UDC 654
DOI 10.52171/2076-0515_2024_16_03_87_93

Cyber Attacks Present in Blockchain Technology and Security of Blockchain Technology

T.Sh. Alekberova

Azerbaijan Technology University (Sh.I. Khatai ave., 103, Ganja city, AZ2011, Azerbaijan)

For correspondence: Alekberova Tamara / e-mail: t.elekberova@atu.edu.az

Abstract

"Blockchain" technology and the rules of its use are one of the most relevant topics in the cyber world recently. But despite the topicality of the topic, people have very little information about the essence of this technology, the dangers that exist within it, and the methods of protection. This article analyzes the components of Blockchain technology, analyzes the information about the classification of Blockchain risks and the measures that can be taken to ensure the security of Blockchain technology.

Keywords: Blockchain technology, cryptography, consensus protocol, cyber-attacks, mining.

Received *28.12.2023*
Revised *19.09.2024*
Accepted *23.09.2024*

For citation:
T.Sh. Alekberova
[Cyber Attacks Present in Blockchain Technology and Security of Blockchain Technology]
Herald of the Azerbaijan Engineering Academy, 2024, vol. 16, № 3, pp. 87-93 *(in Azerbaijani)*

Blokçeyn texnologiyasında mövcud olan kiber hücumlar və Blokçeyn texnologiyasının təhlükəsizliyi

T.Ş. Ələkbərova

Azərbaycan Texnologiya Universiteti (Şah İsmayıl Xətai prospekti, 103, Gəncə ş., AZ2011, Azərbaycan)

Xülasə

"Blockchain" (Blokçeyn) texnologiyası və ondan istifadə qaydaları son zamanlar kiber dünyanın ən aktual mövzularından biridir. Lakin mövzunun aktual olmasına baxmayaraq, insanlar bu texnologiyanın mahiyyəti, daxilində mövcud olan təhlükələr və qorunma üsulları haqqında çox az informasiyaya malikdirlər. Bu məqalədə Blokçeyn texnologiyasının komponentləri analiz edilir, Blockchain risklərinin sinifləndirilməsi və Blokçeyn texnologiyasının təhlükəsizliyini təmin etmək üçün görülə biləcək tədbirlər haqqında məlumatlar təhlil edilir.

Açar sözlər: blokçeyn texnologiyası, kriptoqrafiya, konsensus protokolu, kiber hücumlar, mining.

Анализ кибератак, доступных в технологии Блокчейн, и безопасность технологии

Т.Ш. Алекберова

Азербайджанский технологический университет (проспект Шах Исмаил Хатаи, 103, г.Гянджа, AZ2011, Азербайджан)

Аннотация

Технология Blockchain («Блокчейн») и правила ее использования в последнее время являются одной из самых актуальных тем в кибермире. Но, несмотря на актуальность темы, у людей очень мало информации о сути этой технологии, опасностях, которые в ней существуют, и методах защиты. В статье анализируются компоненты технологии «Блокчейн», анализируется информация о классификации рисков данной технологии и мерах, которые могут быть предприняты для обеспечения безопасности технологии «Блокчейн».

Ключевые слова: технология Блокчейн, криптография, протокол консенсуса, кибератаки, майнинг.

Giriş

Blokçeyn Texnologiyasına ümumi baxış – bu terminin Azərbaycan dilində hərfi mənası blok zənciridir. Blokçeyn texnologiyası müxtəlif növ əməliyyatları avtomatik və onlayn rejimdə qeydiyyata alan kitabçadır. Bu texnologiyanın yaranma tarixi kimliyi hələ də dəqiq bilinməyən Satoshi Nakamoto təxəllüsü istifadə edən bir şəxs və ya qrup tərəfindən dərc edilən "Bitcoin: A Peer-to-Peer Electronic Cash System" başlıqlı məqalədə 31 oktyabr 2009-cu ildə açıqlanmışdı [1].

Bəzən paylanmış kitab texnologiyası DLT olaraq adlandırılan Blokçeyn, mərkəzləşdirilməmiş şəbəkə və kriptoqrafik heşinqdən istifadə etməklə istənilən rəqəmsal aktivin tarixini dəyişməz və şəffaf edir. Burada tranzaksiyalar maynerlər tərəfindən yoxlanılır və blok şəklində blokçeyn adlanan hamıya açıq bir reyestrə qeyd edilir. Hər bir blokun başlığında bir öncəki blokun başlığının SHA256 kriptoqrafik heş funksiyası ilə iki dəfə hesablanmış heşi yazılır. Bununla da Bitkoin şəbəkəsində əvvəlcədən yerinə yetirilmiş bütün tranzaksiyalar bir zəncirlə əlaqələndirilmiş olur. Bu zəncirdə hər hansı tranzaksiyanı dəyişmək demək olar ki, mümkün deyil. Çünki tranzaksiyanın dəyişilməsi üçün zəncirdəki bütün blokların dəyişilməsi lazımdır.

Blokçeyn rəqəmsal aktiv məlumatlarının şifrələnmiş bloklarının saxlanıldığı və birlikdə zəncirləndiyi, məlumatlar üçün xronoloji tək həqiqət mənbəyi təşkil edən rəqəmsal kitab və ya verilənlər bazasıdır. Burada olan Rəqəmsal aktivlər paylanır, kopyalanmır və ya köçürülmür. Rəqəmsal aktivlər qeyri-mərkəzləşdirilmişdir ki, bu da birdən çox tərəf arasında real vaxtda əlçatanlığa, şəffaflığa və idarə etməyə imkan verir. Blokçeyn kitabçaları şəffafdır. Edilən hər hansı dəyişiklik bütövlük və etibarlılığı qoruyaraq sənədləşdirilir. Blokçeyn kitabçaları həmçinin ictimaidir və özünəməxsus təhlükəsizlik tədbirləri ilə qurulur və bu hal demək olar ki, hər sektor üçün əsas texnologiyaya çevrilir.

Texniki baxımdan blokçeyn (“block” – blok + “chain” – zəncir) informasiya bloklarının zənciridir. Bitkoin blokçeyninin strukturuna əsasən hər bir Bitkoin bloku dörd komponentdən ibarətdir: blokun ölçüsü (Size), tranzaksiya sayğaçı (TXs), blokun başlığı (Header) və tranzaksiyalar (Tranzactions) [1].

Blokun ölçüsü blokdakı baytların tranzaksiya sayğacı isə tranzaksiyaların saylarını göstərir. Tranzaksiyalar – bloka daxil olan tranzaksiyaların siyahısıdır. Blok başlığına altı sahə daxildir:

• Version – proqram/protokol yeniləmələrini izləmək üçün istifadə olunur;

• PreviousHash – zəncirdə bilavasitə əvvəl gələn blokun heşi;

• Timestamp – blokun yaradılması tarixi qeyd olunur. Vaxt möhürü blokçeynindəki məlumatların blokun qeydə alınmış generasiya vaxtı qaydasında saxlanmasını təmin edir, beləliklə, zəncirdəki məlumatların mənbəyi blokun vaxt möhürünə uyğun olaraq izlənilə bilər;

• 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. Blokun Merkle ağacı kökünün hash dəyərini qeyd edir;

Blok orqanı əməliyyat məzmununu və əlaqəli məlumatları öz daxilində saxlayır. Hər bir əməliyyat məlumatı rəqəmsal imza ilə qeyd olunur. Blok məlumatlarının təhlükəsizliyini təmin etmək üçün rəqəmsal imza mexanizmindən istifadə olunur. Blok gövdəsinə

aşağıdakılar daxildir:

1)Num Transactions Bytes: Num tranzaksiyaların tutduğu baytların sayını qeyd edir.

2) Num Transactions: Blokdakı əməliyyatların sayını qeyd edir.

3) Əməliyyatlar: Blokda çoxlu əməliyyat məlumatlarını qeyd edir.

Blokçeyn texnogiyası üç addım ilə həyata keçirilir:

1) Tranzaksiyanın yaradılması mərhələsi
2) Tranzaksiyanın təsdiqlənməsi mərhələsi
3) Blokun zəncirə əlavə edilməsi mərhələsi.

Blockchain texnologiyasında kiber hücumlar

Bu bölmədə, KPMG ("Klynveld Peat Marwick Goerdeler") üzv firmalarının təcrübələri əsasında, Blockchain tətbiqləri ilə əlaqədar on əsas risk qrupları müəyyənləşdirmişdir [2-4]. Bu risk ölçülərinin bəziləri bir-birinə bağlıdır. Bu ölçülər həmçinin Blockchain-in həyat dövrü boyunca fərqli variantlarına malikdir.

Həmçinin araşdırıcılar, blokçeyn texnologiyasi ilə əlaqədar olan risk hadisələrini, əlaqə protokollarını və dizayndakı zəifliklərdən yararlanmaq üçün təhlükəsizlik boşluqlarını blokçeyn texnologiyası ilə əlaqəli sinifləndirilmiş formada [2], [4] izah edirlər.

Blockchain generasiyasına uyğun olaraq üç kateqoriyaya ayırırlar [3-6]:

1) Birinci nəsil Blockchain 1.0.
2) İkinci nəsil Blockchain 2.0.
3) Üçüncü nəsil Blockchain 3.

Aşağıdakı, Blockchain risklərinin sinifləndirilməsi qeyd edilir:

- Blockchain 1.0 və 2.0 ümumi riskləri.
- İkili xərclənmə (Double spending).
- 51% hücumu və ya Gold finger.
- Kupça təhlükəsizliyi (private key security).
- PoS-da xüsusi səhv.
- Şəbəkə səviyyəli hücum.
- Malleability hücumu.
- Ethereum şəbəkəsinə qarşı həqiqi DOS hücumu.
- DPoS-da xüsusi səhv.
- Blok istehsalçılarının razılaşması.
- Seçici fəallığından istifadə etmək.
- Ölçülü hücumlar.
- BLOCKCHAIN 2.0 təhlükəsizlik boşluqları
- Təkrar daxil olma zəifliyi (DAO hücumu).
- Parity multisig pul kisəsi.
- Ether qrupunun sahibi.
- Hərbi hökumət hücumları.
- BLOCKCHAIN 3.0 təhlükəsizlik boşluqları
- Hyper ledger Fabric-ə hücum
- İstifadəçiyə özəl Blockchain tətbiqlərində ümumi risklər

Blokçeyn texnologiyasının işləmə prinsipi

Blokçeyn texnologiyasının necə işlənməsini Google Docs sənədinin necə işlədiyi ilə müqayisə etməklə təhlil etmək olar. İstifadəçi Google Sənədi yaradıb onu bir qrup insanla paylaşdığı zaman, sənəd kopyalanmaq və ya köçürülmək əvəzinə sadəcə paylaşılır. Bu vəziyyət hər kəsə eyni vaxtda əsas sənədə çıxış imkanı verən mərkəzləşdirilməmiş paylama zənciri yaradır.

Sənədə edilən bütün dəyişikliklər real vaxt rejimində qeydə alınır və dəyişikliklər tamamilə şəffaf olur. Bununla belə, qeyd etmək lazım olan əhəmiyyətli bir məsələ ondan ibarətdir ki, Google Sənədlərdən fərqli olaraq, blokçeyndəki orijinal məzmunu və məlumatları bir dəfə yazdıqdan sonra dəyişdirilə bilməz, bu hal blokçeyn texnologiyasının təhlükəsizlik səviyyəsini artırır.

Blokçeyn teknologiyasının təhlükəsizliyi necə qorunur?

Blokçeyn texnologiyası (Blockchain), mərkəzi olmayan və şəffaf bir struktura malik olduğundan təhlükəsiz bir sistem olaraq qiymətləndirilir. Lakin bəzi təhlükəsizlik riskləri də mövcuddur ki, onların qarşısını almaq üçün müxtəlif tədbirlər görülməlidir. Blokçeyn texnologiyasının təhlükəsizliyini təmin etmək üçün görülə biləcək bəzi tədbirlər aşağıdakılardır:

Kriptoqrafiya: Blokçeyn texnologiyası, təhlükəsizlik üçün kriptoqrafiyadan istifadə edir. Blok zincirlər (Blokçeyn), kriptoqrafik protokollardan biri olan SHA-256 alqoritmi ilə qorunur. Bu alqoritm, hər blokun məzmununu yəni transaksiyaların siyahısı və blok header-i birləşdirərək "hash" adlanan bir dəyər yaradır. Blok zincirlərin hash dəyərləri isə kriptoqrafiya tətbiq edilərək qorunur. Kriptoqrafiya, məlumatların təhlükəsizliyini təmin etmək üçün istifadə edilən bir mənbəyə sahibdir. Blok zincirlərin hash dəyərləri tətbiq edilərək qorunması prosesi blokların əlavə edilməsi və blokların təsdiqlənməsi zamanı istifadə olunan bir prosesdir. Blokçeyn'də, hər blok özündən öncəki bloka dair daxilində bir hash dəyəri saxlayır. Bu hash dəyəri, əvvəlki blokda olan məlumatların tərkibindən təşkil olunur. Buna görə də, əgər bir blokda yerləşən məlumat dəyişdirilsə, bu zaman hash dəyəri də dəyişəcək və blokların bir-birinə qoşulması prosesi nizamsız olacaq. Bu proses isə blokların bir-birinə qoşulması ilə birlikdə tam şəkildə qorunur və hər hansı bir müdaxilə olmadan blokçeyn dəyişdirilə bilməz. Blokçeyn-in bu qorunma forması, həm də təsdiqləmə prosesini və yeni blokların təhlükəsiz əlavə edilməsini təmin edir. Buna görə də, bir blok əlavə olunmadan əvvəl, əvvəlki blokların hash dəyərlərinin təsdiq edilməsi lazımdır. Bu, blokların qorunması üçün əlavə bir tədbirdir.

Mərkəzi Olmayan Struktur: Blokçeyn texnologiyası, mərkəzi bir orqanın olmadığı bir sistemdir. Bu verilənlər çoxlu nodlar arasında dağıdılır və bütün nodların eyni blokları görməsi təmin edilir. Bu, blokların məlumatlarının manipulyasiyasına və ya silinməsinə qarşı qorumanı təmin edir. Bu səbəbdən, mərkəzi bir serverin qırılması və ya ələ keçirilməsi riski yoxdur.

Mining: Blokçeyn texnologiyası, blokların doğrulanması və təsdiq edilməsi üçün "Mining" adlanan bir proses istifadə edir. Mining, Blokçeyn texnologiyasıin təhlükəsizliyini artıran və blokların düzgün bir şəkildə doğrulanmasını təmin edən riyazi bir əməliyyatdır.

Konsensus Protokolu: Blokçeyn texnologiyasında konsensus protokolu, Blokçeyn şəbəkəsi üzərindəki düyümlərin müxtəlif blokları təsdiqləməklə və yeni blokların yaradılması üçün icazə verilməsi ilə bağlı qərarlar qəbul etməsi üçün istifadə olunur. Konsensus protokolu, hər bir blokun təsdiqlənməsi və bloklar arasında təhlükəsiz məlumat alış-verişi təmin etmək üçün əhəmiyyətli bir rol oynayır. Müxtəlif konsensus protokolları mövcuddur, lakin ən populyar olanları Proof of Work (PoW) və Proof of Stake (PoS) protokollarıdır.

Təsdiq (Validation): Blokçeyn texnologiyası üzərindəki hər bir əməliyyat, şəbəkədəki digər node-lar tərəfindən təsdiq edilir. Bu təsdiq prosesi, yanlış əməliyyatların şəbəkəyə daxil edilməsinə mane olur və Blokçeyn texnologiyasıin bütövlüyünü qoruyur.

Ölçülə bilənliyi: Blokçeyn texnologiyası böyük miqdarda əməliyyatları idarə etmə imkanına malik olmalıdır. Ölçülə bilənlik, Blokçeyn-lərin təhlükəsizliyini təmin etmək üçün vacib bir faktordur.

Ağıllı müqavilələr: Blok zincir texnolo-

giyası, ağıllı müqavilələr vasitəsi ilə təmin edilən təhlükəsizlik üçün də istifadə edilir. Ağıllı müqavilələr, müqavilələrin avtomatik olaraq icrasına imkan verir və tərəflər arasında mütəxəssis olmadan icra edilə bilir. Bu, müqavilələrin icrasında qarışıqlığın azaldılmasına və təhlükəsizliyin artırılmasına imkan verir.

Ölçülü Xərclər: Blokçeyn texnologiyası, ölçülü xərclər vasitəsi ilə təhlükəsizliyin artırılması üçün istifadə edilir. Blokçeyn texnologiyası, hər bir əməliyyat üçün minimum bir ölçülü xərc tələb edir. Bu, sürətli və təhlükəsiz əməliyyatları təmin etməyə imkan verir.

İstifadəçilər Tərəfindən Hərəkətli Ortalama Təsdiqlənməsi: Blokçeyn texnolo-giyasında, hər bir blok, təsdiqlənmək üçün istifadəçilər tərəfindən müəyyən bir sayda keçid edilməlidir. Bu, blokların təsdiqlənməsində daha çox istifadəçinin iştirak etməsini və təhlükəsizliyin artırılmasını təmin edir.

Ölçülü Kodlu Güncəlləmələr: Blokçeyn texnologiyası, ölçülü kodlu güncəlləmələr vasitəsi ilə təhlükəsizliyin təmin edilməsindən istifadə edir. Bu, Blokçeyn protokollarının ən son versiyası ilə uyğunlaşdırılmağın və köhnə blokların müəyyən bir müddət ərzində qalmaqda olmasının təmin edilməsinə imkan verir.

Dağınıq Şəbəkə: Blokçeyn texnologiyası dağınıq bir şəbəkə üzərində işləyir. Bu, Blokçeyn-dəki hər bir əməliyyatın bütün şəbəkə üzərindəki düyümlər tərəfindən təsdiqlənməsini və doğrulanmasını tələb edir. Bu, əməliyyatların tək bir mərkəzi nöqtədə olmaması və Blokçeyn protokolunun bütün düyümlər tərəfindən tətbiq edilməsi səbəbi ilə təhlükəsizliyi artırır.

İzlənilmə: Blokçeyn texnologiyası, hər bir əməliyyatı qeyd etdiyi üçün izlənilməyi təmin edir. Bu, əməliyyatların kimliklərini doğrulamaq və hər hansı bir bəd niyyətli istifadə hallarında aşkar etmək üçün istifadə edilə bilər.

Dəyişməzlik: Blokçeyn texnologiyası, məlumatların dəyişilməzliyini təmin edir. Blokçeyn şəbəkəsindəki məlumatlar bir dəfə blokda yadda saxlanıldıqdan sonra dəyişməz və bu əməliyyatı geri qaytarmaq mümkün deyil. Bu, Blokçeyn şəbəkəsindəki məlumatların təhlükəsizliyini təmin edir.

Əlçatanlıq: Blokçeyn texnologiyası, hər hansı bir məlumatın və ya əməliyyatın əlçatanlığını təmin edir. Blokçeyn şəbəkəsindəki hər hansı bir əməliyyat, Blokçeyn şəbəkəsindəki bütün düyümlər tərəfindən təsdiqlənir və təsdiqləmə prosesi açıq şəkildə görünür. Bu, Blokçeyn şəbəkəsindəki məlumatların təhlükəsizliyini təmin edir.

Nəticə

Bu addımlar Blokçeyn şəbəkəsindəki düyümlər arasında məlumatın təsdiqlənməsini və qərarların qəbul edilməsini daha təhlükəsiz və əhatəli etmək üçün istifadə edilir. Bu, Blokçeyn şəbəkəsindəki hər hansı bir nöqtənin müdaxiləsinin, təhlükəsizliyin pozulmasına səbəb olma ehtimalını azaldır. Göstərilən addımlar, Blokchain təhlükəsizliyinin təmin edilməsi üçün ən vacib addımlardandır. Hər bir addımın doğru tətbiq edilməsi və Blokchain-in müvafiq tənzimləmələrə uyğun olması halında, Blokchain təhlükəsizliyinin təmin edilməsi daha da yüksək səviyyəyə çatdırıla bilər. Lakin bütün bunlara baxmayaraq, hər zaman bir təhlükə və ya zərər faktoru mövcud ola bilər, bu səbəbdən Blokchain-lə işləmək üçün tədbirlər də hazırlanmalıdır.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. Blokçeyn Texnologiyaları: Komponentləri, Tətbiqləri və Problemləri. İmamverdiyev Y.N. İnformasiya cəmiyyəti problemləri, 2019, №2, 18–32 *(in Azerbaijani)*

2. KPMG International, 2017. Securing the chain, retrieve fromttps //

home.kpmg.com/xx/ena/home/insights/2017/0 5/ securing-the-blockchain-fs.html

3. **Huru H., Ui-jun B., Mu-gon S., Kyunghee C., Myung-Sup K.** 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. The International Journal of Network Management, Vol29, Issue2.1-36. Information Risk Approaches. Chinese Business Review, Vol. 10, No. 12, pp. 1106-1110 *(in English)*

4. Cybersecurity Risks of Blockchain Technology Ihab M. Abdelwahed, Nagy Ramadan, Hesham Ahmed Hefny International Journal of Computer Applications (0975 – 8887) Volume 177. No. 42, March 2020. *(in English)*

5. Blokçeyn texnologiyasının təhlükəsizlik məsələləri. "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı, 14 dekabr 2018-ci il *(in Azerbaijani)*

6. *https://www.ama.com.az/archiveofjournal*