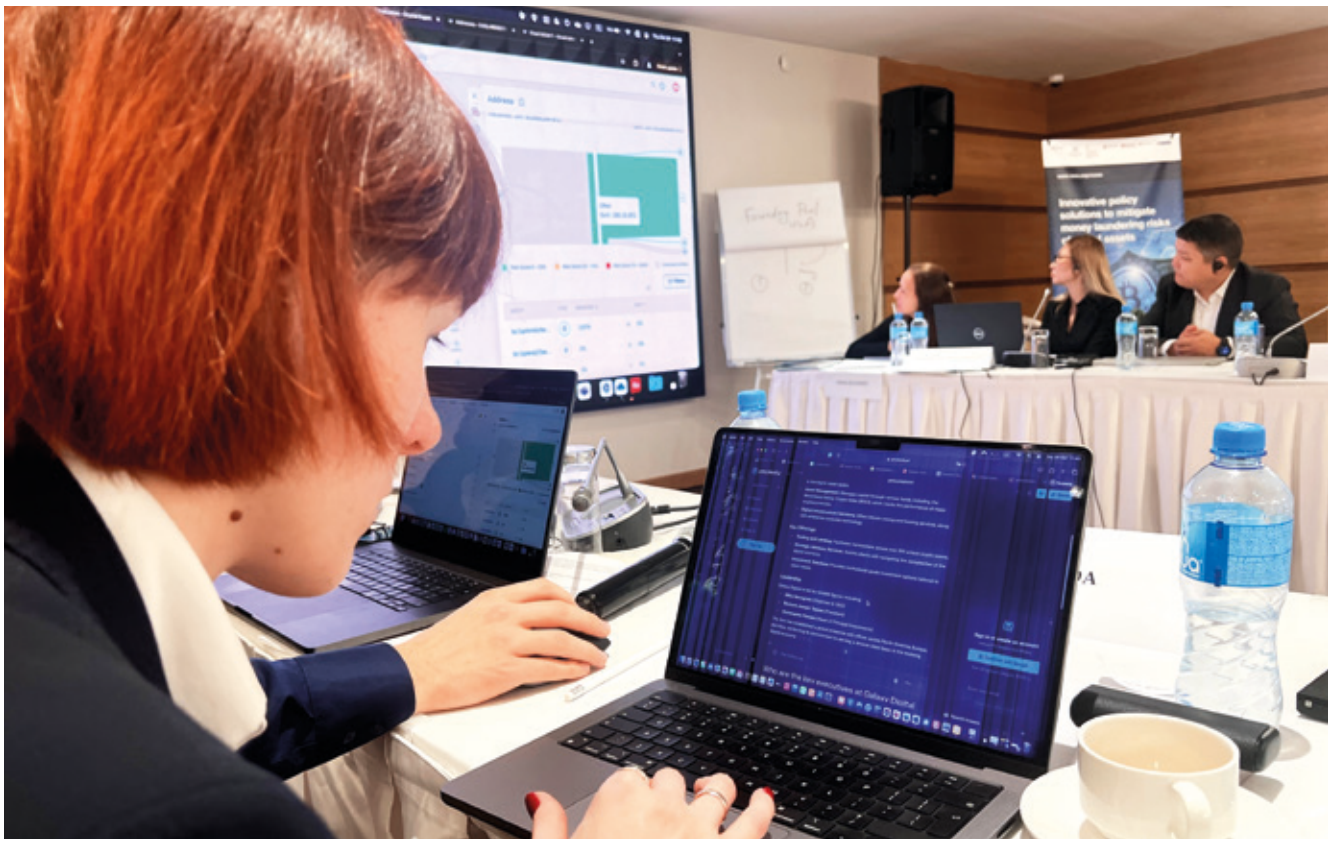
նորարարական քաղաքականության լուծումներ» ծրագրի հիմնական նպատակն է, որն իրականացվում է ԵԱՀԿ-ի Տնտեսական և բնապահպանական գործունեության համակարգողի գրասենյակի (OCEEA) ղեկավարությամբ:

Այս ծրագրի վերջնական նպատակն է զարգացնել պետական մարմինների կարողությունները՝ հակազդելու այս վիրտուալ ակտիվների հատուկ խոցելի գործոններին: Ծրագրի իրականացման ընթացքում ԵԱՀԿ Տնտեսական և բնապահպանական գործունեության համակարգողի գրասենյակը ՄԱԿ-ի Թմրամիջոցների և հանցավորության դեմ պայքարի գրասենյակի Փողերի լվացման դեմ պայքարի համաշխարհային ծրագրի հետ միասին, շարունակում է աջակցել Արևելյան Եվրոպայի և Կովկասի երեք երկրներին՝ Վրաստանին, Մոլդովային և Ուկրաինային՝ իրենց վիրտուալ ակտիվների և վիրտուալ ակտիվների ծառայություն մատուցողների կարգավորող դաշտը ֆինանսական գործողությունների հատուկ աշխատանքային խմբի առաջարկություններին համապատասխանեցնելու հարցում՝ միաժամանակ այս երեք երկրների համապատասխան իրավապահ մարմիններին տրամադրելով կարողությունների զարգացման և տեխնիկական աջակցություն:

Այս ծրագրի արդյունավետությունը բարձրացնելու նպատակով ԵԱՀԿ-ի թիմը համագործակցում է ՄԱԹՀԳ-ի հետ, որն իր փորձագիտական ներուժով և գործնական վերապատրաստման ծրագրերով աջակցում է կրիպտոարժույթների, փողերի լվացման և ահաբեկչության ֆինանսավորման ռիսկերի, հետաքննության, առգրավման և բռնագանձման, կարգավորման և հաճախորդների պատշաճ ստուգման գործում: ԵԱՀԿ-ի Տնտեսական և բնապահպանական գործունեության համակարգողի գրասենյակը շարունակում է աջակցել համապատասխան մարմիններին, այդ թվում՝ կենտրոնական բանկերին, հիմնական ֆինանսական հաստատությունների համապատասխանության վերահսկողության բաժիններին, ֆինանսական հետախուզության ստորաբաժանումներին, գլխավոր դատախազություններին, արդարադատության և ներքին գործերի նախարարություններին՝ աջակցելով անձնակազմի համար կանոնակարգերի և ուղեցույցների մշակմանը, իրազեկման բարձրացման միջոցառումների կազմակերպմանը և կրիպտոարժույթների օգտագործմամբ իրականացվող հանցագործությունների հետաքննության գործում միջգերատեսչական և միջազգային համագործակցությանը:

Սույն փաստաթուղթը ստեղծվել է Գերմանիայի, Իտալիայի, Լեհաստանի, Ռումինիայի, Միացյալ Թագավորության և Միացյալ Նահանգներից կողմից ֆինանսավորվող«Վիրտուալ ակտիվների հետ կապված փողերի լվացման ռիսկերը մեղմելու նորարարական քաղաքականության լուծումներ» ծրագրի շրջանակներում:

OSCE Organization for Security and Co-operation in Europe



Գրետա Բարկաուսկիենեն Ղազախստանի Աստանա քաղաքում անցկացնում է սեմինար հետաքննիչների համար: Օգտագործելով իր հսկայական փորձը որպես փողերի լվացման դեմ պայքարի փորձագետ և Լիտվայի ՊՄԳ նորարարական կենտրոնի ազգային մարտավարական համագործակցության խմբի համակարգող՝ նա ներկայացնում է ինչպես պետական, այնպես էլ մասնավոր շահագրգիռ կողմերի լավագույն փորձը՝ շահառու երկրների իրավունքներն ու հնարավորությունները ընդլայնելու համար:

Վրաստանի Թբիլիսի քաղաքում անցկացված քննիչների սեմինարները նվիրված էին կրիպտոարժույթի ակտիվների առգրավման հիմնական խնդիրներին, ներառյալ հնարավոր բռնագրավման համար պաշտպանված օբյեկտների նախապատրաստումը: Այս սեմինարները սերտորեն կապված էին հետագա գործողությունների հետ, որոնք ուղղված էին բլոկչեյնում կրիպտոարժույթի ակտիվների հայտնաբերման, փոխանցման և վերականգնման հմտությունների բարձրացմանը: Լուսանկարը Մայքլ Գրոմեկի:

Թվային ակտիվների մասին պատկերացում. Պարզեցված ուղեցույց

Թվային ակտիվների մասին պատկերացում. Պարզեցված ուղեցույց

Այս բաժնում կներկայացվեն տարբեր թվային ակտիվների, ՖԻԱՏ փողերի և կրիպտոարժույթների միջև տարբերությունները: Կանդրադառնանք նաև տարբեր տեսակի կրիպտոարժույթների և դրանց շուրջ ենթակառուցվածքների առաձնահատկություններին:

Շաճախ շփոթություն է առաջանում, թե որն է վիրտուալ ակտիվների, կրիպտոակտիվների և կրիպտոարժույթների միջև տարբերությունը:

Պարզ լեզվով ասած՝ **թվային ակտիվը** ամենալայն հասկացությունն է: Դա թվային տեսքով գոյություն ունեցող ակտիվ է: Այն ներառում է պատկերներ, տեսանյութեր, երաժշտություն, օրինակ՝ MP3 ձևաչափով, փաստաթղթեր և վիրտուալ արժույթներ:

Վիրտուալ ակտիվը թվային ակտիվների ավելի նեղ կատեգորիա է: Ըստ ՖԳԱԽՄ-ի[1]՝ վիրտուալ ակտիվներ (կրիպտոակտիվներ) նշանակում են արժեքի ցանկացած թվային տեսքով ներկայացում, որը կարող է թվային եղանակով վաճառվել, փոխանցվել կամ օգտագործվել վճարման համար: Այն չի ներառում ՖԻԱՏ արժույթների թվային ներկայացումը:

Ի տարբերություն դրա՝ **կրիպտոակտիվն** ընդգրկում է ավելի նեղ ոլորտ: Այն ակտիվ է, որը պահպանում է արժեքը, բայց պետք է փոխանցվի բաշխված ռեեստրի տեխնոլոգիայի (DLT) միջոցով: Բլոկչեյնը DLT-ի տեսակ է: Դուք կարող եք ունենալ վիրտուալ ակտիվ, օրինակ՝ առցանց խաղի մետաղադրամ, որը կրիպտոակտիվ չի համարվում, քանի որ այն փոխանցվում է խաղի խաղացողների միջև՝ առանց բաշխված ռեեստրի տեխնոլոգիայի օգտագործման:

Բլոկչեյնը ներկայումս բաշխված ռեեստրի տեխնոլոգիայի ամենահայտնի տեսակն է, սակայն գոյություն ունեն նաև այլ DLT տեխնոլոգիաներ, ինչպիսիք են Hashgraph-ը, Iota Tangle-ը, R3 Corda-ն և շատ ուրիշներ: Այս ուղեցույցի համատեքստում մենք կենտրոնանում ենք բլոկչեյնի վրա հիմնված ֆինանսների վրա:

Թվային ակտիվների շրջանակներում գոյություն ունեն ակտիվների բազմազան տեսակներ, այդ թվում՝ կրիպտոարժույթները, որոնք նոր տեսակի արժույթներ են և գործում են բլոկչեյն տեխնոլոգիայի միջոցով, ինչպես նաև ոչ փոխարկելի ժետոնները (NFT), որոնք պատկերային ակտիվներ են:

Շեղինակի թույլտվությամբ (ըստ Ալեքսանդրա Անդհովի, «Շաշվողական իրավունք», Կարնով, 2022թ.)

1 Ֆինանսական գործողությունների հատուկ աշխատանքային խումբ, աղբյուրը՝ https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies

Այսպիսով, երբ կրիպտոակտիվը մշակվում է վաճառելու, փոխանցելու կամ վճարման համար օգտագործման նպատակով, մենք այն անվանում ենք կրիպտոարժույթ: Կարող եք հանդիպել նաև «վիրտուալ արժույթ» տերմինը, որը օգտագործվում է որպես կրիպտոարժույթի հոմանիշ: Կրիպտոարժույթի և վիրտուալ արժույթի միջև հիմնական տարբերությունը դրանց հիմքում ընկած տեխնոլոգիան է: Կրիպտոարժույթներն օգտագործում են բլոկչեյն, մինչդեռ պարտադիր չէ, որ վիրտուալ արժույթները հիմնված լինեն բլոկչեյնի վրա: Այս ուղեցույցը հիմնականում կկենտրոնանա կրիպտոարժույթներով կատարված հանցագործությունների վրա:

Կրիպտոարժույթներ և ՖԻԱՏ արժույթներ

Ավանդական մետաղադրամները և թղթադրամները, որոնք հայտնի են որպես «ՖԻԱՏ արժույթ» կամ «ֆիատ փողեր» դարեր շարունակ եղել են մեր տնտեսության հիմնասյունը: Սակայն տեխնոլոգիաների զարգացման հետ մեկտեղ ի հայտ եկան փողի նոր ձևեր՝ ջնջելով շոշափելիի և վիրտուալի միջև սահմանները: ՖԻԱՏ արժույթի էլեկտրոնային փոխանցումների դեպքում մարդիկ օգտագործում են «էլեկտրոնային փող» (e-money): «E-money»-ն կամ էլեկտրոնային փողը ներկայացնում է մեզ ծանոթ ՖԻԱՏ արժույթը թվային տեսքով, որը հնարավորություն է տալիս իրականացնել էլեկտրոնային գործարքներ՝ առանց փոխելու դրա արժեքը: Էլեկտրոնային փողը ֆիատ արժույթի թվային ներկայացումն է:

Ի տարբերություն ՖԻԱՏ-ի, կրիպտոարժույթները գործում են ապակենտրոնացված միջավայրում: Դրանք որևէ կառավարության կամ կենտրոնական բանկի հետ կապ չունեն, և դրանց արժեքը որոշվում է տարբեր գործոններով, այդ թվում՝ պահանջարկը, տեխնոլոգիան և վստահությունը:

Բիթքոյնը, որն այս ոլորտի առաջատարն է, ցույց է տվել այս արժույթների ներուժը: Դրա արժեքը հասել է նշանակալի բարձրությունների: 2021 թվականին բիթքոյնի արժեքը գերազանցել է 64 000 դոլարը մեկ մետաղադրամի համար: Կրիպտոարժույթները, ինչպիսիք են Բիթքոյնը և Թեթերը (Tether), չեն երաշխավորվում որևէ կառավարության կամ կենտրոնական բանկի կողմից: Թեև վիրտուալ արժույթներն այնքան հին չեն, որքան ՖԻԱՏ արժույթը, այդուհանդերձ, դրանք այնքան էլ նոր չեն, որքան շատերը ենթադրում են: Առաջին վիրտուալ արժույթներից մեկը՝ «E-Gold»-ը կամ էլեկտրոնային ոսկին, ներկայացվել է գրեթե 30 տարի առաջ՝ 1996 թվականին:

Հակիրճ տեղեկություններ «E-Gold»-ի մասին

Առաջին հանրաճանաչ վիրտուալ արժույթներից մեկը կոչվում էր «E-Gold» (էլեկտրոնային ոսկի): 1996 թվականին Դուգլաս Ջեքսոնի և Բերրի Դաունիի կողմից հիմնադրված «E-Gold»-ը հնարավորություն էր տալիս օգտատերերին բացել հաշիվ, որի արժեքն արտահայտված էր ոսկու գրամներով (կամ այլ թանկարժեք մետաղներով), ինչպես նաև կատարել գումարի ակնթարթային փոխանցումներ այլ E-Gold հաշիվների:

2005 թվականին E-Gold-ն ուներ 2,5 միլիոն հաշվետեր, որոնք օրական կատարում էին միջինում 6,3 միլիոն ԱՄՆ դոլարի չափով գործարքներ: Այն հայտնի էր իր արդյունավետության, ցածր միջնորդավճարների և աշխարհի տարբեր երկրներում հասանելիության շնորհիվ: Սակայն խիստ կանոնակարգերի բացակայությունը նաև նպաստավոր միջավայր ստեղծեց անօրինական գործունեության համար: 2007 թվականին Միացյալ Նահանգներում երդվյալ ատենակալների մեծ կազմը (Grand jury) մեղադրեց E-Gold-ին փողերի լվացման, դավադրության և չլիցենզավորված դրամական փոխանցումների բիզնես գործունեություն ծավալելու մեջ, ինչի արդյունքում, ի վերջո, 2009 թվականին E-Gold-ը փակվեց ԱՄՆ դատարանների կողմից: E-Gold-ը առաջ բերեց մի շարք նմանակներ, ինչպիսիք են e-Bullion.com-ը, Pecunix.com-ը և այլն:[2]

Այս ոլորտը քննարկելիս կարևոր է լինել հստակ, քանի որ վիրտուալ արժույթները կարող են վերաբերել ինչպես էլեկտրոնային փողերին, այնպես էլ կրիպտոարժույթներին, ինչը երբեմն կարող է շփոթություն առաջացնել:

Այս ուղեցույցում մենք կենտրոնանում ենք կրիպտոարժույթների վրա:

2 «Ֆեդերալները մեղադրում են «E-Gold»-ին կիբերհանցագործներին օգնելու մեջ», NBC News, 2007թ. մայիս
(Հասանելի է http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helpingcybercrooks հղումով
«Ինտերնետային արժույթի ընկերությունն ընդունում է փողերի լվացման մեջ իր մեղքը», The Industry Standard, 2008թ. հուլիս Հասանելի է http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering հղումով:
«Էլեկտրոնային ոսկու գործարքների հակիրճ նկարագրություն» (1996) E-Gold: Հասանելի է http://www.e-gold.com/unsecure/synopsis.htm հղումով:

Հիմքում ընկած տեխնոլոգիան. Բլոկչեյն

Բլոկչեյնը բաշխված ռեեստրի տեխնոլոգիայի (DLT) տեսակ է: Այս նոր տեխնոլոգիան առաջին անգամ ի հայտ եկավ 2008 թվականին Սատոշի Նակոմոտոյի[3] հրապարակած զեկույցում («սպիտակ թուղթ»): Բլոկչեյնը սահմանվում է որպես ապակենտրոնացված, քանի որ այն չունի գեթ մեկ վերահսկող կենտրոն կամ պատասխանատու անձ:

Գոյություն ունեն բլոկչեյնի բազմաթիվ տեսակներ: Բլոկչեյնը միայն հիմքում ընկած տեխնոլոգիան է: Պատկերացրեք յուրաքանչյուր բլոկչեյնը որպես առանձին շենք: Թեև յուրաքանչյուրի արտաքին տեսքը և նպատակները կարող են շատ տարբեր լինել, սակայն, եթե նայեք ներսից, կտեսնեք, որ գրեթե բոլոր շենքերը կառուցված են աղյուսով և ցեմենտով:

Ինչպես շենքերի դեպքում, յուրաքանչյուր ոք կարող է մուտք գործել որոշ բլոկչեյններ առանց թույլտվության, մինչդեռ որոշները պահանջում են հաստատում՝ նախքան միանալու թույլտվություն ստանալը:

Այս առումով մենք տարբերակում ենք հանրային և մասնավոր բլոկչեյններ: Հանրային բլոկչեյնները կոչվում են «թույլտվություն չպահանջող» և սովորաբար պահանջում են ավելի քիչ թափանցիկություն կամ վերահսկողություն, մինչդեռ «թույլտվություն պահանջող» բլոկչեյնները հաճախ օգտագործվում են կորպորատիվ նպատակներով և պահանջում են, որ միանալ ցանկացող անձը նախապես ստանա հաստատում:

Բլոկչեյնն այդպես է կոչվում, քանի որ օգտատերերն ավելացնում կամ փոփոխում են տվյալների «բլոկները», և այս բլոկները միմյանց հետ կապվում են շղթայով ժամանակագրական կարգով (ըստ ժամանակի): Երբ որևէ օգտատեր ստեղծում կամ վերբեռնում է նոր բլոկ (օրինակ՝ բիթքոյնով նոր գործարք), բլոկչեյնի բոլոր մյուս օգտատերերը պետք է հաստատեն նոր բլոկը՝ օգտագործելով «կոնսենսուսի մեթոդներ», որոնք ներառում են բավականին բարդ մաթեմատիկական հավասարումներ՝ վստահելիության ապահովման համար:

Քանի որ բոլոր բլոկները փոխկապակցված են, գրեթե անհնար է վերադառնալ նախորդ բլոկին և փոխել այն: Սա նշանակում է, որ համակարգը չի կարող կոտրվել: Ցանկացած նոր տեղեկատվություն, ներառյալ հին տվյալների փոփոխությունները, գրանցվում են նոր բլոկում:

Բլոկչեյնն աշխատում է այնպես, որ այն հնարավորություն է տալիս տվյալ շղթային միացված բոլոր օգտատերերին տեսնել շղթայի ամբողջ պատմությունը («ռեեստրը»): Այսպիսով, բիթքոյնի բլոկչեյնի դեպքում օգտատերերը կարող են տեսնել կատարված յուրաքանչյուր գործարք: Սա թույլ է տալիս քննիչներին իրականացնել հետաքննություններ: Բլոկչեյնը «բաշխված ռեեստրի տեխնոլոգիա» կամ DLT անվանումը ստացել է ռեեստրի՝ բոլոր օգտատերերի միջև բաշխված լինելու պատճառով:

Այն նման է «Google աղյուսակին (sheet)», որի վրա բոլորը կարող են համատեղ աշխատել և տեսնել նախորդ տարբերակները: Քանի որ ամեն ինչ տեսանելի է և չի կարող փոփոխվել առանց բոլոր օգտագործողների իմացության, այն ապահովում է բարձր մակարդակի թափանցիկություն, վստահություն և անվտանգություն: Բացի այդ, այն նաև հարձակումների նկատմամբ շատ դիմացկուն է, քանի որ յուրաքանչյուր օգտատիրոջ մոտ կա բլոկչեյնի կրկնօրինակը, և չկա կենտրոնացված որևէ տարբերակ, նույնիսկ եթե մեկ օգտատեր (բլոկչեյնի տերմինաբանությամբ՝ «հանգույց») ենթարկվի հարձակման և դուրս գա շարքից, համակարգը շարունակում է աշխատել:

Հեղինակի թույլտվությամբ (ըստ Ալեքսանդրա Անդհովի, «Շաշվողական իրավունք», Կարնով, 2022թ.)

3 Ս.Նակամոտո (2008թ.) «Համակարգչից համակարգիչ էլեկտրոնային վճարային համակարգ, Բիթքոյն»: Հասանելի է https://bitcoin.org/en/bitcoin-paper հղումով

Կրիպտոարժույթների տեսակները

Կրիպտոարժույթները տարբերելու երկու եղանակ կա:

• Արդյո՞ք դրանք փոխարկելի են, թե ոչ փոխարկելի
• Արդյո՞ք դրանք կենտրոնացված են, թե ապակենտրոնացված

Տարբերակիչ այս հատկանիշներն մանրամասն նկարագրված են ստորև:

Փոխարկելի և ոչ փոխարկելի արժույթներ

Փոխարկելի արժույթներն ունեն ՖԻԱՏ արժույթին համարժեք արժեք և կարող են փոխանակվել հետ՝ «սովորական» փողի: Նման փոխարկելիությունը երաշխավորված չէ, քանի որ կրիպտոարժույթները չեն ապահովագրվում որևէ կառավարության կամ հաստատության կողմից: Կրիպտոարժույթի փոխարկելիությունը ՖԻԱՏ արժույթի հիմնված է շուկայի և ընդունվող մասնավոր առաջարկների վրա: Սա կրիպտոարժույթի այն տեսակն է, որտեղ տեղի են ունենում հանցագործությունների մեծ մասը:

Փոխարկելի արժույթների օրինակներ են Բիթքոյնը և E-Gold-ը: Ոչ փոխարկելի արժույթները նման են համակարգչային խաղի ոսկե մետաղադրամներին, որոնք մնում են տվյալ խաղի շրջանակներում: Այս արժույթներով կատարված հանցագործությունների հավանականությունն ավելի փոքր է, քանի որ դրանք իրական աշխարհում արժեք չունեն: Այնուամենայնիվ, որոշ մարդիկ գտնում են խաղի սահմաններից դրանցով առևտուր անելու ձևեր՝ դարձնելով դրանք փոխարկելի խաղի շրջանակներից դուրս, նույնիսկ եթե դա հակասում է խաղի կանոններին: Օրինակ՝ ինչ-որ մեկը կարող է «հավաքած ոսկե մետաղադրամները» մեկ խաղացողից փոխանցել մեկ այլ խաղացողի, իսկ գործարքը վճարվում է կանխիկ գումարով:

Կենտրոնացված և ապակենտրոնացված արժույթներ

Կենտրոնացված կրիպտոարժույթները վերահսկվում են մեկ մարմնի կողմից, որը թողարկում է արժույթը, սահմանում է դրա կանոնները, վարում է վճարումների մատյան և իրավունք ունի այն հանել շրջանառությունից: Կենտրոնացված արժույթները կարող են լինել փոխարկելի կամ ոչ փոխարկելի: Ոչ փոխարկելի արժույթները միշտ կենտրոնացված են (քանի որ, օրինակ, խաղի ընթացքում հնարավոր չէ որևէ արժույթ ունենալ, եթե տվյալ խաղը պատասխանատու չէ այդ արժույթի համար): Կենտրոնացված փոխարկելի արժույթը փոխանակելիս փոխարժեքը որոշվում է շուկայի առաջարկի և պահանջարկի հիման վրա, կամ այն սահմանում է ադմինիստրատորը: Կենտրոնացված արժույթի լավ օրինակ է E-Gold-ը:

Կենտրոնացված փոխարկելի արժույթը փոխանակելիս փոխարժեքը որոշվում է շուկայական առաջարկով և պահանջարկով, կամ այն սահմանում է ադմինիստրատորը: Կենտրոնացված արժույթի լավ օրինակ է E-Gold-ը: Ապակենտրոնացված արժույթները, մյուս կողմից, չունեն կենտրոնական վերահսկող մարմին և գործում են համակարգչից համակարգիչ (peer to peer) ցանցի հիման վրա: Պատկերացրեք ապակենտրոնացված համակարգը նման է համացանցին: Ճիշտ այնպես, ինչպես չկա ամբողջ համացանցի համար պատասխանատու գեթ մեկ վերահսկիչ, նույն կերպ ապակենտրոնացված համակարգը չունի գեթ մեկ հիմնական վերահսկիչ: Չնայած այն հանգամանքին, որ մարդկանց մեծամասնությունն ամեն օր օգտվում է համացանցից, չկա գեթ մեկ ընկերություն, որին վճարվում է դրա համար: Փոխարենը, տարբեր մատակարարների վճարվում է տարբեր ծառայությունների համար: Ահա թե ինչպես է օգտագործվում բլոկչեյն ցանցի տեխնոլոգիան, որն ընկած է այնպիսի կրիպտոարժույթների հիմքում, ինչպիսին է Բիթքոյնը: Գործարքները կառավարվում են ցանցի միջոցով, և որևէ կառույց չի վերահսկում դրանք: Ստորև ներկայացված է 2023 թվականի օգոստոսի 23-ի դրությամբ ամենամեծ շուկայական կապիտալն ունեցող տասը կրիպտոարժույթների ցանկը՝ հիմնվելով ծանոթագրության հղման վրա.[4]

4 Բոլոր կրիպտոարժույթները (2023թ.) CoinMarketCap. Հասանելի է https://coinmarketcap.com/all/views/all/ հղումով

Անվանումը	Նշան	Շուկայական կապիտալ (23 օգոստոսի, 2023թ.)	Համեմատվում են հետևյալ երկրների համախառն ներքին արդյունքի հետ[5]
Bitcoin	BTC	$514,912,135,787	Սուդան
Ethereum	ETH	$201,475,414,760	Հայիթի
Tether USDt	USDT	$82,835,552,223	Սոմալի
BNB	BNB	$33,285,580,473	Անդորրա
XRP	XRP	$27,991,699,189	Կյուրասաո
USD Coin	USDC	$26,005,195,827	Լեսոտո
Cardano	ADA	$9,357,776,591	Սենթ Վինսենթ և Գրենադիններ
Dogecoin	DOGE	$8,965,846,112	Հյուսիսային Մարիանյան կղզիներ
Solana	SOL	$8,792,761,272	Սամոա
TRON	TRX	$6,938,358,042	Ամերիկյան Սամոա

Կեղծ արժույթներ և անանուն մետաղադրամներ

Կեղծ արժույթները ներառում են հաշիվներ, որոնք օգտագործում են կեղծանուններ, ինչը նշանակում է, որ թեև գործարքները ուղղակիորեն կապված չեն անհատների հետ, որոշ նույնականացնող տեղեկատվություն պահպանվում է: Օրինակ՝ կրիպտոարժույթ գնելու համար օգտագործվող սովորական ՖԻԱՏ արժույթի բանկային հաշիվը կապված է նույնականացնող տվյալների հետ:

Այս կատեգորիայի մետաղադրամներից են Bitcoin-ը և Ether-ը:

Մյուս կողմից, անանուն (գաղտնի) մետաղադրամներն ավելի մեծ անանունություն են ապահովում՝ օգտագործելով ժամանակակից կրիպտոգրաֆիկ մեթոդներ՝ գործարքի մանրամասները և դրանց հետ կապված նույնականացման տվյալները թաքցնելու համար, ինչը դժվարացնում է դրանք հետևելը սկզբնական օգտագործողին: Այդպիսի մետաղադրամների օրինակներ են «Monero»-ն և «Zcash»-ը:

Կրիպտոդրամապանակներ

Կրիպտոարժույթի դրամապանակը այն տեղն է, որտեղ պահվում է կրիպտոարժույթը: Այն կարելի է համեմատել ժամանակակից աշխարհում փողի պահպանման տարբեր ձևերի հետ:

Փողը գալիս է տարբեր ձևերով: Դրա մի մասը պահվում է ոսկու ձուլակտորների տեսքով խոշոր բանկերում, մի մասն էլ շրջանառվում է թղթադրամների, առցանց բանկային փոխանցումների կամ կրիպտոարժույթների տեսքով:

Կրիպտոարժույթի դրամապանակները նույնպես ներկայացվում են տարբեր ձևերով՝ հեռախոսի հավելվածի, USB կրիչի նման սարքի կամ պարզապես ծրագրային ապահովման տեսքով (որը մի փոքր նման է ձեր էլ. փոստի հասցեին), որին դուք հասանելիություն կունենաք մուտքանունն ու գաղտնաբառը մուտքագրելուց հետո: Չնայած կրիպտոարժույթի դրամապանակների տարբեր տեսակներ կան, դրանք օգտագործում են նույն

5 Ըստ Համաշխարհային բանկի ՀՆԱ-ի տվյալների (ԱՄՆ $), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false

տեխնոլոգիան: Շատերն ունեն 12, 18 կամ 24 բառից բաղկացած վերականգնման գաղտնաբառեր, որոնք թույլ են տալիս վերաբացել դրամապանակը:

Կրիպտոդրամապանակների հասցեները

Կրիպտոարժույթի դրամապանակի հասցեները նման են բանկային հաշվեհամարներին: Ինչ-որ մեկի բանկային հաշվեհամարն ունենալը դեռ չի նշանակում, որ կարելի է հասանելիություն ունենալ նրա միջոցներին: Կրիպտոդրամապանակի հասցեները բաղկացած են երկար, բարդ հաջորդականություններից, որոնք պարունակում են բազմաթիվ մեծատառեր, փոքրատառեր և թվեր: Ահա երկու օրինակ.

TRON կրիպտոարժույթի դրամապանակը
TYm3NTSyk85t9UHSd68DY4vGWQADHXpaXJ

Bitcoin կրիպտոարժույթի դրամապանակը
Bc1qu5z7kn0v2krhglsnan4c0m5f76xk69p53wjwgh

Ավանդական բանկային հաշվի համարների և կրիպտո-դրամապանակների հասցեների միջև տարբերությունն այն է, որ դրամապանակի հասցեի համեմատ բանկային հաշվի համարից կարելի է շատ տեղեկություններ ստանալ: Այդուհանդերձ, կրիպտո-դրամապանակների հասցեները կարող են տարբեր լինել՝ կախված բանկային հաշվի համարից: Իրավապահ մարմինները կարող են հեշտությամբ վերծանել IBAN համարը և կապվել համապատասխան մարմնի հետ:
IBAN-ը միջազգային բանկային հաշվեհամար է: Այն կարող է պարունակել մինչև 34 տառ և թիվ: IBAN-ի համարը սկսվում է երկրի կոդով, ապա անվտանգության ստուգման երկնիշ թվով, այնուհետև շարունակվում բանկային և հաշվի տվյալներով:
Օրինակ՝

IBAN:

- **LT44 3250047338696265**

  LT-ն նշում է Լիտվայի Հանրապետությունը,

  32500-ը՝ «Revolut Bank» ՓԲԸ-ն

  47338696265 -ը օգտատիրոջ հաշվեհամարն է[6]

Եթե հետաքննության ընթացքում ի հայտ գա նմանատիպ IBAN բանկային հաշվի համար, ապա հետաքննությունը վարող պաշտոնյան կիմանա, որ պետք է կապ հաստատել Լիտվայի «Revolut» բանկի հետ: Այս տեղեկատվությունը կարելի է ստանալ այսպես կոչված «IBAN-ի ստուգման համակարգերից», ինչպիսիք են iban.com-ը կամ https://wise.com/gb/iban/checker-ը: Այնուհետև կարելի է սկսել հաշվի օգտատիրոջ անձնական տվյալները ստանալու գործընթացը:
Կեղծ անանուն կրիպտոարժույթների դեպքում, ինչպիսին է Բիթքոյնը, ոչ մի իրավապահ մարմին չի կարող նույնականացնել հաշվետիրոջ անձնական տվյալները նման հետևյալ հաշվեհամարի հիման վրա՝ bc1qu5z7kn0v2krhglsnan-4c0m5f76xk69p53wjwgh:
Հաշվի սեփականատիրոջ նույնականացման տվյալները գտնելու համար անհրաժեշտ է հատուկ ծրագրային ապահովում, օրինակ՝ **բլոկչեյնի վերլուծող ծառայություններ մատուցող հարթակը**: Բլոկչեյնի վերլուծական ծառայությունները մատուցողները կարող են բացահայտել օգտատերերի նույնականացման տվյալները և հետևել տարբեր կրիպտոարժույթների միջև գործարքներին, ինչը տարածված մարտավարություն է, որն օգտագործվում է կրիպտոարժույթների գողության դեպքում: Նման ծառայությունների

6 IBAN և ֆինանսական հաստատությունների կոդերը, Լիտվայի բանկ, https://www.lb.lt/en/iban-and-financial-institution-codes

մատուցողների կարողությունը որոշելու, թե որ ֆինանսական հաստատությունները կամ Կրիպտոարժույթի փոխանակման բորսաներն (VASP՝ վիրտուալ ակտիվների ծառայություններ մատուցողներ) ունեն նույնականացման այս տվյալները, կախված է այն երկրի օրենսդրությունից, որտեղ նրանք իրականացնում են իրենց գործունեությունը: Այդ իսկ պատճառով միջազգային կառույցները, ինչպիսին է ԵԱՀԿ-ն, օգնում են իրենց մասնակից պետություններին կիրառել միջազգային լավագույն փորձը այս ոլորտում:

Կրիպտոդրամապանակի դիտարկիչներ

Քանի որ հանրությանը հասանելի բլոկչեյնի առաջատար տեսակները բաց են բոլորի համար, ուստի այսպես կոչված «կրիպտոդրամապանակի դիտարկիչի» միջոցով կարելի է դիտարկել դրամապանակում կատարվող բոլոր գործարքները:

Կրիպտոդրամապանակի դիտարկիչը որոնման համակարգ է, որը հատուկ նախատեսված է բլոկչեյնի տվյալները դիտելու համար: Այն տրամադրում է մանրամասն տեղեկատվություն առանձին բլոկների, գործարքների և դրանց հետ կապված դրամապանակների մասին:

Պատկերացրեք, թե այն բլոկչեյնի գործարքների «Google» համակարգն է:

Ուշադրություն դարձրեք.

Կրիպտոարժույթի յուրաքանչյուր տեսակի համար կարող է պահանջվել դրամապանակի տարբեր դիտարկիչ: Լավագույն մոտեցումն է՝ որոնման համակարգում մուտքագրել հետաքրքրող կրիպտոարժույթի անվանումը և ավելացնել «wallet explorer» (դրամապանակի դիտարկիչ) կամ «blockchain explorer» (բլոկչեյնի դիտարկիչ) արտահայտությունը՝ ծառայություն մատուցող առաջատար հարթակները գտնելու համար: Նման ծառայությունները սովորաբար անվճար են:

Կրիպտոդրամապանակների դիտարկիչների հիմնական կիրառությունները.

- **Գործարքների ստուգում.** Դրամապանակների դիտարկիչները հնարավորություն են տալիս օգտվողներին համոզվել, որ գործարքը տեղի է ունեցել: Երբ ինչ-որ մեկը պնդում է, որ կրիպտոարժույթ է ուղարկել, ապա դրա իրականությունը կարելի է հաստատել դիտարկիչի օգնությամբ՝ գործարքի համարը կամ դրամապանակի հասցեն օգտագործելով գործարքը որոնելու միջոցով:

- **Աուդիտ և հաշվառում.** Ֆիզիկական անձանց կամ ձեռնարկությունների համար, որոնք պետք է կատարեն գործարքների հաշվառում, դիտարկիչները կարող են տրամադրել մանրամասն տվյալներ գործարքի կատարման ժամանակի, փոխանցված գումարի և ընդգրկված հասցեների մասին:

- **Հետազոտություն և վերլուծություն.** Ծրագրավորողները, հետազոտողները և վերլուծաբանները հաճախ օգտագործում են դրամապանակի դիտարկիչներ՝ բլոկչեյնի ընդհանուր վիճակն ու ակտիվությունն ուսումնասիրելու համար: Նրանք կարող են տեսնել, թե քանի գործարք է տեղի ունենում, գործարքների ծավալը և այլ տվյալներ:

- **Դրամապանակի մնացորդ.** Դրամապանակի հասցեն դիտարկիչում մուտքագրելով կարելի է ստուգել կոնկրետ կրիպտոարժույթի դրամապանակի մնացորդը և տեսնել նրա գործարքների պատմությունը:

Անվճար դրամապանակի դիտարկիչներ.
Հեշտ է գտնել դրամապանակի դիտարկիչներ յուրաքանչյուր տեսակի կրիպտոարժույթի համար՝ պարզապես սովորական ինտերնետային որոնման համակարգում մուտքագրելով «best free XXX cryptocurrency wallet explorer» (XXX կրիպտոարժույթի դրամապանակի լավագույն անվճար դիտարկիչ) արտահայտությունը:

Այս գործիքների օգնությամբ յուրաքանչյուր ոք կարող է ուսումնասիրել և ստուգել գործարքները բլոկչեյնում՝ նույնիսկ առանց որևէ կրիպտոարժույթ ունենալու կամ տեխնոլոգիայի մասին խորացված գիտելիքներ ունենալու:

Կրիպտոարժույթների փոխանակում

«Սովորական» փողի պես, որևէ տեսակի կրիպտոարժույթը մեկ ուրիշի կամ ՖԻԱՏ արժույթի փոխանակելու համար անհրաժեշտ է օգտագործել հատուկ հարթակ: Գոյություն ունի հարթակների երեք հիմնական տեսակ՝ օգտատերերի միջև փոխանակումներ (P2P), կենտրոնացված փոխանակման հարթակներ (CEX) և ապակենտրոնացված փոխանակման հարթակներ (DEX):

P2P նշանակում է **peer-to-peer**, այսինքն՝ մի անձից մյուս անձին, կամ ավելի հաճախ մի օգտատիրոջից մյուս օգտատիրոջը (քանի որ իրավաբանական անձինք կարող են վաճառել կամ առաջարկել իրենց ակտիվները)։ Այստեղ օգտատերերը գնում են կրիպտոարժույթը ոչ թե բուն հարթակից, այլ մյուս օգտատերերից։ Այսպիսի P2P փոխանակման օրինակներից էր LocalBitcoin.com կոչվող ֆիննական հարթակը, որը դադարեցրել է իր գործունեությունը։

Փոխանակման նման հարթակներն իրենց սեփական վիրտուալ ակտիվները, և դրանց օգտատերերը միմյանց հետ չեն համընկնում։

P2P փոխանակումները կատարվում են փողերի լվացման դեմ պայքարի և ահաբեկչության ֆինանսավորման դեմ պայքարի կանոնակարգերի[7] համաձայն և պահանջում են օգտատերերի մասին մանրամասն տեղեկություններ։ Նրանք նաև պետք է հետևեն այն երկրների օրենսդրությանը, որտեղ դրանք գործում են։

Ապակենտրոնացված փոխանակումները նշում են, որ դրանք գործում են ֆայլերի ավտոմատ փոխարկիչների նման (օրինակ՝ .doc-ը .pdf-ի)։ Դրանք հիմնականում օգտագործվում են մի կրիպտոարժույթից մեկ այլ կրիպտոարժույթի և ավելի հազվադեպ՝ ՖԻԱՏ-ից որևէ կրիպտոարժույթի փոխանակումների համար։ Ապակենտրոնացված փոխանակումների միջոցով փոխանցվող միջոցները պահանջում են հատուկ տեխնոլոգիաներ հետևելու համար։

Սա ընդամենը «սառցաբեկորի երևացող մասն է»։ Գոյություն ունեն նաև փոխանակման հարթակների նոր տեսակներ, ինչպես վերը նշված ապակենտրոնացված փոխանակման հարթակներն են։ Դրանք են արտաբորսայական (OTC) փոխանակման հարթակները, խառնիչ և քողարկիչ հարթակները։ Սա արագ զարգացող տեխնոլոգիա է, որը մշակվում է օգտագործողների գործարքների հետքերը թաքցնելու նպատակով։ ԵԱՀԿ-ի անդամ երկրներից շատերը միջոցներ են ձեռնարկում նման գործիքների օգտագործումը սահմանափակելու համար։

Խառնիչներ և քողարկիչներ

Խառնիչները և քողարկիչները կրիպտոարժույթների գործարքների գաղտնիությունն ու անանունությունը բարձրացնելու համար նախատեսված ծառայություններ են։ Դրանց հիմնական գործառույթը տարբեր օգտատերերի միջոցները խառնելն է՝ դրանց սկզբնական աղբյուրը թաքցնելու համար։

Խառնիչներ

Սրանք կենտրոնացված կամ ապակենտրոնացված ծառայություններ են, որոնք խառնում են տարբեր աղբյուրներից կրիպտոարժույթների միջոցները՝ դրանց ծագումը թաքցնելու համար։ Օգտատերերն իրենց կրիպտոարժույթները (օրինակ՝ Բիթքոյնը) ուղարկում են խառնիչին, որն այնուհետև խառնում է այդ մետաղադրամները այլ օգտատերերի կամ իր սեփական մետաղադրամների հետ։

«Խառնման գործընթացի» ավարտից հետո ծառայությունն օգտատիրոջ նշված հասցեին ուղարկում է համարժեք քանակությամբ մետաղադրամներ՝ գանձելով որոշակի վճար։ Այս մեթոդը դժվարացնում է մետաղադրամների ծագումը հետևելը։ Այդուհանդերձ, կենտրոնացված խառնիչները կառավարվում են մեկ սուբյեկտի կողմից, որը կարող է պոտենցիալ գրանցել գործարքները։

Եվրոպոլի EC3 թիմն առաջարկում է «ապախառնման» դասընթացներ, որոնք հասանելի են միայն իրավապահ մարմինների հաստատված աշխատակիցների համար։

Խառնիչների նմանատիպ ծառայություններ ավանդական բանկային համակարգում

Խառնիչների աշխատանքն ինչ-որ չափով նման է սովորական բանկերին, որտեղ միջոցներն ավանդադրվում են և հանվում։ Պատկերացրեք խոշոր ֆինանսական հաստատություն, որտեղ տարբեր ֆիզիկական անձինք գումար են ավանդադրում։ Եթե այդ հաստատությունը համախմբեր բոլոր ավանդները և դրանք բաժաներ հաշվետերերին՝ առանց նշելու յուրաքանչյուր դոլարի ծագումը, ապա դա նման կլիներ խառնման գործընթացին։ Այս դեպքում միջոցներն անցնում են հայտնի կառույցի (օրինակ՝ կենտրոնացված խառնիչի) վերահսկողության տակ, և դրանք ներսում խառնվում են մյուս միջոցների հետ։ Բլոկչեյնի առաջատար վերլուծական ծառայություններ մատուցողները պնդում են, որ առաջարկում են ավտոմատացված կամ ձեռքով «ապախառնում» (demixing) ծառայություններ[8] առաջատար խառնիչների մեծ մասի համար՝ հնարավորություն տալով հետևել նմանատիպ գործարքներին։

7 Սա վերաբերում է միայն այն կրիպտոբորսաներին, որոնք գործում ՖԳԱԽՄ-ի 15-րդ հանձնարարականն իրականացնող երկրներում, որը տվյալ երկրներից պահանջում է կրիպտոարժույթների հետ գործ ունեցող ֆինանսական կազմակերպություններին ընդգրկել ՓԼ/ԱՖ դեմ պայքարի իրենց համակարգում։

8 Մինչև սույն փաստաթղթի հրապարակման վերջնաժամկետը հեղինակը չի կարողացել հաստատել կամ հերքել այս պնդումները

Քողարկիչներ

Քողարկիչները նման են խառնիչներին, և շատ համատեքստերում տերմինները օգտագործվում են փոխարինաբար: Քողարկիչի հիմնական նպատակը նույնպես գործարքների գաղտնիության բարձրացումն է: Ոմանք քողարկիչները համարում են խառնիչների ավելի կատարելագործված տարբերակներ: Դրանք օգտագործում են բարդ ալգորիթմներ՝ ապահովելու, որ խառնված մետաղադրամները հնարավոր չլինի կապել դրանց սկզբնական աղբյուրների հետ:

Քողարկիչների նմանատիպ ծառայություններ ավանդական բանկային համակարգում

Քողարկիչները կարելի է համեմատել այնպիսի բանկային հաշիվների հետ, որոնք բացվում են հարկային ապաստարան (հարկման արտոնյալ ռեժիմով տարածք) համարվող երկրներում կամ օֆշորային բանկերում, որոնք հայտնի են բարձր գաղտնիության և անանունության ապահովմամբ: Նման բանկերը սովորաբար կիրառում են բարդ կառուցվածքներ և գաղտնիության պահպանման համար նախատեսված ծառայություններ: Կրիպտոարժույթների աշխարհում քողարկիչներն օգտագործում են ժամանակակից մաթեմատիկական ալգորիթմներ՝ գործարքների անանունությունն առավելագույնս ապահովելու համար՝ առաջարկելով ավելի բարձր մակարդակի պաշտպանություն, քան ստանդարտ խառնիչները: Քողարկիչի միջոցով գործարքին հետևելը բարդ ու ժամանակատար գործընթաց է, սակայն ոչ անհնարին:.

Տարբերություններ և նմանություններ

Թեև թե՛ խառնիչները, և թե՛ քողարկիչները ծառայում են նույն նպատակին, այն է՝ բարձրացնել գործարքների գաղտնիությունը, դրանց միջև տարբերությունները հաճախ կապված են դրանց մեթոդների և բարդության աստիճանի հետ: Սա նման է հիմնական վեբ բրաուզերները ավելի բարձր մակարդակի գաղտնիության ֆունկցիաներ ունեցող բրաուզերների հետ համեմատելուն: Երկուսն էլ թույլ են տալիս դիտարկել համացանցը, սակայն մեկն առաջարկում է ավելի առաջադեմ գործիքներ անանունությունը պահպանելու համար:

ՎԱԾՄ-ներ և ԿԱԾՄ-ներ

Վիրտուալ ակտիվների ծառայություններ մատուցող (ՎԱԾՄ կամ VASP) հարթակներն իրականացնում են հետևյալ գործունեությունը.

- Նպաստում են վիրտուալ ակտիվների և ՖԻԱՏ արժույթների միջև փոխանակմանը
- Նպաստում են մեկ կամ մի քանի տեսակի վիրտուալ ակտիվների միջև փոխանակմանը,
- Նպաստում են վիրտուալ ակտիվների՝ մեկ դրամապանակից մյուսը փոխանցմանը,
- Մատուցում են վիրտուալ ակտիվների վաճառքի հետ կապված ֆինանսական ծառայություններ:

ՎԱԾՄ-ների հետ կապված մի շարք տերմիններ են փոխարինաբար օգտագործվում: «ՎԱԾՄ» տերմինը սահմանել է Ֆինանսական գործողությունների հատուկ աշխատանքային խումբը (ՖԳԱԽ): Սակայն, «ԿԱԾՄ» հապավումը, որը նշանակում է կրիպտոարժույթների ծառայություններ մատուցող, ավելի հաճախ օգտագործվում է Եվրամիությունում՝ ՎԱԾՄ-ի փոխարեն: ԿԱԾՄ-ով սահմանված ծառայությունների շրջանակն ավելի լայն է, քան ՎԱԾՄ հարթակներինը: Երբեմն նաև օգտագործվում են «բորսա» («exchanges») և «բրոքեր» («broker») տերմինները, սակայն դրանք ներկայացնում են ՎԱԾՄ-ի կամ ԿԱԾՄ-ի բազմաթիվ տեսակներից ընդամենը մեկը:

Թվային ակտիվների հետ կապված հանցագործությունների դեմ պայքարի կանոնակարգ

Թվային ակտիվների հետ կապված հանցագործությունների դեմ պայքարի կանոնակարգ

Չորս ամենակարևոր տեղեկությունները, որոնք անհրաժեշտ է հավաքել

Երբ հավանական տուժողը ներկայանում է ոստիկանական բաժանմունք և պնդում, որ ինքը կրիպտոարժույթի խարդախության զոհ է դարձել, ապա անհրաժեշտ է հավաքել չորս կարևոր տվյալ։

Կրիպտոարժույթային գործարքներն անդառնալի են. դրանց հաստատվելուց և բլոկչեյնում գրանցվելուց հետո զգալի ջանքեր կպահանջվեն այդ միջոցները խարդախության զոհ դարձած անձին վերադարձնելու համար: Այնուամենայնիվ, թեև ջանքերն իսկապես նշանակալի են, վերադարձնելն անհնարին չէ։

Ժամանակ

Առաջին հիմնական տարրը ժամանակն է։ Կրիպտոարժույթի գործարքները ոչ միշտ են անմիջապես մտնում բլոկչեյն: Շաճախ, նախքան բլոկչեյնում գրանցվելը, միջոցները որոշ ժամանակ պահվում են բանկում կամ կրիպտոարժույթների լիցենզավորված բրոքերի մոտ: Պարզելը, թե արդյոք դա իրականում այդպես է, առաջին և ամենակարևոր հարցն է, քանի որ այն դեռևս հնարավորություն է տալիս հետ վերադարձնել գործարքը։

Ֆինանսական հաստատություն

Շաջորդ ամենակարևոր հարցը տուժողին հարցնելն է, թե որ կրիպտոարժույթների բրոքերից կամ ֆինանսական հաստատությունից է օգտվել ՖԻԱՏ արժույթը փոխանցելիս։

Եթե փոխանցումն իրականացվել է ցածր ռիսկային իրավազորության շրջանակներում գործող բրոքերի միջոցով, որը ֆինանսական հաստատությունների նկատմամբ կիրառել է փողերի լվացման դեմ պայքարի կանոնակարգեր, հնարավոր է, որ գործարքը դադարեցվի:

Չափ

Երրորդ ամենակարևոր հարցը գործարքի չափն է, քանի որ փողերի լվացվման դեմ պայքարի շեմը գերազանցող խոշոր գումարները ենթակա են ստուգման վիրտուալ ակտիվների կամ կրիպտոակտիվների ծառայություններ մատուցողների կողմից։ Եթե տուժողը խոշոր փոխանցում է կատարել լիցենզավորված բորսային, ապա հնարավոր է կապ հաստատել այդ բորսայի հետ և կանխել փոխանցված միջոցների փոխակերպումը որևէ կրիպտոարժույթի:

Կրիպտոարժույթի տեսակը

Եվ վերջապես, վերջին կարևոր հարցն այն է, թե ինչ տեսակի կրիպտոարժույթ կամ վիրտուալ ակտիվ է գնվել: Որոշ տեսակների, ինչպիսին է Բիթքոյնը, հեշտությամբ կարելի է հետևել։ Կրիպտոարժույթների այլ տեսակներ, որոնք հայտնի են որպես անանուն մետաղադրամներ, ինչպիսիք են՝ Monero և Zcash-ը, մշակվել են հետևումն ու հետաքննություններն ավելի դժվարացնելու համար, բայց նույնիսկ դրանց հետքերը հայտնաբերելը որոշակի ջանքեր է պահանջում։

Եթե տուժողի բանկային հաշվից գործարքը բոլորովին վերջերս է կատարվել, ապա բոլոր ջանքերը պետք է ուղղված լինեն բլոկչեյնում դրանց հայտնվելը կանխելուն: Եթե գործը ընդունվում է ոստիկանական բաժանմունքում և նախաքննության համար այն փոխանցվում է այլ գործընկերների, ովքեր կարող են գործը վերցնել միայն օրեր անց, կարող է զգալիորեն նվազեցնել հաջողության հասնելու հնարավորությունները։

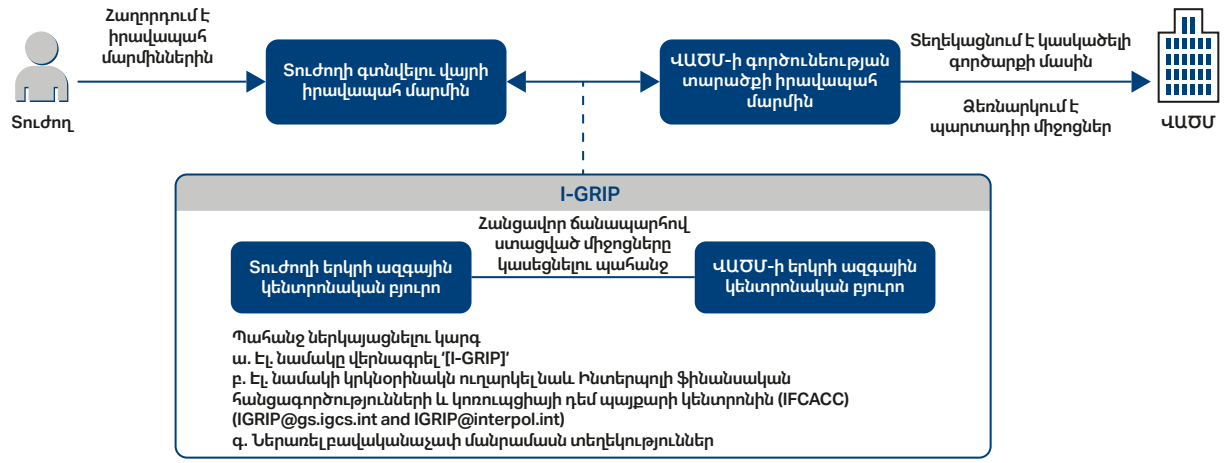
Ահա երեք օրինակ, որոնք լայն տարածում ունեն և պատկերացում են տալիս են այս հայեցակարգի մասին։

Օրինակ 1. Եթե հավանական տուժողի դեպքում միջազգային բանկից ՖԻԱՏ դրամական միջոցների փոխանցումը, օրինակ, սկսվում է ուրբաթ երեկոյան, և դրա մասին իրավապահ մարմիններին հայտնում են շաբաթ առավոտյան, ապա դեռ հնարավոր է կապվել բանկի հետ և կանգնեցնել գործարքը: Եթե տուժողը չի կապվել բանկի հետ, ապա նա պետք է անհապաղ կապ դա անի։ (Տե՛ս ԻՆՏԵՐՊՈԼ-ի «IGrip» լուծումը, էջ 23)

Օրինակ 2. Նույնիսկ եթե խարդախության զոհ դարձած անձը իր բանկային հաշվից մեծ գումար է փոխանցել կրիպտոարժույթի բրոքերին, և փոխանցումն արդեն դուրս է եկել տուժողի հաշվից, հաճախորդի բանկային հաշվում կարող է լինել տեղեկատվություն, որում նշվում է վիրտուալ ակտիվների/կրիպտոակտիվների ծառայություն մատուցողների անունը, որին ուղարկվել է փոխանցումը: Այս դեպքում, եթե փոխանցումն ուղարկվել է խոշոր բրոքերներից մեկին, օրինակ՝ Binance-ին, ապա հաճախորդը պետք է անհապաղ կապվի հաճախորդների սպասարկման հետ՝ զրույցի (չատ) պատուհանի միջոցով կամ էլեկտրոնային նամակ ուղարկի հետևյալ վերնագրով. **«Շտապ. Կասեցնել փոխանակումը. խարդախություն»** fraud@nameofthebroker.domain կամ compliance@nameofthebroker.domain հասցեներին՝ տեղեկացնելով, որ տվյալ IBAN-ից, տվյալ չափով և տվյալ ժամանակահատվածում եկող փոխանցումը չպետք է մշակվի։

Իրավապահ մարմինների աշխատակիցները կարող են նաև պահանջել կանգնեցնել միջոցները, օրինակ՝ Binance-ի պետական իրավապահ մարմինների հարցումների համակարգի միջոցով: https://www.binance.com/en/support/law-enforcement: Խոշոր բրոքերները կամ փոխանակման հարթակները և վիրտուալ ակտիվների ծառայություն մատուցող այլ հարթակներ, որպես կանոն, ունեն ընթացակարգ, որը կարող է օգնել իրավապահ մարմիններին հայտնաբերել և կասեցնել փոխանցումը։ Ոլորտի մասնակիցներից շատերն ունեն էլեկտրոնային փոստի հասցեներ, ինչպիսին են compliance@name-of-the-broker.com կամ fraud@name-on-of-the-broker.com, որոնք կարող են օգտագործվել հրատապ դեպքերի մասին հաղորդելու համար։

«I-GRIP-ի սխեմա»[9]



Աղբյուրը՝ պատկերը տրամադրվել է ԻՆՏԵՐՊՈԼԻ կողմից

Միևնույն ժամանակ, տուժողի գտնվելու վայրի իրավապահ մարմինը կարող է դիմել ԻՆՏԵՐՊՈԼ-ին՝ **«Վճարումների գլոբալ օպերատիվ միջամտություն»** (I-GRIP) գործիքի միջոցով վճարումը կասեցնելու պահանջով: Սա ուղիղ կապ է այն տարածքի իրավապահ մարմնի հետ, որտեղ գտնվում է ՎԱԾՄ-ն: Ինտերպոլը գործարկել է I-GRIP-ը՝ ակտիվների վերականգնման նախնական փուլերի իրականացման նպատակով միջազգային համագործակցությունը բավականաչափ արագացնելու համար:
I-GRIP հայցում ստանալու դեպքում ՎԱԾՄ-ի տարածքի իրավապահ մարմինը կարող է ձեռնարկել անհրաժեշտ միջոցներ հանցավոր ճանապարհով ստացված եկամուտների հետագա մշակումը իրենց երկրի օրենսդրության համաձայն կասեցնելու համար: Անհրաժեշտ միջոցառումները կարող են տարբեր եղանակներով իրականացվել: Իրավապահ մարմինները կարող են պարզապես ստացող ՎԱԾՄ-ին տեղեկացնել կասկածելի գործարքի մասին, որպեսզի ՎԱԾՄ-ը կարողանա կայացնել կասկածելի հաշիվը կասեցնելու կամ նույնիսկ գործարքները հետ կանչելու ինքնուրույն որոշում:

Բացի այդ, իրավապահ մարմինները կարող են օգտագործել իրենց վարչական լիազորությունները պարտադրելու ՎԱԾՄ-ին կասեցնել կասկածելի հաշիվը: Ավելին, իրավապահ մարմինը կարող է ներքին հետաքննություն սկսել I-GRIP պահանջող մարմինների կողմից իրականացվող հետաքննությանը զուգահեռ և կասկածելի հաշվի վրա արգելանք դնելու մասին հրաման արձակել:
Եթե ԵԱՀԿ մասնակից պետության իրավական դաշտը թույլ է տալիս, մեկ այլ հնարավորություն կարող է լինել անհապաղ գործ հարուցելը, ներառյալ հավանական տուժողի հաղորդումը, քանի որ ժամանակը կրիպտո-արժույթների հետ կապված հետաքննության ամենակարևոր պայմաններից մեկն է:

Օրինակ 3. Եթե հավանական զոհը լիովին համոզված չէ, թե որ կրիպտոարժույթի բրոքերին են ուղարկվել միջոցները, և փոխանցման տվյալներում կան տառերի հապավումներ և թվեր, օրինակ՝

1C5Eu4UpeK5djG3QiKwhcLELtF-wHT146dG

ապա սա կարող է վկայել այն մասին, որ միջոցները փոխանակվել են կամ պատրաստվում են փոխանակվել կրիպտոարժույթի դրամապանակի:

9 ԻՆՏԵՐՊՈԼ, Վիրտուալ ակտիվների առգրավման ուղեցույց (2023թ. հոկտեմբեր), էջ 40

Այդպիսի դրամապանակները կարելի է համեմատել բանկային հաշիվների կամ էլեկտրոնային փոստարկղների հետ, որտեղ պահվում են միջոցները: Որոշակի հմտությամբ այդպիսի դրամապանակում պահվող միջոցները կարող են վերականգնվել կամ սառեցվել: Թեև տառերի և թվերի նման համադրությունը անսովոր է կրիպտոարժույթին անծանոթ անձանց համար, այս ոլորտում փորձառու հետաքննիչներն այդպիսի համադրություններից կարող են ստանալ տեղեկատվություն, որը կարելի է համեմատել վարկային քարտի համարի հետ: Կրիպտոարժույթի դրամապանակի հասցե ունենալը նման է վարկային քարտի համար ունենալուն, բայց առանց անձնական տվյալների, ինչպիսիք են անունը կամ թողարկող բանկը: Վարկային քարտի համարը ցույց է տալիս քարտի թողարկողը և քարտի տեսակը: Նմանապես, երբ տուժողն իրավապահ մարմիններին է հայտնում կրիպտոարժույթի դրամապանակի հասցեն, ապա արտաքին գործիքների (որոնք միշտ չէ, որ հաջող են) օգնությամբ հնարավոր է դրամապանակի հասցեն կապել կոնկրետ կրիպտոարժույթի կամ կոնկրետ ՎԱԾՄ-ի կամ ֆինանսական միջնորդի հետ: (Լրացուցիչ տեղեկությունների համար տե՛ս «Վիրտուալ ակտիվների հետ կապված հանցագործությունների հետաքննության լրացուցիչ գործիքներ» բաժինը, էջ 47):

Գործարքների յուրաքանչյուր տեսակի համար կիրառվող լավագույն գործելակերպը

Գոյություն ունի բլոկչեյն տեխնոլոգիաների վրա հիմնված գործարքների երեք տեսակ, որոնք հետաքննիչներին կարևոր է իմանալ, քանի որ նրանց կարող է անհրաժեշտ լինել համագործակցել վիրտուալ ակտիվների ծառայություն մատուցողների (VASP) հետ:

Գործարքների տեսակները	Նկարագրություն	Հետաքննության վրա ազդեցությունը
ՖԻԱՏ արժույթից կրիպտո-արժույթի փոխանակում	Տուժողը բանկային փոխանցման, վճարային քարտի, բջջային վճարման կամ կանխիկ վճարման միջոցով ազգային արժույթով վճարում է կատարել ՎԱՃՄ-ին, որը փոխանակում է միջոցները կրիպտոարժույթների:	**Լավագույն գործելակերպ 1** **Հնարավորության դեպքում փորձեք կասեցնել կամ հետ վերադարձնել փոխանցումը** Շաղորդման ներկայացման փուլում ամենամեծ սխալը կլինի կասկածելի հանցագործության գրանցումը և նախաքննության իրականացումը գրասենյակում որևէ մեկին հանձնարարելը: Սա հետաձգում է տուժողի հետ սկզբնական շփումը: Ձգձգող հանգամանքների բացակայության դեպքում գործարքը դեռևս հնարավոր կլինի կասեցնել: Եթե գործարքը կատարվել է ոչ աշխատանքային ժամերին կամ հանգստյան օրերին, ապա դեռևս հնարավոր կլինի կասեցնել բանկից դուրս եկող փոխանցումը, քանի որ որոշ բանկեր բանկային փոխանցումներն իրականացնում են հաջորդ աշխատանքային օրը: Եթե գործարքը կատարվել է քարտային վճարմամբ, ապա կարելի է կապվել քարտը թողարկողի հետ՝ հնարավորության դեպքում վճարման փոխանցումը հետ կանչելու կամ կասեցնելու համար: Կարևոր է պարզել, թե որ ֆինանսական հաստատությունն է իրականացրել բանկային փոխանցումը: Սա երևում է բանկի կողմից ներկայացված քաղվածքում: **Լավագույն գործելակերպ 2** **Եթե գործարքը կասեցնել չի հաջողվում, ապա փորձեք պարզել, թե որ ՎԱՃՄ-ին է ուղարկվել փոխանցումը, որպեսզի հնարավորության դեպքում նրանց միջոցով կասեցնել գործարքը և սառեցնել միջոցները:** Եթե կրիպտոարժույթի բրոքերը գործում է հանցագործությունների ռիսկի ցածր մակարդակ ունեցող երկրում, որը ներդրել է փողերի լվացման դեմ պայքարի (ՓԼՊ) /ահաբեկչության ֆինանսավորման դեմ պայքարի (ԱՖՊ) կանոնակարգեր կրիպտոարժույթների ակտիվների համար, ապա հնարավոր է անհապաղ կապվել բրոքերի հետ և պահանջել սառեցնել կամ վերադարձնել միջոցները, եթե դրանք դեռ չեն փոխանակվել: Երբեմն այս գործընթացը կարող է նախաձեռնել հենց տուժողը: Բրոքերները կարող են այնուհետև կասեցնել միջոցների փոխանակումը, քանի որ ՓԼՊ օրենսդրությունը սահմանում է, որ միջոցները կարող են փոխանցվել միայն այն դեպքում, եթե միջոցների ծագումը հայտնի է, և պարզ է, թե ուր են դրանք ուղարկվում: ՎԱՃՄ-ին տեղեկացնելը, որ կրիպտոարժույթի դրամապանակի նշանակետը խարդախությունն է, կստիպի նրանց գործողություններ ձեռնարկել փողերի լվացման կանոնակարգերի համաձայն դա կանգնեցնելու համար:

Գործարքների տեսակները	Նկարագրություն	Հետաքննության վրա ազդեցությունը
		Թեև դա կախված է ՎԱԾՄ-ի ներքին համապատասխանության քաղաքականությունից, միջոցների ժամանակավոր սառեցումը մի քանի աշխատանքային օրով թույլ կտա իրավապահ մարմիններին կամ դատախազներին միջամտել միջոցների վերադարձման պաշտոնական պահանջով: Դա հնարավոր է, եթե գործեք արագ, և եթե կրիպտոարժույթի բրոքերը պատրաստ է արձագանքել: Երկու գործընթացների ձախողման դեպքում երրորդ հնարավորությունը պարզված ՎԱԾՄ-ի հետ կապ հաստատելն է և խնդրել ներկայացնել իրենց տվյալների բազաներից օգտահաշիվ ստեղծած օգտատիրոջ ինքնությունը հաստատող բոլոր փաստերը (քանի որ հանարավոր է, որ խարդախ է կամ կեղծ անձ), նրանց նույնականացման տեղեկությունները և գործարքի հեշը: Կրիպտոարժույթից կրիպտոարժույթ տուժողը հաղորդում է խարդախության մասին, որը բացառապես բլոկչեյն տեխնոլոգիայի ներսում է, առանց ֆիատ արժույթներ մշակող ավանդական ֆինանսական հաստատությունների հետ կապերի:
Կրիպտո-արժույթից այլ կրիպտո-արժույթի փոխանակում	Տուժողը հայտնում է խարդախության մասին, որը տեղի է ունեցել բացառապես բլոկչեյն տեխնոլոգիայի շրջանակներում, առանց ՖԻԱՏ արժույթներով զբաղվող որևէ ավանդական ֆինանսական հաստատության մասնակցության: Օրինակ՝ տեղի է ունեցել խարդախություն, երբ օգտատիրոջը խաբեությամբ ստիպել են գնել այլ կրիպտոարժույթային պրոդուկտ (օրինակ՝ NFT (ոչ փոխարկելի ժետոններ), Staking և այլն), ինչի արդյունքում նա կրել է ֆինանսական վնասներ:	**Լավագույն գործելակերպ 1** **Գտնել հնարավոր արտոնագրված ֆինանսական միջնորդներին, այսպես կոչված «կենտրոնացված բորսաները», որոնք ներգրավված են եղել փոխանակման գործընթացում: Դրանց հայտնաբերելու դեպքում հնարավոր է այդ միջնորդի միջոցով հավաքել ներգրավված կողմերի ինքնության վերաբերյալ տեղեկություններ:** **Լավագույն գործելակերպ 2** **Շաճախ խարդախության զոհ դարձող անձինք հոգեբանական հարձակումների թիրախ են դառնում, ինչը կիբերանվտանգության զգալի հետքեր է թողնում: Օրինակ՝ կասկածյալները հաճախ իրենց զոհին խնդրում են իրենց հետ կապվել հեռակառավարվող էկրանի ծրագրերի, էլեկտրոնային նամակների կամ հեռախոսազանգերի, նախնական բանկային փոխանցումների, կարճ հաղորդագրությունների կամ հաղորդակցման այլ միջոցներով:** Այս դեպքում զոհերը սովորաբար փորձառու են բլոկչեյնի վրա հիմնված ֆինանսների ոլորտում: Սկզբնական խնդիրն է հավաքել փոխանցման առավել ճշգրիտ և թարմացված տեղեկատվությունը, այն է՝ գործարքների ժամանակը, տուժողի կողմից օգտագործված արժույթների տեսակները, կրիպտոարժույթի դրամապանակների մասին տեղեկություններ, անդորրագրերը (ստացականները), էլեկտրոնային նամակները, կարճ հաղորդագրությամբ հաստատումները և այլ տեսակի տեղեկատվություն: (Ավելի մանրամասն տեղեկություններ կարելի է գտնել հաջորդ «Փաստերի հավաքագրում» բաժնում, էջ 27):

Գործարքների տեսակները	Նկարագրություն	Հետաքննության վրա ազդեցությունը
Կրիպտո-արժույթից ՖԻԱՏ արժույթի փոխանակում	Տուժողը հայտնում է գումարների հափշտակման կամ կորստի մասին	Այս դեպքում տուժողն արդեն ունեցել է կրիպտոարժույթներ, որոնք ուղարկվել են կրիպտոարժույթի բորսա, ապա փոխանակվել են ազգային արժույթի, որը, ամենայն հավանականությամբ, վճարվել է բանկային փոխանցման կամ կանխիկ վճարման միջոցով՝ ֆիզիկական գրասենյակում: ՖԻԱՏ արժույթից կրիպտոարժույթին փոխանցումների պես, այստեղ ևս անհրաժեշտ է գտնել ֆինանսական միջնորդին, որն իրականացրել է ազգային արժույթով փոխանակումը և նախաձեռնել բանկային փոխանցումը: Եթե խոսքը մեծ գումարի մասին է, և ֆինանսական հաստատությունը գտնվում է ռիսկի ցածր մակարդակ ունեցող տարածքում, ապա այն պետք է ստուգի, թե որտեղից են ստացվել գումարները: Այս գործընթացը ձեռքով կատարում են իրավական համապատասխանության մասնագետները: Եթե նման ստուգում իրականացվում է, ապա այն սովորաբար տեղի է ունենում գործարքից հետո 24 ժամից մինչև մի քանի աշխատանքային օրվա ընթացքում: Հնարավորության դեպքում մուտքագրեք կրիպտոարժույթի դրամապանակի հասցեն բլոկչեյնի դրամապանակների դիտարկիչում՝ պարզելու և ստուգելու, թե արդյոք այն կապված է ֆինանսական միջնորդի հետ, որին կարելի է դիմել (տե՛ս «Լրացուցիչ գործիքներ վիրտուալ հանցագործությունների հետաքննիչների համար» բաժինը, էջ 40): Եթե որոնումը հաջողությամբ չի պսակվում, ապա անհրաժեշտ է օգտագործել հատուկ ծրագրակազմ (բլոկչեյնի վերլուծական հարթակ), որը կարող է ցույց տալ՝ արդյոք տվյալ հասցեն կապված է եղել հայտնի որևէ ֆինանսական հաստատության հետ:

Փաստերի հավաքագրում

Փաստերի հավաքագրում

Անձից տեղեկություններ ստանալը

Հետաքննության համար կարևոր 10 տեղեկություն

- **Ակտիվի բնույթը.** ո՞ր կրիպտոարժույթի նախագիծը կամ ոչ փոխարկելի ժետոնն է ներագրավված՝ ներառյալ դրա անվանումը, նշանը և հիմքում ընկած տեխնոլոգիայի առանձնահատկությունները:

- **Գործարքի մանրամասներ.** Տուժողի կատարած գործարքների մասին տեղեկություններ, օրինակ՝ ամսաթիվը, ժամը, գումարը, արժույթը և գործարքի նույնականացման համարները (օրինակ՝ վիրտուալ ակտիվների ծառայություններ մատուցողներից ստացված անդորրագրեր):

- **Դրամապանակի հասցեները.** Ներգրավված կրիպտոարժույթի դրամապանակի հասցեների մանրամասները, թե՛ զոհի, և թե՛ ենթադրյալ խարդախության մեջ կասկածվողի:

- **Շաղորդակցության արձանագրումներ.** զոհի և ենթադրյալ խարդախների միջև ցանկացած հաղորդակցություն, լինի դա էլեկտրոնային փոստով, սոցիալական ցանցերում, զրուցարանային հավելվածներով, հեռախոսազանգերի կամ ֆորումների միջոցով

- **Գովազդային նյութեր.** Վիրտուալ ակտիվների հետ կապված ցանկացած գովազդ, առցանց գրառում կամ այլ գովազդային նյութ, որը տուժողը ստացել է: Էլեկտրոնային նամակների պատճենների դեպքում անհրաժեշտ է պահպանել դրանցում առկա հիպերհղումները, ցանկալի է՝ USB կրիչների վրա: Զգուշացում. այդպիսի նյութեր գրանցելիս մի սեղմեք էլեկտրոնային նյութում տրամադրված հիպերհղումների վրա, քանի որ դրանք կարող են վարակված լինել:

- **Շարթակի վերաբերյալ տվյալներ.** ՎԱԾՄ-ներից տվյալներ պահանջելու մասին տեղեկությունների համար տե՛ս «ՎԱԾՄ»-ներից տվյալներ պահանջելը» բաժինը, էջ 29: Բորսաների անունները հաճախ կարելի է գտնել գործարքի ստացականների վրա:

- **Ուղղորդման մասին տեղեկատվություն.** Տեղեկություններ այն մասին, թե ինչպես է տուժողը իմացել ակտիվի մասին՝ ուղղորդման, առցանց գովազդի, բանավոր տեղեկությունների միջ և այլնի միջոցով:

- **Կոդավորման շեղումներ.** Եթե այդպիսիք կան, ապա իրենցից ներկայացնում են փոփոխված կոդի ցանկացած նշան, որոնք խոչընդոտում են վաճառքը, կամ այլ տեսակի շեղումներ: Հանցավոր գործունեության նպատակով օգտագործվող կայքերի ցանկացած հիպերհղում, և, կախված տվյալ երկրի կանոնակարգերից, երբ տուժողը տրամադրել է իր ֆինանսական տվյալները, ցանկացած մուտքի տվյալներ, որոնք կօգնեն իրավապահ մարմիններին հասկանալ ծրագրակազմը:

- **Ֆինանսական փաստաթղթեր.** Բանկային քաղվածքներ, վարկային քարտերի քաղվածքներ կամ այլ ֆինանսական փաստաթղթեր, որոնք ցույց են տալիս ներդրումների հետ կապված միջոցների փոխանցումը:

- **Ինքնությունը հաստատող տեղեկատվություն.** Ցանկացած տվյալ, որը կարող է օգնել պարզել խարդախին, օրինակ՝ օգտանունները, սոցիալական ցանցի պրոֆիլները, էլ. փոստի հասցեները կամ ցանկացած այլ կոնտակտային տվյալ, որոնք օգտագործվել են տուժողի հետ շփման ընթացքում տուժողի համակարգչի վրա:

- **Տեխնոլոգիական շեղումներ.** Արդյո՞ք տուժողը խարդախության ընթացքում որևէ ծրագրային հավելված է տեղադրել: Այս ծրագիրը հեռացվե՞լ է, թե՞ այն դեռ համակարգչում է: Հնարավո՞ր է որոշել ծրագրաշարի աղբյուրը կամ ծագումը:

Եթե կրպիտոարժույթային գործարքը չի կասեցվել, ապա կարևոր է ստանալ կրիպտոարժույթի դրամապանակի հասցեն, որին ուղարկվել կամ որտեղից ստացվել են միջոցները:

Կրիպտոարժույթի դրամապանակի հասցեների ձեռքբերում

Որո՞նք են բլոկչեյնում հետաքննության համար անհրաժեշտ ամենակարևոր տեղեկությունները:

Գործարքի մանրամասներ. Կրիպտոարժույթի դրամապանակի հասցեն և հեշ համարները

Տարածված սխալ է համապատասխան կրիպտոարժույթի դրամապանակի հասցեների սխալ գրանցումը, քանի որ դրանք բաղկացած են թվերի և տառերի երկար տողերից:

Օրինակ 4. Կրիպտոարժույթի դրամապանակի հասցեն գրանցելիս և այլն, «0» թիվը հեշտությամբ կարելի է շփոթել «O» տառի հետ, կամ «q» տառը՝ «g»-ի հետ: Խորհուրդ է տրվում կրիպտոարժույթի դրամապանակի գրանցված հասցեն մուտքագրել ինտերնետային որոնման համակարգում, ինչպիսիք են Goodle-ը կամ Bing-ը՝ տեսնելու, թե արդյոք դրանք տվյալ հասցեն ճանաչում են: Եթե հասցեն անմիջապես չի հայտնվում, ապա կարելի է օգտագործել դրամապանակի դիտարկման գործիքը: (Տե՛ս նաև Վիրտուալ ակտիվների հետ կապված հանցագործությունների հետաքննության լրացուցիչ գործիքներ» բաժինը, էջ 47):

Եթե կրիպտոարժույթի դրամապանակի հասցեն ճիշտ է, ապա էկրանին անմիջապես հայտնվում է տեղեկատվություն, որից կարելի ստանալ հետևյալ տվյալները.

Բիթքոյնի դեպքում՝ միշտ.

- **Գործարքի գումարի չափը.** Կարելի է տեսնել բիթքոյնի գումարի չափը, որն ուղարկվել կամ ստացվել է յուրքանչյուր գործարքում:
- **Գործարքի ժամանակը.** Կարելի է տեսնել ժամանակային նշումը, թե երբ է գործարքը ներառվել բլոկում:
- **Կրիպտոարժույթի դրամապանակի ընթացիկ մնացորդը.** Կարելի է ստուգել տվյալ պահին դրամապանակում առկա բիթքոյնի ընդհանուր քանակը:
- **Գործարքի հեշ.** Սա յուրաքանչյուր գործարքի առանձին նույնականացուցիչ է, ինչպես օրինակ վճարային ծառայություններ մատուցողների կողմից օգտագործվող գործարքի ID-ն, որը ծառայում է որպես դրա «մատնահետք»:

Շասանելի են որոշ ծառայությունների, բայց ոչ բոլորի դեպքում:

- **Գործարքի չափը.** Որոշ ծառայություններ տրամադրում են մանրամասն տեղեկություններ գործարքի չափի վերաբերյալ, որոնք հաճախ փոխանակվում են առաջատար ՖԻԱՏ արժույթներով, օրինակ՝ ԱՄՆ դոլարով կամ եվրոյով:
- **Ժամային գոտու կարգավորում.** Որ Որոշ հարթակներ տալիս են կանխադրված (default) UTC ժամային գոտին փոխելու հնարավորություն: Օրինակ՝ օգտատերերը կարող են այն հարմարեցնել իրենց տեղական ժամային գոտուն, ինչը կարող է օգտակար լինել ապացույցների հավաքագրման համար:

Հնարավո՞ր է արդյոք մեկ կրիպտոարժույթի դրամապանակի հասցեում պահել տարբեր տեսակի կրիպտարժույթներ

Օգտատերը մեկ հավելվածի միջոցով տարբեր վիրտուալ ակտիվներ հաշվի նույն տվյալներով կարող է մուտք գործելու բազմակի ստորագրությամբ (MultiSig) դրամապանակով: MultiSig-ն օգտագործում է մեկ հավելված՝ տարբեր վիրտուալ ակտիվներ հաշվի նույն տվյալներով կառավարելու համար, ինչը հեշտացնում է տարբեր կրիպտոարժույթների հետ վարվելու գործընթացը:

Ճիշտ այնպես, ինչպես բանկերը տարբեր արժույթների համար հատկացնում են առանձին հաշվի համարներ (օրինակ՝ մեկ հաշվեհամար դոլարային հաշվի համար, մեկ այլը՝ եվրոյի հաշվի համար), տարբեր բլոկչեյնի տեխնոլոգիաների վրա հիմնված կրիպտոարժույթների (օրինակ՝ Բիթքոյն և Տրոն) համար պահանջվում են դրամապանակի առանձին հասցեներ:

MultiSig դրամապանակները պարտադիր չեն պահանջում մի քանի օգտատերերի առկայություն, այլ ենթադրում են մի քանի անձնական բանալիների օգտագործում՝ գործարքը թույլատրելու համար: Մեկ անձը կարող է ունենալ մի քանի անձնական բանալի, կամ ակտիվների կառավարման համար կարող են ներգրավված լինել մի քանի

անձինք, որոնցից յուրաքանչյուրը կունենա իր անձնական բանալին: Սա կարելի է պատկերացնել սմարթֆոնների տեսակների և դրանց օպերացիոն համակարգերի կամ հավելվածների տարբերությունների օրինակով: Որոշ հավելվածներ նախատեսված են բացառապես Apple-ի iOS օպերացիոն համակարգի համար և պահանջում են iPhone-ի առկայություն, մինչդեռ մյուսները հարմարեցված են Android-ի համար և չեն աշխատում Apple-ի սարքերում: Այդուհանդերձ, տարբեր ծրագրավորողների կողմից մշակված տարբեր հավելվածներ կարող են աշխատել Android համակարգում և հասանելի լինել Google Play Store-ում: Նույն կերպ, միևնույն բլոկչեյն տեխնոլոգիայով կառուցված կրիպտոարժույթները, օրինակ՝ Ethereum բլոկչեյնի վրա հիմնված ERC20 ժետոնները (թոքենները), կարող են կառավարվել նույն Ethereum-ի վրա հիմնված դրամապանակի հասցեի միջոցով:

Սա նման է, օրինակ, նրան, որ հավելվածների մեկ խանութը (app store) հնարավորություն է տալիս ներբեռնել բազմաթիվ հավելվածներ, որոնք մշակվել են նույն հարթակի վրա: Նույն կերպ, նույն բլոկճեյնի վրա հիմնված կրիպտոարժույթները, օրինակ, Ethereum-ը, կարող են միասին պահվել Ethereum-ի վրա հիմնված դրամապանակի հասցեում՝ օգտատիրոջ օգտագործումն ավելի պարզեցնելու համար:

Տվյալների հարցում վիրտուալ ակտիվների ծառայություն մատուցողներից

Եթե տուժողը չգիտի, թե վիրտուալ ակտիվների ծառայություններ մատուցող (ՎԱԾՄ) որ հարթակին է փոխանցվել գումարը, նա կարող է ունենալ անդորրագիր, որտեղ նշված են դրամապանակի հասցեները: Եթե նման տվյալներ չկան, ապա դրանք հաճախ կարելի է հայտնաբերել բլոկչեյնի վերլուծության ծրագրային ապահովման միջոցով: Նման ծառայություններ մատուցողներն աշխատում են այն երկրներում, որտեղ օրենքները հստակ սահմանում են, որ վիրտուալ ակտիվները պետք է համապատասխանեն փողերի լվացման դեմ պայքարի (AML) կանոնակարգերին, որոնց համաձայն՝ ՎԱԾՄ-ները պարտավոր են հաստատել իրենց օգտատերերի ինքնությունը և գրանցել բոլոր գործարքները: Օրինակ՝ Եվրոպական միությունում, ԵՄ-ի Փողերի լվացման դեմ պայքարի հինգերորդ դիրեկտիվի համաձայն՝ ՎԱՄԾ-ները պետք է գրանցված լինեն և կատարվեն փողերի լվացման դեմ պայքարի վերաբերյալ տարբեր պարտավորությունները:

Եթե տուժողը գիտի, թե որ ՎԱԾՄ-ին են ուղարկվել կամ որտեղից են եկել միջոցները և դեռևս ունի (կամ կարող է վերականգնել) մուտքի տվյալները, ապա առաջին քայլը տվյալ փոխանակման հարթակից (բորսայից) բոլոր փոխանցումների վերաբերյալ տվյալների դուրսբերումն է: Այս տվյալները կներառեն կատարված գործարքները, ուղարկված կրիպտոարժույթները և դրանց համապատասխան դրամապանակի հասցեները:

Եթե տուժողը վստահ չէ, թե ուր են փոխանցվել միջոցները կամ որտեղից են դրանք ուղարկվել, ապա ՎԱԾՄ-ի անունը երբեմն կարելի է գտնել տուժողի բանկային քաղվածքում կամ քարտի քաղվածքում:

Վիրտուալ ակտիվների կամ փոխանակման հարթակների օրինակներից են՝ PanCake Swap-ը (https://pancakeswap.finance/), Wasabi Wallet-ը (https://wasabiwallet.io), Doge Coin-ը (https://dogecoin.com/) և Shit Coin-ը (https://www.investopedia.com/terms/s/shitcoin.asp): Թեև դրանք կարող են անծանոթ լինել նրանց, ովքեր ակտիվորեն չեն զբաղվում կրիպտոարժույթներով, այս հարթակները լայնորեն կիրառվում են ոլորտում:

Նույնիսկ այն հարթակները, որոնք հայտարարում են, որ լիովին ապակենտրոնացված են (օրինակ՝ Uniswap), օգտատերերին հնարավորություն են տալիս դիտել գործարքների պատմությունը .csv ձևաչափով, որը կարող է օգտակար լինել հետաքննության ընթացքում:

Հաշվի առնելով, որ ամբողջ աշխարհում գործում են հարյուրավոր փոխանակման հարթակներ, հասարակության լայն շրջանակը կամ իրավապահ մարմինները կարող են հեշտությամբ ճանաչել դրանցից ընդամենը մի քանիսը:

Եթե անձը չի կարողանում մուտք գործել ՎԱԾՄ-ի իր հաշիվը, ապա նա դեռևս կարող է օգնության համար դիմել կենտրոնացված ՎԱԾՄ-ին կամ կրիպտոարժույթի դրամապանակին (պահառության ծառայություններ մատուցողին):

Լավագույն գործելակերպին հետևելով՝ փորձը ցույց է տալիս, ՎԱԾՄ-ները սովորաբար հեռախոսով որևէ տեղեկատվություն չեն տրամադրում, ուստի իրավապահ մարմինները պետք է հարցում ուղարկեն ՎԱԾՄ-ին կամ այլ ֆինանսական հաստատություններին, որոնք փոխանակել են տուժողի միջոցները: ՎԱԾՄ-ին հարցումը լրացնելու գործընթացը նկարագրված է 22-րդ

էջում:
Կենտրոնացված ՎԱՃՄ-ից կարող եք ստանալ հետևյալ տեղեկությունները:

- Անուն
- Ազգանուն
- Ծննդյան ամսաթիվ
- Անձը հաստատող փաստաթղթերի պատճենները[10]
- Կատարված գործարքների չափը
- Գործարքների ժամանակային նշումը[11]
- Գործարքի ՖԻԱՏ և կրիպտոարժույթը[12]
- Գործակալի միջնորդավճարի չափը
- Պատժամիջոցների ստուգման և քաղաքականության տեսանկյունից ազդեցիկ անձանց ստուգման հաստատման ժամանակը, ինչպես նաև օգտագործված՝ հսկողության տակ գտնվող անձանց կամ կազմակերպությունների ցուցակների (watchlist) տեսակները:
- **Կրիպտոարժույթի դրամապանակի հասցեն** կամ հասցեները, եթե մի քանի գործարք է իրականացվում կամ գործարքն իրականացվում է մեկից ավելի արժույթով
- Կատարված գործարքների հեշերը

Ավելի քիչ հավանական է, բայց դեռևս հնարավոր է ստանալ հետևյալ տեղեկությունները.

- Շաճախորդի համարը կամ ID-ն, որը գրանցված է գործակալի տվյալների բազայում
- Շաճախորդի հայտարարած բնակության հասցեն[13]
- Շաճախորդի գրանցված հասցեն[14]
- Սոցիալական ապահովության համարը՝ կախված այն երկրից, որտեղ գրանցված է հարթակը:
- Գործակալի (ՎԱՃՄ/ԿԱՃՄ) և հաճախորդի միջև փոխգործակցությունը (հաճախ PDF ձևաչափով, քանի որ հաճախորդների սպասարկումը հաճախ իրականացվում է արտաքին ծրագրային ապահովման մատակարարների միջոցով, ինչպիսիք են Intercom-ը կամ ZenDesk-ը)
- Օգտատերերի կողմից և նրանց ստացված՝ միջոցների առկայությունը հաստատող բոլոր փաստաթղթերը
- IP հասցեն (որը կարող է մոլորեցնող լինել, քանի որ օգտատերերը հակված են VPN-ներ օգտագործել)
- Մուտք գործելու համար օգտագործված սարքը, օրինակ՝ բջջային հեռախոս կամ սեղանի համակարգիչ:
- Ծառայություն մուտք գործելու համար օգտագործված բրաուզերը և դրա տարբերակը, օրինակ՝ Opera, Chrome, Safari, Internet Explorer կամ նմանատիպ:
- Շաճախորդի կենսագրական տվյալների ստուգում՝ օգտագործելով բաց աղբյուրներից ստացված հետախուզական տվյալները (OSINT)[15]
- ՎԱՃՄ աշխատակիցների մեկնաբանությունները կոնկրետ օգտատիրոջ կամ նրա գործարքների վերաբերյալ
- ՎԱՃՄ աշխատակիցների կողմից օգտատիրոջ կամ նրա գործարքների վերաբերյալ իրականացված բլոկչեյն վերլուծական քննություններ
- Այլ իրավապահ մարմինների կամ ֆինանսական հաստատությունների կողմից կոնկրետ օգտատիրոջ վերաբերյալ հարցումներ
- Օգտատիրոջ կողմից նախաձեռնված, բայց չավարտված գործարքներ
- Ֆիզիկական գրասենյակների կամ բանկոմատների դեպքում՝ անձանց կողմից տվյալ տարածքից օգտվելու տեսագրություններ
- Պահանջել օգտատերերի կողմից վերբեռնված բոլոր փաստաթղթերը (ներառյալ ֆինանսական միջոցների և հարստության աղբյուրների ապացույցները), ինչպես նաև հաճախորդների սպասարկման ծառայության ներկայացուցիչների հետ հաղորդակցման ամբողջ պատմությունը:

---

10 Անձը հաստատող փաստաթղթերը կարող են ներառել անձնագիրը, անձը հաստատող քարտ կամ էլեկտրոնային նույնականացում: Այնուամենայնիվ, այս գործընթացը խոցելի է նույն խնդիրների նկատմամբ, ինչ ավանդական կիբերհանցագործությունները, ինչպիսիք են կեղծ կամ կոլեկցիոն իրերի օգտագործումը, որոնք նմանակում են իրական անձը հաստատող փաստաթղթերին (օրինակ՝ «կոլեկցիոն փաստաթղթեր», որոնք հասանելի են այնպիսի կայքերում, ինչպիսին է dokumencik.pl-ը)

11 Անհրաժեշտ է որոշել, թե որ ժամային գոտուն է վերաբերում նշված ժամանակը: Օրինակ՝ Բիթքոյն բլոկչեյնի բոլոր գործարքները գրանցվում են UTC-ով (Լոնդոնի ժամանակով)՝ անկախ օգտատիրոջ գտնվելու վայրից: Գործարքի սխալ ժամանակային նշումը այլ ապացույցների հետ կապելու խնդիրը երբեմն դառնում է կրիտիկական:

12 Թե՛ վիրտուալ, և թե՛ ՖԻԱՏ արժույթները

13 Եթե տվյալ երկրում թույլատրվում է, հնարավոր է ստուգել, թե արդյոք նույն հասցեում գրանցված այլ հաճախորդներ նույնպես գործարքներ են իրականացրել:

14 Արդյո՞ք հարթակը նման տեղեկություններ է հանում հանրամատչելի տվյալների բազաներից:

15 Կարող է ներառել նաև բաց աղբյուրներից հավաքագրված տվյալներ, օրինակ՝ քրեական անցյալի վերաբերյալ տեղեկություններ կամ որոշ ընկերությունների վերջնական շահառուների (UBO) վերաբերյալ տվյալներ, որոնք ստուգվել են հարթակի համապատասխանության ապահովման (compliance) մասնագետների կողմից:

Ոստիկանության աշխատակիցները կարող են լրացուցիչ տեղեկություններ ստանալ տուժողից նրա բանկային հաշվի տվյալների վերաբերյալ, ինչն օգնում է ֆիլտրել ՎԱԾՄ-ներից ստացված տվյալները: Այս տեղեկատվությունը հասանելի կլինի միայն ֆիատից կրիպտոարժույթի փոխանակման գործարքների համար (ոչ թե կրիպտոարժույթից ֆիատի գործարքների համար):

- Տուժողի բանկային հաշվի համարը, որն օգտագործվել է ՎԱԾՄ-ի հաշվին և դրա հաշվից փոխանցում կատարելու համար:
- Շեռախոսահամար. Որոշ օգտատերեր օգտագործում են իրենց հեռախոսի վճարման համակարգը:
- Գործարքի համար օգտագործված վարկային, դեբետային կամ կանխավճարային քարտի տվյալները: Ծառայություն մատուցողի հաշիվը կարող է պարունակել լրացուցիչ տեղեկություններ, ինչպիսիք են երկրորդ մակարդակի հաստատումը բջջային բանկային հավելվածի միջոցով կամ 3D Secure կոչվող SMS ծառայության միջոցով, որը կարելի է ձեռք բերել:
- «Բաց բանկային» (open banking) համակարգ օգտագործող երկրներում հնարավոր է հավելյալ տեղեկություն ստանալ վճարային ծառայություններ մատուցողներից, որոնք կատարում են այդ գործարքները (եթե գործարքներն իրականացվել են «բաց բանկային» համակարգով):

ՎԱԾՄ-ի տվյալների ձևաչափի մասին տեղեկություններ

Արդյունավետության բարձրացման նպատակով խորհուրդ է տրվում գործարքի մասին անհրաժեշտ տվյալները ձեռք բերել «.csv» ձևաչափով, ինչը հեշտացնում է դրանց ներառումը իրավապահ մարմինների համակարգերում: Սովորաբար, իրավապահ մարմինների հարցումներին պատասխանները տրամադրվում են երկու ձևաչափով՝

- «.pdf» ձևաչափով, որում Վիրտուալ ակտիվների ծառայություններ մատուցողը տրամադրում է ուղղակի պատասխաններ իրավապահ մարմինների հարցումներին,
- «.csv» ֆայլով, որը պարունակում է գործարքի վերաբերյալ տվյալներ

Շաճախ ՎԱԾՄ-ներն ունեն իրենց հաճախորդների վերաբերյալ համախմբված տվյալների պանակ, որը ներառում է կարևոր փաստաթղթեր, օրինակ՝ միջոցների առկայության մասին ապացույց և այլ ներբեռնված ֆայլեր: Խոշոր ՎԱԾՄ-ները, որպես կանոն, ունեն իրավապահ մարմինների հարցումներին պատասխանելու սահմանված եղանակ: Փոքր հաստատությունների դեպքում իրավապահ մարմինները կարող են որոշ դեպքերում նշել պահանջվող տվյալները ստանալու համար իրենց նախընտրելի ձևաչափը :

> Խորհուրդ է տրվում ՎԱԾՄ-ներից չպահանջել «.xml» կամ «.xls» ձևաչափով ֆայլեր:Մասնավորապես, «.xlsx» ֆայլերի օգտագործումը չի խրախուսվում՝ կիբերանվտանգության նկատառումներից ելնելով: Կա վտանգ, որ ՎԱԾՄ-ների կողմից տրամադրված ".xlsx" ֆայլերը կարող են պարունակել վիրուսներ, հատկապես՝ ֆայլում ներդրված մակրոսների միջոցով, որոնք կարող են վտանգել իրավապահ մարմինների համակարգիչների պաշտպանվածությունը:

Սակայն, հաճախորդի անձնական տվյալները երբեմն պահվում են տարբեր ձևաչափերով, օրինակ՝ անձնագիրը կամ նույնականացման այլ փաստաթուղթ՝ «.pdf», «.jpeg» ձևաչափով, իսկ տեսանյութերը՝ «.avi» կամ «.mov» ձևաչափով:

Ստացած IP հասցեների հուսալիությունը

Ինտերնետային պրոտոկոլի (IP) հասցեն հաճախ հնարավոր է ստանալ ՎԱԾՄ-ից իրավապահ մարմինների հարցման միջոցով: IP հասցեն սարքի (օրինակ՝ սմարթֆոնի կամ դյուրակիր համակարգչի) բացառիկ նույնացուցիչն է ինտերնետային ցանցում: Պատկերացրեք IP հասցեն որպես թվերի բացառիկ համակցություն, ինչպես հեռախոսահամարը: Օրինակ՝ 193.46.242.201-ը ցույց է տալիս Շվեդիայի Ստոկհոլմ քաղաքը: Սակայն, ինչպես մեկ քաղաքային (ֆիքսված կապի) հեռախոսահամարը օգտագործվել ընտանիքի մի քանի անդամների կողմից, նույն կերպ NAT (Ցանցային հասցեների փոխարկում կամ Network Address Translation) տեխնոլոգիայի շնորհիվ մի քանի սարք կարող օգտագործել միևնույն IP հասցեն:

ՎԱԾՄ-ները հաճախ հայտարարում են, որ կարող են արտահանել IP հասցեները, որոնք գրանցվել են օգտագործողների մուտք գործելու պահին, սակայն այդ տվյալների հուսալիությունը պետք է կասկածի տակ դնել: IP հասցեները ցույց են տալիս միայն, թե որ սարքն է մուտք գործել ինտերնետ, այլ ոչ թե՝ կոնկրետ ով է այն օգտագործել: Դրանք կարող են թաքցվել խարդախների կողմից վիրտուալ մասնավոր ցանցերի (VPN) միջոցով, ուստի IP հասցեները պետք է օգտագործվեն միայն այն դեպքերում, երբ առկա են լրացուցիչ ապացույցներ, որոնք կարող են կապել օգտագործողի IP-ն հնարավոր հանցավոր գործունեության հետ:

Օգտատերերին տանը ինտերնետ հասանելիություն տրամադրող ընկերությունները (որոնք կոչվում են ինտերնետ ծառայություններ

մատուցողներ, «ISP-ներ») հաճախ կարող են պարզել, թե ով է օգտագործել կոնկրետ IP հասցեն կոնկրետ ժամանակահատվածում: Հետաքննության ընթացքում նման ընկերություններից կարող է պահանջվել կապել հասցեն կոնկրետ այն օգտատերերի հետ, ովքեր պայմանագիր են կնքել իրենց ծառայություններ մատուցելու համար: Ցավոք, այս տեղեկատվությունը միշտ չէ, որ հուսալի է, նույնիսկ եթե օգտատերը VPN չի օգտագործում: Քանի որ օգտատերերը կարող են Wi-Fi ցանցեր տրամադրել առանց գաղտնաբառերի, հնարավոր է, որ երբեմն այլ անձինք օգտագործեն նրանք IP հասցեն:

Միայն IP հասցեն իմանալը միշտ չէ, որ ճշգրիտ տեղեկատվություն է տալիս այն մասին, թե ով է կատարել կոնկրետ գործողություն առցանց: Հասարակական հաստատությունների, դպրոցների կամ աշխատավայրերի պես միջավայրերում բազմաթիվ մարդիկ կարող են օգտվել միևնույն Ինտերնետ կապից, ինչն էլ ավելի է բարդացնում առցանց գործողությունները կոնկրետ անձի վերագրելը:

Վերջապես, VPN-ները նախատեսված են օգտագործողի իրական IP հասցեն թաքցնելու համար՝ ստեղծելով այն տպավորությունը, որ կապը ծագում է այլ վայրից: Այնուամենայնիվ, նույնիսկ VPN-ի առկայության դեպքում հնարավոր է, որ որոշակի օգտատիրոջ վարքագիծը կապված լինի որոշակի կայքեր այցելելու հետ՝ կապելով նրանց կոնկրետ IP հասցեի հետ կոնկրետ ժամանակահատվածում:

Սա նշանակում է, որ թեև VPN-ները բարձրացնում են օգտատիրոջ անանունությունը, դրանք առցանց գործողությունները լիովին անհետևելի չեն դարձնում: Որոշ դեպքերում հնարավոր է, որ որոշակի կառույցներ կարողանան կապել առցանց ակտիվությունը առանձին օգտատերերի հետ:

IP հասցեների ձեռքբերում

Կողմ փաստարկներ.

- **Հետևելու հնարավորություն.** IP հասցեները կարող են ծառայել որպես մեկնարկային կետ՝ կասկածյալներին հետևելու կամ կասկածելի գործողությունների ծագումը պարզելու համար: Հնարավոր է, որ դրանք կապվեն այլ հետաքննությունների հետ:

- **Զսպում.** Իմանալով, որ IP հասցեները վերահսկվում են, հանցավոր մտադրություն ունեցող անձինք կարող են խուսափել սեփական ցանցերը անօրինական գործողությունների նպատակով օգտագործելուց:

- **Ապացույցների համակցում.** Այլ ապացույցների հետ միասին IP հասցեները կարող են օգնել ավելի հիմնավորված գործեր կազմել կասկածյալների նկատմամբ:

Դեմ փաստարկներ.

- **Անճշտություն.** Քանի որ մի քանի սարքեր կարող են օգտագործել նույն IP հասցեն, և հաշվի առնելով VPN-ների ու այլ քողարկող գործիքների առկայությունը, միայն IP հասցեների վրա հիմնվելը կարող է հանգեցնել սխալ նույնականացման:

- **Գատնիության խախտման խնդիրներ.** IP հասցեների զանգվածային հավաքագրումը անձանց գաղտնիության իրավունքները, հատկապես եթե դա կատարվում է առանց համապատասխան հիմնավորման:

- **Ռեսուրսատար գործընթաց.** IP հասցեների հետևումը և ստուգումը, հատկապես VPN-ների կամ այլ քողարկող գործիքների օգտագործմամբ, կարող է ժամանակատար լինել և շեղել ռեսուրսները այլ կարևոր հետաքննչական գործողություններից:

Ամփոփելով նշենք, որ թեև IP հասցեները կարող են տրամադրել լրացուցիչ տեղեկություններ սարքի գործունեության և տվյալ պահին կոնկրետ սարքի գտնվելու վայրի մասին, դրանք վերջնականապես չեն նույնականացնում առանձին օգտատերերին: IP հասցեների վրա հիմնված հետաքննությունները օգտակար են միայն այն դեպքում, երբ իրականացվում են զգուշավորությամբ և դիտարկվում են որպես ավելի մեծ գործիքակազմի մաս:

Պահանջվող այլ փաստաթղթեր

ԵԱՀԿ-ի ԵԱՀԿ-ի որոշ մասնակցող պետություններում վիրտուալ ակտիվներով (օրինակ՝ կրիպտոարժույթներով) զբաղվող ընկերությունները համարվում են «պարտավորված ֆինանսական հաստատություններ» կամ միջնորդներ: Դա նշանակում է, որ նրանք պարտավոր են պարբերաբար վերահսկել իրենց հաճախորդների գործունեությունը: Նրանք պարտավոր են վերլուծել կասկածելի վարքագիծ դրսևորող հաճախորդներին և գործարքները, հաճախ օգտագործելով բլոկչեյն վերլուծական գործիքներ՝ ռիսկի հնարավոր աղբյուրները բացահայտելու համար: Այդ ստուգումներն իրականացնելուց և փաստաթղթավորելուց հետո իրավապահ մարմինները կարող են պահանջել դրանք:

Օրինակ՝ Վրաստանի Հանրապետությունում

Ռոման Բիեդան անցկացնում է գործնական սեմինար քննիչների համար Ղազախստանում: Որպես բլոկչեյնի վերլուծության գործիքի պրոդուկտի նախկին պատասխանատու և փորձագետ վկա Եվրոպայի և Միացյալ Նահանգների դատարաններում, նա կենտրոնանում է ոչ միայն գիտելիքների, այլև լավագույն փորձի և ապացույցների հավաքագրման գործընթացում ծագող խնդիրների վերաբերյալ իր պատկերացումների փոխանցման վրա: ԵԱՀԿ-ի այս սեմինարների նպատակն է ապահովել, որ մասնակից պետություններից մեկում առաջացած մարտահրավերները չկրկնվեն մյուսներում:

փոխանակման ծառայություններ մատուցող և Վրաստանի Ազգային բանկում գրանցված ընկերությունները պարտավոր են օգտագործել մասնագիտացված գործիքներ՝ բլոկչեյն գործարքները վերլուծելու համար: **Սա ապահովում է վիրտուալ ակտիվների հոսքի վերահսկման թափանցիկության և անվտանգության մակարդակ:**

Եթե իրավապահ մարմինները չունեն բլոկչեյն վերլուծական նման գործիքներից օգտվելու հնարավորություն, ապա նրանք կարող են պահանջել ՎԱԾՄ-ից տրամադրել հետաքննության համար անհրաժեշտ տվյալները: Այս տեղեկատվությունը կարող է տրամադրվել մատչելի և խմբագրման հնարավորություն ունեցող ձևաչափով, օրինակ՝ PDF ձևաչափով կամ պատկերային ֆայլի տեսքով:

Սա նշանակում է, որ թեև այս գործիքները օգտակար են գործարքների ամբողջականության ապահովման և ապօրինի գործունեության բացահայտման համար, կան ընթացակարգային և իրավական նկատառումներ, որոնք պետք է պահպանվեն այս գործիքների միջոցով ստացված տեղեկատվությունը տարածելիս: Օրինակ՝ բլոկչեյնի վերլուծության և համապատասխանության լուծումներ տրամադրող տարբեր ընկերություններ կարող են ունենալ հատուկ կանոնակարգեր և համաձայնագրեր, որոնք սահմանափակում են գաղտնի կամ խմբագրման հնարավորություն ունեցող տեղեկատվության տրամադրումը իրավապահ մարմիններին առանց նախնական թույլտվության: Սա կարող է խնդիրներ առաջացնել ՎԱԾՄ-ների համար՝ հավաստի տեղեկատվություն տրամադրելու և պայմանագրային սահմանափակումների պատճառով ապացույցների տրամադրումը սահմանափակելու միջև հավասարակշռություն գտնելու հարցում:

Գործերը դատարան հանձնելը

Գործերը դատարան հանձնելը

Վիրտուալ ակտիվների գործերով դատախազներ

Դատախազությանը աշխատելու համար ամուր հիմքեր ապահովելու նպատակով իրավապահ մարմինների աշխատակիցները պետք է լավ տիրապետեն փողերի լվացման դեմ պայքարի (ՓԼՊ) գործողությունների հետ կապված ապացույցների հավաքագրմանը, հատկապես վիրտուալ ակտիվների և կրիպտոարժույթների արագ զարգացող ոլորտում:

Հետաքննության փուլ

- **Հավաքել թվային ապացույցներ.** Հասկանալ և հետևել բլոկչեյն տեխնոլոգիայի և բաշխված ռեեստրների վրա հիմնված գործարքները:

- **Վերլուծել տեղեկությունները.** Ճանաչել այն օրինաչափությունները, որոնք կարող են վկայել փողերի լվացման մասին, ինչպիսիք են կրիպտոարժույթի բորսաներում արագ և խոշոր գործարքները:

- **Հետևել թվային հետքերին.** Հետևել մի քանի վիրտուալ դրամապանակների և հարթակների միջոցով ակտիվների շարժին՝ օգտագործելով հատուկ ծրագրակազմ:

- **Գնահատել ԱԱՄԾ-ներից ստացված նույնականացման տեղեկատվության հավաստիությունը** (Տե՛ս «Անձը հաստատող փաստաթղթերի պատճենների» հետ կապված խնդիրները, էջ 30)

Դատարավորության կամ նախաքննության նախապատրաստում

ա. Գործի ընդհանուր նկարագիր.

- Ուշադրությունը պետք է կենտրոնացնել կրիպտոդրամապանակների, IP հասցեների, գործարքների ժամանակային նշումներ և թվային միջավայրում փոխանակված գումարների վրա:

- Առաջին հերթին անհրաժեշտ է հասկանալ վիրտուալ ակտիվների փոխակերպումը նյութական ակտիվների՝ ինչպես, օրինակ, գույքի կամ ապրանքների, և պարզել դրանց ծագումը:

բ.Հանցագործության տեսակի որոշում.

- Ճանաչել փողերի լվացման նպատակով կրիպտոարժույթի օգտագործման նշանները, ինչպիսիք են «քողարկման» կամ «խառնման» ծառայությունների միջոցով, որոնք նպատակ ունեն թաքցնել միջոցների աղբյուրը: Բլոկչեյնի վերլուծական ծառայություն մատուցող առաջատար հարթակներից մի քանիսն առաջարկում են «ապախառնման ծառայություններ», որոնք պնդում են, որ կարող են վերծանել խառնիչի միջոցով մշակված գործարքները: Եթե գործը ծայրահեղ կարևորություն ունի, ապա ապախառնման ծառայություններ առաջարկվում են ինչպես բլոկչեյնի վերլուծության ծառայություն մատուցող հարթակների կողմից, այնպես էլ իրավապահ մարմինների, օրինակ՝ Եվրոպոլի կողմից առաջարկվող ապախառնման դասընթացների տեսքով:

- Օգտագործել բլոկչեյն գործարքների ռեեստր՝ հանցակազմն ապացուցելու համար:

գ. Հանցավոր գործունեությունն ակտիվների հետ կապելը.

- Հետևել կրիպտոարժույթի դրամապանակներից նյութական կամ այլ վիրտուալ ակտիվների ձեռքբերման գործընթացին: Սա կարող է ներառել կրիպտոարժույթի շարժը բորսայից անձնական դրամապանակ, այնուհետև դեպի այլ կազմակերպություն կամ ծառայություն:

- Պարզել անանունություն ապահովող ծառայությունները կամ կիրառված տեխնիկան և փորձել հետևել ակտիվներին՝ չնայած առկա դժվարություններին:

- Ճանաչել այն օրինաչափությունները, որոնք կարող են վկայել հանցավոր մտադրության մասին, ինչպիսին է փողերի լվացումը, օրինակ՝ կրիպտոարժույթի մեծ գումարների բաժանումը մի քանի դրամապանակների միջև կամ գաղտնի (անանուն) մետաղադրամների օգտագործումը, ինչպիսիք են Monero-ն կամ Zcash-ը:

Ապացույցների ներկայացում.

- Շտապ բացատրել, թե ինչպես են աշխատում կրիպտոարժույթները և բլոկչեյնը, քանի որ շատ դատական պաշտոնյաներ կարող են ծանոթ չլինել այս տեխնոլոգիային:

- Պարզ և հակիրճ ներկայացնել փողերի լվացման թվային հետագիծը՝ սկսած ապօրինի միջոցների աղբյուրից մինչև դրանց վերջնական նպատակակետը: Խորհուրդ է տրվում օգտագործել դիդակտիկ նյութեր և հեշտ ընկալելի, ոչ տեխնիկական լեզու ապացույցների ներկայացման ժամանակ, քանի որ շատ դատախազներ և դատավորներ դեռևս կարող են լիովին ծանոթ չլինել կրիպտոարժույթների հետ կապված բարդություններին:

Լրացուցիչ ապացույցներ.

- Կրիպտոարժույթի փոխանակման փաստեր. Դրանք կարող են ներառել օգտատերերի գործունեության մանրամասները, դրամապանակի հասցեներ, IP գրանցամատյաններ, գործարքների գումարներ և ամսաթվեր:

- Բլոկչեյնի վերլուծության ծրագրային ապահովում. Նման ծրագրակազմը կարող է տեսանելի դարձնել թվային արժույթների հոսքը:

- Թվային դրամապանակների ուսումնասիրություն. Ուսումնասիրել ապարատային դրամապանակները, բջջային դրամապանակները և համակարգչային դրամապանակները: Դրանք կարող են պարունակել գրառումներ, գործարքների պատմություն կամ մետատվյալներ, որոնք կարող են օգտակար լինել:

- IP հասցեների հետևում. Հետևել գործարքների հետ կապված IP հասցեներին՝ կասկածյալների գտնվելու վայրը պարզելու համար: (տե՛ս էջ 31-ը IP հասցեների սահմանափակումների վերաբերյալ):

- Համագործակցություն միջազգային գործակալությունների հետ. Կրիպտոարժույթների ապակենտրոնացված բնույթով պայմանավորված՝ միջազգային համագործակցությունը կարող է կարևոր նշանակություն ունենալ անդրսահմանային գործարքներին հետևելու համար: Սակայն նման համագործակցությունը սովորաբար նախաձեռնվում է գլխավոր քննիչի կողմից քննչական գործընթացի ավելի ուշ փուլերում:[16]

Կրիպտոարժույթային գործարքների և գործունեությունների հետ կապված համապարփակ ապացույցներ հավաքելով, ոստիկանության աշխատակիցները կարող են հետաքննությամբ զբաղվող իրենց քննչական գործընկերներին, ինչպես նաև դատախազների համար ապահովել ամուր հիմքեր գործը կազմելու և հանցագործներին պատասխանատվության ենթարկելու համար:

16 Ֆինանսական հետախուզության ստորաբաժանումները, որոնք համագործակցում են «Egmont Group»-ի հետ, միասին մշակել են փոխանակման համակարգի մեխանիզմ, որը կարելի է գտնել այստեղ. https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf

Բարդ գործերի հետ կապված առաջարկություններ և կապեր

Բարդ գործերի հետ կապված առաջարկություններ և կապեր

Մասնագիտացված խմբեր և փորձագետներ

Բլոկչեյնի վերլուծության ծրագրային ապահովման առաջատար մատակարարները հաճախ ձևավորում են ինչպես կրիպտոարժույթների ոլորտի, այնպես էլ քննչական գործընթացների փորձագետներից բաղկացած մասնագիտական խմբեր, որոնք օգնում են իրավապահ մարմիններին յուրացնել բլոկչեյն վերլուծության նրբությունները՝ ապահովելով այս գործիքների հնարավորությունների առավելագույն օգտագործումը: Խորհուրդ է տրվում ստուգել ձեր գործակալության ներքին ցանցը (ինտրանետը)՝ պարզելու, թե որ ստորաբաժանումներն են արդեն օգտագործում բլոկչեյնի վրա հիմնված վերլուծական ծրագրեր, քանի որ այդ բաժինների գործընկերները, հավանաբար, ունեն առավել շատ պատկերացումներ այս հարցի վերաբերյալ:

Վերապատրաստում և հավաստագրում

Գիտակցելով բլոկչեյն տեխնոլոգիաների բարդությունները և գիտելիքների հուսալի կառավարման կարևորությունը՝ բլոկչեյնի վերլուծության ծրագրային ապահովման առաջատար ծառայություններ մատուցողները նաև առաջարկում են կառուցվածքային վերապատրաստման ծրագրեր: Այս ծրագրերը հաճախ եզրափակվում են տարբեր մակարդակների հավաստագրերի տրամադրմամբ, որոնք ոչ միայն հաստատում են իրավապահ մարմինների աշխատակիցների հմտությունները, այլև զգալիորեն բարձրացնում են նրանց արդյունավետությունը բլոկչեյնի հետ կապված գործերի հետաքննություններում: Թեև որոշ ծառայություններ, օրինակ՝ խորհրդատվական աջակցությունը, կարող են պահանջել լրացուցիչ ֆինանսավորում, երկարաժամկետ եկամուտները, հետաքննչական կարողությունների կատարելագործման տեսանկյունից, կարող են զգալի լինել:

Արտաքին աջակցություն խորացված հետաքննությունների անցկացման համար

Շաստիքային մասնագետների խմբից և վերապատրաստումից բացի գոյություն ունի արտաքին կոմերցիոն ծառայություններ մատուցողների ընդլայնվող շրջանակ, որոնք մասնագիտացած են բլոկչեյնի վրա հիմնված կրիպտոարժույթային գործարքների համապարփակ հետաքննություններ իրականացնելու գործում: Այս կազմակերպությունները գործում են որպես կապալառուներ՝ իրենց մասնագիտացված հմտությունները առաջարկելով իրավապահ մարմիններին:
Նրանց մասնագիտական գիտելիքները կարող են անփոխարինելի լինել, հատկապես բարդ դեպքերում, որտեղ պահանջվում են խորը վերլուծություն և բազմակողմանի հետաքննության մեթոդներ: Իրավապահ մարմինները, օրինակ՝ Ինտերպոլը կամ Եվրոպոլը, տրամադրում են հատուկ աջակցություն և վերապատրաստման դասընթացներ հետաքննիչների համար (տե՛ս «Համագործակցություն թվային ակտիվների փորձագետների հետ» բաժինը, էջ 51): Եթե ձեր թիմը ցանկանում է միանալ առկա վերապատրաստման միջոցառումներին, ապա լրացուցիչ տեղեկությունների համար դիմեք VirtualAssets@osce.org էլ. փոստի հասցեով:

Գործելիս ցուցաբերեք զգուշավորություն

Այդուհանդերձ, թեև արտաքին ծառայություն մատուցողների առավելությունները բազմաթիվ են, գործակալությունները պետք է տեղյակ լինեն նաև հնարավոր խնդիրների մասին: Գաղտնի գործերի հետաքննություններում արտաքին կազմակերպությունների, այդ թվում՝ խորհրդատվական գործակալությունների կամ բլոկչեյնի վրա հիմնված վերլուծական ծառայություններ մատուցողների, ներգրավումը կարող է բարդություններ առաջացնել դատավարության ընթացքում :
Կարևոր է նաև տվյալների անվտանգության հարցը: Գաղտնի տեղեկատվությունը երրորդ անձանց փոխանցելիս անհրաժեշտ է ցուցաբերել առավելագույն զգուշավորություն՝ տվյալների ամբողջականությունը ապահովելու և գաղտնի տեղեկատվության ոչ միտումնավոր արտահոսքը կանխելու համար:

Մաչեյ Շուլցը վարում է հրահանգիչների վերապատրաստման սեմինարը Գդանսկում, որտեղ ԵԱՀԿ մասնակից պետությունների քաղաքականություն մշակողները կիսվում են բարդ գործերի լուծման և ազգային շահառուներին օժանդակելու լավագույն մեթոդներով: Շեշտը դրվում է ոչ միայն բովանդակության որակի, այլև արդյունավետ ներկայացման մեթոդների վրա:

Աջակցություն տուժածներին

Աջակցություն տուժածներին

Խնդիրներ, որոնց մասին տուժողներին պետք է զգուշացնել

Կրիպտոարժույթների հետ կապված մեկ խարդախության զոհերը կարող են հեշտությամբ մեկ այլ խարդախության զոհ դառնալ: Խարդախների կազմակերպված հանցավոր խմբերը չեն սահմանափակվում մեկ հարվածով, այլ նպատակաուղղված կերպով բազմիցս թիրախավորում են իրենց զոհերին: Ստորև ներկայացված են ամենատարածված երկրորդային խարդախությունների մանրամասները:

- «Փրկչի» խաբեությունը. Ֆիզիկական անձի՝ խարդախ ցանցում առաջին անգամ ներքաշվելուց հետո նույն խմբավորման մեկ այլ թևը սկսում է առաջարկել օգնություն՝ ներկայանալով որպես մասնագետ, ով կարող է օգնել վերադարձնել կորցրած ներդրումները: Թվացյալ այս առատաձեռն առաջարկի դիմաց զոհը պետք է վճարի ծառայություն մատուցող ընկերությանը՝ կորցրած միջոցները վերականգնելու համար: Միջոցների փոխանցումից հետո «Փրկիչը» հաճախ անհետանում է՝ կորցրած միջոցների հետ միասին:
- «Ազդարարի» հնարքը. Մեկ այլ կերպարանքով խարդախները կարող են ներկայանալ որպես խարդախ ձեռնարկության դժգոհ նախկին աշխատակիցներ՝ պնդելով, որ ունեն ներքին տեղեկություններ, որոնք, իբր, կարող են օգնել տուժածներին վերադարձնել իրենց ակտիվները: Գործընթացը նույնն է, ինչ «Փրկիչի» դեպքում. Պահանջվում է նախապես վճարել գումար, որից հետո կոնտակտային անձը սովորաբար անհետանում է:
- Դատարան դիմելու պատրանքը. Նման դեպքերում տուժողի հետ կապվում է արհեստավարժ փաստաբան ներկայացող անձը, ով խոստանում է վերադարձնել գումարը, հատկապես երբ հարցը վերաբերում է վիրտուալ ակտիվների ծառայություններ մատուցողներին: Դատավորի կողմից ժամավճարը որոշելուց հետո, այս փաստաբանները պնդում են, որ կազմել են ծավալուն փաստաթղթեր, որոնք երբեմն 40 էջից ավելի են, որոնցում հաճախ մանրամասն նկարագրվում են փողերի լվացման դեմ պայքարի (AML) և ահաբեկչության ֆինանսավորման դեմ պայքարի (CFT) օրենսդրության հիմնարար սկզբունքները, սակայն որոնց իրավական արժեքը սահմանափակ է: Ցավոք, օգտագործված փաստաթղթերը հիմնականում ընդհանուր բնույթ ունեն, և դրանց 99%-ը մնում է անփոփոխ, ինչի արդյունքում ՎԱՃՄ-ները ողողվում են նույնատիպ փաստաթղթերով՝ միայն չնչին փոփոխություններով: Տուժածներից գանձվում են չափազանց մեծ գումարներ այս, մեծամասամբ, ավելորդ ջանքերի համար:

Անհրաժեշտ է գիտակցել, որ ՎԱՃՄ-ների մեծ մասի դեպքում գործարքները, մեկ անգամ իրականացվելուց հետո, դառնում են անշրջելի : «Վարկային քարտի գումարի վերադարձի» պահանջները հաջողության նվազագույն հնարավորություն ունեն: Հետևաբար, նման դատական գործողությունները սովորաբար ոչ միայն անարդյունավետ են, այլև պարզապես դատարկում են տուժողի դրամապանակը:

Օլգա դը Տրուշիսը, AXIS-ի վիրտուալ ակտիվների փորձագետ և Եվրոպոլի Ֆինանսական հետախուզության Պետություն-մասնավոր գործընկերության (EFIPPP) կրիպտոակտիվների ոլորտի ղեկավարներից մեկը, անցկացրեց սեմինար ավանդական ֆինանսական ծառայություններ մատուցողների համար՝ներկայացնելով վիրտուալ ակտիվների և դրանց ծառայություններ մատուցողների (ՎԱՄՏ) հետ կապված ֆինանսական հանցագործությունների կառավարման լավագույն փորձը: Լատվիայի Ազգային բանկի տարածքում կազմակերպված սեմինարին մասնակցում էին նաև ԵԱՀԿ-ի չորս այլ մասնակից պետությունների ներկայացուցիչներ:

Կրիպտոարժույթների օգտագործմամբ կատարված հանցագործությունների առանձին տեսակներ

Կրիպտոարժույթների օգտագործմամբ կատարված հանցագործությունների առանձին տեսակներ

Ստորև ներկայացված են կրիպտոարժույթներով կատարվող ամենատարածված հանցագործությունների տեսակների մանրամասները: Առնվազն պետք է տեղյակ լինել այս տեսակի հանցագործություններից, բայց նաև իմանալ, որ սա ամբողջական ցանկը չէ:

Կրիպտոարժույթների ներդրումային խարդախության սխեմաներ

Ի՞նչ է դա

Կրիպտոարժույթների ներդրումային խարդախությունները խաբեության սխեմաների ամենատարածված տեսակներից են: Սկզբում այս խարդախության թիրախում էին հայտնվում բարձր եկամուտ ունեցող երկրների հարուստ տարեց քաղաքացիները: Սակայն, մարտավարությունը փոխվել է, և այժմ ավելի շատ թիրախավորվում են ֆոնդային բորսայի ներդրողները և կենսաթոշակային տարիքի շեմին գտնվող անձինք: Շատ կարևոր է հետագայում պահպանել զգոնությունը և հետևել խարդախության զարգացումներին:

Այս խարդախության մեխանիզմը հետևյալն է. խարդախները կապ են հաստատում ապահովված անձանց հետ և նրանց ներկայացնում շահավետ ներդրումային հնարավորություններ: Սովորաբար խարդախը, ներկայանալով որպես կրիպտոարժույթների փորձառու ներդրող, կապ է հաստատում ոչինչ չկասկածող անձանց հետ՝ ցուցադրելով ակնհայտ ֆինանսական ապահովվածություն:

Այս խաբեության տարբեր տեսակները

Սովորաբար կիրառվում են հետևյալ տարբերակները.

- **Կանխավճարներ.** Տխարդախները գայթակղում են մարդկանց ներդրումներից բարձր եկամուտների խոստումով: Սակայն գործընթացը սկսելու համար նրանք պահանջում են 250 եվրոյից մինչև 1000 եվրո (կամ համարժեք ազգային արժույթով) կանխավճար, սովորաբար այս միջակայքի ստորին սահմանում: Սկզբնական վճարումը ստանալուց հետո խարդախը պարզապես անհետանում է վճարումից հետո, թողնելով զոհին ֆինանսապես թուլացած՝ առանց որևէ հեռանկարային ներդրման:

- Ավելի բարդ մոտեցման դեպքում գործընթացը ներառում է ուղիղ տեսազանգ, որի ընթացքում խարդախն ցուցադրում է «ֆինանսական հաշիվ», որն իբր պատկանում է ապագա զոհին և որի մնացորդը սկսում է արագ ավելանալ: Թեև այս հաշիվները նախատեսված են օրինական երևալու համար, դրանք իրականում դիզայնի պատճեններ են, որոնք սովորական ֆինանսական հաստատությունների հետ որևէ կապ չունեն:

- Երբեմն խարդախության զոհ դարձած անձինք ստանում են «առաջին վճարումը», օրինակ՝ 50 եվրոյից մինչև 100 եվրո, որը, խաբեբաների պնդմամբ, իրենց ներդրումների տոկոսն է, որպեսզի գայթակղեն զոհին ավելի մեծ գումար ներդնելու համար:

Ներդրումների, ֆինանսների կամ առցանց գործիքների օգտագործման ոլորտում քիչ փորձ ունեցող օգտատերերի համար խարդախները հաճախ տեղադրում են հեռավար մուտքի ծրագրային ապահովում:
Այս ծրագրերը հիմնականում նախատեսված են հեռավար մուտքի, կառավարման և աջակցության համար: Դրանք թույլ են տալիս օգտատերերին ցանկացած վայրից հեռակա մուտք գործել և կառավարել իրենց սեղանի կամ դյուրակիր համակարգիչները և սերվերները:
Տուժողը հաճախ տեղադրում է նման ծրագրեր խարդախի օգնությամբ: Կապը հաստատելուց հետո զոհերը հաճախ մոռանում են հեռացնել ծրագրերը: Ծրագրաշարի մնացած հետքերը կարող են օգտակար լինել իրավապահ մարմինների հետաքննության համար, եթե պատշաճ կերպով պաշտպանված լինեն:

Ծրագրային ապահովման տեսակից կախված՝ այն կարող է ունենալ տարբեր ֆունկցիաներ, ներառյալ.

- **Հեռակա կառավարում.** Օգտատերերը կարող են կառավարել համակարգիչը այլ վայրից այնպես, կարծես գտնվում են դրա առջև: Սա օգտակար է խնդիրների լուծման, հեռակա աջակցության տրամադրելու կամ ֆայլերի հասանելիության համար:

- **Ֆայլերի փոխանցում.** Ծրագրաշարը հնարավորություն է տալիս օգտատերերին ֆայլեր փոխանցել համակարգիչների միջև: Երբեմն ֆայլերի փոխանցման արդյունքում տեղադրվում է «keylogger» լրտեսող ծրագիրը, որը համակարգչում տեղադրվելուց հետո տարիներ շարունակ հետևում է օգտատիրոջ կողմից մուտքագրվող բոլոր տվյալներին և կարող է դրանք փոխանցել խարդախներին:

- **Հեռավար հասանելիություն.** Սա խարդախներին հնարավորություն է տալիս հեռակա կարգով մուտք գործել զոհի համակարգիչ կամ սերվեր, փոփոխել ֆայլերը, տեղադրել ծրագրեր կամ կապեր ստեղծել:

- **Բջջային հասանելիություն.** Սա հնարավորություն է տալիս սմարթֆոններից և պլանշետներից հեռակա կարգով կառավարել սարքերը:

- **Անձնական տվյալների գողություն.** Օրինականության պատրանք ստեղծելու համար խարդախները կարող են պահանջել զոհի անձնական նույնականացման տվյալները՝ իբր գումար փոխանցելու կամ ավանդ ներդնելու նպատակով: Սակայն իրականում նրանք ստանում են զոհի անձնական և ֆինանսական տվյալներին չարտոնված հասանելիություն: Տուժողները մոռանում են արգելափակել իրենց անձը հաստատող փաստաթղթերը ֆինանսական հաստատությունում կամ նույնիսկ ուղարկում են դրանց պատճենները խարդախներին:

Ինչպե՞ս դիմակայել դրան

- **Մի՛ կատարեք հավելյալ փոխանցումներ.** Խարդախները հաճախ խոսում են փոքր վճարների մասին, օրինակ՝ փոխանցման կամ վճարման ծախսեր, որոնք թվում են աննշան խարդախության ընդհանուր գումարի համեմատ: Օրինակ՝ 600 եվրո վճար՝ 60 000 եվրոյի չափով խարդախության համար:

- **Տուժողը չպետք է խզի կապը.** Սովորաբար, երբ տուժածը դիմում է իրավապահ մարմիններին, նրանց կապը խարդախի հետ արդեն կորցրած է լինում: Սակայն, եթե այդ կապը դեռ պահպանվում է, ապա լավ կլինի, որ տուժողը պահպանի այդ կապը քննությանն օգնելու համար, որպեսզի հնարավոր լինի փնտրել օգտագործվող կիբերհանցագործության գործիքները:

- **Տուժածները չպետք է** հեռացնեն իրենց սարքերում տեղադրված որևէ ծրագրակազմ, քանի որ դրանք կարող են թողնել կիբերանվտանգության հետքեր, որոնք օգտակար են հետաքննությունների համար: Այնուամենայնիվ, տուժողը պետք է տեղյակ լինի իր սարքում ծրագրային ապահովման առկայության հնարավորության մասին, որը հետևում է իրենց մուտքագրածին, կամ որը միացված է պահում տեսախցիկը և այլն: Նման դեպքում տուժողը պետք է սահմանափակի իր սարքի օգտագործումը:

- **Ստուգեք, թե ինչ անձնական տվյալներ են հասանելի դարձել.** Հնարավորության դեպքում փոփոխեք բանկային հաշիվների մուտքանուններն ու գաղտնաբառերը, ինչպես նաև պատվիրեք նոր գաղտնաբառեր էլեկտրոնային նույնականացման գործիքների համար, եթե այդպիսի գործիքներ օգտագործվում են:

- **Վերանայեք երկրորդային խարդախությունների վերաբերյալ բաժինը,** որը ներկայացված է վերևում՝ էջ 38-ում:

- **Ձեռնարկվելիք համապատասխան քայլերը կախված են տուժողի կոնկրետ իրավիճակից.** Լրացուցիչ մանրամասների համար տե՛ս «Գործարքների յուրաքանչյուր տեսակի համար կիրառվող լավագույն գործելակերպը» բաժինը, էջ 24:

Այս խարդախության մեկ այլ տարբերակ է կեղծ հայտնի անձանց հավանությունների օգտագործումը: Խարդախները յուրացնում են իրական լուսանկարներ և դրանք կեղծ հաշիվների կամ գովազդային նյութերի հետ տեղադրում՝ տպավորություն ստեղծելով, թե իբր հայտնի անձինք հավանություն են տալիս իրենց սխեմաներին:

Նենգաշորթում և սեռական շանտաժ

Նենգաշորթման (շանտաժ) դեպքերում դրա զոհերը հաճախ ստանում են հնարամտորեն մանրակրկիտ կազմված էլեկտրոնային նամակ, որում նրանց տեղեկացվում է, թե իբր հաքերը մուտք է գործել զոհի համակարգիչ և կարողանում է միանալ դյուրակիր համակարգչին կամ սմարթֆոնին: Սեռական շորթման դեպքում խարդախը պնդում է, թե հաքերը նկարահանել է զոհին ձեռնաշարժության ժամանակ:

Ի՞նչ է դա

Անձը ստանում է խարդախից կողմից ուղարկված էլեկտրոնային նամակ է, որում նշվում է, թե իբր խարդախը կոտրել է զոհի համակարգիչը կամ սմարթֆոնը և ստացել է տեսախցիկին հասանելիություն: Սեռական շորթման դեպքերում խարդախը պնդում է, որ տեսանկարահանել է զոհին ձեռնաշարժության պահին և սպառնում է հրապարակել տեսագրությունը, եթե զոհը չփոխանցի նրան պահանջված գումարը կրիպտոարժույթի տեսքով: Զոհին ստիպում են սեղմ ժամկետներում գումար փոխանցել նշված կրիպտոարժույթի դրամապանակին՝ իբր կանխելու ենթադրյալ տեսագրության տարածումը բիզնես կամ անձնական կոնտակտների շրջանակում, որոնց տվյալները, ըստ հաքերի պնդումների, հայտնաբերվել են զոհի սարքում: Որպես իր պնդումների «ապացույց», հաքերը սովորաբար տրամադրում է տարբեր կայքերի հետ կապված օգտանունների և գաղտնաբառերի ցանկ, որոնք կապված են, ակնարկելով, որ զոհը նույն տվյալներն օգտագործել է չափահասների համար նախատեսված բովանդակություն ունեցող մի քանի կայքերում բովանդակության կայքերում:

Սույն հրապարակման հեղինակին ուղարկված Էլեկտրոնային նամակը.

Թեմա՝ Ես ձայնագրել եմ քեզ (այստեղ խարդախը փոխանցում է արտահոսքից հայտնաբերված գաղտնաբառը)
Ամսաթիվ՝ 2023-06-22 3:32
Ուղարկող՝ «Փրկիր կյանքդ» <xxxxxxxxxf@xxxx.ga> Ստացող՝ XXXXXX@xxxx.com

---

Ողջույն, ես հաքեր եմ և ծրագրավորող, գիտեմ, որ քո գաղտնաբառերից մեկն է՝ (օգտատիրոջ գաղտնաբառը, որը ստացվել է գաղտնաբառերի արտահոսքից)
Քո համակարգիչը վարակվել է իմ անձնական վնասակար ծրագրի միջոցով, քանի որ քո համակարգչի բրաուզերը թարմացված կամ շտկված չէր: Նման դեպքերում բավական է պարզապես այցելես որևէ կայք, որտեղ տեղադրված է իմ «iframe»-ը, և դու ավտոմատ կերպով կվարակվես: Եթե ցանկանում ես ավելին իմանալ՝ որոնիր Google-ում «Drive-by exploit»:

Իմ վնասաբեր ծրագրի միջոցով ես ստացել եմ լիարժեք հասանելիություն քո բոլոր հաշիվներին (տե՛ս վերևում նշված գաղտնաբառը), լիակատար վերահսկողություն քո համակարգչի նկատմամբ և հնարավորություն եմ ունեցել լրտեսելու քեզ հենց քո վեբ տեսախցիկի միջոցով:

Ես հավաքել եմ քո բոլոր անձնական տվյալները, ձայնագրել եմ քո մի քանի տեսանյութ (քո վեբ տեսախցիկով) և ՁԱՅՆԱԳՐԵԼ ԵՄ ՔԵՁ ԻՆՔՆԱԲԱՎԱՐԱՐՄԱՆ ԸՆԹԱՑՔՈՒՄ:

Կարող եմ հրապարակել քո անձնական տվյալները ամենուր, ներառյալ «darknet»-ում, որտեղ շատ հիվանդ մարդիկ կան, ինչպես նաև քո տեսանյութերը կարող եմ ուղարկել քո կոնտակտների ցուցակում ընդգրկված անձանց, տեղադրել դրանք սոցիալական ցանցերում և այլուր:

Միայն դու կարող ես չթողնել ինձ դա անել, և միայն ես կարող եմ օգնել քեզ: Ոչ մի հետք չի մնացել, քանի որ գործս ավարտելուց հետո հեռացրել եմ իմ վնասաբեր ծրագիրը, և այս Էլեկտրոնային նամակն ուղարկվել է ինչ-որ կոտրված սերվերից...

Ինձ կանգնեցնելու միակ ճանապարհը՝ վճարել ճիշտ 400 դոլար բիթքոյնով (BTC):

Սա շատ լավ առաջարկ է՝ համեմատած այն ԱՀԱՎՈՐ վատ բաների հետ, որոնք տեղի կունենան, եթե չվճարես:
Դու կարող ես հեշտությամբ գնել բիթքոյն այստեղ՝ www.xxxxxxx.com, www.xxxxx.com, www.xxxxxx.com կամ գտիր բիթքոյնի բանկոմատ ձեր մոտակայքում կամ փոխանակման հարթակներ Google-ում:

Դու կարող ես բիթքոյնն ուղարկել անմիջապես իմ դրամապանակին կամ նախ ստեղծել քո սեփական դրամապանակն այստեղ www.login.xxxxx.com/en/#/signup/, այնուհետև ստանալ գումարը և փոխանցել իմ դրամապանակին:
Իմ բիթքոյնի դրամապանակն է՝ 17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG
Պատճենիր և տեղադրիր այն: Այն պարունակում է փՈՔՐաՏաՌԵՐ Եվ մԵԾԱտԱռԵՐ: Դու ունես 3 օր ժամանակ:

Քանի որ ես հասանելիություն ունեմ այս էլ. փոստի հաշվին, ես կիմանամ, արդո՞ք դու կարդացել ես այս նամակը, թե ոչ:

Եթե այս նամակը ստանում ես մի քանի անգամ, ապա դա արվում է՝ համոզվելու, որ դու կարդացել ես այն: Իմ փոստի սցենարը այդպես է կարգավորված: Վճարումից հետո, կարող ես անտեսել այն:

Վճարումը ստանալուց հետո ես կջնջեմ քո բոլոր տվյալները, և դու կկարողանաս առաջվա պես հանգիստ ապրել: Հաջորդ անգամ, նախքան համացանցում տեղեկատվություն որոնելը և դիտելը թարմացրու քո բրաուզերը:

Նինա-Լուիզ Չիդլերը Ռիգայում վարում է աշխատաժողով հինգ մասնակից պետություններից քաղաքականություն մշակողների համար: Նա կիսվում է վիրտուալ ակտիվների կարգավորման վերաբերյալ փորձագիտական քննարկումների արդյունքներով: Ժողովը նվիրված էր վիրտուալ ակտիվներին վերաբերող համաեվրոպական օրենսդրությանը՝ նպատակ ունենալով բացահայտել կարգավորման բացթողումները և ընդգծել վերջին զարգացումները, որոնք կարևոր են մասնակից պետությունների համար:

Ինչպե՞ս դիմակայել դրան

Նենգաշորթման նամակներ ստացող տուժածներին աջակցելու լավագույն եղանակը

- **Պահպանել հանգստություն.** Եթե օգտատերը ստացել է սեռական շորթման բնույթի էլեկտրոնային նամակ, ապա անհրաժեշտ է հանգիստ մնալ: Վերևում ներկայացված նամակի օրինակը ցույց է տալիս, որ հանցագործներն օգտագործում են ուժեղ ածականներ՝ վախ ներշնչելու, հրատապ քայլեր ձեռնարկելու դրդելու և խուճապ առաջացնելու համար:

- **Տուժողը չպետք է որևէ կերպ շփվի** ուղարկողի հետ. Սեռական շորթում ենթադրող էլեկտրոնային նամակները սովորաբար չեն որևէ ապացույց կամ կցված ֆայլեր չեն պարունակում: Եթե էլեկտրոնային նամակի հետ ուղարկվում են հղումներ, ապա օգտատերը չպետք է բացի դրանք:

- Օգտատիրոջը պետք է արգելվի ՖԻԱՏ փողերի փոխանակումը կրիպտոարժույթի և դրա փոխանցումը կասկածելի կրիպտոարժույթի դրամապանակին:

- **Ստուգել կրիպտոդրամապանակը.** Կրիպտոարժույթի դրամապանակի իսկությունը ստուգելու եղանակներից մեկը գործիքների, այդ թվում՝ «դրամապանակի դիտարկիչի» միջոցով ստուգումն է: Օրինակ՝ նշված կրիպտոարժույթի դրամապանակը կարելի է ուսումնասիրել հետևյալ հղումով՝

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

- Նախնական ուսումնասիրության ընթացքում, որն անվճար է և տևում է 10 վայրկյանից քիչ, պարզ է դառնում, որ այս դրամապանակի միջոցով կատարվել են բազմաթիվ գործարքներ: Սա հաճախ հակասում է հաքերների այն պնդումներին, թե իբր այս կրիպտոդրամապանակի հասցեն եզակի է և օգտագործվել է միայն մեկ անգամ: Բազմաթիվ գործարքներ կարող են նշանակել, որ այս դրամապանակին գումարներ են փոխանցել տարբեր մարդիկ:

- **Օգտագործել գողացված հաշիվների տվյալների շուկան՝ ի նպաստ տուժողների.** Տուժողները կարող են օգտվել անվճար ծառայություններից, ինչպիսիք են՝ https://haveibeenpwned.com, որոնք թույլ են տալիս միլիարդավոր արտահոսած հաշվի տվյալների մանրակրկիտ ուսումնասիրության միջոցով ստուգել, թե արդյոք իրենց տվյալները չեն բացահայտվել: Մուտքագրելով իրենց էլ.փոստը կամ օգտանունը՝ օգտատերերը կարող են տեսնել, թե արդյոք իրենց տեղեկությունները հայտնվում են որևէ հայտնի արտահոսքում: Եթե հարձակվողը ցուցադրում է օգտագործվող գաղտնաբառը, անմիջապես փոխեք այն բոլոր հարթակներում, որտեղ այն կիրառվում է:

Նենգաշորթության մեջ կասկածվող անձանց գործերը քննելիս կարևոր է հետևել իրենց կրիպտոարժույթի դրամապանակներին վճարումներին։

Այս կերպ հնարավոր է տեսնել, թե արդյոք դրամապանակներից որևէ մեկը կապված է պաշտոնական ֆինանսական հարթակների հետ, ինչը կարող է օգնել իրավապահ մարմիններին բացահայտել, թե ով է փող ուղարկել կասկածյալին։ Թեև շորթման համար նախատեսված դրամապանակին գումար փոխանցելը հանցագործություն չէ, սակայն փոխանցում կատարած անձինք կարող են ունենալ համապատասխան տեղեկություններ կամ ենթարկված լինել նույն անձից նմանատիպ սպառնալիքների, ինչը կարող է օգնել հետաքննությանը։

ԵԱՀԿ քարտուղարությունում՝ Վիեննայում, ուկրաինացի քաղաքական գործիչների համար անցկացվում է վերապատրաստման դասընթաց վիրտուալ ակտիվների կարգավորման բացերը թեմայով՝ շեշտը դնելով ապակենտրոնացված փոխանակման հարթակների վրա։

«Rug Pull» խարդախության սխեմաներ

«Exit» («ելք»), «pump-and-dump» («փողերը քաշել և գցել») կամ «rug pull» («գցել») խարդախությունները (որոնք ծագում են «մեկին խաբել, անհարմար կացության մեջ դնել» փոխաբերությունից) սխեմաներ են, որոնցում խարդախները մեծ իրարանցում են առաջացնում նոր թվային ակտիվի շուրջ: Դա կարող է լինել ցանկացած տեսակի թվային ակտիվ, ոչ միայն նոր կրիպտոարժույթ: Նմանատիպ խարդախություններ են իրականացվել նաև նախագծերի և ոչ փոխարկելի ժետոնների (NFT) դեպքում: Խարդախները արագ լքում են նախագիծը՝ գողանալով ներդրողների գումարները և թողնելով թվային ակտիվն արժեզուրկ:

Ի՞նչ է դա

Այս տեսակի խարդախության նպատակն է ներգրավել հնարավորինս շատ գնորդներ կամ ներդրողներ նոր թվային ակտիվի համար և արհեստականորեն հնարավորինս ուռճացնել դրա ընկալվող արժեքը: Բավականաչափ գումար հավաքելուց հետո խարդախներն անհետանում են (սա «exit» խարդախության «դուրս գալը» իմաստն է) և գումարը վերցնում իրենց: Այս «ելքը» կարող է տեղի ունենալ արագ՝ բոլորի հանկարծակի անհետացմամբ, կամ որոշ ժամանակի ընթացքում, երբ խարդախները դանդաղ դուրս են բերում գումարները և միտումնավոր դադարեցնում ակտիվի հետագա զարգացումը: Վերջինիս դեպքում երբեմն դժվար է տարբերակել իսկական «rug pull» խարդախությունը պարզապես վատ կառավարվող, անհաջող նախագծից: Բոլոր դեպքերում խարդախների դուրս գալը նշանակում է, որ ակտիվը կեղծ է և կորցնում է արժեքը: Խաբեության զոհ դարձած անձինք մնում են կա՛մ մի քանի մետաղադրամով կամ ժետոնով, որոնք արժեն իրենց վճարած գումարի մի փոքր մասը (եթե կարողանան գնորդ գտնել), կա՛մ թվային ակտիվը պարունակում է կոդ, որը ցույց է տալիս, որ ակտիվը ընդհանրապես հնարավոր չէ վաճառել:

Ֆիշինգային խարդախություններ

Ֆիշինգային խարդախությունը համացանցի տարբեր ոլորտներում խաբեության տարածված սխեմա է: Այն նաև տարածված և արդյունավետ խարդախության ձև է թվային ակտիվների ոլորտում:

Ի՞նչ է դա

Խարդախները ներկայանում են որպես պաշտոնական ձեռնարկության ներկայացուցիչներ օրինական տեսք ունեցող կայքերի կամ ընկերության փաստաթղթերի միջոցով և ուղարկում են հազարավոր էլեկտրոնային նամակներ և հաղորդագրություններ՝ հղումներով, որոնք տանում են իրենց կայքի կեղծ տարբերակին: Այդ կայքերը ստեղծվում են մուտք գործել թույլատրելու և պահպանելու յուրաքանչյուր այցելուի անձնական տեղեկությունները, ինչպես նաև բոլոր կրիպտոհասցեները և գաղտնաբառերը (կոչվում են «կրիպտոդրամապանակի բանալիներ»), որոնք նրանք մուտքագրում են: Սա հատկապես կարևոր է կրիպտոհանցագործությունների դեպքում, քանի որ ի տարբերություն այլ տեսակի հաշիվների, եթե կրիպտոդրամապանակի անձնական բանալին գողացվել է, ապա հաշիվը վերականգնելը գրեթե անհնար է: Սա նշանակում է, որ դրամապանակի ներսում գտնվող միջոցները ընդմիշտ կորչում են:

Այս խարդախության տարբեր տեսակները

Բլոկչեյնի վերլուծական ծառայություն մատուցող մի ընկերության հրապարակած զեկույցի[17] համաձայն՝ ֆիշինգային խարդախության նոր տեսակները նոր կրիպտոարժույթ ներդրողներին խաբում են «FOMO»-ով (բաց թողնելու վախով)՝ ստիպելով զոհերին գումար ուղարկել սխալ հաշվեհամարին՝ NFT գնելու հույսով: Սա նշանակում էր, որ տուժողները կորցնում են միայն սխալ հաշվեհամարին ուղարկված գումարը, այլ ոչ թե ամբողջ դրամապանակը:

Տարածվող խարդախության մեկ այլ տարբերակ է «հասցեի թունավորումը», որի ժամանակ խարդախը ստեղծում է մի հասցե, որը նման է այն հասցեին, որին թիրախավորված զոհը նախկինում գումար էր ուղարկել: Այնուհետև խարդախը թիրախին ուղարկում է փոքր գումարի չափով կրիպտոարժույթ՝ հույս ունենալով, որ նա հետագայում անգիտակցաբար վճարում կկատարի նույն կեղծ հասցեին՝ նախատեսված ստացողի փոխարեն:

Ի՞նչ կարելի է անել դրանից խուսափելու համար

Մարդիկ պետք է տեղյակ լինեն կեղծ ֆիշինգային հղումների մասին և ստուգեն բոլոր հղումները:

Կրկնակի ստուգել հասցեները

- Միշտ կրկնակի ստուգեք այն հասցեն, որին գումար եք ուղարկում, հատկապես մեծ գումարների դեպքում: Մի հիմնվեք միայն օպերացիոն համակարգի ժամանակավոր շտեմարանի (clipboard) ֆունկցիաների (այսպես կոչված պատճենել և տեղադրել (copy-paste) ֆունկցիա), քանի որ վնասաբեր ծրագրերը կարող են փոխել դրանք՝ տեղադրելով այլ կրիպտոարժույթի դրամապանակի հասցե, որը տարբերվում է նրանից, ինչը զոհը կարծում էր, որ պատճենել է:

- Օգտագործեք էջանիշներ հաճախ այցելվող կրիպտո կայքերի համար: Սա կօգնի խուսափել սխալ մուտքագրումից կամ ֆիշինգային կայքերում հայտնվելուց:

Ակտիվացնել լրացուցիչ անվտանգության միջոցներ.

- Խորհուրդ է տրվում հնարավորության դեպքում օգտագործել երկու փուլով (գործոնով) նույնականացում (2FA): Սա հավելյալ պաշտպանություն է ստեղծում՝ դժվարացնելով խարդախների մուտքը հաշիվներ:

- Պարբերաբար թարմացրեք և աշխատեցրեք հակավիրուսային ծրագրակազմ՝ ձեր սարքում հնարավոր սպառնալիքներ հայտնաբերելու և հեռացնելու համար: Որոշ վնասաբեր ծրագրեր նախատեսված են կրիպտո գործարքները վերահսկելու կամ clipboard-ի տվյալները փոփոխելու համար:

Օգտագործել գաղտնաբառերի կառավարիչներ. Գաղտնաբառերի կառավարիչները ծրագրային գործիքներ են, որոնք նախատեսված են գաղտնաբառերը պահելու, կառավարելու և ավտոմատ լրացնելու համար: Նրանք հաճախ թույլ են տալիս օգտատերերին ստեղծել անվտանգ նշումներ, որոնք կարող են ապահով կերպով պահպանել կրիպտոարժույթի դրամապանակի համարները տարբեր առցանց հաշիվների համար:

17 Անօրինական կրիպտո էկոհամակարգի վերաբերյալ զեկույց (2023թ.), հասանելի է https://www.trmlabs.com/report հղումով:

Միջնորդի միջոցով հարձակումներ

Ի՞նչ է դա

Այս տեսակի խարդախության դեպքում խարդախները անմիջականորեն չեն թիրախավորում զոհին, այլ փոխարենը որսում են փոխանցվող տվյալների, երբ որևէ մեկը մուտք է գործում իր կրիպտոարժույթի հաշիվ հանրային կամ չպաշտպանված Wi-Fi ցանցում, այսինքն, այնտեղ, որտեղ այցելած կայքերը և համակարգչից կայք ուղարկված տեղեկատվությունը մասնավոր չեն: Խարդախները հավաքում են կրիպտոդրամապանակի հասցեն, մուտքի տվյալները և դրամապանակի բանալիները, և այնուհետև դրանք օգտագործում հաշիվն ամբողջությամբ զավթելու համար:

Ինչպե՞ս դիմակայել կամ խուսափել դրանից

Այս տեսակի խարդախությունից կարելի է խուսափել վիրտուալ մասնավոր ցանցի (VPN) օգտագործմամբ: Դրանք բավականին էժան են, սովորաբար ամսական ընդամենը 3-4 եվրո: VPN-ները գաղտնագրում են օգտատիրոջ ինտերնետային կապը՝ դժվարացնելով չարտոնված անձանց համար տեսնել, թե որ կայքերն են այցելվում կամ ինչ է մուտքագրվում: Այն նաև թաքցնում է օգտատիրոջ սկզբնական IP հասցեն՝ թույլ տալով անանուն մտնել համացանց և թաքցնելով օգտատիրոջ իրական գտնվելու վայրը: Սա թույլ է տալիս օգտատերերին հեռավար մուտք ունենալ իրենց կազմակերպության ռեսուրսներին կամ շրջանցել գրաքննությունը:
(Տե՛ս ավելին «IP հասցեների ձեռքբերում» բաժնում, էջ 31):

Կրիպտոարժույթի փոխանակման հարթակներին նման գործող կեղծ կայքեր

Ի՞նչ է դա

Կեղծ կրիպտոարժույթ ստեղծելու փոխարեն, խարդախը ստեղծում է կրիպտոարժույթի փոխանակման հարթակներին նման կայքեր: Երբ զոհն այցելում է այս կայք՝ իր մի տեսակի կրիպտոարժույթը մեկ այլ տեսակի կամ ՖԻԱՏ արժույթի փոխանակելու համար, խարդախները գողանում են նրա տվյալները և ներդրված կրիպտոարժույթը:

Ինչպե՞ս դիմակայել կամ խուսափել դրանից

Անվտանգությունն ուժեղացնելու համար միշտ կիրառեք երկփուլային նույնականացում (2FA) ձեր փոխանակման հարթակ մուտք գործելու ժամանակ:

Ստուգման այս լրացուցիչ շերտը կարող է ներառել մեկանգամյա կոդի ստացում կարճ հաղորդագրության կամ էլ. փոստի միջոցով, որը պետք է մուտքագրեք մուտք գործելիս:
Կամ, եթե ԵԱՀԿ-ին մասնակից պետությունն առաջարկում է էլեկտրոնային նույնականացման (e-identification) լուծում, ապա մուտքի ժամանակ հավելյալ պաշտպանության համար կարող եք օգտվել դրանից:

Երկրորդային խարդախություններ

Կան նաև երկրորդային խարդախություններ, որոնք տեղի են ունենում այն բանից հետո, երբ զոհն արդեն մեկ անգամ խաբվել է: Դրանք ներկայացված են «Աջակցություն տուժածներին» բաժնում, էջ 37:

Ձախից աջ՝ Մարչին Զարակովսկի, Միխալ Գրոմեկ, Աննա Պաժևսկա և Նինա-Լուիզ Զիդլեր, ովքեր վարում էին վիրտուալ ակտիվների ծառայություն մատուցողների (ՎԱԾՄ) վերահսկողության մարտահրավերներին և առավելություններին նվիրված անկախ սեմինար Ուկրաինայի պատվիրակության համար: Նիստին մասնակցում էին Ուկրաինայի առանցքային հաստատությունների, այդ թվում՝ Ուկրաինայի Ազգային բանկի (ՈւԱԲ), Ուկրաինայի ֆինանսական մոնիթորինգի պետական ծառայությանը (ՖՄՊԾ), Թվային փոխակերպման նախարարության և Ուկրաինայի Ազգային արժեթղթերի և ֆոնդային շուկայի հանձնաժողովի (ԱԱՖՇՀ) ներկայացուցիչներ:
Սեմինարն անց էր կացվում Լեհաստանի ֆինանսների նախարարությունում, որը շարունակում է անվճար տրամադրել իր տարածքները ուկրաինացի պատվիրակների համար մի շարք վերապատրաստման դասընթացներ անցկացնելու համար:

Վիրտուալ ակտիվների հետ կապված հանցագործությունների հետաքննության լրացուցիչ գործիքներ

Վիրտուալ ակտիվների հետ կապված հանցագործությունների հետաքննության լրացուցիչ գործիքներ

Բլոկչեյնի վերլուծության գործիքներ

Բլոկչեյնի վերլուծության լավ գործիքը կամ դրամապանակի լավ դիտարկիչը նշանակում է, որ ոստիկանության աշխատակիցները կարող են իրենց հետաքննությունների մի մասն իրականացնել առանց Վիրտուալ ակտիվների ծառայություններ մատուցողների տեղեկատվության վրա հիմնվելու անհրաժեշտության, որոնք կարող են դանդաղ կամ թերի լինել: Ավելին, ոչ բոլոր ՎԱԾՄ-ներն են դեռևս օգտագործում բլոկչեյնի վերլուծական գործիքներ:

Ինչու՞ է սա կարևոր

Իրավապահ մարմինները հաճախ վիրտուալ ակտիվների ծառայություններ մատուցողներից պահանջում են տեղեկատվություն կրիպտորաժույթի դրամապանակի հասցեների ընթացիկ մնացորդի վերաբերյալ: Թեև ՎԱԾՄ-ների համապատասխանության վերահսկման խմբերը պատրաստ են արձագանքել նման հարցումներին, դա զգալի վարչական խնդիր է դառնում: Ավելի արդյունավետ տարբերակ է կրիպտոարժույթի դրամապանակի հասցեն դրամապանակի դիտարկիչում մուտքագրելը, որն այնուհետև արագ տրամադրում է անհրաժեշտ տեղեկատվությունը առաջատար կրիպտոարժույթների մեծ մասի, բայց ոչ բոլորի վերաբերյալ:

Դրամապանակի դիտարկիչի կողմից տրամադրվող տեղեկատվություն.

- Դրամապանակի ընթացիկ մնացորդը կրիպտոարժույթով և հիմնական ՖԻԱՏ արժույթներով, օրինակ՝ ԱՄՆ դոլարով:
- Կրիպտոարժույթի դրամապանակի ստացած ընդհանուր միջոցները:
- Կրիպտոարժույթի դրամապանակից ուղարկված ընդհանուր միջոցները:
- Գործարքների ժամանակային նշումներ: (Նշում. Գործարքի ժամանակը կարող է տարբեր լինել՝ կախված կրիպտոարժույթի ժամային գոտուց:
- Բլոկչեյնում կատարված վճարները:
- Սկզբնաղբյուր հանդիսացող կրիպտոարժույթի դրամապանակի հասցեները (որտեղից փոխանցվել են միջոցները)
- Նպատակակետ հանդիսացող կրիպտոարժույթի դրամապանակի հասցեները (որտեղ ուղարկվել են միջոցները):

Բլոկչեյնի վերլուծությանը անծանոթ մարդկանց համար այս տվյալները կարող են մակերեսային թվալ: Այնուամենայնիվ, հետաքննության նպատակների համար դրանք կարող են արժեքավոր պատկերացում տալ օրինակ՝ եթե դրամապանակում դիտվում է բազմաթիվ փոքր մուտքային գործարքների և ավելի քիչ թվով խոշոր ելքային գործարքների օրինաչափություն, ապա դա կարող է վկայել թմրանյութերի վաճառքի հետ կապված գործունեության մասին:

Իրական օրինակներ.

Ինչպես պարզվել է, քրեական գործերում օգտագործվել են հետևյալ դրամապանակներ.

- Կրիպտոարժույթի դրամապանակ, որը կապված է եղել սեռական շանտաժի գործի հետ. Բլոկչեյնի դիտարկիչ
- Կրիպտոարժույթի դրամապանակ, որը կապված է եղել Twitter-ի հայտնի հաքերային հարձակման հետ՝ օգտագործելով բլոկչեյնի հետազոտող և «Chain Abuse» տվյալների բազան:

Ինչպես ցանկացած բաց կոդով հետախուզության աղբյուրների դեպքում, նման դիտարկիչներից ստացված ցանկացած տեղեկատվություն պետք է դիտարկել թերահավատությամբ և եզրակացություններ անելուց առաջ ստուգել:

Բլոկչեյնի վերլուծության անվճար գործիքների օրինակներ.

- Block Explorer. Պարզ գործիք, որը տրամադրում է մանրամասն տեղեկատվություն Bitcoin-ի բլոկների, հասցեների և գործարքների մասին: Սա լավ մեկնարկային կետ է սկսնակների համար:
- Etherscan. Այս գործիքը հատուկ է Ethereum բլոկչեյնի համար նախատեսված գործիք է, որը տրամադրում է գործարքների և հասցեների մանրամասն վերլուծություն:
- Blockchair. Այս գործիքն ընդգրկում է բազմաթիվ բլոկչեյններ՝ Bitcoin-ից մինչև Ethereum, դարձնելով այն համընդհանուր նրանց համար, ովքեր ցանկանում են վերլուծել տարբեր ցանցեր:

Օլգա դը Տրուշիսը և Գրետա Բարկաուսկիենեն, ԵԱՀԿ-ի վիրտուալ ակտիվների փորձագետ և Եվրոպոլի Ֆինանսական հետախուզության Պետություն-մասնավոր գործընկերության (EFIPPP) կրիպտոակտիվների ոլորտի աշխատանքային խմբի համաղեկավարները, մասնակցել են EFIPPP-ի 2024 թվականի ապրիլյան լիագումար նիստին Եվրոպոլի գլխավոր գրասենյակում՝ Հաագայում: Միասին նրանք վարում էին գիտելիքների փոխանակման դասընթացները, որոնց ընթացքում տարբեր երկրներից, այդ թվում՝ ԵԱՀԿ-ի շահառու երկրներից ժամանած մասնակիցներն ուսումնասիրել և քննարկել են վիրտուալ ակտիվների ոլորտում կազմակերպված հանցավորության դեմ պայքարի նոր մեթոդները:

Բլոկչեյնի վերլուծության ծառայության մատուցողներ

Բլոկչեյնի վերլուծության ծառայություն մատուցողները դրամապանակի դիտարկիչների առևտրային համարժեքներն են: Նրանք կիրառում են հատուկ ծրագրակազմ՝ նախատեսված բլոկչեյն ցանցերում գործողությունների վերահսկման, վերլուծության և վիզուալիզացիայի համար: Այս գործիքներն օգնում են հետաքննիչներին բացահայտել օրինաչափությունները, հետևել գործարքներին և պատկերացում կազմել բլոկչեյնի ընդարձակ և բարդ աշխարհի մասին: Դրամապանակի դիտարկիչի միջոցով հասանելի տվյալներից բացի, բլոկչեյն վերլուծության ծառայություն մատուցողներն առաջարկում են.

- **Հետևում և հետագծում.** Վերլուծության գործիքների մեծ մասը կարող են հետագծել և հետևել կրիպտոարժույթային գործարքների ուղին՝ սկզբնաղբյուրից մինչև

Վրաստանի ազգային բանկի գլխավոր գրասենյակում Վիրտուալ ակտիվների հարցերի բաժինը վերջին երկու տարիների ընթացքում կարևոր աջակցություն է ստացել ԵԱՀԿ-ի վիրտուալ ակտիվների փորձագետներից: Արդյունքում, MONEYVAL-ում Վրաստանի վարկանիշը բարձրացվել է մինչև «Մեծապես համապատասխանում է» ֆինանսական գործողությունների հատուկ աշխատանքային խմբի 15-րդ առաջարկությանը:

նպատակակետ: Սա կենսական նշանակություն ունի միջոցների հոսքը պատկերացնելու և հնարավոր անօրինական գործունեությունը բացահայտելու համար:

- **Վիզուալիզացիա.** Այս գործիքները հաճախ տրամադրում են վիզուալ սխեմաներ և գծապատկերներ, որոնք նպաստում են մեծ քանակությամբ տվյալների արագ ընկալմանը և թույլ են տալիս կապել կրիպտոարժույթի դրամապանակները ֆինանսական հաստատությունների հետ կամ միմյանց հետ կապել գործարքները կամ դրամապանակի ծառայություն մատուցողներին:

- **Ռիսկերի գնահատում.** Վերլուծելով գործարքների օրինաչափությունները՝ որոշ գործիքներ կարող են գնահատել կոնկրետ դրամապանակների կամ գործարքների հետ կապված ռիսկերը՝ արժեքավոր տեղեկություններ տրամադրելով ֆինանսական հաստատությունների և կարգավորողների համար:

- **Համապարփակ տվյալներ.** Այս գործիքները կարող են դուրս բերել և ներառել տվյալներ տարբեր բլոկչեյններից՝ օգտատերերին տալով կրիպտոարժույթների ոլորտի ամբողջական պատկերը, որը կարող է օգտակար լինել մեծ թվով հետաքննությունների համար:

- **Ապախառնման ծառայություններ.** Որոշ ծառայություններ մատուցողներ պնդում են, որ իրենց ծառայությունները կարող են վերհանել գործարքները խառնիչների և քողարկիչների միջոցով, որոնք ծառայություններ են՝ նախատեսված կրիպտոարժույթային գործարքների գաղտնիությունը և անանունությունը բարձրացնելու համար: (Լրացուցիչ տեղեկությունների համար տե՛ս «Խառնիչներ և քողարկիչներ» բաժինը էջ 19, ինչպես նաև ապախառնման ծառայությունների քննարկումը «Գործերը դատարան հանձնելը» բաժնում, էջ 34):

Օգտագործելով այս գործիքները՝ հետաքննիչները կարող են ավելի լավ հասկանալ բլոկչեյնի բարդ դինամիկան, ինչը թույլ է տալիս հիմնավոր որոշումներ կայացնել և ավելի խորն ընկալել այս հեղափոխական տեխնոլոգիան:

Համագործակցություն թվային ակտիվների ոլորտի փորձագետների հետ

Համագործակցություն թվային ակտիվների ոլորտի փորձագետների հետ

Իրավապահ մարմիններում թվային ակտիվների և դրանց հետ կապված հաշվետվությունների հետ գործ ունենալիս արտաքին կառույցների հետ համագործակցությունը դառնում է անհրաժեշտություն: Նշված կառույցների թվում են միջազգային ոստիկանական կազմակերպությունները, բանկերը և որոշ երկրներում հատուկ ստորաբաժանումները: Նրանց փորձառությունը նպաստում է հետաքննությունների արդյունավետ իրականացմանը:

Տեղական մասնագետների բացահայտում

Շատ կարևոր է գտնել իրավապահ մարմինների՝ վիրտուալ ակտիվների ոլորտում աշխատելու փորձ ունեցող տեղացի աշխատակիցներին: Նրանց կոնտակտային տվյալներն ունենալը կարող է օգտակար լինել հետևյալ պատճառներով՝

- **Նպատակը.** հաշվետվությունների պատրաստման ընթացքում պատասխանել հարցերին և ստանալ հստակ պատկերը:
- **Օրինակ.** Միացյալ Թագավորության Շանցագործությունների դեմ պայքարի ազգային գործակալությունը ստեղծել է հատուկ կրիպտո ոլորտի հարցերով զբաղվող ստորաբաժանում, որը կարող է խորհրդատվական դեր ունենալ բարդ գործերի քննության համար: Վիրտուալ ակտիվների ոլորտում իրավապահ մարմինների միջև համագործակցության կազմակերպման ոգեշնչող օրինակ կարելի է գտնել նաև Եվրոպայի խորհրդի կողմից կազմված 2023թ. Տիպաբանությունների հաշվետվության մեջ.[18]

Միջազգային աջակցություն

Եվրոպոլի փորձագետների հարթակ (ԵՓՀ)

- **Նկարագրություն.** Սա իրավապահ մարմինների աշխատակիցների համար անվճար հարթակ է, որը տրամադրում է գործնական աջակցություն վիրտուալ ակտիվների հետ կապված հարցերում:
- **Մասնակցության իրավասություն.** Եվրոպոլի փորձագետների հարթակին (https://epe.europol.europa.

18 Տե՛ս «Գործերի պահոց», Տիպաբանությունների հաշվետվություն 2023թ., «Փողերի լվացման և ահաբեկչության ֆինանսավորման ռիսկերը վիրտուալ ակտիվների աշխարհում: Մանիվալ, Եվրոպայի խորհուրդ https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4

eu/) միանալու իրավասություն ունենալու համար երկիրը պետք է լինի Եվրոպական Միության անդամ կամ այսպես կոչված օպերատիվ համաձայնագրի[19] մաս կազմի:

- **Առավելությունները.** ԵՓՀ-ն առաջարկում է վիրտուալ ակտիվների ոլորտում հետաքննությունների լավագույն գործելակերպը: Այն նաև տալիս է վեբինարներին մասնակցելու, ինչպես նաև շահագրգիռ կողմերի հետ շփվելու, ինչպես նաև համաժողովներին և այլ ուսումնական գործընթացներին մասնակցելու հնարավորություն:

- **Միանալու գործընթացը.** Եթե ԵԱՀԿ-ի մասնակից պետությունը հանդիսանում է Բուդապեշտի հուշագրի 20-րդ օպերատիվ համաձայնագրի[20] մասնակից (ցանկը ներկայացված է առանձին), ապա այն կարող է դիմել այս հարթակին միանալու համար: Գործընթացը ներառում է:

  - Աշխատանքային էլ. փոստի հասցեով կապ հաստատել Եվրոպոլի օպերատիվ ստորաբաժանման հետ o3@europol.europa.eu հասցեով և նշել, թե ինչպես եք առնչվում վիրտուալ ակտիվների հետ և ինչպես են ձեր գիտելիքները օգնելու մյուսներին:

  - Շստակ նշել միանալու պատճառը, մասնավորապես, կապված վիրտուալ ակտիվների հետ:

- **Ո՞վ կարող է միանալ.** Թեև հարթակը հիմնականում նախատեսված է իրավապահ մարմինների աշխատակիցների համար, սակայն կարող են դիմել նաև ինչպես պետական, այնպես էլ մասնավոր հատվածի փորձագետները:

- **Արժեքը.** Ոչ մի վճար չի պահանջվում: Մուտքն ամբողջությամբ անվճար է:

2019 թվականի հոկտեմբերին Եվրոպոլը ներկայացրեց երկու ուսումնական խաղ՝ «Cryptopol» անվանումով: Դրանք մի քանի անգամ թարմացվել են և ներառում են բազմաթիվ կրիպտոարժույթներ: Նշված խաղերը շարունակում են մնալ անվճար ԵՄ անդամ պետությունների իրավապահ մարմինների աշխատակիցների համար: Տե՛ս o3@europol.europa.eu

ԻՆՏԵՐՊՈԼ-ի ֆինանսական հանցագործությունների և կոռուպցիայի դեմ պայքարի Կենտրոն (IFCACC)

Ինտերպոլի ֆինանսական հանցագործությունների և կոռուպցիայի դեմ պայքարի կենտրոն (IFCACC). Այս կենտրոնի գործունեությունը նպատակաուղղված է անդրազգային ֆինանսական հանցագործությունների դեմ պայքարին՝ գլոբալ ֆինանսական համակարգերը պաշտպանելու նպատակով:

Միանալու իրավասություն. Շամաշխարհային ֆինանսական հանցագործությունների աճող սպառնալիքներին արձագանքելու նպատակով Ինտերպոլը ստեղծել է IFCACC-ը՝ այս մարտահրավերների դեմ պայքարում համախմբված աջակցություն ցուցաբերելու համար: Այն նախատեսված է ոչ միայն իրավապահ մարմինների, այլև միջազգային կառույցների և շահագրգիռ կողմերի համար:

Առավելությունները. IFCACC-ը տրամադրում է.

- Աջակցություն իրավապահ մարմինների կողմից խարդախությունների, վճարային հանցագործությունների դեմ պայքարում և անդրսահմանային հարցումներում:
- Օժանդակություն փողերի լվացման դեմ պայքարի, ակտիվների վերադարձի և վիրտուալ ակտիվների վերաբերյալ պատկերացում կազմելու հարցերում:
- Կոռուպցիայի դեմ վերահսկողական մեխանիզմներ՝ ներառյալ սպորտային միջադեպերի և բարձր մակարդակի քաղաքական չարաշահումների հետ կապված հարցերը:

Միանալու գործընթացը. Քանի որ IFCACC-ն գործում է միջգերատեսչական մոդելով, համագործակցության հնարավորությունները ներառում են՝

- Կապ հաստատել Ինտերպոլի Գլխավոր քարտուղարության կամ Ինտերպոլի Ազգային կենտրոնական բյուրոյի հետ, որը սովորաբար գտնվում է պետության արդարադատության նախարարության և դրա դատական ոստիկանության ներքո:
- Ցույց տալ ֆինանսական հանցագործությունների և կոռուպցիայի դեմ նպատակների հստակ համապատասխանությունը:
- Ներկայացնել համագործակցության կամ կարիքների հնարավոր ոլորտները:

Ո՞վ կարող է միանալ. Իրավապահ մարմիններից բացի ֆինանսական հաստատությունները, միջազգային կազմակերպությունները և մասնավոր հատվածի

19 Շամաձայնագրեր և աշխատանքային պայմանավորվածությունների երկրների հետ https://www.europol.europa.eu/partners-collaboration/agreements

20 Շամաձայնագրեր և աշխատանքային պայմանավորվածությունների երկրների հետ: Եվրոպոլ https://www.europol.europa.eu/partners-collaboration/agreements

ներկայացուցիչները նույնպես կարող են համագործակցել IFCACC-ի հետ: Սակայն համագործակցության խորությունը կարող է տարբեր լինել՝ կախված փոխըգործակցության բնույթից և նպատակներից:

Արժեքը. Քանի որ Ինտերպոլը միջազգային կազմակերպություն է, դրա գլխավոր քարտուղարության հետ համագործակցելու համար որևէ վճար նախատեսված չէ: IFCACC-ի և I-GRIP-ի վերաբերյալ լրացուցիչ տեղեկությունների համար տե՛ս

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

Վիրտուալ ակտիվների տեխնիկական մանրամասների վերաբերյալ լրացուցիչ տեղեկությունների համար

իրավապահ մարմինների աշխատակիցները կարող են էլ. նամակ ուղարկել հետևյալ հասցեին՝innovation@interpol.int

Լրացուցիչ ռեսուրսներ. Իրավապահ մարմինների աշխատակիցները կարող են պահանջել Ինտերպոլի «Վիրտուալ ակտիվների առգրավման ուղեցույցը»՝ vaguidelines@interpol.int

ՄԱԿ-ի թմրամիջոցների և հանցավորության դեմ պայքարի գրասենյակի (UNODC) ծրագրերը վիրտուալ ակտիվների, կիբերհանցագործությունների և փողերի լվացման դեմ պայքարի վերաբերյալ և հետաքննությունների վերաբերյալ աշխատաժողովներ

Ընդհանուր տեղեկություններ. ՄԱԿ-ի թմրամիջոցների և հանցավորության դեմ պայքարի գրասենյակի (UNODC) թիմի ղեկավարությամբ անցկացվող այս համապարփակ սեմինարների շարքը առաջարկում է վիրտուալ ակտիվների, ֆինանսական հանցագործությունների և օրենսդրության համապատասխանության հիմնական ոլորտի խորը ուսումնասիրություն:

Ուսումնական ծրագիրը կառուցված է հիմնական, ընդլայնված և կասկադային (շղթայական) դասընթացներից, որոնք նախատեսված են հրահանգիչների (դասընթացավարների) վերապատրաստման համար: Կասկադային դասընթացը նպաստում է ոլորտում կիրառվող լավագույն փորձի տարածմանը: Սեմինարները ներառում են ինչպես տեսական նյութեր, այնպես էլ գործնական վարժություններ՝ իրավապահ մարմինների մասնակիցներին ապահովելով արժեքավոր հմտություններով՝ վիրտուալ ակտիվներին հետևելու, դրանց հետ կապված գործերը հետաքննելու և հմտորեն կառավարելու գործում:

Մասնակցության իրավասություն. Այս մասնագիտացված դասընթացը կազմակերպվում է տարբեր ոլորտների մասնագետների համար, այդ թվում՝ իրավապահ մարմինների, ֆինանսական հաստատությունների, տեխնոլոգիական ձեռնարկությունների և կրթական հաստատությունների ներկայացուցիչների համար: Դասընթացը հատկապես անգնահատելի ռեսուրս է հանդիսանում քաղաքականություն մշակողների, կարգավորող մարմինների, հետաքննիչների և բոլոր մասնագետների համար, ովքեր մտադիր են հասկանալ վիրտուալ ակտիվների բարդությունները, բլոկչեյնի դինամիկան և ֆինանսական հանցագործությունների կանխարգելման միջոցները:

Գործունեության հիմնական ոլորտները

- **Վիրտուալ ակտիվներ.** Խորապես ուսումնասիրել անընդհատ զարգացող վիրտուալ ակտիվների և դրանց հիմքում ընկած տեխնոլոգիաների ծագումը, զարգացումը և բարդ կողմերը:
- **Գործարքների դինամիկա.** Վերլուծել բլոկչեյն գործարքների կենսափուլը՝ սկզբից մինչև ավարտ:
- **Բլոկչեյնի խորը ուսումնասիրություն.** Բացահայտել այն գործընթացները, որոնց միջոցով գործարքները գրանցվում, հաստատվում և արխիվացվում են բլոկչեյնում:
- **Բլոկչեյնի դատափորձաքննություն.** Ձեռք բերել իրական ժամանակում գործարքների վերահսկման և ֆինանսական հանցագործների՝ իրենց ինքնությունը թաքցնելու համար օգտագործված մեթոդների բացահայտման հմտություններ:
- **ՓԼՊ/ԱՖՊ մարտավարություն.** Յուրացնել, թե ինչպես հարմարեցնել փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մեխանիզմները վիրտուալ ակտիվների փոփոխվող միջավայրին:
- **Ռիսկերի կառավարում.** Ծանոթացնել մասնակիցներին վիրտուալ ակտիվների հետ կապված տարբեր ռիսկերի մեղմման ոսկե ստանդարտներին:
- **Ակտիվների վերահսկողություն.** Մասնակիցներին ծանոթացնել հետաքննությունների ընթացքում վիրտուալ ակտիվների պատշաճ կերպով առգրավման և վիրտուալ ակտիվների կառավարման լավագույն մեթոդներին:

Գրանցման փուլեր.
Շնարավոր մասնակիցները կարող են՝

- Ուսումնասիրել առաջիկա սեմինարների ժամանակացույցը և ամրագրել իրենց տեղերը:
- Պարզել վճարների հնարավոր զեղչերը՝ ելնելով իրենց մասնագիտական ոլորտից՝

լրացնելով համապատասխան ձևաթուղթը:
- Մանրամասն ծանոթանալ և համաձայնվել դասընթացին մասնակցելու պայմաններին:

Թիրախային լսարան.
Սեմինարները նախատեսված են բազմազան լսարանի համար, ներառյալ՝ հետաքննիչներ, իրավաբանական ոլորտի մասնագետներ, ֆինանսական կարգավորող մարմինների աշխատակիցներ, տեխնոլոգիաների առաջամարտիկներ, լրագրողներ և այլն: Դրանք նախատեսված են ինչպես պետական, այնպես էլ մասնավոր հատվածի մասնագետների համար՝ հատկապես վիրտուալ ակտիվներով և համապատասխան ֆինանսական կարգավորումներով հետաքրքրված անձանց համար:

Վճարի կառուցվածքը.
Դասընթացին մասնակցության արժեքը կազմում է մոտավորապես 10 000-ից 20 000 ԱՄՆ դոլար՝ կախված մասնակիցների թվից: Շատուկ զեղչեր կարող են տրամադրվել պետական հատվածի ներկայացուցիչների, գիտական շրջանակների, ոչ առևտրային կազմակերպությունների և լրատվամիջոցների աշխատակիցների համար:
Դասընթացի բովանդակության վերաբերյալ լրացուցիչ տեղեկություններ ստանալու համար կարող եք դիմել ՄԱԹՀԳ-ի վիրտուալ ակտիվների ուսուցման բաժնին՝ cryptocurrency@unodc.org հասցեով:

Լրացուցիչ հնարավորություններ ՄԱԹՀԳ-ի էլեկտրոնային ուսուցման հարթակը հասանելի է հետևյալ հղումով՝ https://www.unodc.org/elearning/en/courses/course-catalogue.html

Բազելի կառավարման ինստիտուտ

Բազելի կառավարման ինստիտուտը
անկախ, ոչ առևտրային կազմակերպություն է, որը նպատակ ունի բարելավել կառավարման համակարգերը և համաշխարհային մակարդակով պայքարել ֆինանսական հանցագործությունների դեմ: Գտնվելով Շվեյցարիայի Բազել քաղաքում ինստիտուտն ակտիվ գործունեություն է ծավալում նաև մի շարք աֆրիկյան երկրներում՝ սերտորեն համագործակցելով Բազելի համալսարանի հետ:

Բազելի ինստիտուտի կրիպտոարժույթների թեմայով սեմինար. Առաջարկում է վերապատրաստման 4-օրյա վիրտուալ համապարփակ դասընթաց՝ նվիրված կրիպտոարժույթների հիմունքներին, ֆինանսական հանցագործությունների և փողերի լվացման դեմ պայքարի համապատասխանության պահանջներին: Դասընթացը ներառում է փողերի լվացման գործնական վարժանք, որը կօգնի մասնակիցներին հետևել ապօրինի գործունեության համար բլոկչեյն օգտագործող գործարքներին:

Մասնակցության իրավասություն.
Դասընթացը բաց է մասնագետների լայն շրջանակի համար, այդ թվում՝ իրավապահ մարմինների, ֆինանսական հաստատությունների, ձեռնարկությունների և նույնիսկ ուսանողների համար: Բովանդակությունը հարմարեցված է քաղաքականություն մշակողների, կարգավորող մարմինների, հետաքննող լրագրողների և վիրտուալ ակտիվներով, բլոկչեյնով և ֆինանսական հանցագործությունների կանխարգելմամբ հետաքրքրված ցանկացածի համար:

Առավելությունները. Բազելի ինստիուտի կողմից կազմակերպվող սեմինարը տալիս է պատկերացում հետևյալի մասին.
- **Կրիպտոարժույթի հիմունքներ.** Պատկերացնել վիրտուալ ակտիվների, բաշխված ռեեստրի տեխնոլոգիայի (DLT) և այլ բաղադրիչների հիմքը, ծագումը և շրջանակը:
- **Գործարքների մեխանիզմներ.** Շասկանալ, Bitcoin-ի ցանցի աշխատանքի, գաղտնագրության և գործարքների կառավարման հիմնարար սկզբունքները:
- **Բլոկչեյն և մայնինգ.** Սովորել, թե ինչպես են պաշտպանվում, պահվում և հաստատվում բլոկչեյնում:
- **Բլոկչեյնի վերլուծություն.** Գործարքների իրական ժամանակում վերահսկման մեթոդներ, հանցագործների կողմից անանունության դեմ պայքար և գործիքների կիրառություն:
- **Պատշաճ ստուգում.** ՓԼՊ/ԱՖՊ ծրագրերի հարմարեցում նոր վճարման եղանակներին:
- **Ռիսկերի կառավարում.** Վիրտուալ ակտիվների ռիսկերը կառավարելու առաջատար մեթոդներն ու աղբյուրները:
- **Ակտիվների բռնագրավում.** Կրիպտոակտիվների բռնագրավման, դրամապանակի կառավարման և այլնի ընթացակարգերն ու նրբությունները:

Ո՞վ կարող է միանալ. Դասընթացը նախատեսված է հետաքննիչների, իրավաբանների, փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասնագետների, ֆինանսական հետախուզության ստորաբաժանումների անդամների, ֆինանսական տեխնոլոգիաների ոլորտի մասնագետների, լրագրողների և այլոց համար: Այն նախատեսված է ինչպես պետական, այնպես էլ մասնավոր հատվածի մասնագետների համար, ովքեր ցանկանում են հասկանալ վիրտուալ ակտիվների և ֆինանսական հանցագործությունների բնույթը:

Արժեքը. 750 շվեյցարական ֆրանկ մեկ անձի համար, իսկ կոնկրետ խմբերի (օրինակ՝ պետական հատվածի ներկայացուցիչների, գիտական շրջանակների, ոչ առևտրային կազմակերպությունների և լրագրողների) համար՝ իջեցված՝ 300 շվեյցարական ֆրանկ մեկ անձի համար։

Լրացուցիչ տեղեկությունների համար դիմել info@baselgovernance.org հասցեով։

Դասընթացի մանրամասները և հասանելի ամսաթվերի համար գրանցման հղումները կարելի է գտնել Բազելի ինստիտուտի սոցիալական ցանցի հարթակներում։

Ֆինանսական հանցագործությունների դեմ պայքարողների հիմնադրամ

Ֆինանսական հանցագործությունների դեմ պայքարողների հիմնադրամը («FinCrime Fighters Foundation») Ստոկհոլմում տեղակայված կազմակերպություն է, որը ստեղծվել է Ֆինանսական հանցագործությունների դեմ պայքարի համաշխարհային կոալիցիայի թվային ակտիվների աշխատանքային խմբի փորձագետների կողմից։ Գործիքի նպատակն է ապահովել արագ և հղումներով հիմնավորված պատասխաններ բլոկչեյնի վրա հիմնված ֆինանսների և Web 3-ի հետ կապված հարցերին։ Հիմնադրամը տրամադրում է անվճար ժետոնային ռեսուրսներ գեներացվող արհեստական բանականության օգնականին, որը նախատեսված է բացառապես պետական և մասնավոր ֆինանսական հանցագործությունների դեմ պայքարողների համար։

Թիմը մշտապես վերբեռնում և վերանայում է վերջին հաշվետվությունները, այդ թվում՝ ԵԱՀԿ-ի հրապարակային նյութերը։ Կարգավորումները կարելի է որոնել ChatGPT-ի նման համակարգում՝ օգնելու մասնագետներին ամենօրյա կտրվածքով տեղեկացված լինել օրենսդրական փոփոխությունների մասին։

https://www.fincrimefighters.com/

Խորհուրդներ իրավապահ մարմիններին հանցագործությունների մասին հաղորդումներ ստանալուց հետո ձեռնարկվող քայլերի մասին

Խորհուրդներ իրավապահ մարմիններին հանցագործությունների մասին հաղորդումներ ստանալուց հետո ձեռնարկվող քայլերի մասին

- **Անմիջական աջակցություն.** Ապահովել, որ տուժողներին տրվի անմիջական ուղղորդում, թե ինչպես պաշտպանել իրենց մնացած թվային ակտիվները և նվազեցնել հետագա ֆինանսական կորուստների ռիսկը։ Դա կարող է ներառել ուղեցույց, թե ինչպես փոխել գաղտնաբառերը, պաշտպանել դրամապանակները կամ տեղափոխել ակտիվները ավելի ապահով հարթակ։

- **Ֆինանսական խորհրդատվություն.** Տուժողներին կապել ֆինանսական խորհրդատվության ծառայությունների հետ, որոնք կարող են օգնել նրանց հասկանալ իրենց կրած վնասները, հնարավոր հարկային հետևանքները և ժամանակի ընթացքում վնասները վերականգնելու կամ մեղմելու ռազմավարությունները։

- **Տեղեկատվական աշխատանք.** Նախաձեռնել հանրային իրազեկման արշավներ և սեմինարներ նմանատիպ խարդախությունների վերաբերյալ։ Որքան իրազեկված լինի հանրությունը, այնքան ավելի դժվար կլինի խարդախների համար մոլորեցնել պոտենցիալ ներդրողներին։

- **Համագործակցություն կրիպտոարժույթների բորսաների հետ.** Սերտ համագործակցել կրիպտոարժույթի փոխանակման հարթակների հետ՝ խարդախների ակտիվներին հետևելու և հնարավորության դեպքում դրանք սառեցնելու նպատակով՝ դժվարացնելով անօրինական ճանապարհով ստացված եկամուտների կանխիկացումը։

- **Միջպետական համագործակցություն.** Քանի որ թվային խարդախությունները հաճախ անցնում են միջազգային սահմանները, անհրաժեշտ է համագործակցել միջազգային իրավապահ մարմինների հետ՝ հանցագործներիներին հայտնաբերելու, ձերբակալելու և պատասխանատվության ենթարկելու համար։

Մարիամ Գրիգալաշվիլին Երևանում անցկացված կրիպտոարժույթների հարկման և փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի քաղաքականությունների հետ դրա փոխակապակցվածությանը նվիրված սեմինարի ընթացքում ՀՀ Կենտրոնական բանկի գործընկերների հետ կիսվում է Վրաստանի և Վրաստանի Ազգային բանկից փորձով։

ԵԱՀԿ-ի հետ համագործակցության ամփոփում և սկզբունքները

ԵԱՀԿ-ի հետ համագործակցության ամփոփում և սկզբունքները

ԵԱՀԿ-ի վիրտուալ ակտիվների հետ կապված հարցերում աջակցության նախաձեռնություն

Ո՞վ ենք մենք

ԵԱՀԿ-ի վիրտուալ ակտիվների հարցերով փորձագիտական խումբը եզակի կարողություններ ունի արձագանքելու քաղաքականություն մշակողների և իրավապահ մարմինների համար վիրտուալ ակտիվների առաջացած մարտահրավերներին: Ելնելով տեխնիկական փորձագիտական գիտելիքների տրամադրման գրեթե հիսուն տարվա փորձից մենք օգնում ենք քաղաքականություն մշակողներին և իրավապահ մարմիններին հասկանալ ԵԱՀԿ-Ի 57 անդամ պետություններում վիրտուալ ակտիվների հետ կապված բարդությունները:

Արժեքը, որը մենք ստեղծում ենք իրավապահ մարմինների և քաղաքականության մշակողների համար

- **Ժամանակակից գիտելիքներ.** Մեր Մեր վերապատրաստման ծրագրերն իրավապահ մարմիններին և քաղաքականություն մշակողներին զինում են արդի գիտելիքներով և ռազմավարություններով, որոնք հարմարեցված են վիրտուալ ակտիվների ոլորտում առկա յուրահատուկ մարտահրավերներին դիմակայելու համար:
- **Գործողությունների արդյունավետություն.** Գործնական ուսուցման շրջանակներում մենք լուծում ենք անհրաժեշտ լոգիստիկ հարցերը, ամրագրում դասընթացների անցկացման վայրերը, հրավիրում ենք ԵԱՀԿ-ի մասնակից պետություններից նախապես ընտրված վիրտուալ ակտիվների ոլորտի փորձագետների, ներկայացնում օրակարգը և կազմում ուսումնառության նպատակները:
- **Վերապատրաստում և փորձագիտական գիտելիքների զարգացում.** Մենք առաջարկում ենք համապարփակ վերապատրաստման ծրագրեր վիրտուալ ակտիվների ոլորտում: Մեր թիմը, որը բաղկացած է քաղաքականություն մշակողների, իրավապահ մարմինների, սովորական բանկերի և WEB3 ընկերությունների համապատասխան մասնագետներից, առաջնահերթություն է տալիս գործնական ուսուցմանը՝ սահմանափակ, բայց հակիրճ տեսական բաղադրիչով: Շիմնական շեշտը դրվում է գործնական վարժությունների վրա՝ ապահովելով իրական կյանքում կիրառելիությունը: Շատկանշական է, որ նախկին մասնակիցները գրանցել են զգալի արդյունքներ՝ ներառյալ փողերի լվացմանն առնչվող բարդ գործերի հաջող հետաքննությունը:
- **Ռեսուրսների տրամադրում.** Մենք համագործակցում ենք բլոկչեյնի առաջատար փորձագետների հետ: Պրոֆեսիոնալ գործիքների կիրառմամբ այս գործնական աշխատանքը հնարավորություն է տալիս մասնակիցներին արդյունավետ կերպով կիրառել ձեռք բերված գիտելիքները խորացված դասընթացների և սեմինարների ժամանակ, որտեղ բարդ զարգացումները վերածում ենք գործնական վարժությունների:
- **Դեպքերի վերլուծություն.** Վերապատրաստման մեր ծրագիրը հաճախ ներառում է իրական ժամանակում դեպքերի ուսումնասիրություններ և օրենսդրական աջակցություն, ինչը հնարավորություն է տալիս պատկերացնել ընթացիկ զարգացումները և լուծել հնարավոր խնդիրները նախքան դրանց իրականում տեղի ունենալը:
- **Ընդլայնելու հնարավորություն և շարունակականություն.** Կասկադային վերապատրաստման մեր

համակարգը ներառում է «հրահանգիչների վերապատրաստման» մոդելը, որի շրջանակներում մենք փորձագետներին հնարավորություն ենք տալիս իրենց երկրներ վերադառնալուց հետո փոխանցել իրենց ստացած գիտելիքները: Սա ապահովում է գիտելիքի ավելի լայն տարածում և փորձի շարունակական զարգացում հայրենի երկրներում:

- **Անվտանգ թվային միջավայրի ձևավորում.** Վիրտուալ ակտիվների ոլորտում քաղաքականություն մշակողներին և իրավապահ մարմիններին համապատասխան հմտություններով զինելով՝ մենք նպաստում ենք ավելի անվտանգ և թափանցիկ թվային ֆինանսական միջավայրի ձևավորմանը:

Միացե՛ք մեզ կիբերանվտանգության ապագան ձևավորելու և բոլորի համար ավելի անվտանգ, ավելի թափանցիկ թվային միջավայր ապահովելու գործում:

Կապ հաստատեք մեզ հետ հետևյալ հասցեով՝ VirtualAssets@osce.org

Կարճ ընտրանի լրացուցիչ ընթերցանության համար

Կարճ ընտրանի լրացուցիչ ընթերցանության համար

ՄԱԿ-ի թմրամիջոցների և հանցավորության դեմ պայքարի գրասենյակ (UNODC)

Վիրտուալ արժույթների օգտագործմամբ հանցավոր ճանապարհով ստացված եկամուտների լվացման դեպքերի հայտնաբերման և հետաքննության հիմնական ուղեցույց (2014թ.):

Չնայած այս 200-էջանոց համապարփակ փաստաթուղթը ՄԱԹՀԳ-ի հրապարակվել է ավելի քան տասը տարի առաջ՝ 2014 թվականին, այն խորապես ուսումնասիրում է մի շարք տերմիններ և ներկայացնում է համատեքստը՝ սույն ակնարկում նկարագրված տերմինների համար: Այն նաև ներառում է ինքնագնահատման հարցաթերթիկներ:

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

Եվրոպայի անվտանգության և համագործակցության կազմակերպություն (ԵԱՀԿ)

Քրեական վարույթներում վիրտուալ արժույթների հետ աշխատելու ձեռնարկ (2022թ.)

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

ԱՄՆ-ի արդարադատության դեպարտամենտ

Իրավապահ մարմինների դերը թվային ակտիվների հետ կապված հանցավոր գործունեության բացահայտման, հետաքննության և քրեական հետապնդման գործում (2022թ.)

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

ԱՄՆ-ի արդարադատության դեպարտամենտի հրապարակած այս զեկույցը լրացնում է իրավապահ մարմինների միջազգային համագործակցության մասին զեկույցը և թարմացնում է «Կրիպտոարժույթների հետ կապված գործերի հետաքննության իրականացման հիմքերը» փաստաթուղթը: Այն ապահովում է համապարփակ տեղեկատվություն ապագա օգտագործման համար

Հեղինակի մասին

Այս ակնարկը կազմվել է ԵԱՀԿ-ի ծրագրի վիրտուալ ակտիվների ոլորտի առաջատար փորձագետներից մեկի՝ Միխալ Գրոմեկի կողմից: Դրա նպատակն է մեղմել վիրտուալ ակտիվների և կրիպտոարժույթների հետ կապված փողերի լվացման ռիսկերը: Ծրագիրն իրականացվում է ԵԱՀԿ-ի տնտեսական և բնապահպանական գործունեության համակարգողի գրասենյակում՝:

Գրոմեկը Ստոկհոլմում գտնվող՝ Nasdaq-ում ցուցակված «VASP Safello» ընկերության համապատասխանության նախկին գլխավոր պատասխանատուն է: Նա ղեկավարում է Ֆինանսական հանցագործությունների դեմ պայքարի համաշխարհային կոալիցիայի թվային ակտիվների աշխատանքային խումբը, որը հիմնադրվել է Եվրոպոլի, Համաշխարհային տնտեսական ֆորումի և Լոնդոնի ֆոնդային բորսայի ռիսկային լուծումների միջև համագործակցության արդյունքում: Գրոմեկը նաև Ֆինանսական հանցագործությունների դեմ պայքարի համաշխարհային կոալիցիայի գործադիր թիմի անդամ է: Նա շարունակում է վերապատրաստման դասընթացներ անցկացնել կառավարությունների և իրավապահ մարմինների համար՝ տրամադրելով աջակցություն օրենսդրության մշակման գործում՝ կանխելու ԵԱՀԿ մասնակից

պետությունների առջև ծառացած խնդիրները: Նա իր փորձը ձեռք է բերել՝ զբաղեցնելով ֆինանսական տեխնոլոգիաների բաժնի ղեկավարի և Ստոկհոլմի տնտեսագիտական դպրոցի ղեկավարների կրթության բաժնի ծրագրի տնօրենի պաշտոնները: Ավելի քան մեկ տասնամյակ նա աշխատել է ֆինանսական տեխնոլոգիաների և վիրտուալ ակտիվների համապատասխանության ոլորտում: Նրա ուսումնասիրությունները հրապարակվել են Forbes.com-ում, ինչպես նաև մի շարք գրքերում և ամսագրերում:

Երախտիքի խոսք

Այս ուղեցույցի բարելավման գործում կարևոր դեր է խաղացել դոկտոր Ալեքսանդրա Անդհովի գրախոսությունն ու ներդրումը: Նրա իրավական փորձառությունն ու մեկնաբանությունները զգալիորեն բարձրացրել են բովանդակության ճշգրտությունը, համապատասխանությունն ու խորությունը: Կոպենհագենի համալսարանի իրավունքի ֆակուլտետի դոցենտի իր փորձով նա արժեքավոր վերլուծություններ և առաջարկություններ է ներկայացրել այս փաստաթղթի մշակման ընթացքում: Դոկտոր Անդհովն ունի փորձ իրավունքի և տեխնոլոգիայի հատման ոլորտում և հանդիսանում է «Ֆինանսական հանցագործության դեմ պայքարողների» հիմնադրամի համահիմնադիրը և գլխավոր իրավախորհրդատուն:

Փաստաթղթի ընթեռնելիությունն ու որակը բարձրացնելու համար դրա լեզվական խմբագրմանը մասնակցել են մի շարք մասնագետներ՝ հիմնականում Գրեյս Մարշալը, որն ապահովել է բովանդակության հստակությունն ու ամբողջականությունը: Որպես Ֆինանսական հանցագործությունների դեմ պայքարի համաշխարհային կոալիցիայի գլխավոր քարտուղար՝ նա օգնել է տեղեկատվությունն ադապտացնել լայն լսարանի համար: Տիկինի Մարշալից բացի, փաստաթղթի գնահատման և խմբագրման աշխատանքներին մեծ ներդրում է ունեցել Դենիսե Ռուդիչը, որն իր հարուստ փորձով ապահովել է ինչպես բովանդակային, այնպես էլ լեզվական ճշգրտություն:

Շավելյալ խմբագրական աջակցություն են ցուցաբերել Գրետա Բարկաուսկիենեն, Էմիլիա Պախոմովը, Սանգյոնգ Կանգը և Վենսան Դանժանը: Լրացուցիչ վերանայել և առաջարկներ են ներկայացրել ԻՆՏԵՐՊՈԼ-ի Ֆինանսական հանցագործությունների և կոռուպցիայի դեմ պայքարի կենտրոնի (IFCACC) մասնագետ Մոնա Ժեսսեին, ինչպես նաև Կիբերհանցագործությունների դեմ պայքարի եվրոպական Կենտրոնի (EC3) աշխատակիցները, մասնավորապես Գերտ Յան վան Շարդվելդը:

ԵԱՀԿ-ի տնտեսական և բնապահպանական գործունեության համակարգողի գրասենյակի թիմը երախտապարտ է ցուցաբերված մեծ աջակցության համար:

Մեր անկեղծ երախտագիտությունն ենք հայտնում Լատվիայի ֆինանսական հետախուզության ստորաբաժանմանը՝ վիրտուալ ակտիվների հետ կապված հարցերով Բալթյան երկրներ կատարած ուսումնական այցի համար էկոհամակարգի առաջնորդների բացահայտման և ընտրության մեջ իրենց կարևոր դերակատարման համար: Մենք նաև մեր երախտագիտությունն ենք հայտնում Լեհաստանի ֆինանսների նախարարությանը վերապատրաստման համար տարածքներ տրամադրելու նրանց շարունակական աջակցության համար: Բացի այդ, մենք խորապես երախտապարտ ենք տարբեր ոլորտների բազմաթիվ հաստատություններին և անհատներին, որոնց ներդրումը կարևոր դեր է խաղացել ծրագրի հաջող իրականացման համար:

ԵԱՀԿ-ի քարտուղարություն
ԵԱՀԿ-ի տնտեսական և
բնապահպանական գործունեության
համակարգողի գրասենյակ
Տնտեսական կառավարման բաժին
Ուոլներստրեսսի 6
1010 Վիեննա, Ավստրիա

Էլ. փոստ՝ virtualassets@osce.org
www.osce.org/eea

Organization for Security and
Co-operation in Europe