Kriptovalyutalarda konfidensiallıq və anonimlik problemləri

Yadigar İmamverdiyev[1], Firəngiz Sadiyeva[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*yadigar@iit.science.az*, [2]*sadiyeva.firengiz@gmail.com*

***Xülasə*— Məqalədə kriptovalyutalarda konfidensiallıq və anonimlik problemləri analiz edilir. Konfidensiallığın təmin edilməsi əksər kriptovalyutalarda əsas problemlərdən biridir və bunun üçün ilk növbədə tranzaksiya tərəflərinin anonimliyi təmin edilməlidir. Anonim kriptovalyutalarda istifadə edilən əsas mexanizmlərə baxılır, ölkələrin anonim kriptovalyutaların hüquqi tənzimlənməsi məsələlərinə yanaşmaları araşdırılır.**

***Açar sözlər*— Bitkoin; kriptovalyuta; anonimlik; gizlilik; konfidensiallıq; anonim kriptovalyuta**

I. GİRİŞ

Fərdin maliyyə ilə əlaqəli məlumatları olduqca sensitiv məlumatlardır və bədniyyətlilərin əsas hədəflərindən biridir. Bunu çoxsaylı fərdi məlumat insidentləri ilə bağlı kütləvi informasiya vasitələrində yer alan xəbərlər də təsdiqləyir. Son onilliyin ən perspektivli və inqilabi maliyyə texnologiyası olan Bitkoin və digər kriptovalyutalar fərdi maliyyə məlumatlarının konfidensiallığının etibarlı qorunması üçün müəyyən vədlər verir [1, 2]. Bitkoin və digər altkoinlərdə fərdi maliyyə məlumatlarının konfidensiallığının təmin edilməsi üçün istifadə edilən əsas yanaşma anonimlik mexanizmləridir [3].

Kriptovalyutaların əsas xarakteristikalarından biri anonimlik hesab olunur: tranzaksiyanı yerinə yetirmək üçün istifadəçidən öz fərdi məlumatlarını daxil etmək tələb edilmir. Belə ki, Bitkoin blokçeynində göndərənin və alanın adları və soyadları deyil, pulqabılarının rəqəmsal ünvanları və köçürülən məbləğ qeydə alınır. Qeyd edək ki, ilk və ən populyar kriptovalyutanın – Bitkoinin Satoşi Nakamoto təxəllüsü altında gizlənən yaradıcısının kimliyi hələ də məlum deyil [2].

Hazırda kriptovalyuta bazarının təxminən yarısına sahib olan Bitkoinin anonim olduğu iddia edilirdi, lakin tədqiqatlar göstərdi ki, əslində Bitkoin anonimliyi yox, psevdo-anonimliyi təmin edir [4]. Bitkoinin bu nöqsanını aradan qaldırmaq üçün təklif edilmiş bir sıra yeni kriptovalyutalar istifadəçilərin və tranzaksiya məlumatlarının anonimliyini daha yüksək səviyyədə qoruya bilər.

Lakin anonimliyin “tərs üzü” də vardır. Anonimlik bədniyyətlilərə müxtəlif cinayət əməllərini, o cümlədən çirkli pulların yuyulması, kibercinayətkarlıq, beynəlxalq terrorizmin dəstəklənməsini rahat şəkildə həyata keçirməyə və hüquq-mühafizə orqanları tərəfindən aşkarlanmaqdan yayınmağa imkan verir. Buna görə əksər dövlətlər anonim kriptovalyutaların istifadəsini tənzimləməyə cəhdlər edirlər.

Bu işin məqsədi kriptovalyutalarda istifadə edilən konfidensiallıq və anonimlik mexanizmlərini və texnologiyalarını, onların istifadəçilərə verdiyi imkanları və cəmiyyətin təhlükəsizliyinə gətirdiyi problemləri analiz etməkdir.

II. KRİPTOVALYUTALARDA ANONİMLİK NƏ ÜÇÜN LAZIMDIR?

Biznes üçün maliyyə əməliyyatlarının konfidensiallığı və sürəti çox vacibdir. Böyük kriptovalyutalar bu məsələlərin öhdəsindən həmişə gələ bilmir. Mütəxəssislərə görə əksər kriptovalyutaların əsas problemi konfidensiallığın olmamasıdır.

Ödənişlər edilən zaman anonimliyin olmaması biznesə zərər gətirə bilər. Fiat pulları istifadə edilən zaman təşkilatın maliyyə hesabatlarına yalnız vergi xidməti giriş əldə edə bilər, lakin Bitkoin blokçeynində verilənlər bütün istifadəçilərə, o cümlədən rəqiblərə və bədniyyətlilərə əlyetər olur və blokçeyndə baş verən tranzaksiyaları analiz etmək olar. Məsələn, tutaq ki, Bob Alisə 10 BTC hədiyyə edib. Bu zaman o, Alisin pulqabısının ünvanını bilir və Blockchain Explorer-də Alisin maliyyə əməliyyatları haqqında informasiyanı tapa bilər. Alisin tranzaksiyalarının tarixçəsinə görə onun neçə Bitkoinin olduğunu və onları nəyə xərclədiyini öyrənmək olar.

Beləliklə, kriptovalyutalarda maliyyə konfidensiallığı olmadıqda rəqiblər şirkətin kiminlə və hansı qiymətə müqavilələr bağladığını, əməkdaşlara nə qədər ödədiyini izləyə bilərlər. Mütəxəssislərə görə, kriptovalyutalarda konfidensiallığı təmin etmək üçün ilk növbədə onların anonimliyi təmin edilməlidir.

Ənənəvi bankçılıq modeli konfidensiallıq səviyyəsini iştirak edən tərəflərə və etibarlı üçüncü tərəfə məlumatların əldə olunmasını məhdudlaşdırmaq üsulu ilə yüksəldir. Bitkoin blokçeynində isə bütün əməliyyatları şəffaf etmək zərurəti bu ənənəvi üsulu açıq şəkildə pozur. Ancaq məlumat ictimaiyyətə açıq olduğu halda da, Bitkoin sistemi onun konfidensiallığını qoruya bilər. Belə ki, ictimaiyyət bir istifadəçinin müəyyən bir məbləği digər istifadəçiyə göndərdiyini görür, ancaq bu isitfadəçilərin kimliyi ilə bağlı məlumat əldə edə bilmir.

III. BİTKOİNİN ANONİMLİK MEXANİZMİ

Ənənəvi maliyyə sistemlərində tranzaksiyaların həyata keçirilməsi üçün istifadəçilərin adlarından istifadə olunur, lakin Bitkoində psevdo-adlardan istifadə olunur.

DOI: 10.25045/NCInfoSec.2019.14

Bitkion şəbəkəsində anonimliyi təmin etmək üçün Bitkoin pulqabılarının rəqəmsal ünvanları istifadə edilir. Bitkoin şəbəkəsində pulqabı dedikdə fayl sistemində bir fayl nəzərdə tutulur. Pulqabıda açıq və gizli açar cütü və yerinə yetirilmiş tranzaksiyalar qeyd olunur. Açarlardan Bitkoinin göndərilməsi və qəbul edilməsi üçün istifadə edilir. Açıq açarı Bitkoinləri qəbul edən şəxs imzanın təsdiqlənməsi üçün, gizli açarı isə Bitkoinləri göndərən şəxs imzalamaq üçün istifadə edir. Bitkoin pulqabısında hər bir Bitkoin ünvanlarına uyğun giriş və çıxışlar saxlanılır [3,4].

Bitkoin ünvanı onun istifadəçisi tərəfindən yaradılan asimmetrik açar cütlüyünün açıq açarından əldə edilmiş bir hərf-ədəd sətrindən ibarətdir. Hər bir istifadəçi pulqabısında bir neçə açar cütü (ünvan) saxlaya bilər və buna görə də anonimlik səviyyəsini artırmaq üçün hər bir tranzaksiya görə yeni bir ünvandan istifadə etmək tövsiyə olunur.

Beləliklə, Bitkoin şəbəkəsində anonimliyi təmin etmək üçün görülən yeganə iş ünvanların psevdo-adlarından istifadə edərək açıq açarları anonim saxlamaqdır. Psevdo-adlar Bitkoin tranzaksiyalarında istifadə edildiyi üçün ümumi təəssürat yaranır ki, bu adlar Bitkoinin anonimliyini təmin edir. Lakin bir sıra mütəxəssislər açıq şəkildə bəyan edirlər ki, Bitkoin anonim deyil və “dünyadakı ən şəffaf ödəmə şəbəkəsi olduğu ehtimal olunur” [3].

Bitkoində qrup identifikasiyası "ünvanların dəyişilməsi" (ing. change addresses) anlayışından istifadə edən dəyişiklik evristikasını tətbiq etməklə istifadəçilərin anonimliyini artıra bilər, lakin tam təmin edə bilməz. Klasterləri xarici mənbələrdə: məsələn, ictimaiyyətə açıq olan blockchain.info, walletexplorer.org kimi xüsusi saytlarda məlumatlar ilə korrelyasiya etdikdə bütün Bitkoin tranzaksiya şəbəkəsinin böyük hissəsini deanonimləşdirmək mümkün olur.

[4]-də Harrigan və Fretter belə bir nəticəyə gəlirlər ki, Bitkoin şəbəkəsindəki ünvanların qruplaşdırılmasının effektiv olmasının səbəbi müəyyən edilmiş ünvanların təkrar istifadəsi və superklasterlərin artmasıdır (məsələn, birjalar, qumar oyunları saytları, qara bazar saytları) [5].

Hər bir tranzaksiya üçün yeni açar cütünün istifadə olunması təhlükəsizliyi artırır. Bəzi hallarda çox girişli tranzaksiyalar həyata keçirilir ki, bu tranzaksiyaların girişləri eyni sahibə məxsus olur. Bu halda bir açarın sahibi aşkar edildikdə, bu açar eyni sahibə məxsus olan digər tranzaksiyaları aşkar edə bilər.

Bitkoinin istifadəçilərini ünvan təkrar istifadə etdikdə və ya birjada verifikasiyadan keçdikdən sonra de-anonimləşdirmək olar. Anonim kriptovalyutalarda isə belə hal mümkün deyil. Onların istifadə etdikləri kriptoqrafik protokollar həmin şəbəkədəki verilənlərin analizini çətinləşdirir. Anonim kriptovalyutanın pulqabı ünvanını yalnız onun sahibi açа bilər.

IV. KRİPTOVALYUTALARDA ANONİMLİK TEXNOLOGİYALARI

Bu bölmədə blokçeyndə saxlanılan tranzaksiyaların miqdarını, göndərən və alanın anonimliyini təmin etmək üçün bəzi texnologiyalara baxılır.

Bu texnoloji həllərə misal olaraq birdəfəlik istifadə ödəniş ünvanları (One-time Use Payment Addresses), gizli ünvanlar (Stealth adresses), qarışdırma (Mixing), CoinJoin, sıfır bilik verməklə isbat (Zero-Knowledge Proofs), zk-SNARKs, Pedersen etibarnamələri (Pedersen Commitments) və halqa imzalarını (Ring Signatures) göstərmək olar.

One-time Use Payment Address – eyni ödəmə ünvanını təkrar istifadə etdikdə, müşahidəçi göndərənin və alanın tranzaksiyalarını izləyə bilir. Yeganə çıxış yolu ünvanı təkrar istifadə etməməkdir. “Birdəfəlik istifadə ödəniş ünvanları” yanaşmasını istifadə etdikdə göndərən hər tranzaksiya üçün yeni bir ünvan yaradır. Yeni ünvan blokçeyndə daha öncə qeyd olunmadığı üçün, müşahidəçinin tranzaksiya axınını izləməsi çox çətin olur. Birdəfəlik istifadə ödəniş ünvanı həm depozitə qoyulan, həm də çıxarılan tranzaksiyaların hər ikisi ilə birbaşa əlaqəlidir.

Stealth Address – Hər yeni ünvan alıcı tərəfindən yaradılmalı və göndərənə çatdırılmalıdır. Alan şəxs hər dəfə yeni e-poçt istifadə etmək üçün bunun vacib olması səbəbini və tranzaksiyanı qəbul etmək üçün hansı ünvandan istifadə edəcəyini göndərən şəxsə bildirməlidir. Stealth ünvanlar göndərənin yeni birdəfəlik istifadə ödəniş ünvanları yaratmasına icazə verməklə bu problemi aradan qaldırır.

Mixing – Ünvandan tranzaksiyaların axınını izləmək çox sadədir. Birdəfəlik istifadə ödəniş ünvanlarından fərqli olaraq Mixing xidməti bu problemi həll edə bilir.

Bitkoin istifadəçiləri bir çox istifadəçidən Bitkoin alan, bunları birlikdə qarışdırıb fərqli vaxtda fərqli ünvanlara göndərən Bitkoin Fog və BitMixer kimi qarışdırma xidmətlərindən (Tumbler də deyilir) istifadə etməklə tranzaksiyaları və daha kiçik miqdarlara bölərək tranzaksiya axınını izləməyi aradan qaldıra bilər. Bunlar bir çox istifadəçinin pulunu digərinə göndərməzdən əvvəl bir müddət nəzarətdə saxlayan və bir-birinə qarışdıran üçüncü tərəf xidmətləridir.

CoinJoin – Mixing xidmətinin zəif tərəfi etibarlı üçüncü tərəf daxil etməsidir. CoinJoin üçüncü tərəf tələbini aradan qaldırmağa çalışan qarışdırma üsuludur. CoinJoin tək bir tranzaksiyanın birdən çox giriş və çıxışlara malik olması xüsusiyyətindən istifadə edir.

Valyutaları tələb olunduğu kimi qarışdırmaq üçün etibarlı üçüncü tərəfə ehtiyac yoxdur. Lakin CoinJoin tranzaksiyasında iştirak edən bütün tərəflər bu tranzaksiyanı imzalamaq üçün bir-birləri ilə əlaqə qurmalıdır. Bu koordinasiya bir çox səbəbdən çətin yerinə yetirilir. Birincisi, istənilən vaxt CoinJoin tranzaksiyasına yetərincə insan qoşulmaya bilər. İkincisi, CoinJoin tranzaksiyasında iştirak edən hər kəs kimin iştirak etdiyini və bu tranzaksiyanın necə qarışdırılacağını bilir.

CoinShuffle – CoinJoin tranzaksiyasında iştirak edən bütün tərəflərin üçüncü tərəf olmadan tranzaksiyalar yarada biləcəyi və heç bir tərəfin sahib olmadığı mərkəzləşdirilməmiş tranzaksiyaların aparılmasına icazə vermək üçün tövsiyə olunan bir üsuldur.

Zero-Knowledge Proofs – sabit paroldan istifadə edən protokolların çatışmayan cəhəti isbat edən (P) tərəfin öz parolunu yoxlayan (V) tərəfə verməsidir. “Sorğu-cavab” tipli protokollar bu nöqsanı aradan qaldırır. Onları həyata keçirən zaman P V-nin zamana görə dəyişən sorğularına cavab verir və V-yə onun adından çıxış edə biləcək informasiya vermir. Bununla belə P öz sirri barəsində qismən məlumat verə bilər. Bu problemi sıfır bilik verməklə isbat protokolları həll edə bilər [6].

Pedersen etibarnamələri – etibarnamələr verilənlərin bir hissəsini gizli saxlayan, lakin onların kriptoqrafik heş kodlarını elan edərək etibarlılığını (commit) təmin edən kriptoqrafik mexanizmlərdir. Verilənlərin ölçüsü çox kiçik olduqda (məsələn, 1 ədəd), onda kobud güc axtarışının köməyi ilə görünən verilənlərin riskini minimuma endirmək üçün örtük faktoru əlavə edilir.

Confidential Transaction-lar Pedersen etibarlılığından Bitkoin tranzaksiyalarının köçürülməsi zamanı miqdarın gizli saxlanması üçün bir vasitə kimi istifadə edir. Bu fikir ilk dəfə 2013-cü ildə Adam Back tərəfindən irəli sürülmüşdür.

Halqa imzaları – Standart bir rəqəmsal imzanı təsdiqləmək üçün yoxlayan imza yaratmaq üçün hansı açıq açarın istifadə edildiyini bilməlidir, bu səbəbdən ünvandan -ünvana vəsait axınını izləmək mümkün olur. Halqa imzalar 2001-ci ildə R. L. Rivest, A. Şamir və Y. Tauman tərəfindən kəşf edilmişdir.

Halqa imzaları imza yaradanın öz açarını və onun tərəfindən seçilmiş bir neçə açıq açarı (bu açıq açar sahiblərinin razılığı və iştirakı tələb olunmur) özündə birləşdirən açarlar qrupundan istifadə etməklə yaradılır. Üçüncü tərəf nəticədəki imzanın qrupdakı açarlardan biri istifadə olunaraq yaradıldığını yoxlaya bilər, lakin qrupdakı hansı açarın imzalayana aid olduğunu müəyyən etmək mümkün deyil. Bu? açıq açarlardan istifadə edərək bir halqa tənliyini qurmaqla həll edilir, burada bir hesablamanın çıxışı digərinin girişinə çevrilir. Gizli açarlardan birini bilən şəxs (z) halqa tənliyinin son çıxışının ilkin girişi olan (v)-ə bərabər olmasını təmin edir.

Blokçeyndə göndərənin naməlum olduğu əməliyyatları təsdiqləmək üçün halqa imzaları istifadə edilə bilər.

Gizli ünvanlar yalnız alıcının konfidensiallığını və gizliliyini təmin edir. Pedersen etibarlılığı yalnız tranzaksiyaların miqdarının konfidensiallığını və gizliliyini təmin edir. Halqa imzaları yalnız göndərənin konfidensiallığını və gizliliyini məhdud şəkildə qoruyur. Zk-SNARKs isə alanın deyil, göndərən və miqdarın konfidensiallığını və gizliliyini təmin edir [7].

MimbleWimble protokolu tranzaksiyaları izləmək üçün elliptik əyrilər metodunu, həmçinin Confidential Transactions və CoinJoin mexanizmlərini istifadə edir. Confidential Transactions ödəniş ünvanlarını və həcmini gizlədir, CoinJoin isə tranzaksiya girişlərini və çıxışlarını qarışdırmaqla bir neçə tranzaksiyanı birləşdirir.

Mimble Wimble-də ənənəvi ünvanlar yoxdur, onların əvəzinə pulqabıları bir-biri ilə verilənləri mübadilə edirlər. Bu zaman MimbleWimble blokçeynində tranzaksiyaların tarixçəsi saxlanılmır. Orada sahiblər və pulların vəziyyəti haqqında məlumat yazılır. Beam yaradıcılarının qiymətləndirilməsinə görə belə blokçeynlər Bitkoin blokçeynindən ən azı üç dəfə kiçik olacaq.

V. ANONİM KRİPTOVALYUTALAR

Bəzi kriptovalyutalar rahat ödəniş və ya sürətli tranzaksiyalara, bəziləri isə istifadəçilər üçün anonimlik təmin etməyə daha çox diqqət yetirirlər.

Ümumiyyətlə, anonim kriptovalyutalarda aşağıdakı xüsusiyyətləri təmin etmək tələb olunur.

- *Gizlilik:* Bütün tranzaksiyaların hansı ünvandan gəldiyi, hansı ünvana göndərildiyi və miqdarının rəqiblər tərəfindən müşahidə edilməməsi təmin edilir.
- *İzlənilməzlik:* Göndərilən və ya alınan valyutaların izlənilməməsi və tranzaksiya tarixi ilə arasındakı əlaqənin aşkarlana bilməməsi təmin edilir.
- *Dəyişkənlik:* Bütün valyutaların cüt şəkildə bir-birindən ayrılmaz olması və nəticədə bir-birilərini əvəz edə bilməsi təmin edilir.

İlk anonim kriptovalyuta Bytecoin 2012-ci ildə buraxılmışdır. Həmin vaxtdan xeyli belə kriptovalyuta meydana çıxmışdı, onlardan Monero, Dash, PIVX, Verge və Zcash populyarlıq qazanıb.

Monero – CryptoNote istifadə edən Bytecoin əsasında hazırlanmışdır və tranzaksiyaların detallarını görmək üçün açıq açarı paylamağa imkan verir.

Konfidensiallığı təmin etmək üçün Monero halqa imzaları və gizli ünvanları istifadə edir, onlar sikkələri, tranzaksiyaların həcmlərini və onların ünvanlarını gizlədirlər. Moneronun nöqsanı – tranzaksiyanın ölçüsünün böyük olması və miqyaslanma problemləridir. Bir tranzaksiya hesabında Monero blokçeyni Bitkoin blokçeynindən beş dəfə böyükdür.

2017-ci ildə Monero kodunda aşkarlanmış boşluqlar sayəsində tədqiqatçılar real tranzaksiyaları saxtalardan ayırmağa nail olmuşdular.

Dash – Bitkoində olan bəzi problemləri həll edir. Bitkoin bərabərhüquqlu birranqlı şəbəkə olduğu halda, Dash ikiranqlı arxitektura ilə işləyir. Birinci səviyyədə Bitkoin kimi mayninq vasitəsilə valyutalar buraxılır və yeni bloklar blokçeynə yazılır, ikinci səviyyədə isə əsas qovşaqlar, yəni Masternodlar yerləşir. Dash anonim kriptovalyutasında PrivateSend mexanizmi istifadə edilir, o bir neçə istifadəçinin pullarını qarışdırır və onları bir tranzaksiyada birləşdirir. Qarışdırma Masternodlarda baş verir, qarışdırmadan sonra alanı və göndərəni izləmək praktiki olaraq mümkün deyil, lakin onlar barədə informasiya Masternodlarda qalır. Bu səbəbdən Dash-ı tamamilə konfidensial kriptovalyuta hesab etmək olmaz. Bundan başqa, Dash Bitkoin-dən daha az təsdiqləmə vaxtı ilə ikiqat xərcləmə (ing.double spending) problemini həll edən InstantSend adlı sürətli tranzaksiya təqdim edir.

PIVX – əvvəllər Darknet kimi tanınan PIVX (Private Instant Verified Transaction) gizli ani yoxlanmış tranzaksiyalar mənasını verir. PIVX Dash-ın bir forkudur, yəni özünün texniki əlamətlərini, sürətli tranzaksiya yerinə yetirə bilmək bacarığını və əsas qovşaqlarını Dash-dan götürmüşdür. Lakin Dash-dan fərqli olaraq PIVX PoW (Proof of Work) istifadə edən maynerlər yox, tranzaksiyaları təsdiqləmək üçün əsas qovşaqlar istifadə edən PoS (Proof of Stake) konsensus alqoritmindən istifadə edir.

Verge – əvvəllər DogeCoinDark olaraq tanınırdı. Anonimlik təmin etmək üçün əlavə kriptoqrafik metodlar istifadə etmək əvəzinə, göndərən və alanın IP ünvanlarını və coğrafi yerlərini gizlətmək üçün Tor və I2P-nin inteqrasiyasına əsaslanır. Verge-nin Bitkoin əsasında olmasına baxmayaraq, əməliyyatlarda kriptoqrafik metodlardan istifadə etmir. Buna görə də blokçeyndəki tranzaksiyalar şəffafdır.

Zcash – kriptovalyutada sıfır bilik verməklə isbat protokolu zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) istifadə edilir. Zcash-də anonim tranzaksiyaları yalnız şifrlənmiş z-ünvanlarından həyata keçirmək olar, onlar blokçeyndə görünmür. Belə tranzaksiyalar ediləndə vəsaitlər yandırılır və yeni sikkələrə mübadilə edilir. zk-SNARKs – sıfır bilik verməklə isbatın yeni formasıdır və Zcash bu alqoritmin ilk geniş yayılmış tətbiqidir.

Zcash-ın nöqsanları zk-SNARKs texnologiyasının mürəkkəbliyi və etibarlı quraşdırma (trusted setup) tələbinin olmasıdır. Zcash yaradıcıları zk-SNARKs-ın başlanğıc parametrləri üçün təsadüfi parametrlər istifadə edirlər. Bu parametrlər bədniyyətlilərin əlinə düşsə, şəbəkədə verilənləri saxtalaşdıra bilər. Bundan başqa, Zcash blokçeynində bir tranzaksiya Bitkoin blokçeynindən səkkiz dəfə böyükdür.

Zcash-da anonimlik istəyə bağlıdır və ekranlaşdırılmış tranzaksiyaları həyata keçirmək üçün həm göndərən, həm də alandan şəffaf ünvanlar əvəzinə ekranlaşdırılmış (ing. shielded) ünvanlardan istifadə etmək tələb olunur. Zcash valyutaların orta hesabla təxminən 6.3%-i ekranlaşdırılmış ünvanlardan istifadə etdikləri müşahidə edilib [8,9].

VI. ANONİM KRİPTOVALYUTALARIN HÜQUQİ TƏNZİMLƏNMƏSİ MƏSƏLƏLƏRİ

Anonimlik – istifadəçinin öz tranzaksiyalarının gizliyinin saxlanmasına olan şərtsiz hüququ kimi başa düşülür. Bununla yanaşı, anonimlik pulların yuyulması və digər kriminal sxemlərinin hissəsi kimi qanunsuz hesab olunur. Belə hallara çoxsaylı misallar vardır.

Bitkoin ilk illərində narkotik tacirlərinin əsas valyutasına çevrilmişdi. Bunun səbəbi qanunsuz mallarla anonim ticarət platforması olan Silk Road veb saytı idi, sayt 2011-ci ildən fəaliyyət göstərirdi. Onun sahibi 2013-cü ildə həbs edilmiş və ömürlük həbsə məhkum edilmişdi. 2012-2013-cü illərdə saytda 1,2 milyon dollarlıq alqı-satqı edilmişdi, ümumi məbləğ 9,5 milyon bitkoin təşkil etmişdi. Alqı-satqıdan gələn komissiya haqqı sayəsində Silk Road təxminən 600 min bitkoin qazanmışdı [10].

Silk Road pulqabısı – alıcılar, satıcılar və bu tranzaksiyalar haqqında öyrənmək istəyən üçüncü tərəflər arasında yüksək səviyyədə bir anonimlik təmin etməyə yönəlmişdi. O, "Tor brauzer paketi" kimi nisbətən asan istifadə olunan brauzer interfeysinin yaranması ilə mümkün olan bir neçə anonim şəbəkədən biri idi [10].

Dövlətlərin bir çoxunda kriptovalyutalarla həyata keçirilən daxili alış-veriş üçün ciddi KYC (Know your customer) – müştərini tanıma prosesi tətbiq olunur və kriptovalyuta istifadə etmək üçün qeydiyyatdan keçən istifadəçilərin fərdi məlumatları tələb olunur.

Dövlətlər anonim kriptovalyutaların tranzaksiyalarını izləyə bilmirlər və buna görə anonim kriptovalyutalara mənfi yanaşırlar, bəzən onları tamamilə qadağan edirlər. Məsələn, 2018-ci ildə Cənubi Koreyada anonim kriptotreydinq, Yaponiyada isə kriptovalyutaların özü qadağan edilmişdir. Lakin belə qadağaların effektivliyi birqiymətli deyil.

Bəzi mütəxəssislər buna mane olmağın mümkün olmadığını söyləyirlər. Yaponiya vətəndaşları anonim altkoinləri yapon kriptovalyuta birjalarında deyil, digər meydançalarda əldə edə bilərlər.

ABŞ güc strukturları açıq blokçeynli kriptovalyutalar (o cümlədən Bitkoin və Ethereum) istifadə etməklə qanunsuz maliyyə fəaliyyətinin monitorinqində uğurlar qazanıblar. Lakin anonim kriptovalyutaların blokçeynlərində edilmiş tranzaksiyalar xeyli yüksək konfidensiallıq səviyyəsinə malikdir. ABŞ Milli Təhlükəsizlik Nazirliyi qeyri-qanuni pul köçürmələrini aşkarlamaq məqsədi ilə anonim kriptovalyuta blokçeynlərində tranzaksiyaların izlənməsi texnologiyasını işləməyi planlaşdırır.

Ödəniş iştirakçılarını identifikasiya etmək üçün yeni analitika vasitələri işləmək lazımdır. Daha bir istiqamət-anonim rəqəmsal aktivlərin istifadəsi ilə əlaqədar problemlərin həllinə yönəlmiş qanunvericilik tədbirlərinin işlənməsi tövsiyə olunur.

NƏTİCƏ

Anonim kriptovalyutalar maliyyə əməliyyatlarının gizliliyini və konfidensiallığını qiymətləndirən hər bir kəsə (biznesə – tranzaksiyalar haqqında həssas informasiyanı, şəxslərə – şəxsi həyatın toxunulmazlığını təmin etmək üçün) lazımdır. Lakin kriptovalyutaların anonimliyi kibercinayətkarlıqla mübarizəni xeyli çətinləşdirir. Anonim kriptovalyutaların dələduzluq, Darknet-də ödənişlər üçün istifadəsi halları onların cəmiyyətdə nüfuzuna xələl gətirir. Lakin anonim kriptovalyutalardan cinayətkarlar istifadə edə bilsələr də, onların əsas məqsədləri fərdi məlumatların mühafizəsidir.

İSTİNADLAR

[1] Y. Imamverdiyev “Blokçeyn texnologiyaları: komponentləri, tətbiqləri və problemləri”, İnformasiya cəmiyyəti problemləri, 2019, №2, s. 18–32.

[2] Y. Imamverdiyev, F. Sadiyeva, “Kriptovalyuta verilənlərinin intellektual analizi məsələləri,” İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri IV respublika konfransı, s. 47-53, 2018.

[3] M. C. K. Khalilov and A. Levi “A survey on anonymity and privacy in bitkoin-like digital cash systems”, IEEE Communications Surveys & Tutorials, 20(3), pp. 2543-2585, 2018.

[4] M. Harrigan and C.Fretter, “The unreasonable effectiveness of address clustering”, Conferences on Ubiquitous Intelligence & Computing, pp. 368-373, 2016.

[5] M. Paquet-Clouston, B. Haslhofer and B. Dupont, “Ransomware payments in the bitkoin ecosystem”, Journal of Cybersecurity, 5(1), tyz003, 2019.

[6] J. H. Lee, “Rise of anonymous cryptocurrencies”, Brief Introduction. IEEE Consumer Electronics Magazine, 8(5), 20-25, 2019.

[7] D. Yang, J. Gavigan and Z. Wilcox-O’Hearn “Survey of confidentiality and privacy preserving technologies for blockchains”, R3, Zcash Company, Res. Rep, 2016.

[8] D. Hopwood, S. Bowe, T. Hornby and N. Wilcox, "Zcash protocol specification (version 2018.0-beta-9)", 2018.

[9] P. Dikshit, and S. Kunwar, “Efficient weighted threshold ECDSA for securing Bitkoin wallet,” Asia security and Privacy (ISEASP), pp 1-9, 2017.

[10] L. J. Trautman “Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?,” Richmond Journal of Law and Technology, 20(4). 2014.

PRIVACY AND ANONIMITY ISSUES IN CRYPTOCURRENCIES

Yadigar Imamverdiyev[1], Firangiz Sadiyeva[2]

[1, 2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]yadigar@iit.science.az, [2]sadiyeva.firengiz@gmail.com

Abstract – The paper analyzes privacy and anonymity issues in cryptocurrencies. Confidentiality is one of the main issues in most cryptocurrencies, and for that, the anonymity of the transaction participants must be ensured. The main mechanisms used in anonymous cryptocurrencies are reviewed, and countries' approaches to the legal regulation of anonymous cryptocurrencies are being investigated.

Keywords *– Bitcoin; cryptocurrency; anonymity; Privacy, confidentiality; anonymous cryptocurrency*