DOI 10.52209/1609-1825_2026_1_453 UDC 004.89

Development of a Blockchain-Based Electronic Voting System

[1]**BALKENOV Alimzhan,** *Cand. of Tech. Sc., Professor, a.baikenov@aues.kz,*
[1]**YUN Timur,** *Bachelor's Degree, t.yun@aues.kz,*
[1]***KHIZIROVA Muhabbat,** *Cand. of Phys. and Math. Sc., Professor, hizirova73@mail.ru,*
[1]**KASIMOV Abdurazak,** *Cand. of Tech. Sc., Professor-Researcher, a.kasimov@aues.kz,*
[2]**KARIBAEV Beibit,** *PhD, Senior Lecturer, b.karibayev@aues.kz,*
[1]NPJSC «Almaty University of Power Engineering and Telecommunications named after Gumarbek Daukeyev», 126/1 A. Baitursynova Street, Almaty, Kazakhstan,
[2]NPJSC «Al-Farabi Kazakh National University», 71 Al-Farabi Avenue, Almaty, Kazakhstan,
**corresponding author.*

Abstract. *The article discusses the development and analysis of an electronic voting system utilizing blockchain technology, with the goal of improving the security, transparency, and reliability of electoral processes. The study emphasizes the importance of addressing vulnerabilities inherent in traditional voting systems, such as the risks of data manipulation and unauthorized access. A detailed examination of blockchain's theoretical principles is presented, highlighting its decentralized architecture, data immutability, and cryptographic security features. The practical component of the research focuses on the creation of a prototype system, designed using a modular approach and incorporating advanced cryptographic techniques and consensus mechanisms to ensure data integrity and system robustness. Experimental findings demonstrate the high effectiveness of the proposed solution, indicating its suitability for deployment in large-scale electoral contexts. The article concludes by exploring potential directions for future system enhancements and the integration of blockchain technology into existing electronic voting infrastructures.*

Keywords: *blockchain, electronic voting, security, transparency, cryptography, decentralization.*

Introduction.

With the rapid evolution of information technologies and the ongoing digital transformation of society, traditional voting methods are increasingly criticized for their inherent weaknesses, including susceptibility to result falsification, counting inaccuracies, and a lack of transparency in the voting process [1–3]. These shortcomings underscore the need for innovative approaches that can strengthen the reliability and credibility of electoral procedures.

Blockchain technology, characterized by its decentralization, immutability, and cryptographic security, offers a promising framework for addressing these issues [4-5]. Its integration into electronic voting systems facilitates the development of a secure, distributed, and transparent infrastructure. In such a system, each vote is recorded as a distinct transaction, inherently resistant to unauthorized alterations [6–8]. This methodology not only mitigates the potential for election manipulation but also fosters greater confidence among voters and the broader public [9].

This study examines the theoretical underpinnings of blockchain technology within the context of electronic voting, outlining its key advantages and the practical challenges of implementation. Particular emphasis is placed on designing an architecture capable of preserving data integrity and security in large-scale electoral settings. The proposed system features a transaction management module, digital wallets for voter authentication, a block-generation mechanism, blockchain formation, and a decentralized network for node-to-node data exchange. Furthermore, the system incorporates consensus validation protocols, automated smart contracts, and scalability measures to ensure effective performance in real-world applications. The solution is designed to strike a balance between transparency and privacy, enabling verifiable election outcomes while safeguarding the anonymity of individual votes.

Materials and Methods.

In the present study, contemporary tech-

nologies and programming libraries were employed to develop a prototype of a blockchain-based electronic voting system, aimed at ensuring high levels of security, fault tolerance, and a decentralized architectural framework [10]. The system was implemented in C++, enabling the use of robust and efficient tools for asynchronous network communication and cryptographic operations.

At the core of the system lies the blockchain infrastructure, constructed using a set of custom-designed classes, including Wallet, Vote, Transaction, Block, and Node.

The Wallet class manages the generation of cryptographic key pairs for individual voters, utilizing the Ed25519 algorithm. This algorithm offers a favorable balance between performance and security, delivering 256-bit key lengths with high-speed processing while providing a security level comparable to a 3072-bit RSA key. The public key, formatted in PEM, is used to validate digital signatures, while the private key is used to sign the votes.

Voting data is encapsulated within the Vote and Transaction classes. When a new Vote object is created, it constructs a string composed of the voter's identifier, the candidate's identifier, and a unique nonce. This string is then digitally signed with the voter's private key. The resulting binary signature is encoded in Base64 to enable safe and convenient storage and transmission in JSON format (see Figure 1). This vote object is then transformed into a Transaction object using a specialized constructor, and the transaction is subsequently propagated through the network.

1. The Block class handles the construction of blocks that aggregate transactions. During the creation of a new block, a Proof-of-Work (PoW) mechanism is applied, requiring the computation of a block hash that meets a predefined difficulty criterion. To maintain data integrity and ensure tamper resistance, the system employs the SHA-256 cryptographic hash function. Block validation is performed by recalculating the hash and comparing it with the stored hash value to confirm consistency and authenticity.

2. As illustrated in Figure 2, the system node – implemented through the Node class – facilitates network communication using the Boost.Asio library. The blockchain infrastructure is organized as a peer-to-peer (P2P) network, where each node functions both as a server and a client. Nodes concurrently accept incoming TCP connections via a TCP acceptor bound to a designated IP address and port, while also initiating outbound connections to other peer nodes. This bidirectional connectivity supports decentralized data exchange, synchronization of the blockchain ledger, and the propagation of transactions and new blocks across the network.

Communication between nodes is orchestrated through Session objects, which are responsible for the asynchronous reception and transmission of JSON-formatted messages. Incoming messages are processed by the handleMessage() function, which determines the appropriate response based on the message type – whether it pertains to a transaction, a new block, or a blockchain synchronization request. The corresponding logic then performs validation, adds the data to the local memory pool, or updates the blockchain accordingly. Upon completion of the implementation of all system components, the overall architecture of the prototype is illustrated in Figure 3.

Results and Discussion.

To assess the performance of the developed blockchain-based voting system, a test environment was configured within a local network using an emulator designed to simulate node behavior and interactions. Voter wallet information was securely stored in an SQLite database, providing dependable preservation of user identifiers and чcryptographic key pairs essential for generating and verifying digital signatures. The network architecture was built on the TCP protocol, with communication managed via the Boost.Asio library, allowing each node to operate concurrently as a server (receiving incoming connections) and as a client (initiating outbound connections to peers). Data exchange was carried out using JSON-formatted messages, which facilitat-


```
        "candidateId": "CandidateB",
        "nonce": 491,
        "publicKey": "-----BEGIN PUBLIC KEY-----
\nMCowBQYDK2VwAyEAJg1B7dU52Vzg6L+ZICXDFA76ScjghvHB2uDOO+gBUkc=
\n-----END PUBLIC KEY-----\n",
        "signature":
"peHg83fJn2HExicEaQX/y93NtGyHjmMdKegRSJn9uX9mdkAUNO5angUlSx3+7Be
ymjWTjLaPNNSSv60HcpTMCQ==",
        "voterId": "voter28"
```


Figure 1 – Transaction structure

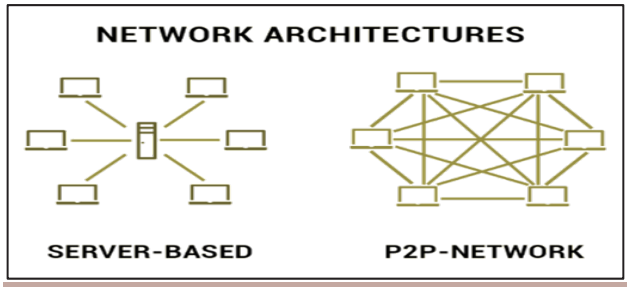

Figure 2 – Network architectures

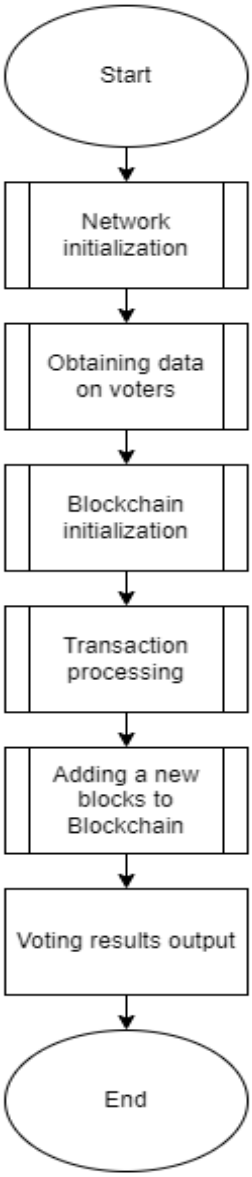

Figure 3 – Flowchart of Blockchain-Based Electronic Voting system

ed efficient serialization and deserialization, as well as rapid transmission of information among nodes.

Testing confirmed a high level of system security and transparency. All vote-related transactions were accurately generated and signed using the Ed25519 cryptographic algorithm, then reliably recorded on the blockchain in a tamper-resistant and immutable format. Each node performed transaction validation by verifying digital signatures and cross-checking public keys against database records, effectively preventing fraudulent behavior and double voting. A more detailed overview of the transaction processing workflow is provided in Figure 4.5.

Once a sufficient number of transactions had been collected, the system initiated an automated mining process to generate new blocks, during which validated transactions were selectively removed from the pending transaction pool. Testing demonstrated that new data were promptly integrated into each node's local blockchain, and synchronization across the peer-to-peer network was achieved with minimal latency.

In addition, the tests confirmed the system's high fault tolerance and its capacity to function effectively under increased operation-

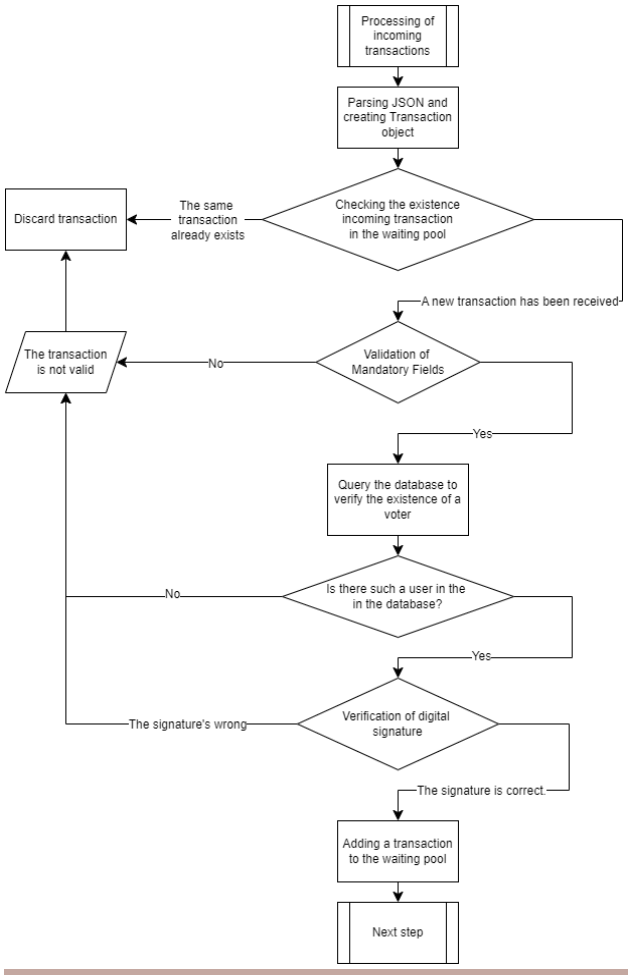

Figure 4 – Transaction processing

```
>> blokcheinbaik
Подпись успешно декодирована:
  Columns 1 through 24

    99    97   110   100   105   100    97   116   101    95   105   100    58    53    44   110   111   110    99   101    58    55    54    52

  Columns 25 through 26

    53    55
```

Figure 5 – Transaction processing with the use of digital signature

al load – an essential attribute for its potential application in large-scale electoral processes. The recorded response times underscored the system's efficiency within a distributed network environment, wherein nodes continuously exchange transactions and blocks to maintain the integrity and immutability of the voting ledger.

Despite these promising results, certain limitations persist, particularly in regard to system scalability and the full preservation of voter anonymity. For instance, as the number of participants grows, synchronization delays may emerge, and maintaining an appropriate balance between transparency and confidentiality necessitates the incorporation of advanced cryptographic mechanisms.

Conclusion

Blockchain technology has proven to be a highly promising tool for improving the security and transparency of electronic voting systems. The prototype developed in this study – featuring a custom-built blockchain and network message exchange mechanism – has demonstrated that a distributed ledger can effectively mitigate risks related to vote tampering and unauthorized access. The integration of advanced cryptographic techniques guarantees the immutability of records and ensures the authenticity of each vote, thereby fostering greater trust among voters.

Testing within a controlled local network environment validated the system's operational stability, effective inter-node communication, and consistent blockchain synchronization. Nonetheless, the results also highlighted areas requiring further enhancement, particularly in terms of scalability and voter anonymity. Future development should focus on optimizing the software architecture, improving the user interface, and implementing advanced security protocols to strengthen the system's overall resilience and performance.

In conclusion, the prototype underscores the viability of applying blockchain technology to electronic voting, offering a secure, transparent foundation that can be further developed and scaled for use in real-world electoral processes.

REFERENCES

1. Benabdallah A., Audras A., Coudert L., El Madhoun N., Badra M. Analysis of blockchain solutions for E-voting: A systematic literature review // IEEE Access. – 2022– Vol. 10. – P. 70746–70759.
2. Нурпеисов Е. К., Аунасова А. М. Трансформация избирательной системы в Республике Казахстан // Вестник КазНУ. Серия юридическая. – 2023. – №103(2). – С. 45–56.
3. Володенков С. В., Федорченко С. Н. Традиционные политические институты в условиях цифровизации: риски и перспективы трансформации // Политология. – 2022. – №4. – С. 8–25.
4. Жумагалиева А. М., Шекербек А. А., Байбулова М. Г., Онгарбаева А. И., Токкулиева А. Анализ внедрения технологии блокчейн в систему электронного голосования // Известия НАН РК. Серия физико-математическая. – 2024. – №1. – С. 136–151.
5. Mukherjee A., Majumdar S., Kolya A. K., Nandi S. A Privacy-Preserving Blockchain-based E-voting System: https://arxiv.org/abs/2307.08412
6. Onur C., Yurdakul A. ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol – 2022: https://arxiv.org/abs/2204.00057
7. Hakak S., Khan W. Z., Gilkar G. A., Assiri B., Alazab M., Bhattacharya S., Reddy G. T. Recent Advances in Blockchain Technology: A Survey on Applications and Challenges– 2020-: https://arxiv.org/abs/2009.05718
8. Khan S. N., Loukil F., Ghedira-Guegan C., Benkhelifa E., Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends // Peer-to-Peer Networking and Applications. – 2021. –

DOI:10.1007/s12083-021-01119-1
9. Xiao Y., Zhang N., Lou W., Hou Y. T. A Survey of Distributed Consensus Protocols for Blockchain Networks // IEEE Communications Surveys & Tutorials. – 2020. – Т. 22, №2. – С. 1432–1465.
10. Паскарь В., Гагарина Л. Г., Слюсарь В. В. Разработка методики и программного комплекса для дистанционного электронного голосования на основе блокчейн- платформы Ethereum – 2021 – Известия высших учебных заведений. Электроника: https://cyberleninka.ru/

Блокчейн технологиясы негізінде электрондық дауыс беру жүйесін әзірлеу

*[1]**БАЙКЕНОВ Алимжан Сергеевич,** т.ғ.к., профессор-оқытушы, a.baikenov@aues.kz,*
*[1]**ЮН Тимур Эдуардович,** бакалавр, t.yun@aues.kz,*
*[1]***ХИЗИРОВА Мухаббат Абдисаттаровна,** ф.-м.ғ.к., профессор-оқытушы, hizirova73@mail.ru,*
*[1]**КАСЫМОВ Абдуразак Оразгельдиевич,** т.ғ.к., профессор-зерттеуші, a.kasimov@aues.kz,*
*[2]**КАРИБАЕВ Бейбит Абдирбекович,** PhD, аға оқытушы, b.karibayev@aues.kz,*
[1]«Ғұмарбек Дәукеев атындағы Алматы энергетика және байланыс университеті» КеАҚ, А. Байтұрсынұлы көшесі, 126/1, Алматы, Қазақстан,
[2]«Әл-Фараби атындағы Қазақ ұлттық университеті» КеАҚ, әл-Фараби даңғылы, 71, Алматы, Қазақстан,
**автор-корреспондент.*

***Аңдатпа.** Сайлау процесінің қауіпсіздігін, ашықтығы мен сенімділігін арттыруға бағытталған блокчейн технологиясына негізделген электрондық дауыс беру жүйесін әзірлеу және зерттеу ұсынылған. Зерттеудің өзектілігі нәтижелерді бұрмалау және деректерге рұқсатсыз қол жеткізу мүмкіндігі сияқты дәстүрлі дауыс беру жүйелерінің әлсіз жақтарын жою қажеттілігіне байланысты. Блокчейн технологиясының теориялық негіздеріне кешенді талдау жүргізілді, орталықтандырылмаған архитектураның, ақпараттың өзгермейтіндігінің және криптографиялық қорғауды қолданудың негізгі артықшылықтары анықталды. Жұмыстың практикалық бөлігі деректердің тұтастығы мен тұрақтылығын қамтамасыз ету үшін заманауи криптографиялық әдістер мен консенсус алгоритмдерін қолдана отырып, модульдік дизайн арқылы жүзеге асырылатын жүйенің прототипін жасауды қамтиды. Эксперименттердің нәтижелері ұсынылған шешімнің жоғары тиімділігін растады, оның жаппай сайлау жағдайында қолдану әлеуетін көрсетті. Жүйені одан әрі оңтайландыру және блокчейн-технологияларды қолданыстағы электрондық дауыс беру инфрақұрылымдарына интеграциялау перспективалары талқыланады.*

***Кілт сөздер:** блокчейн, электронды дауыс беру, қауіпсіздік, ашықтық, криптография, орталықсыздандыру.*

Разработка системы электронного голосования на основе технологии блокчейн

*[1]**БАЙКЕНОВ Алимжан Сергеевич,** к.т.н., профессор-преподаватель, a.baikenov@aues.kz,*
*[1]**ЮН Тимур Эдуардович,** бакалавр, t.yun@aues.kz,*
*[1]***ХИЗИРОВА Мухаббат Абдисаттаровна,** к.ф.-м.н., профессор-преподаватель, hizirova73@mail.ru,*
*[1]**КАСЫМОВ Абдуразак Оразгельдиевич,** к.т.н., профессор-исследователь, a.kasimov@aues.kz,*
*[2]**КАРИБАЕВ Бейбит Абдирбекович,** PhD, старший преподаватель, b.karibayev@aues.kz,*
[1]НАО «Алматинский университет энергетики и связи имени Гумарбека Даукеева», ул. А. Байтурсынова, 126/1, Алматы, Казахстан,
[2]НАО «Казахский национальный университет имени аль-Фараби», пр. аль-Фараби, 71, Алматы, Казахстан,
**автор-корреспондент.*

***Аннотация.** Представлены разработка и исследование системы электронного голосова-*

ния на основе технологии блокчейн, направленной на повышение безопасности, прозрачности и надежности избирательного процесса. Актуальность исследования обусловлена необходимостью устранения слабых мест традиционных систем голосования, таких как возможность фальсификации результатов и несанкционированного доступа к данным. Проведен комплексный анализ теоретических основ блокчейн-технологии, выявлены ключевые преимущества децентрализованной архитектуры, неизменяемости информации и использования криптографической защиты. Практическая часть работы включает разработку прототипа системы, реализованного посредством модульного проектирования с использованием современных методов криптографии и алгоритмов консенсуса для обеспечения целостности и устойчивости данных. Результаты экспериментов подтвердили высокую эффективность предложенного решения, демонстрируя его потенциал для применения в условиях массовых выборов. Обсуждены перспективы дальнейшей оптимизации системы и интеграции блокчейн-технологий в существующие инфраструктуры электронного голосования.

Ключевые слова: *блокчейн, электронное голосование, безопасность, прозрачность, криптография, децентрализация.*

REFERENCES

1. Benabdallah A., Audras A., Coudert L., El Madhoun N., Badra M. Analysis of blockchain solutions for E-voting: A systematic literature review [Elektronnyi resurs] // IEEE Access. – 2022. – Vol. 10. – P. 70746–70759. – Rezhim dostupa: https://hal.science/hal-03717773/document
2. Nurpeisov E. K., Aunasova A. M. Transformatsiya izbiratel'noi sistemy v Respublike Kazakhstan [Elektronnyi resurs] // Vestnik KazNU. Seriya yuridicheskaya. – 2023. – №103(2). – S. 45–56. – Rezhim dostupa: https://cyberleninka.ru/article/n/transformatsiya-izbiratelnoy-sistemy-v-respublike-kazahstan
3. Volodenkov S. V., Fedorchenko S. N. Traditsionnye politicheskie instituty v usloviyakh tsifrovizatsii: riski i perspektivy transformatsii [Elektronnyi resurs] // Politologiya. – 2022. – №4. – S. 8–25. – Rezhim dostupa: https://cyberleninka.ru/article/n/traditsionnye-politicheskie-instituty-v-usloviyah-tsifrovizatsii-riski-i-perspektivy-transformatsii
4. Zhumagalieva A. M., Shekerbek A. A., Baibulova M. G., Ongarbaeva A. I., Tokkulieva A. Analiz vnedreniya tekhnologii blokcheyn v sistemu elektronnogo golosovaniya [Elektronnyi resurs] // Izvestiya NAN RK. Seriya fiziko-matematicheskaya. – 2024. – №1. – S. 136–151. – Rezhim dostupa: https://journals.nauka-nanrk.kz/fm/article/view/4863
5. Mukherjee A., Majumdar S., Kolya A. K., Nandi S. A Privacy-Preserving Blockchain-based E-voting System [Elektronnyi resurs]. – 2023. – Rezhim dostupa: https://arxiv.org/abs/2307.08412
6. Onur C., Yurdakul A. ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol [Elektronnyi resurs]. – 2022. – Rezhim dostupa: https://arxiv.org/abs/2204.00057
7. Hakak S., Khan W. Z., Gilkar G. A., Assiri B., Alazab M., Bhattacharya S., Reddy G. T. Recent Advances in Blockchain Technology: A Survey on Applications and Challenges [Elektronnyi resurs]. – 2020. – Rezhim dostupa: https://arxiv.org/abs/2009.05718
8. Khan S. N., Loukil F., Ghedira-Guegan C., Benkhelifa E., Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends [Elektronnyi resurs] // Peer-to-Peer Networking and Applications. – 2021. – DOI: 10.1007/s12083-021-01119-1. – Rezhim dostupa: https://link.springer.com/article/10.1007/s12083-021-01119-1
9. Xiao Y., Zhang N., Lou W., Hou Y. T. A Survey of Distributed Consensus Protocols for Blockchain Networks [Elektronnyi resurs] // IEEE Communications Surveys & Tutorials. – 2020. – T. 22, №2. – S. 1432–1465. – Rezhim dostupa: https://doi.org/10.1109/COMST.2020.2969706
10. Paskar' V., Gagarina L. G., Slyusar' V. V. Razrabotka metodiki i programmnogo kompleksa dlya distantsionnogo elektronnogo golosovaniya na osnove platformy blokcheyn Ethereum [Elektronnyi resurs] // Izvestiya vysshikh uchebnykh zavedenii. Elektronika. – 2021. – Rezhim dostupa: https://cyberleninka.ru/article/n/razrabotka-metodiki-i-kompleksa-programmnyh-sredstv-dlya-distantsionnogo-elektronnogo-golosovaniya-na-osnove-blokcheyn-platformy