ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

КАЙЫРЫМДЫЛЫҚ ҚОРЫ HALYK CHARITY FOUNDATION

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ
«ХАЛЫҚ» ЖҚ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК РЕСПУБЛИКИ КАЗАХСТАН»
ЧФ «Халық»

NEWS

OF THE ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
«Halyk» Private Foundation

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

1 (349)

JANUARY – MARCH 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

ЧФ «ХАЛЫҚ»

В 2016 году для развития и улучшения качества жизни казахстанцев был создан частный Благотворительный фонд «Халык». За годы своей деятельности на реализацию благотворительных проектов в областях образования и науки, социальной защиты, культуры, здравоохранения и спорта, Фонд выделил более 45 миллиардов тенге.

Особое внимание Благотворительный фонд «Халык» уделяет образовательным программам, считая это направление одним из ключевых в своей деятельности. Оказывая поддержку отечественному образованию, Фонд вносит свой посильный вклад в развитие качественного образования в Казахстане. Тем самым способствуя росту числа людей, способных менять жизнь в стране к лучшему – профессионалов в различных сферах, потенциальных лидеров и «великих умов». Одной из значимых инициатив фонда «Халык» в образовательной сфере стал проект Ozgeris powered by Halyk Fund – первый в стране бизнес-инкубатор для учащихся 9-11 классов, который помогает развивать необходимые в современном мире предпринимательские навыки. Так, на содействие малому бизнесу школьников было выделено более 200 грантов. Для поддержки талантливых и мотивированных детей Фонд неоднократно выделял гранты на обучение в Международной школе «Мирас» и в Astana IT University, а также помог казахстанским школьникам принять участие в престижном конкурсе «USTEM Robotics» в США. Авторские работы в рамках проекта «Тәлімгер», которому Фонд оказал поддержку, легли в основу учебной программы, учебников и учебно-методических книг по предмету «Основы предпринимательства и бизнеса», преподаваемого в 10-11 классах казахстанских школ и колледжей.

Помимо помощи школьникам, учащимся колледжей и студентам Фонд считает важным внести свой вклад в повышение квалификации педагогов, совершенствование их знаний и навыков, поскольку именно они являются проводниками знаний будущих поколений казахстанцев. При поддержке Фонда «Халык» в южной столице был организован ежегодный городской конкурс педагогов «Almaty Digital Ustaz.

Важной инициативой стал реализуемый проект по обучению основам финансовой грамотности преподавателей из восьми областей Казахстана, что должно оказать существенное влияние на воспитание финансовой грамотности и предпринимательского мышления у нового поколения граждан страны.

Необходимую помощь Фонд «Халык» оказывает и тем, кто особенно остро в ней нуждается. В рамках социальной защиты населения активно проводится работа по поддержке детей, оставшихся без родителей, детей и взрослых из социально уязвимых слоев населения, людей с ограниченными возможностями, а также обеспечению нуждающихся социальным жильем, строительству социально важных объектов, таких как детские сады, детские площадки и физкультурно-оздоровительные комплексы.

В копилку добрых дел Фонда «Халык» можно добавить оказание помощи детскому спорту, куда относится поддержка в развитии детского футбола и карате в нашей стране. Жизненно важную помощь Благотворительный фонд «Халык» оказал нашим соотечественникам во время недавней пандемии COVID-19. Тогда, в разгар тяжелой борьбы с коронавирусной инфекцией Фонд выделил свыше 11 миллиардов тенге на приобретение необходимого медицинского оборудования и дорогостоящих медицинских препаратов, автомобилей скорой медицинской помощи и средств защиты, адресную материальную помощь социально уязвимым слоям населения и денежные выплаты медицинским работникам.

В 2023 году наряду с другими проектами, нацеленными на повышение благосостояния казахстанских граждан Фонд решил уделить особое внимание науке, поскольку она является частью общественной культуры, а уровень ее развития определяет уровень развития государства.

Поддержка Фондом выпуска журналов Национальной Академии наук Республики Казахстан, которые входят в международные фонды Scopus и Wos и в которых публикуются статьи отечественных ученых, докторантов и магистрантов, а также научных сотрудников высших учебных заведений и научно-исследовательских институтов нашей страны является не менее значимым вкладом Фонда в развитие казахстанского общества.

С уважением,
Благотворительный Фонд «Халык»!

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.).
Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*

Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.

Тематическая направленность: *серия физика и информационные коммуникационные технологии.*

В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*

Периодичность: *4 раз в год.*

Тираж: *300 экземпляров.*

Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*

http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1. Namber 349 (2024). 136–151
https://doi.org/10.32014/2024.2518-1726.247

UDC 004.4

© A.M. Jumagaliyeva[1], A.A. Shekerbek[2*], M.G. Baibulova[2], A.I. Ongarbayeva[2],A. Tokkuliyeva[2], 2024
[1]Kazakh University of Technology and Business, Astana, Kazakhstan;
[2]Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan.
E-mail: *shekerbek80@mail.ru*

ANALYSIS OF IMPLEMENTATION BLOCKCHAIN TECHNOLOGY TO ELECTRONIC VOTING SYSTEM

Jumagaliyeva Ainur Maxsimovna — Senior Lecturer, Department of Information Technology Kazakh University of Technology and Business Astana, Kazakhstan
E-mail: *jumagalievaainur.m@gmail.com*, *https://orcid.org/0000-0001-8632-5209;*
Shekerbek Ainur Azimbaevna — Doctoral student of the Department of Information Systems of the Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
E-mail: *shekerbek80@mail.ru, https://orcid.org/0000-0002-1088-42391;*
Baibulova Makbal Gabbasovna — Senior Lecturer, Department of Information Systems, Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
E-mail: m.gabbasovnaa@gmail.com, *https://orcid.org/0000-0002-9373-1261;*
Ongarbayeva Ainagul — Senior lecturer, Department of Information Security, L.N. Gumilyov Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
E-mail: *ainagul.ongarbaeva@gmail.com*, *https://orcid.org/0000-0001-7094-0557;*
Tokkulieva Aizhan — Senior Lecturer, Department of Information Security, Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan
E-mail: *aizhan_tk@mail.ru, https://orcid.org/0000-0002-5019-2413.*

Abstract. This article conducted an in-depth analysis of implementing blockchain technology within electronic voting systems, aimed at enhancing security, transparency, and efficiency. The relevance of this study is evident in the increasing reliance on electronic voting systems globally and the imperative to ensure their security and transparency. Key hypotheses of the research included the premise that blockchain technology has the potential to enhance security, transparency, and efficiency in electronic voting systems. By conducting a comprehensive literature review and comparative analysis of blockchain-based systems against traditional voting mechanisms, the study identifies the potential of blockchain to address common vulnerabilities in electronic voting, such as security concerns and voter privacy. Through theoretical modeling and simulations, the research evaluated blockchain's capacity to improve electoral integrity and proposes solutions to scalability and regulatory challenges. Additionally, it featured a comparative analysis of how different countries are adopting blockchain in their voting systems,

highlighting the varied approaches and outcomes experienced globally. This international perspective shed light on best practices and the challenges faced in diverse regulatory and technological environments. The findings underscored the transformative potential of blockchain in redefining electronic voting systems, emphasizing the need for ongoing research, development, and collaborative efforts to overcome technical and regulatory hurdles for widespread adoption.

Keywords: blockchain technology, electronic voting systems, integrity, security, voter privacy, scalability challenges, regulatory considerations

© А.М. Джумагалиева[1], А.Ә. Шекербек[2*], М.Г. Байбулова[2], А.И. Онгарбаева[2], А.К. Токкулиева[2], 2024

[1]Қазақ технология және бизнес университеті, Астана, Қазақстан;
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
E-mail: *shekerbek80@mail.ru*

ЭЛЕКТРОНДЫҚ ДАУЫС БЕРУ ЖҮЙЕСІНЕ БЛОКЧЕЙН ТЕХНОЛОГИЯСЫН ЕНГІЗУДІ ТАЛДАУ

Джумагалиева Айнур Максимқызы — Қазақ технология және бизнес университетінің ақпараттық технологиялар кафедрасының аға оқытушысы, Астана қ., Қазақстан
E-mail: *jumagalievaainur.m@gmail.com*б, *https://orcid.org/0000-0001-8632-5209;*
Шекербек Айнұр Әзімбайқызы — Л.Н.Гумилев атындағы Еуразия ұлттық университетінің ақпараттық жүйелер кафедрасының докторанты, Астана, Қазақстан
E-mail: *shekerbek80@mail.ru, https://orcid.org/0000-0002-1088-42391;*
Байбулова Мақбал Габбасқызы — Л.Н.Гумилев атындағы Еуразия ұлттық университетінің ақпараттық жүйелер кафедрасының аға оқытушысы, Астана, Қазақстан
E-mail: *m.gabbasovnaa@gmail.com, https://orcid.org/0000-0002-9373-1261;*
Онгарбаева Айнагуль Игиликовна — Л.Н. Гумилев атындағы Еуразия ұлттық университетінің Ақпараттық қауіпсіздік кафедрасының аға оқытушысы, Астана қ., Қазақстан
E-mail: *ainagul.ongarbaeva@gmail.com*, *https://orcid.org/0000-0001-7094-0557;*
Токкулиева Айжан Қоңырбайқызы — Л.Н.Гумилев атындағы Еуразия ұлттық университетінің Ақпараттық қауіпсіздi кафедрасының аға оқытушысы, Астана қ., Қазақстан
E-mail: *aizhan_tk@mail.ru, https://orcid.org/0000-0002-5019-2413.*

Аннотация. Бұл мақала қауіпсіздікті, ашықтықты және тиімділікті арттыруға бағытталған электрондық дауыс беру жүйелерінде блокчейн технологиясын енгізуге терең талдау жасады. Бұл зерттеудің өзектілігі бүкіл әлемде электронды дауыс беру жүйелерін қолданудың өсуінен және олардың қауіпсіздігі мен ашықтығын қамтамасыз ету қажеттілігінен айқын көрінеді. Зерттеудің негізгі гипотезаларына блокчейн технологиясының электрондық дауыс беру жүйелерінің қауіпсіздігін, ашықтығын және тиімділігін арттыру әлеуеті бар деген алғышарттар кірді.Әдебиетке жан-жақты шолу жасау және дәстүрлі дауыс беру тетіктері бар блокчейн негізіндегі жүйелерге салыстырмалы талдау жүргізу арқылы зерттеу сайлаушылардың қауіпсіздігі мен құпиялылық мәселелері сияқты электрондық дауыс берудегі жалпы осалдықтарды шешу үшін блокчейннің әлеуетін анықтайды. Теориялық модельдеу мен модельдеуді пайдалана отырып, зерттеу блокчейннің сайлаудың тұтастығын жақсарту қабілетін бағалады және ауқымдылық пен реттеу мәселелеріне ұсынылған шешімдерді ұсынды. Сонымен қатар, әртүрлі елдердің блокчейнді өздерінің дауыс беру жүйелеріне қалай енгізетініне салыстырмалы талдау ұсынылып, дүние жүзінде байқалған әртүрлі тәсілдер мен нәтижелер көрсетілді. Бұл халықаралық перспектива әртүрлі реттеуші және технологиялық орталарда кездесетін озық тәжірибелер мен қиындықтарға жарық түсірді. Қорытындылар электрондық дауыс беру жүйелерін қайта елестету үшін блокчейннің трансформациялық әлеуетін атап өтті, кең таралған қабылдауға техникалық және реттеуші кедергілерді еңсеру үшін үздіксіз зерттеулер, әзірлемелер және бірлескен күш-жігер қажеттілігін көрсетеді.

Түйін сөздер: блокчейн технологиясы, электронды дауыс беру жүйелері, тұтастық, қауіпсіздік, сайлаушылардың құпиялылығы, масштабтау мәселелері, реттеу аспектілері

© А.М. Джумагалиева[1], А.А. Шекербек[2*] , М.Г. Байбулова[2], А.И. Онгарбаева[2],А.К. Токкулиева[2], 2024

[1]Казахский университет технологий и бизнеса, Астана, Казахстан;
[2]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.
E-mail: *shekerbek80@mail.ru*

АНАЛИЗ ВНЕДРЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В СИСТЕМУ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

Джумагалиева Айнур Максимовна — старший преподаватель кафедры информационных технологий Казахский университет технологии и бизнеса, Астна, Казахстан
E-mail: *jumagalievaainur.m@gmail.com*б, *https://orcid.org/0000-0001-8632-5209;*
Шекербек Айнур Азимбаевна — докторант кафедры информационных систем Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: *shekerbek80@mail.ru, https://orcid.org/0000-0002-1088-42391;*
Байбулова Макбал Габбасовна — старший преподаватель кафедры информационных систем Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: m.gabbasovnaa@gmail.com, *https://orcid.org/0000-0002-9373-1261;*
Онгарабаева Айнагуль Игиликовна — старший преподаватель кафедры информационной безопасности Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: *ainagul.ongarbaeva@gmail.com*, *https://orcid.org/0000-0001-7094-0557;*
Токкулиева Айжан Конурбаевна — старший преподаватель кафедры информационной безопасности Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
E-mail: *aizhan_tk@mail.ru*, https://orcid.org/0000-0002-5019-2413.

Аннотация. В статье был проведен углубленный анализ внедрения технологии блокчейн в системах электронного голосования, направленный на повышение безопасности, прозрачности и эффективности. Актуальность этого исследования очевидна в растущем использовании систем электронного голосования во всем мире и необходимости обеспечения их безопасности и прозрачности. Ключевые гипотезы исследования включали предпосылку о том, что технология блокчейна потенциально может повысить безопасность, прозрачность и эффективность систем электронного голосования. Проводя всесторонний обзор литературы и сравнительный анализ систем на основе блокчейна с традиционными механизмами голосования, исследование определяет потенциал блокчейна для устранения распространенных уязвимостей в электронном голосовании, таких как проблемы безопасности и конфиденциальности избирателей. С помощью теоретического моделирования и симуляций исследование оценило способность блокчейна повысить честность выборов и предложило решения проблем масштабируемости и регулирования. Кроме того, был представлен сравнительный анализ того, как разные страны внедряют блокчейн в свои системы голосования, выявив различные подходы и результаты, наблюдаемые во всем мире. Этот международный взгляд пролил свет на передовой опыт и проблемы, с которыми приходится сталкиваться в различных нормативных и технологических средах. Полученные результаты подчеркнули преобразующий потенциал блокчейна в переосмыслении систем электронного голосования, акцентировав необходимость постоянных исследований, разработок и совместных усилий для преодоления технических и нормативных препятствий для широкого внедрения.

Ключевые слова: технология блокчейн, системы электронного голосования, целостность, безопасность, конфиденциальность избирателей, проблемы масштабируемости, нормативные аспекты

Introduction

The advent of blockchain technology heralds a transformative era for secure and transparent digital transactions, extending its influence into the realm of electronic voting systems. With a global market for blockchain technology projected to exceed $20 billion by 2024, its decentralized, immutable, and transparent characteristics offer a novel approach to overcoming the longstanding challenges of security, privacy, and trust in electronic voting processes. Notably, pilot blockchain voting projects in several countries have demonstrated a potential to increase voter participation by up to 5%, while significantly reducing the risk of electoral fraud (Alam et.al., 2021).

This study focuses on the application of blockchain technology in developing automated electronic voting systems that promise not only enhanced security and transparency but also improved efficiency. The escalating interest in blockchain, fueled by its success in the financial sector, underscores its potential to revolutionize electronic voting systems. This research aims to illuminate blockchain's applicability and viability in reinforcing democratic practices, emphasizing the critical need to fortify electronic voting systems against fraud and manipulation.

By evaluating current research and contrasting blockchain-based systems with traditional voting mechanisms, this analysis highlights the advantages and challenges of adopting blockchain in electoral processes. It endeavors to provide insights into how this emerging technology can be harnessed to foster a more transparent, secure, and efficient electoral process, contributing to the broader discourse on blockchain's potential beyond finance.

Materials and methods

This study employs a mixed-methods approach to analyze the impact of blockchain technology on enhancing the security, transparency, and efficacy of electronic voting systems. Initially, a comprehensive literature review was conducted to gather insights from existing research, case studies, and pilot projects involving blockchain in voting systems. This review helped in identifying the technological strengths and limitations of blockchain in the electoral context.

The integration of blockchain technology into electronic voting systems represents a pivotal shift towards enhancing electoral integrity and efficiency. (Pawlak et al., 2021) conducted a systematic review identifying both the challenges and opportunities presented by blockchain for e-voting, emphasizing the technology's potential to mitigate traditional security concerns while also highlighting scalability as a significant hurdle. (Khudoykulov et al., 2021) presented a practical implementation of a blockchain-based e-voting system, demonstrating its feasibility and the technology's capacity to ensure transparency and immutability of votes. (Majumder et al., 2023) explored the landscape of blockchain in e-voting, focusing on a comprehensive review that outlines open research challenges, particularly in voter anonymity and system scalability. (Huang et al., 2022) proposed a conceptual framework for a secure blockchain-based e-voting system, stressing the importance of cryptographic principles in safeguarding vote integrity. (Schulz *et al.,* 2022) analyzed trends in blockchain-based e-voting systems, identifying key technological advancements and the necessity for robust regulatory frameworks to support widespread adoption.

These works collectively underscore the transformative potential of blockchain in e-voting systems while cautioning against unresolved technical and regulatory challenges. The consensus across studies suggests that while blockchain can significantly enhance the security and transparency of electronic voting, its implementation must be carefully managed to address scalability, voter privacy, and regulatory compliance.

Subsequently, a comparative analysis was undertaken, contrasting the performance of blockchain-based voting systems with traditional electronic and paper-based voting methods. Criteria for comparison included system security, voter anonymity, auditability, scalability, and user accessibility. Theoretical modeling played a crucial role in understanding the potential implementation challenges and benefits of blockchain voting systems under various scenarios. Simulations were created to assess the resilience of these systems against common security threats and to evaluate their performance in terms of processing speed and transaction costs.

In addition, an analytical framework was developed to quantify the improvements blockchain technology could bring to electronic voting systems. This framework considered both technical metrics, such as system throughput and fault tolerance, and socio-political metrics, such as voter satisfaction and trust.

The impact of blockchain technology in electronic voting systems (e-voting) is profound, offering transformative improvements in security, transparency, and efficiency. By leveraging blockchain, e-voting systems can achieve a higher degree of vote integrity and voter privacy, significantly reducing the risks of fraud and tampering. Blockchain technology in e-voting systems offers a secure, transparent, and tamper-proof environment for casting and counting votes, aiming to enhance the integrity and trustworthiness of electronic voting processes. At its core, blockchain is a distributed ledger technology that records transactions across a network of computers, making it nearly impossible to alter data retrospectively without the consensus of the network.

In the context of e-voting, blockchain is utilized to create a secure and immutable record of each vote. When a voter casts their vote through an electronic interface, the vote is encrypted and transmitted over the network. This encrypted vote acts as a transaction on the blockchain. Once the transaction is verified by multiple nodes in the network, it is added to a block along with other transactions. Each block is then linked to the previous one, creating a chronological chain of blocks—hence the term blockchain. This chaining of blocks ensures that once a vote is recorded in a ledger, it cannot be altered or deleted without altering all subsequent blocks and the consensus of the network, which is practically impossible due to the cryptographic security measures in place. Additionally, blockchain's distributed nature means that the record of votes is not stored in a single location but is replicated across multiple nodes, making the system highly resistant to hacking and data manipulation. Moreover, blockchain enables the anonymization of votes while still verifying that each vote is cast by a registered voter. This is achieved through the use of cryptographic techniques that ensure the voter's identity is separate from their vote, thus preserving the secrecy of the ballot. Transparency is another key advantage of using blockchain in e-voting. Although the votes are anonymized, the blockchain ledger is transparent and can be audited by any participant in the network. This means that all stakeholders can verify the integrity of the voting process and the correctness of the vote count, fostering trust in the electoral process.

The decentralized nature of blockchain ensures that no single entity can control the voting process, enhancing trust among voters. Additionally, blockchain's immutable ledger allows for transparent and verifiable record-keeping, enabling any participant to audit the voting process in real-time (Baudier et.al., 2021). This technological shift not only promises to mitigate traditional challenges associated with e-voting systems but also paves the way for a more democratic and accessible voting mechanism globally.

Blockchain technology introduces pivotal characteristics to electronic voting systems, enhancing their integrity, security, and transparency:

1) Decentralization: Eliminates single points of failure by distributing data across a network, enhancing security and resilience against tampering.

2) Immutability: Once recorded, the data cannot be altered, ensuring the permanence and verifiability of votes.

3) Consensus Mechanisms: Facilitate agreement on data validity among participants, ensuring only legitimate votes are recorded, without the need for a central authority.

3) Transparency: Blockchain allows for a transparent audit trail, where each transaction (vote) is traceable and publicly verifiable, enhancing the credibility of the voting process.

4) Security: Advanced cryptographic techniques used in blockchain ensure that data is securely encrypted, safeguarding against unauthorized access and ensuring voter privacy.

In the following sections, we delve into the practical aspects of our research by presenting key snippets from our Jupyter notebook. This code encapsulates the core functionalities of proposed electronic voting system, underpinned by blockchain technology. It demonstrates the implementation of essential components such as the Block class, Blockchain class, and the simulation of an e-voting process. This visual representation offers a hands-on glimpse into the underlying code that drives our blockchain-based solution, highlighting its potential to enhance electoral integrity, security, and transparency.

```
Ввод [1]: import hashlib
          import json
          import datetime

Ввод [2]: class DateTimeEncoder(json.JSONEncoder):
              def default(self, obj):
                  if isinstance(obj, datetime.datetime):
                      return obj.isoformat()
                  return json.JSONEncoder.default(self, obj)

          class Block:
              def __init__(self, index, timestamp, vote_data, previous_hash):
                  self.index = index
                  self.timestamp = timestamp
                  self.vote_data = vote_data
                  self.previous_hash = previous_hash
                  self.hash = self.calculate_hash()

              def calculate_hash(self):
                  block_data = {
                      "index": self.index,
                      "timestamp": str(self.timestamp),
                      "vote_data": self.vote_data,
                      "previous_hash": self.previous_hash
                  }
                  return hashlib.sha256(json.dumps(block_data, sort_keys=True).encode()).hexdigest()
```

Figure 1. Block Class and DateTimeEncoder

This figure1 presents the implementation of the Block class and the DateTimeEncoder class. The Block class represents a single block in the blockchain. It has attributes such as index, timestamp, vote_data, previous_hash, and hash. The calculate_hash() method computes the hash of the block using SHA-256 hashing algorithm. The DateTimeEncoder class is a custom JSON encoder used to serialize datetime objects to ISO 8601 format.

```
class Blockchain:
    def __init__(self):
        self.chain = [self.create_genesis_block()]

    def create_genesis_block(self):
        return Block(0, datetime.datetime.now(), "Genesis Block", "0")

    def get_latest_block(self):
        return self.chain[-1]

    def add_block(self, new_block):
        new_block.previous_hash = self.get_latest_block().hash
        new_block.hash = new_block.calculate_hash()
        self.chain.append(new_block)

    def is_chain_valid(self):
        for i in range(1, len(self.chain)):
            current_block = self.chain[i]
            previous_block = self.chain[i - 1]

            if current_block.hash != current_block.calculate_hash():
                return False

            if current_block.previous_hash != previous_block.hash:
                return False

        return True
```

Figure 2. Blockchain Class

This figure 2 presents the implementation of the Blockchain class, which manages the chain of blocks. The Blockchain class has methods to create the genesis block (create_genesis_block()), retrieve the latest block (get_latest_block()), add a new block to the chain (add_block()), and validate the integrity of the blockchain (is_chain_valid()).

```
Ввод [3]: # Creating a simple e-voting blockchain
          blockchain = Blockchain()

Ввод [4]: # Simulating e-voting process
          votes = ["Candidate A", "Candidate B", "Candidate A", "Candidate A"]
          for vote in votes:
              blockchain.add_block(Block(len(blockchain.chain), datetime.datetime.now(), vote, blockchain.get_latest_block().hash))

Ввод [5]: # Verifying blockchain integrity
          print("Blockchain is valid:", blockchain.is_chain_valid())

          Blockchain is valid: True
```

Figure 3. Creating an e-voting blockchain

Figure 3 illustrates a simulated e-voting process using blockchain technology. In this example, a simple blockchain is created specifically for managing e-voting transactions. Votes are represented as blocks in the blockchain, each containing information about the candidate voted for, timestamp of the vote, and the hash of the previous block.

Ввод [7]:

```
# Displaying blockchain contents
print("\nBlockchain contents:")
for block in blockchain.chain:
    print(json.dumps(vars(block), indent=4, cls=DateTimeEncoder))
```


```
Blockchain contents:
{
    "index": 0,
    "timestamp": "2024-02-16T22:35:10.506255",
    "vote_data": "Genesis Block",
    "previous_hash": "0",
    "hash": "e3a597dce031d8ad111afc208981032b3448359867e4253ff3f609e852f7374b"
}
{
    "index": 1,
    "timestamp": "2024-02-16T22:35:18.134505",
    "vote_data": "Candidate A",
    "previous_hash": "e3a597dce031d8ad111afc208981032b3448359867e4253ff3f609e852f7374b",
    "hash": "e3c9884241af61044d23a31829f16103a455b17bd26c5a4309fcc5dafb3f44ee"
}
{
    "index": 2,
    "timestamp": "2024-02-16T22:35:18.134505",
    "vote_data": "Candidate B",
    "previous_hash": "e3c9884241af61044d23a31829f16103a455b17bd26c5a4309fcc5dafb3f44ee",
    "hash": "9e8462a7937c05d76e6a046e172fed57375d76aa3f2c7b6804148fba6bd4f822"
}
{
    "index": 3,
    "timestamp": "2024-02-16T22:35:18.134505",
    "vote_data": "Candidate A",
    "previous_hash": "9e8462a7937c05d76e6a046e172fed57375d76aa3f2c7b6804148fba6bd4f822",
    "hash": "4bc46bd3d02fca6ca7d0c74fcfb904e8d1771ae237c13886047602cd02857160"
}
{
    "index": 4,
    "timestamp": "2024-02-16T22:35:18.134505",
    "vote_data": "Candidate A",
    "previous_hash": "4bc46bd3d02fca6ca7d0c74fcfb904e8d1771ae237c13886047602cd02857160",
    "hash": "6e6ab9576abaa8a11bb43af0e6d25f6f8b7c5b42c029a7de9894a62c734ef479"
}
```


Figure 4. E-Voting Blockchain Simulation

This figure 4 demonstrates the implementation of an e-voting process using a blockchain. The process involves creating a blockchain instance, simulating the casting of votes, verifying the integrity of the blockchain, and displaying the contents of the blockchain. Each vote is recorded as a block in the blockchain, containing information such as the candidate voted for, timestamp, and cryptographic hashes for integrity verification. The blockchain ensures transparency, security, and tamper-resistance in the e-voting system.

Blockchain Contents and E-Voting

Genesis Block:

• The initial block in the blockchain, denoted as "Genesis Block".

• Typically contains default or initialization data.

• Serves as the starting point of the blockchain.

Candidate Votes:

• Subsequent blocks represent individual votes cast by voters in the e-voting system.

• Each block includes information about the vote, such as the candidate chosen and the timestamp of the vote.

• The vote_data field in each block specifies the candidate for whom the vote was cast.

• The previous_hash field in each block contains the hash of the preceding block, establishing a chronological sequence of votes.

Hashing:

• Each block is associated with a unique cryptographic hash calculated based on its data (e.g., index, timestamp, vote data, and previous hash).

• The hash serves as a distinct identifier for the block and aids in maintaining the integrity of the blockchain.

Blockchain Integrity:

• The previous_hash field ensures that blocks are sequentially linked in the blockchain.

• The blockchain's integrity is upheld by verifying the hash of each block against the calculated hash based on its data.

• Any attempt to alter the data within a block would result in a mismatch in the hash, signaling potential tampering with the blockchain.

Relevance to E-Voting:

• The blockchain structure transparently records each vote as a transaction, ensuring a tamper-resistant record of the voting process.

• By employing cryptographic hashing, the system enhances security, preventing unauthorized modifications to voting data.

• Each vote's inclusion in a block, along with its associated hash and sequential linkage, fosters trust in the integrity and transparency of the e-voting system.

In this section, we explore the foundational mechanism that ensures the security and integrity of the Ethereum blockchain: the Proof-of-Work (PoW) algorithm. This algorithm is crucial for validating transactions and creating new blocks, requiring miners to solve complex cryptographic puzzles (Kaudare et.al., 2020). The code snippet demonstrates how PoW deters malicious activities and secures the network by making computational work a prerequisite for adding to the blockchain. Let's delve into the intricacies of this algorithm and its pivotal role in maintaining a decentralized and trustless system.

```

#Defining the Blockchain Class
class Blockchain:
    #Initializing the Blockchain
    def _init_(self):
        self.chain = []
        self.current_transactions = []
        self.nodes = set()

        # Create the genesis block
        self.new_block(previous_hash='1', proof=100)

```

Figure 5. Creating the genesis blocks

This method initializes the blockchain, creating the genesis block and setting up containers for future transactions and network nodes (Figure 5).

```python
    #Adding New Blocks
    def new_block(self, proof, previous_hash=None):
        block = {
            'index': len(self.chain) + 1,
            'timestamp': time(),
            'transactions': self.current_transactions,
            'proof': proof,
            'previous_hash': previous_hash or self.hash(self.chain[-1]) if self.chain else None,
        }

        # Reset the current list of transactions
        self.current_transactions = []

        # Append the block to the chain
        self.chain.append(block)
        return block

    #Adding New Transactions
    def new_transaction(self, sender, recipient, amount):
        self.current_transactions.append({
            'sender': sender,
            'recipient': recipient,
            'amount': amount,
        })

```

Figure 6. Adding new blocks and transactions

Defines how to create a new block with transactions, its proof of work, and the hash of the previous block, then adds it to the chain. Allows adding a new transaction to the list of current transactions pending to be included in the next mined block (Figure 6).

```python
        return self.last_block['index'] + 1

    #Accessing the Last Block
    @property
    def last_block(self):
        return self.chain[-1]

    #Hashing Blocks
    @staticmethod
    def hash(block):
        # Hash the block using SHA-256
        block_string = json.dumps(block, sort_keys=True).encode()
        return hashlib.sha256(block_string).hexdigest()

    #Proof of Work Mechanism
    def proof_of_work(self, last_proof):
        proof = 0
        while self.valid_proof(last_proof, proof) is False:
            proof += 1
        return proof

    #Validating Proof of Work
    @staticmethod
    def valid_proof(last_proof, proof):
        guess = f'{last_proof}{proof}'.encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"  # Adjust the difficulty by changing the number of leading zeros

```

Figure 7. Automatization of blocks

A property that returns the most recent block in the blockchain. Then a static method that takes a block and returns its SHA-256 hash, ensuring integrity and immutability (Figure 7).

```
# Example usage:

blockchain = Blockchain()

def mine_block():
    # Add a transaction
    blockchain.new_transaction(sender='Alice', recipient='Bob', amount=5)

    # Mine a new block
    last_proof = blockchain.last_block['proof']
    proof = blockchain.proof_of_work(last_proof)
    previous_hash = blockchain.hash(blockchain.last_block)
    new_block = blockchain.new_block(proof, previous_hash)
    print(f"Block mined: {new_block}")

def print_blockchain():
    print(json.dumps(blockchain.chain, indent=2))

# Automate mining and printing blocks
mine_block()
print_blockchain()

mine_block()
print_blockchain()
```

Figure 8. Example Usage: Mining and Printing Blocks

In this code, the mine block function is responsible for adding a transaction, mining a new block, and printing the resulting blockchain (Figure 8). Using the proof-of-work algorithm for blockchain-based e-voting is important because it ensures the security, integrity, and trustworthiness of the voting process. The proof-of-work algorithm requires participants (miners) to solve complex mathematical problems to validate and add transactions to the blockchain. This process makes it extremely difficult for any single entity to manipulate or tamper with the voting data, thus preserving the accuracy and reliability of the election results (Al Barghuthi et.al., 2019,). Additionally, proof-of-work helps maintain decentralization by preventing any centralized authority from controlling the voting process, ensuring fairness and transparency for all participants.

Is it safe to use blockchain?

Blockchain technology provides decentralized security and trust in a number of ways. To begin with, new blocks are always introduced chronologically and linearly. They a A mathematical function converts numerical information into a string of numbers and characters to create hash codes. If this data is changed in any way, the hash code is also changed. This makes the blockchain more secure. Let's look at the areas of application of blockchain. What are the uses of blockchain in engineering? With immutability, traceability, openness, availability and decentralization capabilities, blockchain technology is well suited to engineering systems. Blockchain technology can assist in the supply chain of these engineering systems, as well as streamlining data, process and parties. Because blockchain distributed databases are decentralized and encrypted, they are often used in industries such as finance, healthcare, and supply chain management for secure and transparent recordkeeping. Cryptocurrencies such as Bitcoin use blockchain technology as the basis of their transaction systems (Kadam et. al., 2023).

Results and discussion

Our study's investigation into the implementation of blockchain technology in electronic voting systems has yielded significant insights. The application of blockchain has demonstrated potential benefits in enhancing the integrity, transparency, and efficiency of electronic voting processes. Notably, the security features inherent in blockchain technology, such as encryption and decentralization, have been identified as pivotal in mitigating common vulnerabilities associated with electronic voting systems. Furthermore, the scalability of blockchain systems has been recognized as a crucial factor in facilitating large-scale voting, ensuring system responsiveness and reliability.

The results highlight the transformative potential of blockchain technology in redefining electronic voting systems. Security enhancements brought about by blockchain can significantly reduce the risk of fraud and unauthorized access, thereby increasing trust in electronic voting processes. However, challenges related to scalability and voter privacy remain areas of concern. The study underscores the necessity for ongoing research and development to address these challenges, emphasizing the importance of creating a regulatory framework that supports the adoption of blockchain technology in voting systems. Collaborative efforts between technologists, lawmakers, and electoral authorities are essential in navigating the complexities of integrating blockchain into existing electoral infrastructures.

Challenges	Possible Solutions
Security Concerns	Use robust encryption techniques to secure voter data and transactions. Implement multi-factor authentication for voter identity verification. Regularly audit the system for vulnerabilities and apply patches.
Scalability	Utilize off-chain solutions for processing large volumes of transactions. Implement sharding techniques to distribute the workload across multiple nodes. Explore alternative consensus mechanisms that are more scalable than Proof of Work (PoW).
Voter Privacy	Implement cryptographic techniques like zero-knowledge proofs or homomorphic encryption to preserve voter anonymity. Use pseudonymous identifiers instead of revealing voter identities directly on the blockchain. Implement strict access controls to limit who can view voting data.
Voter Authentication	Utilize biometric authentication, digital signatures, or multi-factor authentication to verify voter identity. Implement identity verification protocols such as KYC before allowing voters to participate. Employ robust anti-spoofing measures to prevent impersonation attacks.
Regulatory Compliance	Ensure compliance with relevant laws and regulations governing elections and data privacy. Collaborate with legal experts to navigate the complex regulatory landscape. Transparently document and report the implementation process to regulatory authorities to demonstrate compliance.

User Experience	Design user-friendly interfaces for both voters and election administrators. Provide clear instructions and guidance throughout the voting process. Conduct usability testing to identify and address any usability issues. Offer support channels for users who encounter difficulties.
Fraud and Manipulation	Implement robust auditing mechanisms to detect and prevent fraudulent activities. Use blockchain-based timestamping to create immutable records of transactions. Implement consensus mechanisms that require most participants to validate transactions, reducing the risk of manipulation by a single entity.
Resilience to Cyber Attacks	Implement distributed architecture to reduce the impact of single points of failure. Regularly conduct security assessments and penetration testing to identify and address vulnerabilities. Employ disaster recovery and contingency plans to mitigate the impact of cyber-attacks. Implement mechanisms for detecting and responding to suspicious activities in real-time.
Trust and Transparency	Utilize blockchain's transparent and auditable nature to increase trust in the e-voting system. Provide stakeholders with access to the blockchain to independently verify the integrity of the voting process. Clearly document the system's design and operation to increase transparency and build trust among users. Leverage cryptographic techniques to ensure the integrity and authenticity of voting data.

Table 1. Challenges and Possible Solutions of implementing blockchain to e-voting

Our investigation into the current landscape of blockchain-based e-voting systems reveals a diverse range of applications across the globe, albeit predominantly at experimental or pilot stages. Notable implementations include:

West Virginia, USA: Pioneering in the United States, West Virginia offered blockchain-based mobile voting for military personnel and overseas voters during the 2021 midterm elections, marking a significant step towards integrating blockchain in electoral processes (Nigmatov et.al., 2023).

Estonia: A forerunner in e-governance, Estonia has utilized blockchain technology since 2005, with nearly 44% of votes cast online in the 2019 parliamentary elections. This underscores the country's leading position in digital governance and e-voting (Merrell, 2022).

South Korea and Russia: Both countries have conducted blockchain-based e-voting pilots, reflecting a growing interest in blockchain's potential to enhance electoral integrity and efficiency (Alvi et.al., 2022).

Switzerland, Brazil, and the UAE: These regions have explored blockchain e-voting in various capacities, from local elections in Swiss cantons to participatory budgeting in São Paulo and governmental process trials in Dubai (Gupta et.al., 2023).

Sierra Leone: Markedly, Sierra Leone's 2022 presidential election represented one of the first instances of blockchain technology applied in a national election, despite facing criticism and skepticism (Tripathi et.al., 2023).

India, Japan, and the Philippines: These countries have conducted localized blockchain voting trials, aiming to improve electoral participation and decision-making transparency (Almadani et.al., 2023).

Canada: Ontario's exploration of blockchain for municipal elections in 2023 aimed to assess the technology's viability in enhancing voting process security and transparency (Khan et.al., 2021).

The varied applications of blockchain-based e-voting systems highlight a global trend towards digitalization and technological integration into the electoral process. However, the path to widespread adoption is fraught with challenges. Technical hurdles demand the development of secure, robust, and user-friendly platforms, while regulatory and legal barriers necessitate adapting electoral laws to accommodate blockchain's nuances. Building public trust is crucial, as skepticism about the technology's reliability and security remains a significant obstacle. Moreover, the applicability of blockchain in e-voting is not universal; its effectiveness varies based on each country's specific legal, electoral, and societal contexts. Overcoming these challenges requires a multidisciplinary approach, involving technological innovation, legal reform, and public education, to unlock blockchain's potential for enhancing electoral transparency, integrity, and participation globally.

Conclusion

In conclusion, the analysis of blockchain technology in electronic voting systems reveals its potential to significantly enhance electoral integrity, transparency, and security. By leveraging blockchain, we can address key vulnerabilities of traditional electronic voting methods, particularly in ensuring the immutability and anonymity of votes. Despite the promising advantages, challenges such as scalability, regulatory compliance, and the technical complexity of blockchain implementation necessitate further research and collaboration. The study highlights the need for comprehensive frameworks that facilitate the integration of blockchain into existing electoral systems while ensuring they are accessible, secure, and user-friendly. Future advancements in blockchain technology hold the promise of transforming not only electronic voting systems but also a wide range of industries by providing enhanced security, transparency, and efficiency.

REFERENCES

Al Barghuthi N.B., Hamdan I., Al Suwaidi S., Lootah A., Al Amoudi B., Al Shamsi O. & Al Aryani S. (2019, November). An analytical view on political voting system using blockchain technology-uae case study. In *2019 Sixth HCT Information Technology Trends. — ITT.* — Pp. 132-–137. — IEEE. — *https://doi.org/10.1109/itt48889.2019.907507*

Alam S., Shuaib M., Khan W.Z., Garg S., Kaddoum G., Hossain M.S. & Zikria Y.B. (2021). Blockchain-based initiatives: current state and challenges. — *Computer Networks*, — *198*, — 108395. — *https://doi.org/10.1016/j.comnet.2021.108395*

Almadani M.S., Alotaibi S., Alsobhi H., Hussain O.K. & Hussain F.K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. — *Internet of Things*, — 100844. — *https://doi.org/10.1016/j.iot.2023.1008441*

Alvi S.T., Uddin M.N., Islam L. & Ahamed S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. — *Journal of*

King Saud University-Computer and Information Sciences, — *34*(9), — 6855–6871. — *https://doi.org/10.1016/j.jksuci.2022.06.0141*

Baudier P., Kondrateva G., Ammi C. & Seulliet E. (2021). Peace engineering: The contribution of blockchain systems to the e-voting process. *Technological Forecasting and Social Change*, — *162*, — 120397, — *https://doi.org/10.1016/j.techfore.2020.1203971*

Gupta S., Gupta A., Pandya I.Y., Bhatt A. & Mehta K. (2023). End to end secure e-voting using blockchain & quantum key distribution. — *Materials Today: Proceedings*, — *80*, — 3363–3370. — *https://doi.org/10.1016/j.matpr.2021.07.2541*

Huang J., He D., Chen Y., Khan M.K. & Luo M. (2022). A Blockchain-Based Self-Tallying Voting Protocol With Maximum Voter Privacy. — *IEEE Transactions on Network Science and Engineering*, *9*(5), — 3808–3820. — doi: *10.1109/TNSE.2022.3190909*

Kadam P., Nikam P., Raut H., Hutke S. & Mathi S. (2023, June). Blockchain Based e-Voting System. In *2023 3rd International Conference on Intelligent Technologies. — CONIT.* — Pp. 1–6. — IEEE. — *https://doi.org/10.1109/conit59222.2023.10205939*

Kaudare A., Hazra M., Shelar A. & Sabnis M. (2020, June). Implementing electronic voting system with blockchain technology. In *2020 International Conference for Emerging Technology. — INCET.* — Pp. 1–9. IEEE. — *https://doi.org/10.1109/incet49848.2020.9154116*

Khan K.M., Arshad J. & Khan M.M. (2021). Empirical analysis of transaction malleability within blockchain-based e-Voting. — *Computers & Security*, — *100*, — 102081. — *https://doi.org/10.1016/j.cose.2020.1020811*

Khudoykulov Z., Tojiakbarova U., Bozorov S. & Ourbonalieva D. (2021, November). Blockchain based e-voting system: Open issues and challenges. In *2021 International Conference on Information Science and Communications Technologies (ICISCT.* — *P*p. 1–5. — IEEE. doi: *10.1109/ICISCT52966.2021.96702451*

Majumder S., Ray S., Sadhukhan D., Dasgupta M., Das A.K. & Park Y. (2023). ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain and Zero Knowledge Property. *IEEE Open Journal of the Communications Society*. doi: *10.1109/OJCOMS.2023.3348468*

Merrell I. (2022). Blockchain for decentralised rural development and governance. — *Blockchain: Research and Applications*, *3*(3), — 100086. — *https://doi.org/10.1016/j.bcra.2022.100086*

Nigmatov A., Pradeep A. & Musulmonova N. (2023, June). Blockchain Technology in Improving Transparency and Efficiency in Government Operations. In *2023 15th International Conference on Electronics, Computers and Artificial Intelligence. — ECAI.* — Pp. 01–06). IEEE. — doi: 10.1109/ECAI58194.2023.10194154 *https://doi.org/10.1109/ecai58194.2023.101941541*

Pawlak M. & Poniszewska-Marańda A. (2021). Trends in blockchain-based electronic voting systems. — *Information Processing & Management*, — *58*(4), — 102595. — *https://doi.org/10.1016/j.ipm.2021.1025952*

Schulz K.A., Gstrein O.J. & Zwitter A.J. (2020). Exploring the governance and implementation of sustainable development initiatives through blockchain technology. — *Futures*, — *122*, — 102611. — *https://doi.org/10.1016/j.futures.2020.102611*

Tripathi G., Ahad M.A. & Casalino G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. — *Decision Analytics Journal*, — 100344. — *https://doi.org/10.1016/j.dajour.2023.1003441*

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),

ISSN 1991-346X (Print)

Подписано в печать 28.03.2024.
Формат 60x881/8. Бумага офсетная. Печать–ризограф.
21,0 п.л. Тираж 300. Заказ 1.

РОО «Национальная академия наук РК» 050010,
Алматы, ул. Шевченко, 28, т. 272-13-19