IRSTI 50.41.25
UDC 004.41 **DOI 10.70239/arsu.2025.t80.n2.08**

DEVELOPMENT OF A VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY

SARSIMBAYEVA S.M.*, BAZARBAYEV S.ZH.

***Sarsimbayeva Saule Musaevna** - Candidate of physical and mathematical sciences, associate professor, K. Zhubanov Aktobe regional university, Aktobe, Kazakhstan
E-mail: saulesarsi@gmail.com, http://orcid.org/0000-0003-1536-3042
Bazarbayev Sultan Zharasovich - Master's student, K. Zhubanov Aktobe regional university, Aktobe, Kazakhstan
E-mail: sbazarbaev550@gmail.com, http://orcid.org/0000-0009-8786-3738

Abstract. Various electronic voting systems have been developed. But most of such systems have such disadvantages as lack of transparency and the possibility to check the correctness of vote counting. The article considers the development of voting systems using blockchain technology. It shows the possibility of increasing transparency, security and reliability of electoral processes on the basic of blockchain technology, especially in conditions of limited recources. The practical implementation developed by the authors is shown - an electronic voting system based on blockchain technology using smart contracts in the Solidity language and a user interface in Python with the Web3.py library. An analysis of existing solutions is carried out, their disadvantages are identified, the system architecture is proposed and the main functions are implemented: registration of candidates, voting, protection against duplicate votes and automatic counting of results. The results of testing in the Ganache environment confirmed the correctness of the system and its resistance to external influences. In comparison with analogs, the design of the system proposed by the authors using blockchain technology is simple, accessible and highly reliable, which makes it promising for implementation. The study of the evolution of electronic voting systems, the use of blockchain technology for electronic voting systems contribute to the development of effective solutions for democratic governance.

Key words: blockchain, voting systems, electronic voting, smart contract, decentralization, data security, privacy.

Introduction

In the context of rapid digitalization and the growth of cyber-attacks, ensuring the transparency, security and reliability of voting results is becoming a critical task for modern democratic processes. Traditional voting methods, such as paper ballots and centralized electronic systems, are vulnerable to fraud, external interference, and technical failures, which reduces voters' trust in the system and can lead to the delegitimization of elections [1,2,3].

Blockchain technology provides an alternative approach based on a decentralized data storage structure and the use of smart contracts to automate key procedures. In blockchain in these systems, each vote is recorded as a transaction in an immutable chain of blocks, which eliminates the possibility of falsifying results and ensures a high degree of security and transparency [4,5,6].

However, as noted in the work of Bhavani, D. D., et al. [7] and the study by Hajian Berenjestanaki M., et al. [8], the implementation of such systems is associated with a number of challenges, including technical complexity, lack of intuitive user interfaces, and the need for significant resources for deployment. In addition, many existing solutions are focused on large-scale electoral processes and are not adapted for use in resource-constrained settings such as educational institutions, local initiatives, or pilot projects. Despite the obvious advantages of blockchain voting solutions, several important issues remain unresolved, such as the high technical complexity of most of the implemented prototypes, the lack of intuitive interfaces for end users, difficulties with deploying solutions in conditions of limited infrastructure, and limited integration capabilities in educational and local initiatives.

Thus, there is a need to create a voting system that is easy to use, secure, and accessible to a wide range of users, which can be quickly deployed and tested without significant technical and financial costs. This work aims to address these issues by developing and testing voting systems based on blockchain technology using smart contracts in the Solidity language and an interface developed in Python.

The aim of the work is to study the possibility of developing a decentralized voting system based on blockchain technology and implemented using smart contracts in the Solidity language and an external user interface in Python with the Web3.py library. Unlike most existing solutions focused on large-scale systems with high complexity of configuration [1,7], the proposed system is developed with an emphasis on accessibility, ease of deployment and application in conditions of limited computing resources.

Materials and methods of research

In today's digital environment and the rise of cyberattacks, ensuring the transparency and reliability of the voting system is of particular importance. Traditional voting systems are subject to the risks of falsification and external interference, which threatens democratic principles and citizens' trust in election results. The introduction of blockchain technology eliminates these shortcomings through the use of decentralized data storage and the use of smart contracts that ensure automatic fulfillment of voting conditions without third-party intervention.

Blockchain is a distributed database that stores information in a sequential chain of blocks. Each block includes a hash of the previous block, a timestamp, and a set of transactions. This mechanism ensures the integrity of the data and protects it from counterfeiting, since any change to the contents of a block will change its hash and break the chain of blocks. The main elements of a blockchain include nodes that store a copy of the entire chain of blocks, transactions that are records of user actions, and a consensus mechanism that ensures data consistency between all nodes in the network. Depending on the type of blockchain, different consensus mechanisms can be used, such as Proof of Work or Proof of Stake.

The key element of the blockchain voting system is smart contracts - a program code stored in the blockchain and automatically executed when predetermined conditions are met. The smart contract defines the voting logic, including the registration of candidates, the recording of votes, and the counting of results. Since the execution of the contract is controlled by a decentralized network, the possibility of data falsification and outside interference is excluded. In this paper, the Solidity programming language, specially developed for work in the Ethereum network, was chosen for the implementation of the smart contract. The language provides built-in mechanisms for event processing and protects against data overflows, which is critical for ensuring the reliability of the voting system. To create the external interface, the Python language with the Web3.py library is used, which provides connection to the Ethereum network, execution of contract calls and processing of events in the blockchain. This combination of tools allows for the implementation of a convenient and secure interface for users, ensuring automatic data transfer between the smart contract and the user interface.

Results and its discussion

When developing the blockchain voting system, a careful selection of tools was carried out. Solidity was chosen as the programming language for writing smart contracts due to its flexibility and built-in security tools. The platform for developing smart contracts was the Truffle framework, which simplifies the process of compiling and deploying contracts in the Ethereum network. Ganache was used as a testing environment - a local blockchain that emulates the operation of the Ethereum network and allows you to track the execution of transactions in real time. Python with the Web3.py library was used to create the external interface, which made it possible to implement convenient interaction with the blockchain and automate the process of transferring data between the interface and the smart contract.

The architecture of voting systems based on blockchain technology is diverse [9,12]. The architecture of the system developed by the authors includes three main components: blockchain, smart contract and user interface. The blockchain stores data on registered candidates, users who voted and election results. The smart contract manages the voting process, including candidate registration, vote processing and results counting. The external Python interface with the Web3.py library provides user interaction with the system, including vote registration, checking the voting status and displaying the results. Figure 1 shows the voting user interface, which provides the ability to select a candidate, send a

vote and view the current results. This approach makes the voting process transparent and simple for all categories of users. (Figure 1).

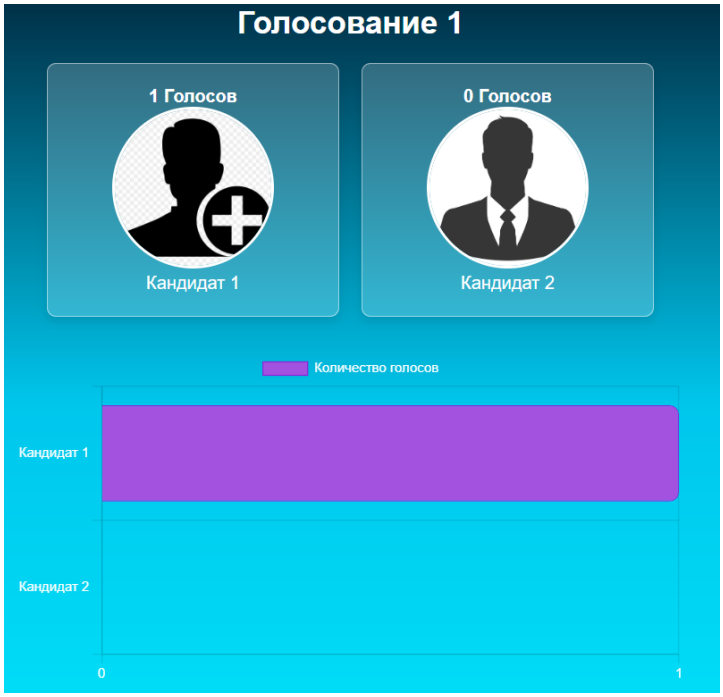

Figure 1. Voter interface

The system starts with the registration of candidates, which is done by calling the appropriate smart contract method. After registration, the user gets the opportunity to vote by choosing one of the candidates. When sending a vote, the smart contract verifies the user's right to vote, preventing the possibility of re-voting. The vote is registered in the blockchain as a transaction, after which the votes are automatically counted and the results are updated. Thanks to the decentralized data storage mechanism, the voting results are protected from external interference and falsification.

During the smart contract implementation phase, variables and data structures were defined to store the list of candidates, registered users, and voting results. The main methods of the contract include:

- method of registration of candidates;
- method of sending a voice with user rights verification;
- method of counting votes and publishing the results.

The smart contract also implements a mechanism to protect against double voting based on the mapping structure, which checks the user's status and blocks re-sending of the vote. The smart contract code includes error handling and protection against external attacks due to strict data control and fulfillment of transaction conditions.

The external interface is implemented in Python using the Web3.py library. At the interface initialization stage, a connection to the smart contract is made via the Ganache URL takes place. User input is checked for correctness, including checking the candidate name format and the absence of duplicate voting. Voting results are displayed in the interface in real time, which increases the usability of the system for end users.

The voting system was tested in the Ganache environment on a local blockchain. During the testing, the correctness of the transactions was confirmed, including the registration of candidates, sending votes and counting the results. The system’s resistance to external attacks showed the absence of vulnerabilities in the voting mechanism, due to strict data verification and decentralized storage of

information. Figure 2 (Figure 2) shows successfully executed transactions in the Ganache environment, reflecting the user's interaction with the smart contract. The window displays key transaction parameters, such as the sender, recipient, hash, amount of gas and execution status, which confirms the correct operation of the system during testing.

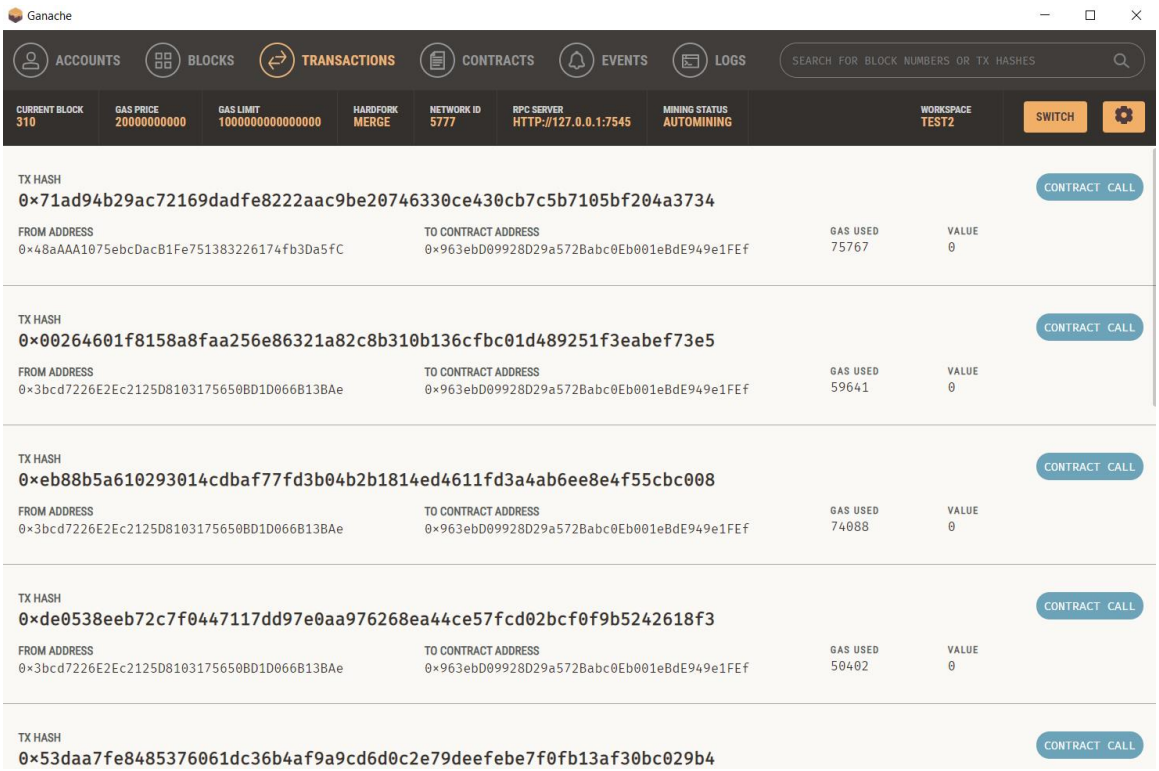

Figure 2. Examples of successful transactions in the Ganache environment

The results of the smart contract execution confirmed the successful implementation of all declared functions. The system correctly processes the registration of candidates, accepts votes from users and automatically calculates the results. The Python interface ensures a stable connection with the smart contract and instantly displays the voting results.

The analysis of the system's resistance to external influences showed a high degree of protection against attempts to falsify data. Protection against double voting, verification of user rights at the stage of sending a vote and the use of a distributed data storage structure ensure a high level of system reliability. Thus, the developed blockchain-based voting system demonstrated successful fulfillment of all functional requirements and resistance to external threats.

Evaluation of the accuracy and reliability of the system

The developed blockchain-based voting system was tested in the conditions of an emulated Ethereum network using the Ganache development environment. During the testing, tests were conducted on the correctness of the main functions of the system, including registration of candidates, sending votes and automatic calculation of results. The testing results showed that the system stably performs all the declared functions without failures and errors. The accuracy of the system was verified by multiple tests with different voting scenarios. In particular, the following situations were simulated:

- voting when there are several registered candidates;
- sending votes from different users;
- attempts to vote again from one account;
- completion of voting and automatic counting of results.

In all tests, the system correctly processed input data, excluded the possibility of repeated voting and ensured accurate vote counting. Verification of the voting results showed their full compliance with the actual votes sent, which indicates the high accuracy of the smart contract. The reliability of the system is ensured by the use of a decentralized data storage mechanism, which eliminates the possibility of substitution or deletion of information about votes. Since each vote is recorded in the blockchain as a transaction, the data is protected from changes after they are added to the chain of blocks. Additional protection is provided by the mechanism for checking the user's access rights to vote and control over the uniqueness of the sent vote using the mapping structure in the smart contract.

To assess the competitiveness of the developed system, comparative tests were conducted with other existing blockchain solutions, such as Follow My Vote and Voatz [13-17]. The main comparison criteria included: accuracy of voice processing, protection against double voting, ease of use of the interface, transaction processing speed, resistance to external attacks.

Follow My Vote System [16] is based on the BitShares blockchain and uses the Delegated Proof of Stake (DPoS) consensus mechanism. The main advantage of this solution is the high speed of transaction processing due to the use of a delegated confirmation mechanism. However, during testing, a dependence of the system speed on the number of active nodes in the network was revealed, which can reduce performance during periods of high load.

Voatz [17] uses a private blockchain based on Hyperledger Fabric with the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. This ensures high transaction speeds, but limits the level of decentralization, since control over the network nodes remains with the system operator.

Unlike the above solutions, the developed system uses the Ethereum blockchain with open access to the network and the Proof of Work (PoW) consensus mechanism, which ensures a high degree of decentralization and reliability of data storage. Despite the potentially lower transaction processing speed in the Ethereum network compared to private blockchains, the tests showed stable operation of the system under standard load during voting. In addition, integration with Python through the Web3.py library made it possible to implement an intuitive interface, which simplifies the use of the system by end users.

Thus, in comparison with similar solutions on the blockchain, the developed system demonstrated a high degree of reliability and data protection due to the use of the open Ethereum network and strict control of transactions at the smart contract level.

One of the key advantages of blockchain technology is its high resistance to data falsification due to decentralized storage of information and cryptographic protection of blocks. During testing, a series of tests were conducted aimed at checking the system’s resistance to possible threats, including:

- attempts to change votes already submitted;
- attempts at double voting;
- interference in the vote counting process from outside;
- attacks on the Ethereum network with the aim of breaking consensus.

A test of the system's resistance to attempts to change data showed that the structure of the Ethereum blockchain excludes the possibility of changing already added blocks without recalculating all subsequent blocks in the chain. Since the Ethereum network uses the Proof of Work mechanism, successfully changing data in the blockchain would require colossal computing resources, which makes an attack on the network virtually impossible in terms of hardware costs and energy consumption.

Attempts to re-vote were successfully blocked at the smart contract level by using a mapping structure that records the fact that a user has voted and prohibits sending a second vote from the same address. When attempting to send a second vote, the smart contract returned an error message and rejected the transaction.

Tampering with the vote counting process was impossible due to the automatic execution of the smart contract conditions in the blockchain. The vote counting was performed automatically after the end of the voting period, and the results were stored in the blockchain in an immutable form.

The test results confirmed the high resistance of the system to external attacks and data falsification due to the use of protection mechanisms embedded in the Ethereum blockchain architecture and the logic of the smart contract. The use of a decentralized network and strict data control at the code level provided reliable protection against attempts to interfere with the voting process and change the results.

Most electronic voting systems have shortcomings, such as lack of transparency and the ability to verify the correctness of vote counting. The developed voting system based on blockchain technology using a smart contract allows you to protect against external influence during vote counting, from duplicate votes. Compared with similar systems, the system proposed by the authors using blockchain technology is simple, accessible and highly reliable, which makes it promising for implementation. The study conducted by the authors and the proposed electronic voting system based on blockchain technology will contribute to the transparency of elections and the democratization of governance at any level.

Conclusion

In the course of the performed research, the set goal was achieved - a - a voting system based on blockchain technology using a smart contract implemented in the Solidity programming language was developed. The developed system includes a smart contract that ensures the registration of candidates, voting and automatic vote counting, as well as an external interface in Python, implemented using the Web3.py library for communication with the Ethereum blockchain.

During the research, a smart contract for voting on the blockchain was successfully tested. During the testing process, the system demonstrated stable operation, correct execution of all functions and protection against attempts at repeated voting. The smart contract implements an automatic vote counting mechanism, guaranteeing the accuracy and reliability of the voting results.

Implemented an external interface for voting using Python. The external interface provides ease of use through an intuitive interface and direct interaction with the smart contract via the Web3.py library. Users can register in the system, vote, and receive voting results in real time.

The system has demonstrated resistance to hacking and falsification attempts. Thanks to the use of the Proof of Work consensus mechanism in the Ethereum network and the built-in smart contract checks for unique voting, the system is reliably protected from repeated voting and external interference. Attempts to change data or violate the voting algorithm were successfully blocked at the level of smart contract logic. Thus, the developed voting system demonstrated a high level of reliability, security and functionality, which confirms the successful implementation of the project and the achievement of the set objectives.

The developed system has significant potential for further development and improvement, such as adding new features to expand voting capabilities, optimizing the vote counting algorithm through asynchronous processing methods. Thus, the developed blockchain voting system not only demonstrates the successful implementation of the basic functionality, but also lays the foundation for further improvements and extensions, which opens up broad prospects for implementation in real voting scenarios.

References

1. Hajian Berenjestanaki M., Barzegar H. R., El Ioini N., & Pahl C. (2023). Blockchain-based e-voting systems: a technology review. Electronics, 13(1), 17. doi:10.3390/electronics13010017

2. Poniszewska-Marańda A., Pawlak M., & Guziur J. (2020). Auditable blockchain voting system-the blockchain technology toward the electronic voting process. International Journal of Web and Grid Services, 16(1), 1-21.

3. Sharma S., & Dubey V. (2019) Decentralized Voting System Using Blockchain Technology. Journal of Computer Applications, 42, 1. doi:10.22214/ijraset.2023.53179

4. Nguyen H., & Nguyen T. (2021) Blockchain-based Voting Systems: A Comprehensive Survey.

Journal of Computer Science and Technology, 36,1.

5. Sharp M., Njilla L., Huang C. T., & Geng T. (2024). Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal. Network, 4(4), 426-442. doi:10.3390/network4040021

6. Kannoly A., Arun S., Subramanian G., Pandey S. K., & Arumugaselvi M. (2020). Impact of blockchain in the voting system. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9. doi:10.35940/ijitee.H6515.079920

7. Bhavani D. D., Gayathri R., Bhagavanthu M., Sheeba A., Sampoornam M., & Bhuvaneshwari P. (2025). Blockchain-Based Voting Systems Enhancing Transparency and Security in Electoral Processes. In ITM Web of Conferences, 76, 02004. EDP Sciences. doi:10.1051/itmconf/20257602004

8. Hajian Berenjestanaki M., Barzegar H. R., El Ioini N., & Pahl C. (2023). Blockchain-based e-voting systems: a technology review. Electronics, 13(1), 17. doi:10.3390/electronics13010017

9. Ohize H. O., Onumanyi A. J., Umar B. U., Ajao L. A., Isah R. O., Dogo E. M., ... & Ibrahim M. M. (2025). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Computing, 28(2), 132.

10. Melovic S., Stefanovic D., & Dakic D. (2025, March). Design and Implementation of an Electronic Voting System Using Blockchain Technology. In 24th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-6). IEEE.

11. Bamakhrama M., Al-Zaabi A., Al-Shateri A., Al-Ghailani K., Al-Kindi M., & Pavithran D. (2024, February). Casting Votes in the Digital Age: Designing a Blockchain-Powered E-Voting System. In International Congress on Information and Communication Technology (pp. 183-195). Singapore: Springer Nature Singapore.

12. Oprea S.V., et al. (2023) Conceptual architecture of a blockchain solution for E-voting in elections at the university level. IEEE Access, 11 (pp.18461-18474).

13. Nikhare R.V., Chandavarkar B.R. (2023) A Comparative Analysis of Traditional versus Blockchain-based Voting Systems. In 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, (pp. 1-7).

14. Patel K., et al. (2022) Comparative study of blockchain-based voting solutions. Intelligent Sustainable Systems: Proceedings of ICISS. Singapore: Springer Nature Singapore, (pp. 671-686).

15. Gochhi S.K., et al. (2024) Blockchain-Based Comparative Analysis of E-Voting Systems: A Review. International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC). – IEEE, (pp. 1-6).

16. Official website Follow My Vote. [Electronic resource] – URL: https://followmyvote.com/ (date of access 2.05 .2025).

17. Official website Voatz. [Electronic resource] – URL: https://voatz.com (date of access 2.05.2025).

Әдебиеттер тізімі

1. Hajian Berenjestanaki M., Barzegar H. R., El Ioini N., & Pahl C. (2023). Blockchain-based e-voting systems: a technology review. Electronics, 13(1), 17. doi:10.3390/electronics13010017

2. Poniszewska-Marańda A., Pawlak M., & Guziur J. (2020). Auditable blockchain voting system-the blockchain technology toward the electronic voting process. International Journal of Web and Grid Services, 16(1), 1-21.

3. Sharma S., & Dubey V. (2019) Decentralized Voting System Using Blockchain Technology. Journal of Computer Applications, 42, 1. doi:10.22214/ijraset.2023.53179

4. Nguyen H., & Nguyen T. (2021) Blockchain-based Voting Systems: A Comprehensive Survey. Journal of Computer Science and Technology, 36,1.

5. Sharp M., Njilla L., Huang C. T., & Geng T. (2024). Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal. Network, 4(4), 426-442. doi:10.3390/network4040021

6. Kannoly A., Arun S., Subramanian G., Pandey S. K., & Arumugaselvi M. (2020). Impact of blockchain in the voting system. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9. doi:10.35940/ijitee.H6515.079920

7. Bhavani D. D., Gayathri R., Bhagavanthu M., Sheeba A., Sampoornam M., & Bhuvaneshwari P. (2025). Blockchain-Based Voting Systems Enhancing Transparency and Security in Electoral Processes. In ITM Web of Conferences, 76, 02004. EDP Sciences. doi:10.1051/itmconf/20257602004

8. Hajian Berenjestanaki M., Barzegar H. R., El Ioini N., & Pahl C. (2023). Blockchain-based e-voting systems: a technology review. Electronics, 13(1), 17. doi:10.3390/electronics13010017

9. Ohize H. O., Onumanyi A. J., Umar B. U., Ajao L. A., Isah R. O., Dogo E. M., ... & Ibrahim M. M. (2025). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. Cluster Computing, 28(2), 132.

10. Melovic S., Stefanovic D., & Dakic D. (2025, March). Design and Implementation of an Electronic Voting System Using Blockchain Technology. In 24th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-6). IEEE.

11. Bamakhrama M., Al-Zaabi A., Al-Shateri A., Al-Ghailani K., Al-Kindi M., & Pavithran D. (2024, February). Casting Votes in the Digital Age: Designing a Blockchain-Powered E-Voting System. In International Congress on Information and Communication Technology (pp. 183-195). Singapore: Springer Nature Singapore.

12. Oprea S.V., et al. (2023) Conceptual architecture of a blockchain solution for E-voting in elections at the university level. IEEE Access, 11 (pp.18461-18474).

13. Nikhare R.V., Chandavarkar B.R. (2023) A Comparative Analysis of Traditional versus Blockchain-based Voting Systems. In 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, (pp. 1-7).

14. Patel K., et al. (2022) Comparative study of blockchain-based voting solutions. Intelligent Sustainable Systems: Proceedings of ICISS. Singapore: Springer Nature Singapore, (pp. 671-686).

15. Gochhi S.K., et al. (2024) Blockchain-Based Comparative Analysis of E-Voting Systems: A Review. International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC). – IEEE, (pp. 1-6).

16. Official website Follow My Vote. [Electronic resource] – URL: https://followmyvote.com/ (date of access 2.05 .2025).

17. Official website Voatz. [Electronic resource] – URL: https://voatz.com (date of access 2.05.2025).

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ НЕГІЗІНДЕ ДАУЫС БЕРУ ЖҮЙЕСІН ҚҰРУ

САРСИМБАЕВА С.М.*, БАЗАРБАЕВ С.Ж.

***Сарсимбаева Сауле Мусаевна** - Физика-математика ғылымдарының кандидаты, қауымдастырылған профессор, Қ.Жұбанов атындағы Ақтөбе өңірлік университеті, Ақтөбе қ., Қазақстан
E-mail: saulesarsi@gmail.com, http://orcid.org/0000-0003-1536-3042
Базарбаев Султан Жарасович - Магистрант, Қ.Жұбанов атындағы Ақтөбе өңірлік университеті, Ақтөбе қ., Қазақстан
E-mail: sbazarbaev550@gmail.com, http://orcid.org/0000-0009-8786-3738.

Аңдатпа. Электрондық дауыс берудің әртүрлі жүйелері құрылған. Бірақ мұндай жүйелердің көпшілігінде ашықтықтың болмауы және дауыстарды санаудың дұрыстығын тексеру мүмкіндігінің жоқшылығы сияқты кемшіліктері бар. Мақалада блокчейн технологиясын қолдана отырып дауыс беру жүйелерін құру мәселелері қарастырылған. Блокчейн технологиясы негізінде, әсіресе шектеулі ресурстар жағдайында сайлау процестерінің ашықтығын, қорғалуын және сенімділігін арттыру мүмкіндігі көрсетілген. Авторлар практикада іске асырылған қосымша ұсынылған - блокчейн технологиясына негізделген электронды дауыс беру жүйесі, Solidity тіліндегі

ақылды келісімшарттардан және Web3.py кітапханасы қолданылған Python тілінде құрылған пайдаланушы интерфейсіннен тұратын. Мақала авторлары қолданыстағы шешімдерге талдау жүргізіп, олардың кемшіліктерін анықтады, жүйенің архитектурасын ұсынды және қосымшаның негізгі функцияларын іске асырды: кандидаттарды тіркеу, дауыс беру, қайталанған дауыстардан қорғау және нәтижелерді автоматты түрде есептеу. Ganache ортасындағы тестілеу нәтижелері жүйенің дұрыс жұмыс істеуін және сыртқы әсерлерге төзімділігін растады. Аналогтармен салыстырғанда, авторлар ұсынған блокчейн технологиясына негізделген жүйенің дизайны қарапайымдылығымен, қол жетімділігімен және жоғары сенімділігімен ерекшеленеді, бұл жүйені қолданысқа енгізу үшін перспективалы етеді. Авторлардың электронды дауыс беру жүйелерінің эволюциясын зерттеуі, электронды дауыс беру жүйелері үшін блокчейн технологиясын қолдану демократиялық басқарудың тиімді шешімдерін құруға ықпал етеді.

Түйін сөздер: блокчейн, дауыс беру жүйелері, электронды дауыс беру, ақылды келісімшарт, орталықсыздандыру, мәліметтер қауіпсіздігі, құпиялылық

РАЗРАБОТКА СИСТЕМЫ ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

САРСИМБАЕВА С.М.[*], БАЗАРБАЕВ С.Ж.

[*]**Сарсимбаева Сауле Мусаевна** - Кандидат физико-математических наук, ассоциированный профессор, Актюбинский региональный университет имени К.Жубанова, г. Актобе, Казахстан
E-mail: saulesarsi@gmail.com, http://orcid.org/0000-0003-1536-3042
Базарбаев Султан Жарасович - Магистрант, Актюбинский региональный университет имени К.Жубанова, г. Актобе, Казахстан
E-mail: sbazarbaev550@gmail.com, http://orcid.org/0000-0009-8786-3738.

Аннотация. Разработаны различные системы электронного голосования. Но большинство таких систем имеют такие недостатки как отсутствие прозрачности и возможности проверки правильности подсчета голосов. В статье рассмотрены вопросы разработки систем голосования с использованием технологии блокчейн. Показана возможность повышения прозрачности, защищенности и достоверности электоральных процессов на основе технологии блокчейн, особенно в условиях ограниченных ресурсов. Показана разработанная авторами практическая реализация - система электронного голосования на основе технологии блокчейн с использованием смарт-контрактов на языке Solidity и пользовательского интерфейса на языке Python с библиотекой Web3.py. Проведен анализ существующих решений, выявлены их недостатки, предложена архитектура системы и реализованы основные функции: регистрация кандидатов, голосование, защита от повторных голосов и автоматический подсчет результатов. Результаты тестирования в среде Ganache подтвердили корректность работы и устойчивость системы к внешним воздействиям. В сравнении с аналогами предложенное авторами конструкция системы с применением технологии блокчейн отличается простотой, доступностью и высокой надежностью, что делает его перспективным для внедрения. Исследование эволюции систем электронного голосования, использование технологии блокчейн для систем электронного голосования способствуют разработке эффективных решений для демократического управления.

Ключевые слова: блокчейн, системы голосования, электронное голосование, смарт-контракт, децентрализация, безопасность данных, конфиденциальность