Fərdi məlumatların mühafizəsi üçün blokçeyn texnologiyaları: imkanları və perspektivləri

Yadigar İmamverdiyev[1], Günay Muradova[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*yadigar@iit.science.az*, [2]*gmuradova9@gmail.com*

***Xülasə*— Məqalədə blokçeyn texnologiyalarının fərdi məlumatların mühafizəsində istifadəsi imkanlarının araşdırılmasına baxılır. Blokçeyn texnologiyasının qısa xarakteristikası verilmiş və mövcud araşdırmaların qısa analizi aparılmışdır. Blokçeyn texnologiyası ilə fərdi məlumatların təhlükəsizliyinin təmin edilməsi imkanları və yarana biləcək problemlər analiz edilmişdir.**

Açar sözlər — fərdi məlumatlar; blokçeyn; gizlilik, gizliliyin qorunması, GDPR

I. GİRİŞ

Big Data dövründə fərdi məlumatlar davamlı olaraq toplanır və analiz edilir, bu da innovasiyalara və iqtisadi inkişafa səbəb olur. Şirkətlər və təşkilatlar topladıqları məlumatları xidmətləri fərdiləşdirmək, korporativ qərar qəbuletmə prosesini optimallaşdırmaq, gələcək tendensiyaları proqnozlaşdırmaq və daha bir çox digər məqsədlər üçün istifadə edirlər. [1]

Lakin məlumatların sürətlə artdığı və əlçatan olduğu bir dövrdə fərdi məlumatlar böyük təhlükələr altına düşür. Fərdi məlumatların qeyri-qanuni istifadə olunması hallarına çox təsadüf olunur. Fərdi məlumatlar bir çox hallarda onların sahiblərinin razılığı olmadan toplanır, bu məlumatların digər məqsədlər üçün istifadəsi üçün həmin şəxslərdən icazə alınmır. Smart cihazlardan və sosial şəbəkələrdən istifadə fərdi məlumatların qorunmasını bir qədər də çətinləşdirir.

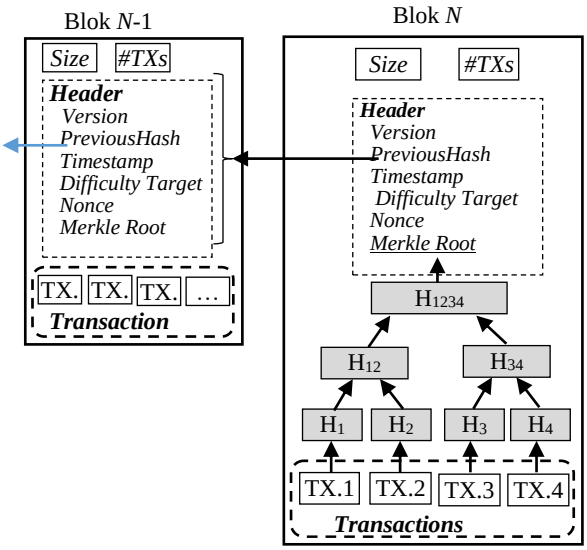
Belə şəraitdə fərdi məlumatların konfidensiallığını dəstəkləyən texnoloji alətlərin yaradılması olduqca zəruridir. İnformasiya təhlükəsizliyi üzrə tədqiqatçılar fərdi məlumatlara yönəlmiş təhdidlərə qarşı müxtəlif üsullar hazırlamışlar. Anonimləşdirmə, kriptoqrafik üsullar ilə fərdi məlumatları qorumağa çalışırlar, lakin onlar hazırda praktikada geniş istifadə olunmaq üçün yetərli deyil [1].

Son illərdə yeni rəqəmsal reyestr sistemləri ortaya çıxmışdır [2]. Blokçeyn texnologiyası və ya paylanmış reyestr texnologiyası Bitkoinin yaradılması anından – 2009-cu ildən məlumdur. Bitkoin blokçeyn texnologiyası ilə işləyən ilk rəqəmsal kriptovalyuta hesab edilir. Bu sistem istifadəçilərə bitkoinləri mərkəzləşdirilmiş tənzimləyici olmadan icma tərəfindən təsdiqlənən blokçeyn texnologiyasından istifadə edərək təhlükəsiz şəkildə ötürməyə imkan verir. Blokçeynin təhlükəsiz, şəffaf, anonim olması və verilənlərin tamlığını üçüncü tərəf olmadan həyata keçirməsi onun populyarlığının artmasına səbəb oldu. Bitkoin timsalında bir neçə il ərzində praktiki olaraq fasiləsiz həyata keçirilməsi onun digər sahələrə tətbiqi məsələsini ortaya çıxardı.

Hazırda blokçeyn texnologiyasının bir çox sahələrdə tətbiqi üzrə pilot layihələr həyata keçirilir. Anonimliyi və konfidensiallığı müxtəlif dərəcədə dəstəkləyən xüsusi protokollardan istifadə etməklə blokçeyn texnologiyası tibbi, maliyyə və digər sahələrdə fərdi məlumatların mühafizəsini təmin edə bilər. Bu məqsədlə təqdim olunan işdə fərdi məlumatların mühafizəsi üçün blokçeyn texnologiyalarının imkanları, perspektivləri və problemləri analiz edilir.

II. BLOKÇEYN TEXNOLOGİYALARININ QISA XARAKTERİSTİKASI

Texniki baxımdan, adından da göründüyü kimi, blokçeyn (“block” – blok + “chain” – zəncir) informasiya bloklarının zənciridir. Şəkil 1-də Bitkoin blokçeyninin strukturu təsvir olunur.



Şəkil 1. Bitkoin blokçeyninin strukturu

Şəkildə göstərildiyi kimi, hər bir Bitkoin bloku dörd komponentdən ibarətdir: blokun ölçüsü (*Size*), tranzaksiya sayğacı (*#TXs*), blokun başlığı (*Header*) və tranzaksiyalar (*Tranzactions*). Blokun ölçüsü və tranzaksiya sayğacı, uyğun olaraq, blokdakı baytların və tranzaksiyaların saylarını göstərir. Tranzaksiyalar – bloka daxil olan tranzaksiyaların siyahısıdır. Blok başlığına altı sahə daxildir:

DOI: 10.25045/NCInfoSec.2019.45

- *Version* – versiya nömrəsi (konsensus protokolunun yenilənməsini izləmək üçün istifadə edilir);
- *PreviousHash* – *zəncirdə* bilavasitə əvvəl gələn blokun heşi;
- *Timestamp* – blokun yaradılması tarixi;
- *Target* – hədəf *qiyməti*, mayninq prosesində bu qiymətdən kiçik olan heş axtarılır;
- *Nonce* – *mayninq* alqoritmində istifadə edilən sayğac;
- *Merkle Root* – bloka daxil olan bütün tranzaksiyaların heşləri əsasında yaradılan binar ağacdır.

Blokçeyn texnogiyası üç addım ilə həyata keçirilir: 1) Tranzaksiyanın yaradılması; 2) Tranzaksiyanın təsdiqlənməsi; 3) Blokun zəncirə əlavə edilməsi.

III. BLOKÇEYNİN NÖVLƏRİ

Tədqiqatçılar blokçeyn texnologiyalarını “Blockchain 1.0” (kriptovalyutalar), “Blockchain 2.0” (ağıllı müqavilələr), “Blockchain 3.0” (dövlət idarəçiliyi, təhsil, elm, mədəniyyət və s. sahələrdə tətbiqlər) kimi inkişaf mərhələlərinə ayırırlar.

Blokçeynin digər sahələrdə tətbiqi cəhdləri onun yeni növlərinin meydana çıxmasına gətirib çıxardı. Mütəxəssislər blokçeyn verilənlərinə girişlə əlaqədar olaraq blokçeynləri *açıq* (ing. public) və *özəl* (ing. private) olmaqla iki sinfə bölməyi tövsiyə edirlər [2].

Blokçeynlər tranzaksiyaları emal etməyə, yəni tranzaksiyaların yeni bloklarını yaratmağa qoyulan məhdudiyyətdən asılı olaraq *inkluziv* (ing. permissionless) və *ekskluziv* (ing. permissioned) blokçeynlərə bölünürlər. İnkluziv blokçeyndə istənilən qovşaq tranzaksiyaların yeni blokunu yarada bilər. Ekskluziv blokçeyndə isə tranzaksiyaların emalını yalnız seçilmiş qovşaqlar həyata keçirə bilərlər.

Ethereum platformasının sahibi Vitalik Buterin 2015-ci ildə şirkət bloqunda nəşr etdiyi məqalədə blokçeynləri 3 sinif üzrə təsnif edir [9]:

- *açıq blokçeyn* (ing. public blockchain) – tamamilə açıq blokçeyndir, tranzaksiyalar azad şəkildə həyata keçirilir və onlara heç kim nəzarət etmir, hər bir kəs konsensus prosedurunda iştirak edə bilər;
- *konsorsium blokçeyni* (ing. consortium blockchains) – konsensus proseduruna seçilmiş qovşaqlar nəzarət edir;
- *özəl blokçeyn* (ing. fully private blockchain) – mərkəzi orqan bütün tranzaksiyaları izləyir və nəzarət edir.

Böyük Britaniya hökumətinin baş elmi məsləhətçisi ser Mark Walport da oxşar təsnifat təklif edir [2]. O, paylanmış reyestrlər və onların dövlət idarəetməsində potensialı mövzusundakı məruzəsində blokçeynləri aşağıdakı 3 sinfə bölür:

- *inkluziv reyestrlər* (ing. permissionless public ledgers) – burada tranzaksiyaları təsdiqləyən mərkəzi orqan yoxdur. Bitcoin və Ethereum belə reyestrlərə misaldır;
- *ekskluziv açıq reyestrlər* (ing. permissioned public ledgers) – burada tranzaksiyaları müəyyən subyektlər təsdiqləyir. Bunlar idarəedici orqan, səlahiyyətli əməkdaş, müəssisə və s. ola bilər. İstifadəçilər verilənlərə baxa bilərlər (xüsusilə vacib informasiya gizli saxlana bilər);
- *ekskluziv özəl reyestrlər* (ing. permissioned private ledgers) – əvvəlki növə oxşayır, fərq ondadır ki, verilənlər hamıya açıq deyil.

Hibrid blokçeyn. Açıq və özəl blokçeynlər arasında bir balansdır, onu «qismən demərkəzləşmiş» və ya «konsorsium blokçeyni» də adlandırırlar. Məsələn, on sənaye təşkilatının konsorsiumunda hər bir təşkilat blokçeyn şəbəkəsində özünün mayninq/yoxlama qovşağını dəstəkləyir. Bu halda blok ən azı yeddi qovşaq tərəfindən imzalandıqda həqiqi ola bilər. Bütün qovşaqların blokçeyndən oxumaq üçün açıq girişi ola bilər və ya bu yalnız konkret qovşaqlara məhdudlaşdırıla bilər [9]. Lakin demərkəzləşmənin azalması səbəbindən blokçeyn yazılarının saxtalaşdırılması ehtimalı var [2].

IV. GDPR VƏ BLOKÇEYN: ZİDDİYYƏTLƏR

Avropa İttifaqının Verilənlərin Mühafizəsi haqqında Ümumi Qanunu (General Data Protection Regulation, GDPR) 25 may 2018-ci ildən qüvvəyə minmişdir. GDPR istifadəçilərə öz fərdi məlumatları üzərində nəzarət imkanı verməyə yönəlib. Vətəndaşlara öz fərdi məlumatlarına baxmaq və düzəliş etmək hüququ, verilənlərin emalına etiraz etmək hüququ, verilənlərin sızması baş verdikdə məlumatlandırılmaq hüququ, unudulmaq hüququ (yəni, fərdi məlumatlarının operator tərəfindən dərhal, izafi rəsmiyyət olmadan məhv edilməsini tələb etmək hüququ) verilir. Bu hüquqların başqa şəxslərin və təşkilatların hüquq və azadlıqlarına, bütovlükdə cəmiyyətin maraqlarına zidd olmaması gözlənilir. GDPR öz istifadəçilərinin məlumatlarını istifadə edən və saxlayan şirkətlər üçün sərt qaydalar müəyyən edir.

GDPR-in texnoloji baxımdan neytral olduğu iddia edilsə də, blokçeynə münasibətdə bir çox məsələlər meydana çıxır. Blokçeyn layihələrində fərdi məlumatların emalı texnologiyası bir çox cəhətdən GDPR tələbləri ilə ziddiyyət təşkil edir. GDPR-də müəyyən edilən fərdi məlumatın subyekti, kontrolleri, prosessoru kimi rolları blokçeyndə birqiymətli təyin etmək çətindir, çünki blokçeyn mahiyyətinə görə demərkəzləşmiş texnologiyadır.

Fərdi məlumatların subyektlərinin unudulmaq hüququnu, düzəliş etməkhüququnu və emalı məhdudlaşdırmaq hüququnu təmin etmək məsələsində də blokçeyn texnologiyası çətinliklərlə qarşılaşır. Blokçeyn praktiki olaraq redaktə olunmur, onda saxlanılan verilənləri yeniləmək, silmək, dəyişmək, düzəliş etmək mümkün deyil.

Fərdi məlumatların transsərhəd ötürülməsi zamanı mühafizə tədbirlərinin həyata keçirilməsi çətinləşir, çünki blokçeyn-sistemdə kontrollerlər maynerlərin yerləşmə yerini həmişə dəqiq müəyən edə bilmirlər və müvafiq tədbirləri tətbiq etmək mümkün olmur. Verilənlərin minimallaşdırılması və onların saxlanma müddətlərinin məhdudlaşdırılması tələbini də blokçeyndə reallaşdırmaq problemlidir.

Bu suallara fərdi məlumatların mühafizəsi sahəsində Fransada səlahiyyətli orqan olan CNIL (Commission Nationale de l'Informatique et des Libertés – İnformatika və insan

azadlıqları üzrə Milli Komissiya) [3] və Avropa Blokçeyn Forumu öz hesabatlarında cavab verməyə çalışırlar [4].

GDPR-də ilk növbədə fərdi məlumat kontrolleri məsuliyyət daşıyır. Blokçeyn modelində bir neçə tərəf kontroller kimi çıxış edir. Bu problemi həll etmək üçün subyektlər xüsusi təyinatlı yeni obyekt yaratmalı və ya müqavilə ilə bir kontroller müəyyən etməlidirlər. Digər obyektlər blokçeyn və mayninq validatorlarından istifadə edirlər.

Fərdi verilənlərin blokçeyndə saxlanmasını mümkün olduqca minimallaşdırmaq lazımdır. Blokçeynin əsas təyinatı tranzaksiyanın baş verdiyini və ya yazının həqiqi olduğunu təsdiqləməkdir. Əgər tranzaksiyalarda və yazılarda fiziki şəxslər iştirak edirsə, onda onlarda fərdi məlumatlar mütləq olacaq. Lakin belə fərdi məlumatları blokçeyndən kənarda saxlamaq, blokçeynə isə onları sübut edən heş-kodu daxil etmək olar. Bu GDPR-in verilənlərin minimallığı və təhlükəsizlik tələblərini yerinə yetirməyə imkan verir.

V. BLOKÇEYN TEXNOLOGİYASININ TƏKMİLLƏŞDİRİLMƏSİ İSTİQAMƏTLƏRİ

Blokçeyn texnologiyası tədqiqatçıların qarşısına praktiki ehtiyaclardan qaynaqlanan müxtəlif tədqiqat problemləri qoyur. Blokçeynlərin ən aktual problemləri arasından miqyaslanma məsələlərini, təhlükəsizliyin və gizliliyin təmin edilməsini qeyd etmək olar [2].

Hazırda blokçeynin məlum olan ən fundamental təhlükəsizlik boşluğu təkrar xərcləmə (ing. double spending), “51 % hücumu”, Sivilla hücumu (ing. Sybil attack) və DDoS hücumudur. Bu hücumların Bitkoin şəbəkəsində baş tutması ehtimalı hazırda olduqca kiçikdir. Digər blokçeyn layihələrində həmin hücumların qarşısını almaq üçün müxtəlif əlavə tədbirlər nəzərdə tutulur.

Geniş yayılmış blokçeyn texnologiyası kimi Bitkoinin əsas problemi tranzaksiyaların emal sürətinin olduqca aşağı olmasıdır (saniyədə 6-7 tranzaksiya); müqayisə üçün qeyd edək ki, bu göstərici VISA sistemində 2000-dir. Ümumiyyətlə, blokçeyn-şəbəkənin miqyaslanması məsələsi əlaqəli üç parametrin – təhlükəsizlik, demərkəzləşmə və miqyaslanmanın optimallaşdırılması arasında balanslaşdırmanı tələb edir. Tranzaksiyaların emal sürətini yüksəltmək üçün blokçeyn ya təhlükəsizliyi, ya da demərkəzləşməni qurban verməlidir. Praktikada yüksək sürət nümayiş etdirən blokçeynlərdə, adətən, demərkəzləşmə güzəştə gedilir və hazırda mərkəzləşmə meylləri üstün gəlir.

Miqyaslanmanın təmin edilməsi üçün yanaşmaların işlənməsi aktiv tədqiqat istiqamətlərindəndir. Bu sahədə bəzi təşəbbüsləri xatırlatmaq olar: qlobal reyestrin qovşaqların bir qrupu tərəfindən idarə edilən daha kiçik altreyestrlərə bölünməsi, saxlanmanı optimallaşdırmaq üçün əvvəlki tranzaksiyaların silinməsi, blokçeynlər iyerarxiyasından istifadə edilməsi (məsələn, Lighting Network texnologiyası), blokçeynin seqmentlərə bölünməsi (ing. sharding), blokun ölçüsünün artırılması (məsələn,SegWit) və s.

PoW (Proof of Work) konsensus protokolunun icrası böyük xərclər tələb edir. Bitkoin şəbəkəsi mayninqə bütöv bir dövlətin istehlak etdiyi qədər elektrik enerjisi sərf edir. Xərcləri minimallaşdırmaq üçün çox sayda alternativ konsensus protokolları təklif edilmişdir, lakin əksər kriptovalyutalarda PoW protokolunun hansısa forması istifadə edilir. PoW kimi paylanmış konsensus protokolunun ən böyük problemlərindən biri şəbəkəni təhlükəsiz, lakin olduqca yavaş etməsidir. Bu blokçeynin bütün dominant atributları: demərkəzləşmə, təhlükəsizlik və miqyaslanma arasında balanslaşdırmanın nəticəsidir.

VI. MÖVCUD TƏDQİQATLARIN ANALİZİ

[5]-də blokçeyn identifikasiya xidmətlərini, yəni uPort, Sovrin və ShoCard-ı tənqidi analiz edilmiş, müasir rəqəmsal xidmətlərin çatışmazlıqları aşkar edilmişdir. Mövcud identifikasiya idarəetmə sistemlərində identifikasiya atributlarının məhdudiyyətlərini və zəif cəhətlərini aradan qaldırmaq üçün təhlükəsizlik tələblərinə yüksək səviyyədə cavab verən DNS-IdM təklif edilmişdir. Smart əlaqəyə əsaslanan DNS-IdM identifikasiya idarəetmə sistemi istifadəçilərə fərdi məlumatlarını qorumağa imkan verir, konsepsiyanı öz-özünə yerinə yetirir.

[6]-da Blokçeyn texnologiyası ilə Avropa Birliyinin informasiya təhlükəsizliyi çərçivəsində qarşılıqlı nöqtələri müzakirə etmiş və smart şəhərlərdə blokçeyn əsaslı layihələrin daha yaxşı inkişaf etdirilməsi üçün tövsiyələr verilmişdir. Həmçinin məqalədə blokçeynin klassifikasiyası, paylanmış reyestr texnologiyaları (ing. Distributed Ledger Technology, DLT) və blokçeynlər haqqında ətraflı araşdırma aparılmışdır.

[7]-də fərdi məlumatların sızma riskini azaltmaq üçün blokçeyn əsaslı məlumat idarəetmə sistemi təklif edilmişdir. GDPR fərdi məlumatları mərkəzləşdirilməmiş və etibarlı paylama və izləmə sxeminə uyğundur. Təklif olunan blokçeyn əsaslı identifikasiya idarəetmə sistemləri ilə GDPR subyektləri (istifadəçi, kontroller və prosessor) arasında məlumat mübadiləsini nümayiş etdirir. GDPR məhdudiyyətlərinə görə fərdi məlumatları şəbəkə xaricində saxlama arxitekturasından istifadə edilmişdir, bu, blok ölçüsünü də azaldır. Təklif olunan arxitektura təsdiq üçün multiçeyn istifadə edərək prototip yaradır. Bu tədqiqatda təklif olunan fərdi məlumatları idarəetmə sisteminə əsaslanan blokçeynin konfidensiallığı yoxlamaq üçün fərdi məlumatları paylaşmaq, silmək, dəyişdirmə və izləmə xüsusiyyətlərini təqdim edir.

[8]-də göstərilir ki, tibbi məlumatların mübadiləsi üçün DLT əsaslı sistemin dizaynı və istifadə vəziyyəti nəzərə alınmalıdır. Fərdi məlumatların yalnış istifadəsi və istifadə zamanı yaranmış riski minimuma endirmək üçün iki dizayn təklif edilmişdir. Dizaynlardan biri kütləvi yayımlanan IOTA reyestrinə, digəri isə IOTA və IPFS (InterPlanetary File System) çoxluğuna əsaslanır. İlk dizayn daha sadədir, lakin fərdi məlumatların ələ keçirilmə riskini minimuma endirmək üçün xüsusi diqqət tələb edir. İkinci dizayn isə daha mürəkkəbdir, böyük sənədlərin mübadiləsinə imkan yaradır.

[9]-də gizliliyin qorunması funksiyaları və əhatə dairəsi barədə məlumat verilmiş, GDPR və ISO/IEC 29100: 2011 standartlarının IoT-da gizlilik təhdidlərinin faktiki həlli vəziyyəti analiz edilmişdir. Burada əsas məqsəd müvafiq həllərin müasir qanuni prinsiplərə və gizlilik standartlarına uyğunluğunu yoxlamaq və gizliliyə təhdidləri azaltmaqdır.

[10]-da blokçeyn ilə GDPR tələblərini “barışdırmağın” və gizliliyin daha geniş şəkildə təmin edilməsinin mümkünlüyü

araşdırılır, GDPR-ə uyğun məlumat idarəçiliyində blokçeyn həllərinin güclü və zəif tərəfləri analiz edilir. GDPR tələbləri ilə bəzi mövcud blokçeyn həlləri və tətbiqləri arasındakı uyğunsuzluqlar və həll yolları araşdırılır.

[11]-də GDPR "fərdi məlumatlar" , "vizual fərdi məlumat" termini ilə əlaqələndirilir. GDPR kontekstində vizual fərdi məlumatlar üçün “Data Protection-by-Design” tətbiqi kimi maşın təliminin, təsvirin işlənməsi, kriptoqrafiya və blockçeynin qarşılıqlı əlaqəsi araşdırılır. Məqalədə fərdi məlumatların qorunması qaydaları araşdırılır və GDPR-ə uyğun fərdi məlumatların qorunması ilə hazırlanan video nəzarət sistemlərinin inkişafı üçün təkliflər təqdim edilir.

[12]-də DLT ilə kontrollerlər və məlumat prosessorları arasında konseptual model təklif edilmişdir. Məqalə blokçeyn tətbiqinin GDPR uyğun əməliyyatları üçün faydalı məqamları təqdim etmək məqsədi daşıyır və ancaq DLT həllinin tətbiq oluna biləcəyi vacib cəhətləri göstərir.

[13]-də gizlilik və təhlükəsizlik riskləri ilə fərdi məlumatların təhlükəsizliyi üçün potensial təhlükələrlə bağlı problemlər araşdırılmışdır. IoT sistemi İnternetdə məlumatları, o cümlədən fərdi məlumatları ötürməyə imkan verir. Bu çərçivədə GDPR standartları nəzərdən keçirilmişdir. Fərdi məlumatların yalnış istifadəsinin qarşısını alan riskləri qiymətləndirmək üçün tədqiqat aparılmışdır. Bundan əlavə, fərdi məlumatların təhlükəsizliyi üçün dünya miqyasında gizlilik standartının inkişaf etdirilməsi təklif olunmuşdur.

NƏTİCƏ

Bitkoin göstərdi ki, kriptoqrafiya və düşünülmüş iqtisadi stimullar vasitəsilə fərdi məlumatlar daxil olmaqla informasiyanın təhlükəsiz saxlanılması və emalı metodu yaratmaq mümkündür. Bu təcrübədən çıxış edərək, Bitkoin-in əsasında dayanan blokçeyn texnologiyasından fərdi məlumatların təhlükəsizliyinin təmin olunması istiqamətində bir platforma yaratmaq üçün istifadə etmək olar.

Lakin fərdi məlumatların qorunması sahəsində de-fakto model qanun hesab edilən GDPR ilə blokçeyn texnologiyaları arasında bir çox ziddiyyət vardır. Mütəxəssislərin qənaətinə görə, bu texnologiyanın öz yüksək potensialına nail olması onun GDPR-ə nə dərəcədə uyğun reallaşdırılmasından asılı olacaq.

Bu məqsədlərə çatmaq üçün faydalı ola biləcək yeni elmi-texniki tədqiqatlar aparılır. Bu tədqiqatlar miqyaslanma və ya idarəetmə sturukturunun təkmilləşdirilməsi problemlərini həll etməyə çalışırlar ki, məsuliyyətin bir neçə iştirakçı arasında bölünməsini təmin etməyə yönəlmişdir. Tədqiqatlarda ən çox rast gəlinən metodlara sıfır bilik verməklə isbat, gizli ünvanlar, şifrləmə, vəziyyət kanalları və halqa imzaları, küyün əlavə edilməsi və s. daxildir. Bu metodların bəziləri digərlərinə nisbətən daha perspektivli olsalar da, blokçeyn texnologiyası qarşısında duran çağırışların həll edilməsi üçün bu metodların birləşdirilməsi tələb edilir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikası Dövlət Neft Şirkətinin (SOCAR) Elm Fondunun mailyyə yardımı ilə yerinə yetirilmişdir – **Müqavilə № 23LR – AMEA**.

İSTİNADLAR

[1] Y. İmamverdiyev “Big Data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı, pp. 109-113, 2016.

[2] Y. İmamverdiyev “Blokçeyn texnologiyaları: komponentləri, tətbiqləri və problemləri,” İnformasiya cəmiyyəti problemləri, no. 2, pp. 18–32, 2019.

[3] Solutions for a responsible use of the Blockchain in the context of personal data. CNIL (Commission Nationale Informatique & Libertés). 2018. https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

[4] Van Eecke, P., & Haie, A. G. (2018). Blockchain and the GDPR: The EU Blockchain Observatory Report. Eur. Data Prot. L. Rev., 4, 531.

[5] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, & K. Dahal “DNS-IdM: A blockchain identity management system to secure personal data sharing in a network”, Applied Sciences, vol. 9, no. 15, Article 2953, 2019.

[6] L.F.M. Ramos, & J.M.C. Silva “Privacy and data protection concerns regarding the use of blockchains in smart cities,” In 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), pp. 342-347, 2019.

[7] M. Onik, C. Kim, N. Lee, & J. Yang, “Privacy-aware blockchain for personal data sharing and tracking”, Open Computer Science, vol 9, no. 1, pp. 80-91, 2019.

[8] D. Hawig, C. Zhou, S. Fuhrhop, A.S. Fialho, N. Ramachandran ”Designing a distributed ledger technology system for interoperable and General Data Protection Regulation-compliant health data exchange: A use case in blood glucose data,” Journal of Medical Internet Research, vol. 21, pp. 12, 2019.

[9] S.C.Cha, T.Y.Hsu, Y.Xiang, & K.H.Yeh, “Privacy enhancing technologies in the Internet of Things: Perspectives and challenges,” IEEE Internet of Things Journal, vol 6, no 2, Article 2159-2187, 2018.

[10] D. Hofman, V. L. Lemieux, A.Joo, & D. A. Batista “The margin between the edge of the world and infinite possibility,” Records Management Journal, no 29 (1/2), pp. 240-257, 2019.

[11] M.N. Asghar, N.Kanwal, B.Lee, M.Fleury, M.Herbst, & Y.Qiao “Visual surveillance within the EU General Data Protection Regulation: A technology perspective,” IEEE Access, vol.7, pp. 111709-111726, 2019.

[12] P. Hristov & W. Dimitrov, “The blockchain as a backbone of GDPR compliant frameworks,” Calitatea, vol. 20, no. 1, Article 305, 2019.

[13] N. Fabiano “Internet of Things and blockchain: legal issues and privacy. The challenge for a privacy standard.” IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 727-734, 2017.

BLOCKCHAIN TECHNOLOGIES FOR PERSONAL DATA PROTECTION: OPPORTUNITIES AND PERSPECTIVES

Yadigar İmamverdiyev[1], Gunay Muradova[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
[1]*yadigar@iit.science.az*, [2]*gmuradova9@gmail.com*

Abstract – The paper discusses the possibilities and prospects of using blockchain technology to protect personal data. A brief description of blockchain technology is given and an analysis of existing research is carried out. The possibilities of ensuring the security of personal data using the blockchain technology and the potential problems that arise during this are analyzed.

Keywords – personal data, blockchain, privacy, privacy preserving, GDPR