Informatics

BLOKÇEYN ŞƏBƏKƏSİNİN KOMPONENTLƏRİNİN İŞLƏNMƏSİ İLƏ İNFORMASİYA MÜBADİLƏSİNİN TƏHLÜKƏSİZLİYİ

Abdulhüseyn Vəfadar oğlu Ağayev
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

THE SECURITY OF INFORMATION TRANSMITION THROUGH THE DEVELOPMENT OF THE BLOCKCHAIN NETWORK COMPONENTS

Abdulhuseyn Vafadar Aghayev
Azerbaijan Technical University, Baku, Azerbaijan: abdulhuseyn.aghayev@gmail.com
https://orcid.org/0000-0003-4930-0672

Abstract. Blockchain technology is an emerging technology that has the potential to change the way information is stored and transmitted. Its main components are the concepts of decentralization, transparency and distribution, which, in short, are the absence of any central control system between the source and the destination, the interdependence of the blocks used by the participating parties as a chain, and continuously, the registration and storage, and finally, authorization processes after authentication of the information it needs by means of a key belonging to the original owner, as in asymmetric encryption, with the possibility of any loss and at the time of need, stored at millions of points. The purpose of this summary is to discuss the application of information security for data transmission against cyber attacks in blockchain technology. Different methods of implementing security measures such as encryption, digital signatures and multi-signature transactions, different types of cyber-attacks that blockchain technology is vulnerable to and how to prevent these attacks has also been discussed. Also, the role of smart contracts in ensuring secure data transfer and the importance of developing secure protocols has been emphasized. In terms of security, it has also considered the future of blockchain technology and how it can be used to further increase the security of data transmission.

Keywords: *distributed ledger, decentralization, transparency, node, hash*

1. Giriş

Blokçeyn şəbəkəsinin qurulmasının əsas üstünlüyü komponentlərindən də izah verildiyi kimi, de-mərkəzləşmiş olmasıdır ki, bu məntiqin köməkliyi ilə zəncir daxilində iştirak edən tərəflərin ötürülən məlumatlarının saxlanıldığı blokları bütün tərəflərdə qeydiyyata alınır [1, s. 24-28]. Bu tərəflərin isə özlərinin deşifrə edə bilməsi ilə onlara aid olan blokları zəncir kimi qeydə alır. Paylanmışlıq komponenti ilə bütün iştirakçılar üçün həmin zəncir daxilində kopyalanaraq saxlanılır. Ancaq, blok daxilində ötürülən datanın əvvəlki heşi (əgər ilk blok deyilsə, ilkdirsə susmaya görə 0-larla əhatələnəcək), müddəti, indiki heşi və mayninq dövrü ərzində hansı prinsipə istinad etdiyinə dair aldığı dəyər - nons (neçə dəfəyə bu heşi eyniləşdirə bilib) kimi məlumatlarla özünü formalaşdırır ki, burda da SHA256 kimi aktual və ən güclü sayılan 256 bitlik heş alqortimindən istifadə edilir [2]. Məqalə daxilində blokçeyn texnologiyası SWOT təhlil metodu ilə komponentləri ilə analiz ediləcək.

2. Komponentlərin təhlili

Blokçeyn texnologiyasının informasiya mübadiləsi, habelə daha kompleks planlar daxilində həm təhlükəsizlik, həm də aktual seçim ola bilməsi məsələsi üçün əsas komponentləri üzərindən təhlili vacibdir. Əsas komponentlərin (şəffaflıq, paylanmışlıq, de-mərkəzləşmə) SWOT (güclü, zəif, imkanları, təhdidləri) təhlil metodu üzərindən bir-biriləri ilə əlaqələndirərək, sıra ilə analiz edək.

Şəffaflıq çoxqatlı təsdiq və şifrələmə üsulları ilə tərəflərə yüksək səviyyədə təhlükəsizlik təmin edir. Şəffaflıq bir başa de-mərkəzləşmə komponentini də özü ilə daşıyır ki, bu da həmin komponentə də müvafiq üstünlüyü qatır. Ancaq, bununla belə istifadəçi sayı cəhətdən məhduddur və platforma daxilində əlavə istifadəçi cəlbi zamanı çətinlik yaradır. Təhdidləri isə, yeni olması, yəni sınaqdan keçirilə bilməməsi, təhlükəsizlik qüsurlarının olması kimi məqamlardır.

Paylanmışlıq komponenti isə özündə səmərəlilik, təhlükəsizlik, daha az xərc və şəffaflığın özünü birləşdirir. Miraslılıq, yüksək tələb və tətbiqlilik kimi imkanları özündə daşıyır. Paylanmışlıq xüsusiyyəti özündə bütün blokların qeydiyyatını daşıdığı kimi, təhdid olaraq hər zaman hücum

vektoru kimi əlçatandır və eləcə də qanun, standartlar çərçivəsində normallaşdırma problemi burda da özünü göstərir.

De-mərkəzləşmə xüsusiyyətinin əsas güclü tərəfi kimi hər hansısa asılılığın olmaması, hesabatlılığın rahatlığı, xidmət və qiymət səmərəliliyi və eləcə də, məsul tərəflərin az olması ilə problemin aşkar edilməsinin rahatlığı kimi məqamları qeyd etmək mümkündür. Zəif tərəfləri, bu kimi texnologiyaların istifadə edildiyi iqtisadi regionlarda nəzarət mexanizmləri, siyasi tətbiqi və fərqli iqtisadiyyatlara orientasiyası kimi hallar ilə tərif olunur.

3. Blokçeyn şəbəkəsində informasiya mübadiləsi zamanı baş verə biləcək kibertəhdidlər

Blokçeyn şəbəkəsi ilə informasiyanın ötürülmə prinsipi və ötürülməsi prosesinin kökündə duran məsələlərə aydınlıq gətirdikdən sonra, bu prosesin təhdidləri, aktual olaraq, hansı risklərlə qarşılaşma ehtimalı ilə bağlı məqamlara və onlardan mühafizə üsulları, habelə onlara qarşı mexanizmlərə aydınlıq gətirək.

Blokçeyn texnologiyasında TCP/UDP nəqliyyat protokollarından da bildiyimiz paketlər kimi, blokçeyn texnologiyasında da məhz belə bloklar zəncir formasında toplanır və vahid nod şəklində formalaşır. Daha sonra isə, paylanmışlıq komponenti ilə bütün iştirakçılar üçün həmin zəncir daxilində kopyalanaraq saxlanılır. Məhz təhdidlərdən biri, zərərli nodlar sayılır. Şəbəkədə zərərli nodlar məlumatları oğurlamaq və ya tranzaksiya, əməliyyatlara müdaxilə etmək üçün istifadə edilir [3]. Bu nodlar istifadəçiləri cəlb etmək və onların məlumatlarını oğurlamaq üçün "Bal qabı" kimi çıxış edir. Həmçinin blokçeyn zəncirində saxlanılan məlumatları manipulyasiya etmək və ya şəbəkənin konsensus mexanizmini pozmaq üçün istifadə edilir [4, s. 80-84]. Təkrarlanan hücumlarda hücum edən tərəfin pul və ya məlumatlara çıxış əldə etmək üçün aktual tranzaksiya və ya əməliyyatı təkrarladığı hücum növüdür. Bu növ hücum blokçeyn şəbəkəsində əməliyyatların tamlığı üçün dinamik adlı olduğundan mümkündür, çünki zərərverici orijinal deşifrə metodu ilə göndərənin kopyalaya və ya başqa noda yönləndirə bilir [3]. Sybil hücumları hücum edən tərəfin şəbəkə daxilində çoxsaylı nodlara nəzarət etmək üçün çoxsaylı tərəflər yaradan hücum növü kimi sayılır. Bu zərərvericilərə məlumatlı və əməliyyatları manipulyasiya etməyə imkan yaradır. DDoS hücumu da bu şəbəkələr daxilində ən aktual hücum növlərindən biridir. Kiberhücumlardan da bildiyimiz kimi, onlayn xidmətlərdə çoxsaylı məmbələrdən sorğular göndərərək, mənsəb tərəfinin əlçatanlığına qarşı edilən hücum [3]. Blokçeyn məhz bu növ hücumlara qarşı çox həssasdır, çünki nəzarət mexanizmi və de-mərkəzləşmə bu istiqamətdə təhdid yaradır. Yarış hücumu da bu hücum növlərindən biridir. İki və ya daha çox tranzaksiya şəbəkədə eyni nodda sürətli ardıcıllıqla göndərildikdə baş verən hücum növüdür. Bu hücum növündə zərərverici öz hesabından qarşı tərəfə pul köçürmək üçün nod göndərdikdə, bu əməliyyat emal edilməzdən öncə, ilk əməliyyatı geri qaytaran ikinci əməliyyatı icra edir [5, s. 394-411]. Finney hücumunda isə, zərərverici mayner onun ünvanına ödəniş edən əməliyyat yarada və onu özündə cəmləyən blokları yenidən mayninq formasında özünə qazandıra bilər. Bu hücum Hal Finney-in adını daşıyır ki, həmin şəxs məhz ilk olaraq bu təklifi irəli sürmüşdü. Bu hücumlardan əlavə 51% hücumu da yuxarda qeyd etdiyimiz hücumlardan [6].

4. Blokçeyn şəbəkəsində informasiya mübadiləsi zamanı baş verə biləcək kibertəhdidlərə qarşı mexanizmlərin işlənməsi

İdeal sistem və ya şəbəkə olmasa da, əsas məqsəd risk vektorunu və təhdidlərin qlobal problemlərini daimi aradan qaldırmaq və onlara qarşı əks-tədbir planları həyata keçirmək mütləqdir. Çoxfaktorlu autentifikasiya, biometrik metodlar bunlara nümunədir [7]. Rolları müəyyənləşdirərək, avtorizasiya edən zaman icazə və səlahiyyətləri aydınlaşdırmaq lazımdır. Hər lokal şəbəkə kimi, bu şəbəkəni də xarici müdaxilələrdən qorumaq üçün müəyyən avadanlıqlarla (şəbəkələrarası ekran, bal qabı, Veb tətbiqlər üçün şəbəkələrarası ekran, yük balanslaşdırıcısı və s.) təmin etmək lazımdır. Daimi olaraq, şəbəkə üzərindən edilən aktlara nəzarət və monitorinq imkanı yaradılmalı və daimi audit həyata keçirilməlidir [8].

Şəbəkəyə daxil olduqda isə daha da kompleks mexanizmlərlə işləmək üçün, icazə verilən bloklar üzərindən məlumat mübadiləsi və ya əməliyyatların icrası və nəzarəti təmin edilməlidir. Cihazların təhlükəsizlik modullarından daimi istifadəsi təmin edilməlidir ki, şifrələmə ilə birgə blokçeyn məlumatlarını çoxqatlı qorunmasına köməklik göstərəcək [6]. De-mərkəzləşmiş proqramlar vasitəsilə birdən çox maşına yerləşdirməklə, məlumatların tamlığını qorumağa və kiberhücum riskini azaltmağı təmin etmək də mümkün edir [9].

Kiberhücum üzərindən xüsusi tədbirlər kimi aşağıdakı hallara riayət etmək olar:

1. Alternativ konsensus alqoritm istifadəsi: məsələn, Səhm çıxarışı (Proof of Stake - PoS) kimi 51% hücumlara daha davamlı olan alqoritmlər;
2. Çoxsaylı yoxlama nöqtələrinin istifadəsi: blokçeyn şəbəkəsində etibarlılığını yoxlamaq üçün istifadə edilə bilən yoxlama məntəqələri ilə Finney hücumu kimi ikiqat gəlirliliyin qarşısını alır;
3. Təyin edilmiş şahid (SegWit) istifadəsi: əməliyyatın imzalanmasını blokçeyn şəbəkəsindən ayırır və bu da zərərvericilərin şəbəkədə informasiyanı təhrif edə bilməməsinə hədəflənir;
4. Daha uzunmüddətli blok müddətlərinin tətbiqi: daha çox şəbəkəyə nəzarət etməyi çətinləşdirməsi üçün;
5. Hücumun dəyərini artırmaq: bunun vasitəsilə 51% kimi hücumun tətbiqi daha da çətinləşir ki, mayninq edən tərəf daha çox resursa sahib olmalıdır və risk (motivasiya mənbəyi maddi gəlir) vektoru daha da kompleksləşir;
6. Reputasiya sistemlərinin tətbiqi: keçmiş fəaliyyətə əsaslanaraq zərərverici tərəfləri müəyyənləşdirmək;
7. Sosial verifikasiya: CAPCTHA və ya daha uyğun verifikasiya metodları;
8. Əlaqə saylarının limitləndirilməsi: Sybil kimi hücumların qarşısını almaqda daha effektivdir;
9. Şəbəkənin fəaliyyətinin monitorinqi: Sybil hücumlarının tədqiqinə imkan yaradır;
10. Rəqəmsal imzaların tətbiqi: saxta şəxsiyyətlərin yaradılmasının qarşısını alır;
11. Dərəcə limitləyicisi (Rate Limiting): göndəriləcək tərəfə sorğuların sürətinə nəzarəti ilə birgə DDoS kimi hücumların qarşısını almaqda effektivdir;
12. Ödəniş markeri: Yarış hücumlarını aşkar etməyə imkan yaradır ki, ödəniş hədəfləri və prioritetini müəyyənləşdirməsində rol oynayır;
13. Təhlükəsiz ödəniş protokolları;
14. Server vaxtının sinxronizasiyası: bütün sorğuların eyni müddətdə və sıralama ilə icrasınn təmin edir;
15. Tranzaksiya təkrarlarının tətbiqi: Tranzaksiya təkrarı Finney hücumunun qarşısını almaq üçün bir çox şəbəkəyə əməliyyatları təkrarlayır və bu zaman zərərverici hücumu həyata keçirə bilməsi üçün iki dəfədən də çox xərc etməlidir;
16. Nons;

Bu siyahını daha da çox artırmaq mümkündür, çünki bu şəbəkədə hələ təhdidlər və hücum vektorları çox genişdir. Bu kimi tətbiqlərlə riski minimuma endirə bilmək mümkün olsa da, informasiyaya qarşı təhdid daim mövcuddur [10].

5. Nəticə

Qeyd edildiyi kimi blokçeyn şəbəkəsində informasiyanın təhrif olunması riski, eləcə də paylaşılanlıqla birgə manipulyasiyaya meyillik olsa da, informasiya mübadiləsi riskinin aktual riskləri və təhdidləri üçün müəyyən mexanizmlərlə tədbir planları qurmaq mümkündür. Blokçeyn şəbəkələrində informasiya mübadiləsi zamanı baş verə biləcək kibertəhdidlər üçün ilkin risk vektorunu təyin etməyin metodları qeyd edilmişdir. Texnologiyanın davamlı inkişafında metodların versiya olaraq, statik qalmaması və davamlı zəifliklərlə qarşılaşmasını nəzərə alaraq, metodların izahları daha geniş təhrif edilmişdir. Statik yanaşmaların texnologiya inkişaf etdikcə aktuallığını və effektivliyini itirməsi dinamik yanaşmanı daha da aktual edir. Paylanmış reyestri tərifi zamanı qeyd edildiyinə əsasən, blokçeyn texnologiyası informasiyanın saxlanma və ötürmə üsulunda inqilab etmə potensialına malikdir. O,

misilsiz səviyyələrdə təhlükəsizlik, məxfilik, şəffaflıq və de-mərkəzləşmə təklif edir, istifadəçilər üçüncü tərəfə və ya mərkəzi sistemə ehtiyac olmadan məlumatları təhlükəsiz şəkildə saxlamağa və ötürməyə imkan verir. Bundan əlavə blokçeyn, texnologiyası prosesləri avtomatlaşdıra və xərcləri azalda bilən ağıllı müqavilələr kimi yeni proqram növlərini inkişaf etdirmək üçün istifadə edilə bilər ki, bunların da öz təhdidləri və həll yolları ilə bağlı təkliflər irəli sürülmüşdür. Çünki, ağıllı müqavilələr avtomatlaşdırılmış və de-mərkəzləşmənin daha aktual olduğu mühitlərdə daha obyektiv yanaşmanı tətbiq etməyə imkan yaradır.

ƏDƏBIYYAT

1. Blockchains: The great chain of being sure about things by Alex Tapscott and Don Tapscott, 2016, 348 s.
2. Zhong H., Li Y., & Zhang, Y. (2020). A Comprehensive Survey on Security and Privacy of Blockchain Systems. IEEE Access, 8, s. 36-62.
3. Li J., Gervais A., Karame G.O., Capkun S. "Security and privacy challenges in blockchain systems," Computer, vol. 50, no. 7, 2017, s. 259-286.
4. Blockchain Technology Explained: The Ultimate Beginner's Guide About Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts by Mark Gates, 2019, 122 s.
5. Wust, K., Bano, S., & Meiklejohn, S. (2018). A secure sharding protocol for open blockchains. In 2018 IEEE Symposium on Security and Privacy (SP). IEEE, s. 82-88.
6. Ha S.J., Li M., Yoon M. L. "A survey of attacks and defences on blockchain technology," International Journal of Network Security, vol. 20, no. 2, 2018, s. 191-220.
7. Li X., Li J., & Liu C. (2019). A survey on security and privacy in blockchain systems. Information Fusion, 50, s. 36-44.
8. Valli S.K. "A survey of blockchain security issues and challenges," International Journal of Computer Science and Information Security, vol. 16, no. 11, 2018, s. 140-151.
9. Lee S., Kim S., & Kim Y. (2017). Anomaly Detection-based Defense against Malicious Nodes in Blockchain Networks. In 2017 IEEE International Conference on Blockchain (ICBC). IEEE, s. 10-14.
10. Al-Nemrat A. "Blockchain cyber-attacks: An analysis of threats and mitigation techniques," International Journal of Computer Applications, vol. 159, no. 20, 2018, s. 16-23.

BLOKÇEYN ŞƏBƏKƏSİNİN KOMPONENTLƏRİNİN İŞLƏNMƏSİ İLƏ İNFORMASİYA MÜBADİLƏSİNİN TƏHLÜKƏSİZLİYİ

A.V.Ağayev

Xülasə. Blokçeyn texnologiyası informasiyanın saxlanması və ötürülməsi üsulunu dəyişdirmək potensialına malik yeni inkişaf edən bir texnologiyadır. Əsas komponentləri de-mərkəzləşmə, şəffaflıq və paylanmışlıq anlayışlarıdır ki, bunlara qısaca müvafiq olaraq, mənbə və təyinat arasında hər hansısa mərkəzi idarəetmə sisteminin olmaması, iştirak edən tərəflərin istifadə etdikləri blokların zəncir kimi bir birilərindən asılılığı və davamlı olaraq, qeydiyyata alınması və saxlanması, və son olaraq, milyonlarla nöqtədə saxlanılaraq, hər hansısa itkinin olmama ehtimalı və ehtiyac anında assimmetrik şifrələmədə olduğu kimi, əsl sahibinə məxsus açar vasitəsilə ona lazım olan məlumatın autentifikasiya edildikdən sonra, avtorizasiyası prosesləridir. Məqalənin əsas məqsədi blokçeyn texnologiyasının məlumat ötürülməsi zamanı kiberhücumlara qarşı informasiya təhlükəsizliyinin tətbiqinin müzakirəsidir. Şifrləmə, rəqəmsal imza və çox imzalı əməliyyatlar kimi təhlükəsizlik tədbirlərinin həyata keçirilməsinin müxtəlif üsulları, blokçeyn texnologiyasının həssas olduğu müxtəlif kiberhücum növləri və bu hücumların qarşısının necə alınacağı da müzakirə edilib. Eləcə də, təhlükəsiz məlumat ötürülməsinin təmin edilməsində ağıllı müqavilələrin rolunu və təhlükəsiz protokolların hazırlanmasının vacibliyi vurğulanıb. Həmçinin, təhlükəsizlik aspektindən baxıldıqda, blokçeyn texnologiyasının gələcəyi və onun məlumat mübadiləsi zamanı təhlükəsizliyini daha da artırmaq üçün necə istifadə oluna biləcəyi nəzərdən keçirilib.

Açar sözlər: *paylanmış reyestr, de-mərkəzləşmə, şəffaflıq, nod, heş.*

Accepted: 20.11.2023