Informatics

ÜSTÜN MƏXFİLİYİN QORUNMASI TEXNİKALARI İLƏ AĞILLI MÜQAVİLƏLƏRDƏ MƏLUMAT MƏXFİLİYİNİN TƏKMİLLƏŞDİRİLMƏSİ

Abdulhüseyn Vəfadar oğlu Ağayev
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan

THE ENHANCING DATA CONFIDENTIALITY IN SMART CONTRACTS THROUGH THE ADVANCED PRIVACY-PRESERVING TECHNIQUES

Abdulhuseyn Vafadar Aghayev
Azerbaijan Technical University, Baku, Azerbaijan: abdulhuseyn.aghayev.v@student.aztu.edu.az
https://orcid.org/0000-0003-4930-0672

Abstract. This research paper delves into the imperative domain of bolstering data confidentiality within smart contracts through the integration of advanced privacy-preserving methodologies. Smart contracts, pivotal components of blockchain technology, execute self-executing contracts with predefined conditions and are increasingly utilized across various sectors, necessitating stringent data protection measures. The paper addresses the pressing need for fortified data privacy within smart contracts and investigates cutting-edge approaches to mitigate privacy challenges. Two focal techniques under scrutiny are zero-knowledge proofs (SBÇs) and homomorphic encryption. SBÇs facilitate the validation of computations without revealing sensitive data, enabling parties to verify transaction authenticity without disclosing the underlying information. Meanwhile, homomorphic encryption permits computations on encrypted data, preserving confidentiality by allowing operations on encrypted information without the need for decryption. By analyzing these advanced privacy-preserving techniques, this study aims to address the vulnerabilities in data confidentiality present in smart contracts. Its findings hold significant promise in fortifying the security and confidentiality of transactions, thus contributing substantially to the evolution of secure blockchain technology. This research underscores the pivotal role of innovative privacy-enhancing mechanisms in safeguarding sensitive data within smart contracts, ensuring the trust and integrity essential for their widespread adoption.

Keywords: *zero-knowledge proofs, confidentiality, homomorphic encryption, secure transactions.*

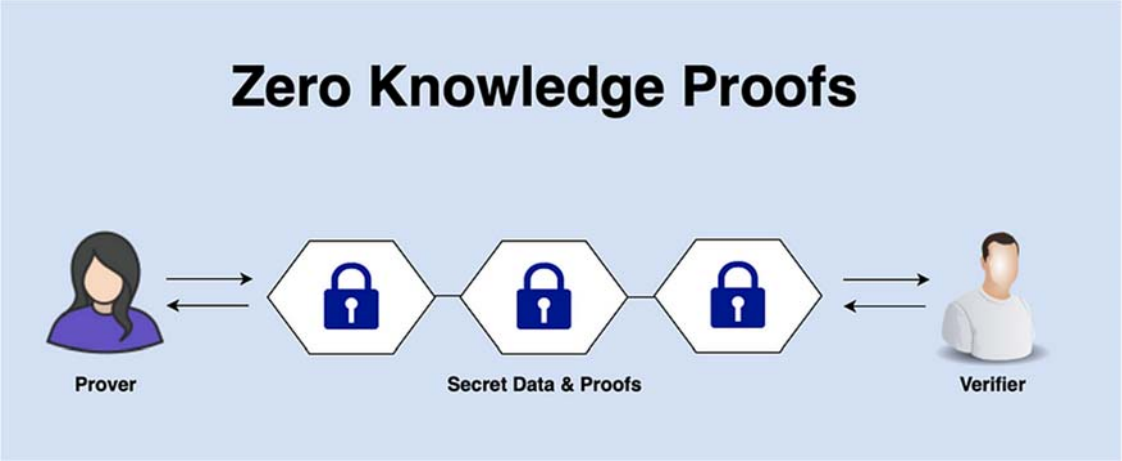
Giriş

Blokçeyn texnologiyası sahəsində ağıllı müqavilələr əvvəlcədən müəyyən edilmiş şərtlərlə özünü icra edən müqavilələr kimi dayanır və sənayelərarası əməliyyatlarda inqilab edir. Lakin onların yeniliklərinə və səmərəliliyinə baxmayaraq, ağıllı müqavilələrin özünəxas şəffaflığı kritik bir narahatlıq doğurur: həssas məlumatların zəifliyi. Bu müqavilələr mərkəzləşdirilməmiş şəbəkələrdə işlədiyi üçün məlumatların məxfiliyi etibarlılığın, təhlükəsizliyin və uyğunluğun təmin edilməsində diqqət mərkəzinə çevrilir. Ağıllı müqavilələr çərçivəsində məlumat məxfiliyinin gücləndirilməsinin vacib vəzifəsinin müzakirə edilməsi və təkmilləşdirilmiş məxfilik tədbirlərinə təcili ehtiyacın həlli vacib məqamdır. Maliyyə əməliyyatlarından tutmuş şəxsi qeydlərə qədər həssas məlumatların aşkarlanması potensial pozuntulara və icazəsiz girişə qarşı ciddi qorunma tələb edir. Məlumatların məxfiliyinin təmin edilməsi təkcə texniki problem deyil, həm də müxtəlif sənaye sahələrində istifadəçi inamını və qanunlara uyğunluğu artırmaq üçün fundamental məsələdir.

Ağıllı müqavilələrdə təhlükəsizlik zəifliklərini azaltmağa yönəlmiş innovativ məxfiliyi qoruyan üsullar vasitəsilə irəliləməsi ən aktual məsələdir. Xüsusilə, məlumatların məxfiliyini artırmaq üçün üstün metodologiyalar kimi SBÇ-lər və homomorfik şifrələmənin tətbiqlərinin tədqiqatı çox önəmlidir. Tranzaksiyaları yoxlamaq və şifrələnmiş məlumatlar üzərində hesablamalar aparmaq üçün yeni üsullar təqdim edən bu imkanlar ağıllı müqavilələr çərçivəsində həssas məlumatların qorunmasında əhəmiyyətli irəliləyişi təmsil edir. Ağıllı müqavilələr müxtəlif sənaye sahələrinə nüfuz etməyə davam etdikcə, məxfiliyi qoruyan güclü texnikaların tətbiqi vacib olur. Bu araşdırma təkcə məlumatların məxfiliyini gücləndirmək üçün deyil, həm də blokçeyn əsaslı əməliyyatlarda etimad və bütövlüyü təşviq etmək üçün bu inkişafların əhəmiyyətini izah etmək məqsədi daşıyır.

Ağıllı müqavilələrdə Sıfır-Bilik çıxarışları

Sıfır Bilik Sübutları (SBÇ) mürəkkəb şifrələmə texnikasını təmsil edir ki, bu da bir tərəfə çıxarışın həqiqətindən kənar heç bir məlumatı aşkar etmədən digər tərəfə çıxarışın doğruluğunu yoxlamağa imkan verir (Şəkil) [1]. Ağıllı müqavilələr kontekstində SBÇ-lər əməliyyatların bütövlüyünü və həqiqiliyini yoxlayarkən məlumatların məxfiliyinin təmin edilməsində əsas rol oynayır.



Sıfır-Bilik Çıxarışı (SBÇ) [6]

1. **Təkmilləşdirilmiş məxfilik:** SBÇ-lər ağıllı müqavilələrdə güclü mexanizm təqdim edir ki, bu da əməliyyat iştirakçılarına həssas məlumatları aşkarlamadan, əməliyyatların doğruluğunu yoxlamağa imkan verir [2]. Bu imkan müvafiq məlumatların məxfiliyini qoruyarkən əməliyyatın düzgünlüyünün yoxlanılmasını təmin edir və mərkəzləşdirilməmiş sistemlərdə məlumatların konfidensiallığının pozulması ilə bağlı mühüm narahatlığı aradan qaldırır.
2. **Açıqlamadan əməliyyatların yoxlanılması:** SBÇ-lərin əsas üstünlüklərindən biri onların xüsusi əməliyyat təfərrüatlarını açıqlamadan hesablamaları və əməliyyatları yoxlamaq qabiliyyətindədir [3]. Bu funksionallıq məxfiliyə xələl gətirmədən məlumatların və ya əməliyyatların düzgünlüyünü və qanuniliyini təsdiq etməyin vacib olduğu hallarda həyati əhəmiyyət kəsb edir.
3. **Məxfiliyi qoruyan autentifikasiya:** SBÇ-lər müəyyən edilə bilən məlumatları aşkar etmədən ağıllı müqavilələrdə istifadəçilərin şəxsiyyətini yoxlamaq üçün bir üsul təqdim edir [4]. Bu xüsusiyyət, maraqlı tərəflərin legitimliyini yoxlamaqla yanaşı, istifadəçi autentifikasiya proseslərinin məxfiliyi qorumağa davam etməsini təmin edir. Bu, şəxsi məlumatların açıqlanmasına ehtiyac olmadan istifadəçinin şəxsiyyətini yoxlamağa imkan verir.

SBÇ-lərin ağıllı müqavilələrə inteqrasiyası məlumatların məxfiliyi problemlərini aradan qaldırmaq üçün güclü həll yoludur. Bu kriptoqrafik protokollardan istifadə etməklə ağıllı müqavilələr etibarlı şəkildə işləyə və ciddi məxfilik standartlarını qoruyarkən iştirakçılar arasında etimadı artıra bilər [5].

Bundan əlavə, SBÇ-lərin istifadəsi ağıllı müqavilə funksionallığı üçün vacib olan yoxlama və yoxlama aspektlərinə xələl gətirmədən istifadəçi məxfiliyinə üstünlük verən mərkəzləşdirilməmiş sistemlərin inkişafına əhəmiyyətli dərəcədə töhfə verir [6].

Homomorfik Kriptoqrafiya və ağıllı müqavilələrdə tətbiqi

Homomorfik şifrələmə şifrənin açılmasına ehtiyac olmadan məlumatların məxfiliyini qoruyaraq şifrələnmiş verilənlər üzərində hesablamalar aparmağa imkan verən kriptoqrafik paradiqmadır [7]. Onun ağıllı müqavilələrə inteqrasiyası təhlükəsiz hesablamalara imkan verərkən məlumatların məxfiliyini təmin etmək üçün təməlqoyma həlli təklif edir:

- **Şifrələnmiş məlumatlar üzrə təhlükəsiz hesablamalar:** Homomorfik şifrələmə ağıllı müqavilələrə proses boyu həssas məlumatların məxfiliyini qoruyaraq birbaşa şifrələnmiş məlumatlar

üzərində hesablamalar aparmağa imkan verir [8]. Bu imkan, əsas məlumatları aşkar etmədən məxfiliyi qoruyarkən hesablamaların aparılmasını təmin edir.

- **Məxfiliyi qoruyan məlumat əməliyyatları:** Ağıllı müqavilələr çərçivəsində homomorfik şifrələmə şifrələnmiş məlumatlar üzərində müxtəlif əməliyyatların həyata keçirilməsinə icazə verməklə həssas məlumatların məxfi qalmasını təmin edir [9]. Bu funksionallıq məlumatların icazəsiz ələ keçməsinin qarşısını alaraq onların təhlükəsiz işlənməsini təmin edir.
- **Şifrələnmiş əməliyyatların yoxlanılması:** Homomorfik şifrələmə şifrəsi açılmış məlumatları aşkar etmədən hesablamaları və əməliyyatları yoxlamağa imkan verir [10]. Bu xüsusiyyət hesablamaların düzgünlüyünün və qanunauyğunluğunun yoxlanılmasını təmin edir, əsas həssas məlumat isə şifrələnmiş və təhlükəsiz olaraq qalır.

Ağıllı müqavilələrə Homomorfik Kriptoqrafiyanın tətbiq edilməsi məlumatların məxfiliyinin və konfidensiyallığının təmin edilməsi istiqamətində mühüm addımdır. O, şifrələnmiş məlumatlarda hesablamalara icazə verərək və blokçeyn şəbəkəsinin bütövlüyünü qoruyaraq, təhlükəsiz və fərdi əməliyyatlar üçün yol açır. Homomorfik Kriptoqrafiyanın tətbiqi təhlükəsiz və məxfiliyi qoruyan ağıllı müqavilə ekosistemlərinin yaradılmasına əhəmiyyətli töhfə verir [11]. Onun tətbiqi hesablama prosesləri zamanı həssas məlumatların şifrələnmiş qalmasını təmin etməklə mərkəzləşdirilməmiş sistemlərdə məlumatların konfidensiallığının və məxfiliyin pozulması ilə bağlı narahatlıqları aradan qaldırır.

Nəticə

SBÇ-lər və Homomorfik Kriptoqrafiyanın ağıllı müqavilələrə inteqrasiyası mərkəzləşdirilməmiş sistemlərdə məlumatların məxfiliyinin və əməliyyatların bütövlüyünün gücləndirilməsi istiqamətində transformativ addım kimi dayanır. Lakin bu innovativ üsullar təkmilləşdirilmiş məxfilik və təhlükəsizliyə yol açdıqca, gələcək tədqiqatlar və potensial problemlər üçün bir neçə yol yaranır. Bu sahədə gələcək tədqiqatlar ağıllı müqavilə mühitlərində SBÇ-lər və Homomorfik Kriptoqrafiyanın səmərəliliyinin və miqyasının artırılmasına yönəldilə bilər. Hesablama yükünü və emal vaxtlarını azaltmaq üçün bu üsulların sadələşdirilməsi onların geniş yayılmasına əhəmiyyətli dərəcədə kömək edəcəkdir.

Bundan əlavə, bu məxfiliyi qoruyan metodların potensial zəiflikləri və məhdudiyyətlərinin aradan qaldırılması tədqiqat üçün mühüm sahə olaraq qalır. SBÇ-lərin və Homomorfik Kriptoqrafiyanın tətbiqində zəifliklərin başa düşülməsi və yumşaldılması yaranan təhdidlərə və hücumlara qarşı möhkəm təhlükəsizliyin təmin edilməsi üçün çox vacibdir. Habelə, blokçeyn platformaları və ağıllı müqavilə ekosistemləri arasında qarşılıqlı fəaliyyət və standartlaşdırma da problemlər yaradır. Gələcəkdə SBÇ-lərin və Homomorfik Kriptoqrafiyanın müxtəlif blokçeyn şəbəkələrində problemsiz inteqrasiyasını asanlaşdıran universal freymvörklərin inkişafına yönəldilə bilər. Proqramçılar, istifadəçilər və tənzimləyici qurumlar arasında bu üstün kriptoqrafik üsulların öyrədilməsi və mənimsənilməsi həyati əhəmiyyət kəsb edəcək. Bu üsullar inkişaf etdikcə, inkişaf edən məxfilik qaydalarına hərtərəfli başa düşülmə və uyğunluğun təmin edilməsi onların real dünya tətbiqlərinə uğurlu inteqrasiyası üçün vacib olacaqdır.

Yekun olaraq, SBÇ-lər və Homomorfik Kriptoqrafiya ağıllı müqavilələr çərçivəsində məlumatların məxfiliyi ilə bağlı problemlərə perspektivli həllər təklif etsə də, davam edən tədqiqat səyləri gizlilik, təhlükəsizlik və mərkəzləşdirilməmiş sistemlərə etibarın təmin edilməsində öz potensiallarını reallaşdırmaq üçün miqyaslılıq, təhlükəsizlik zəifliklər, qarşılıqlı fəaliyyət və təlim təşəbbüslərini həll etməlidir.

ƏDƏBIYYAT

1. Goldwasser, S., Micali, S., & Rackoff, C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1), 1989, p. 186-208.
2. Ben-Sasson E., Chiesa A., Tromer E. & Virza M. Succinct non-interactive zero knowledge for a von Neumann architecture. In Advances in Cryptology – EUROCRYPT 2014 Springer, p. 90-108. https://eprint.iacr.org/2013/879.pdf

3. Groth J. Short pairing-based non-interactive zero-knowledge arguments. In Advances in Cryptology – EUROCRYPT 2010 Springer, p. 321-340. https://www.iacr.org/archive/asiacrypt2010/6477323/6477323.pdf
4. Micali S., Rabin M.O. & Kilian J. Zero-knowledge sets. In Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, Springer, 2000, p. 185-196.
5. Camenisch J. & Stadler M. Efficient group signature schemes for large groups. In Advances in Cryptology – EUROCRYPT'97, Springer, 1997, p. 410-424. https://link.springer.com/chapter/10.1007/BFb0052252
6. https://miro.medium.com/v2/resize:fit:828/format:webp/1*yxf5aQNPsJFi2Zdc8z779A.png
7. Gentry C. A fully homomorphic encryption scheme. Stanford University, Tech. Rep, 2009(2), p. 1-36. https://crypto.stanford.edu/craig/craig-thesis.pdf
8. Brakerski Z. & Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2011, p. 505-524.
9. van Dijk M., Gentry C., Halevi S. & Vaikuntanathan V. Fully homomorphic encryption over the integers. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2010, s. 24-43.
10. Smart N.P. Fully homomorphic encryption primitives. Cryptology ePrint Archive, Report 2010, 169 p.
11. Gentry C. & Halevi S. Implementing Gentry's fully-homomorphic encryption scheme. Advances in Cryptology– EUROCRYPT 2011, Springer, p. 129-148. https://eprint.iacr.org/2010/520.pdf

ÜSTÜN MƏXFİLİYİN QORUNMASI TEXNİKALARI İLƏ AĞILLI MÜQAVİLƏLƏRDƏ MƏLUMAT MƏXFİLİYİNİN TƏKMİLLƏŞDİRİLMƏSİ

A.V.Ağayev

Xülasə. Bu tədqiqat işində üstün məxfiliyi qoruyan metodologiyaların inteqrasiyası vasitəsilə ağıllı müqavilələr daxilində məlumat məxfiliyinin artırılması araşdırılmışdır. Blokçeyn texnologiyasının əsas komponentlərindən biri olan ağıllı müqavilələr əvvəlcədən müəyyən edilmiş şərtlərlə özünü icra edən müqavilələrin işləməsini təmin edir və ciddi məlumatların qorunması tədbirləri tələb edən müxtəlif sənaye sahələrində getdikcə daha çox istifadə olunur. Məqalədə ağıllı müqavilələr daxilində məlumatların məxfiliyinin gücləndirilməsinin əhəmiyyətindən bəhs edilir və məxfilik problemlərini azaltmaq üçün üstün yanaşmalar araşdırılır. Baxılan iki əsas üsul sıfır-bilik çıxarışları (SBÇ) və homomorfik şifrələmədir. SBÇ-lər həssas məlumatları aşkar etmədən hesablamaların yoxlanılmasını asanlaşdırır, tərəflərə həssas məlumatları aşkar etmədən əməliyyatın həqiqiliyini yoxlamağa imkan verir. Eyni zamanda, homomorfik şifrələmə şifrənin açılmasına ehtiyac olmadan şifrələnmiş məlumatlar üzərində hesablamaların aparılmasına imkan verməklə məxfiliyi qoruyur. Tədqiqatda əsas məqsəd qabaqcıl məxfiliyi qoruyan bu texnikaları təhlil edərək, ağıllı müqavilələrdə mövcud olan məlumatların məxfiliyinə dair zəifliklərin həllini araşdırmaqdır. Onların tapıntıları əməliyyatların təhlükəsizliyinin və məxfiliyinin yaxşılaşdırılmasında əhəmiyyətli vədlər verir və bununla da təhlükəsiz blokçeyn texnologiyasının inkişafına önəmli töhfə verir. Bu araşdırma ağıllı müqavilələrdə məxfi məlumatların qorunmasında, onların geniş şəkildə mənimsənilməsi üçün tələb olunan etimadın və dürüstlüyün təmin edilməsində innovativ məxfiliyi artıran mexanizmlərin əsas rolunu vurğulayır.

Açar sözlər: *sıfır-bilik çıxarışları, məxfilik, homomorfik şifrələmə, təhlükəsiz tranzaksiyalar.*

Accepted: 11.03.2024