Development of a decentralized voting system based on blockchain technology

Nazarii Savorona[1,†], Oleh Suprun[1,†], Oleksandr Provotar[1,†], Tetiana Savorona[2,†], Olha Suprun[1,3,*,†] and Vitalii Nechyporuk[3,†]

[1] *Taras Shevchenko National University of Kyiv, Volodymyrska Str., 64/13, Kyiv, 01601, Ukraine*
[2] *Lviv Polytechnic National University, Stepan Bandera Str., 12, Lviv, 03058, Ukraine*
[3] *National Aviation University, Liubomyra Huzara Ave. 1, Kyiv, 03058, Ukraine*

Abstract

This paper focuses on the design and implementation of a decentralized polling system based on Blockchain technology. Ensuring transparency, security, anonymity, and immutability of survey data, the system uses PBFT consensus in the context of voting. The development was done using an Agile approach, Golang for the backend, Vue.js 3 for the frontend, IntelliJ IDEA integrated development environment, Postman for testing, and GitHub Copilot for automatic code completion. The project was managed via Jira. The deliverables include a prototype system, analog analysis, and testing. The novelty lies in the use of modern tools, providing an independent survey with transparency and reliability. The developed system can be successfully implemented in various industries, including NGOs, companies, and government agencies, due to its modular structure and easy adaptability to user needs.

Keywords

anonymity, blockchain, validator, decentralization, ring signature, voting system, transaction

1. Introduction

At the current stage of development of survey systems and Blockchain technologies, innovative solutions aimed at improving the transparency, security and anonymity of surveys are being actively studied and developed. In this context, Blockchain acts as a promising technological basis that ensures the immutability and high level of trust in data storage [1, 2]. Despite the potential benefits, there are challenges related to the speed, scalability and cost of implementing such systems.

The relevance of this work is due to the need to develop a decentralized survey system based on Blockchain that meets modern requirements of transparency and anonymity, especially in the context of democratic processes. The need for new approaches to the development of survey systems that ensure a high level of trust in survey processes is becoming crucial in choosing research areas.

The goal of this work is to create a decentralized Blockchain-based polling system with a focus on transparency, security, and anonymity. To achieve this goal, specific tasks have been set, including analyzing decentralization approaches, researching Blockchain technology, designing a voting system, and implementing software components for validators and a web application. The result is an efficient electronic voting system that combines the principles of Blockchain and digital signatures, ensuring reliability and anonymity in voting.

CH&CMiGIN'24: Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, January 24–27, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
nazarii.savorona@knu.ua (N. Savorona); oleh.suprun@knu.ua (O. Suprun); a.i.provotar@gmail.com (O. Provotar); tetiana.savorona.bi.2021@lpnu.ua (T. Savorona); olhasuprun@knu.ua (O. Suprun); vitalii.nechyporuk@npp.nau.edu.ua (V. Nechyporuk)
0009-0008-8027-8235 (N. Savorona); 0000-0002-6243-3720 (O. Suprun); 0000-0002-6556-3264 (O. Provotar); 0009-0001-9310-9173 (T. Savorona); 0000-0002-1196-5655 (O. Suprun); 0000-0003-3580-9953 (V. Nechyporuk)

2. Review of existing electronic voting systems

2.1. General description of electronic voting systems, analysis of specific electronic voting systems

Electronic voting systems include software and hardware for organizing voting using electronic means. They are used for various types of voting, such as political elections, corporate meetings, or public polls.

Electronic voting systems usually consist of several key components, including modules for creating and managing ballots, conducting voting, processing results, and auditing. Ensuring security is a critical aspect to preserve the confidentiality of votes and prevent fraudulent results.

Recently, the use of Blockchain technology has been gaining popularity in e-voting systems. Blockchain promotes transparency and immutability of voting results while ensuring the confidentiality of votes [3].

For a full analysis of electronic voting systems, it is worth consider several popular systems that exist today.

2.1.1. Google Forms

Google Forms is a tool for creating online surveys and questionnaires. In particular, it is noted:

- ease of use: the intuitive interface allows users to quickly create surveys without programming or complex settings;
- variety of questions: the ability to choose different types of questions to create detailed surveys;
- easy distribution: the ability to distribute surveys through links or embedding on web pages for easy completion from any device;
- automatic data processing: the system automatically collects and organizes data using Google Sheets tools for further analysis.

Despite these advantages, Google Forms has limitations:

- lack of specialization: it is a general-purpose tool, which can limit its functionality and security for conducting votes;
- lack of cryptography: the lack of built-in cryptography and digital signatures can create a risk of falsification of results;
- limited flexibility: The system has limited options for customizing question types and processing results;
- data storage: Google Forms stores data on its servers, which may violate privacy and personal data protection regulations [4, 5].

2.1.2. Helios Voting

Helios Voting is an electronic voting system that uses cryptographic protocols [6]. The main features include:

- Privacy protection: Applies cryptographic voting protocols to anonymize and protect voters' personal information;
- Vote verification: Provides voters with the ability to verify that their votes are counted correctly and avoid fraud;
- Voting flexibility: The ability to customize voting types and requirements to adapt to different scenarios;

- Remote voting: Allows voting remotely via the Internet, making the process easier and more accessible.

Disadvantages include:

- Difficulty of use: The interface is complex and requires a high level of technical expertise, which can create barriers for a wide audience;
- Limited scalability: May face difficulties when processing large numbers of votes or conducting large-scale polls;
- Limited customization: Limited options for customizing voting and result processing options, which can limit flexibility and responsiveness to user needs.

2.1.3. Voatz

Voatz is an electronic voting system for mobile devices that uses biometric data for security. It provides convenience and transparency of voting, but has limited accessibility and possible risks of cyberattacks. Insufficient security controls and the lack of open source code cast doubt on the transparency of the system. Vote privacy and deployment costs are also issues to consider [7].

2.1.4. Estonian i-Voting

Estonia has implemented electronic voting through the i-Voting system, which requires an electronic ID. Key features include cryptographic vote protection, the ability to change a vote, and efficient voting. Disadvantages include reliance on an electronic ID, risk of cyberattacks, limited anonymity, and limited accessibility for those without internet access or technical skills [8].

2.2. Problems of existing electronic voting systems

While e-voting systems offer numerous benefits, they also face a number of problems and challenges:

- The most obvious problem is security: hacking, data theft and other cybercrime can undermine the credibility of e-voting data theft and other cybercrime can destroy the credibility of electronic voting and change the election results [9];
- Ensuring the anonymity of votes is a difficult task in the digital environment, cryptography can help, but it cannot always guarantee absolute privacy, absolute privacy;
- e-voting systems can suffer from technical problems that may prevent problems that may prevent voters from casting their ballots or even influence the election results;
- In areas with limited access to the Internet or where people may not have the necessary have the necessary technology, e-voting may be difficult to conduct, to conduct;
- In systems that allow for the alteration of votes, there is a risk that this feature may be misused, systems that allow for vote changes, there is a risk that this feature may be misused, leading to situations where voters are forced to change their vote under pressure.

These issues can be addressed in a number of ways, including improving cryptographic methods, improving infrastructure, and conducting educational campaigns for citizens.

3. Consideration of blockchain technology and related tools in electronic voting systems

3.1. Description of Blockchain technology

Blockchain technology, or blockchain, is a type of decentralized database that stores data in the form of a sequence of "blocks" [10]. Each block contains information about transactions that took place

over a certain period, as well as a cryptographic hash of the previous block in the chain, which ensures data integrity and immutability (Figure 1).

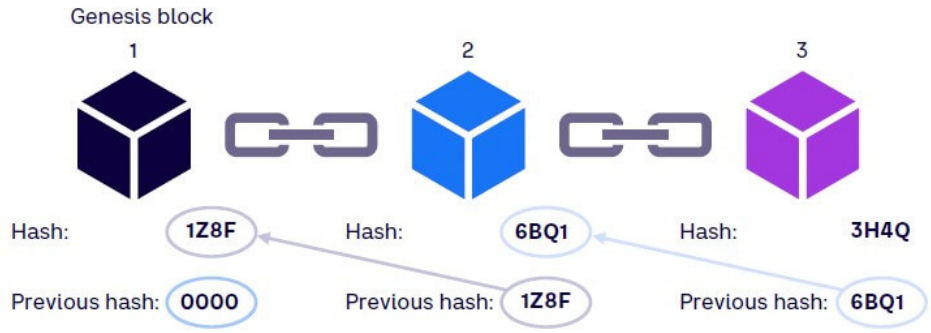

Figure 1: Connections of blocks in Blockchain.

The main characteristics of Blockchain technology include:

- decentralization, which implies the absence of a central point of control, this makes the system more resistant to attacks, all network participants (nodes) have the same copy of the entire Blockchain;
- all transactions are stored without encryption, in open form, for viewing by all network participants, which increases transparency;
- one of the key features of Blockchain is the inability to change already recorded data, which ensures a high level of trust in the recorded data;
- the use of cryptography allows to ensure the confidentiality of transactions, protection against manipulation and unauthorized access to data.

Blockchain has found a large number of applications, ranging from cryptocurrencies like Bitcoin to broader applications such as supply chain management, elections, and many others [11].

3.2. Advantages of using Blockchain

Blockchain technology can improve the transparency, reliability and security of electronic voting. Its advantages include the immutability of votes, open access to data for verification, secure cryptography, decentralization, automation of vote counting, and the ability to trace a vote by a voter. However, the use of blockchain in e-voting poses challenges such as anonymity, scalability, and energy efficiency, and requires further research.

3.3. The concept of keys

A cryptographic key is a digital sequence of a certain length, created according to certain rules, using random number generators and calculated using a special algorithm. A cryptographic key is the main component of cryptographic operations. The security of most cryptographic schemes generally depends on key security [12]. A private key is a positive integer of constant length, which is generated using the following generators. Public key is obtained from the private key by means of mathematical transformations. It is important to note that for cryptographic algorithms that are considered to be sufficiently reliable, the reverse process, i.e. obtaining a private key from a from the public key, is impossible in practice (Figure 2).

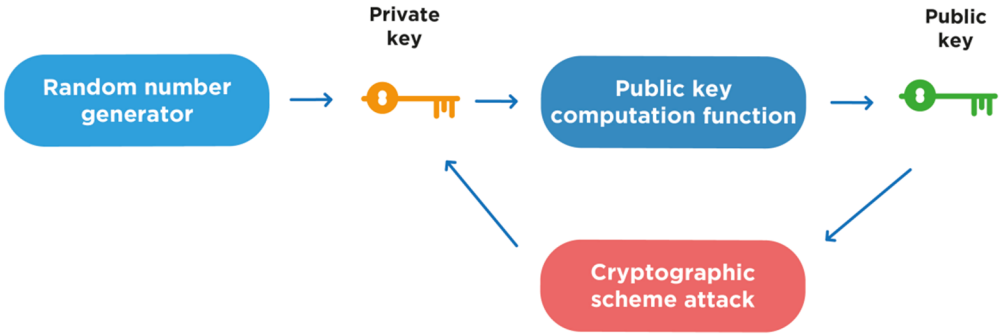

Figure 2: Private and public keys.

3.4. Ring signature

The ring signature plays a key role in digital voting. A digital signature verifies the authenticity and integrity of documents, protecting them from modification. Ring signatures use the public keys of users in a group, ensuring anonymity among ring members (Figure 3). Users create signatures using their own and other members' public keys and are verified without identifying a specific author.

In order to create a signature on behalf of the group, the user needs to enter the public keys of all ring participants (including their own) at the entrance of the algorithm and use their private key as a secret. Recall that the public keys of each participant are publicly available.

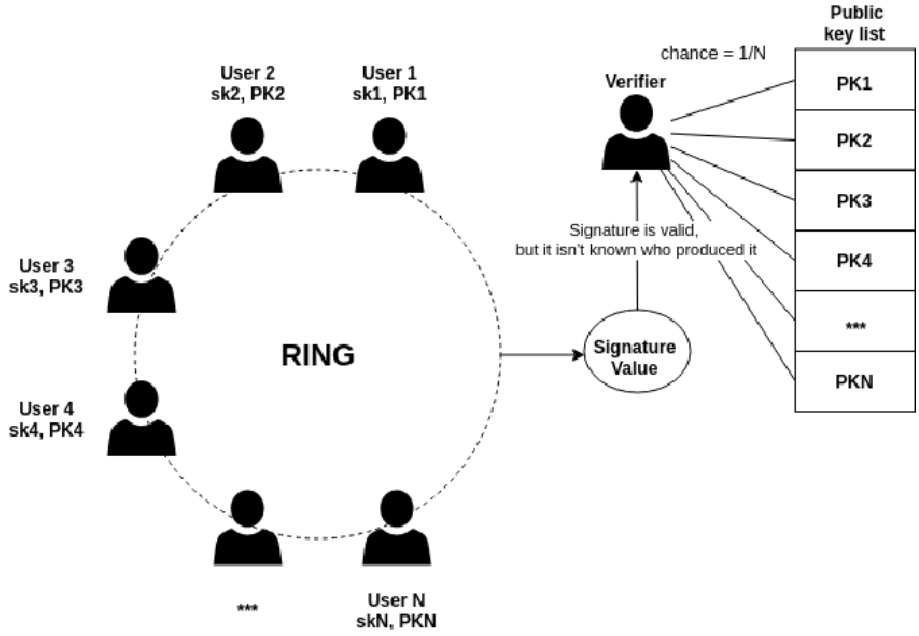

Figure 3: Ring signature and its validation.

When the verifier checks the value of a signature, it can make sure that the signature was created by one of the group members, but it is not known by whom. Only with probability $1/N$, he can determine that the signature was calculated by a specific member of the ring. It is worth noting that a user can be disclosed only in case of collusion of all other group members [13].

4. Designing an electronic voting system based on blockchain

4.1. Defining functional requirements for the system

When designing Blockchain-based e-voting, it is important to ensure:

- public access to votes without voter identification;
- the ability to change votes by adding new data;
- preventing double voting;
- voter anonymity;
- accessibility for voters regardless of location and device type;
- intuitive user interface.

These functional requirements will facilitate transparent and fair voting by allowing the public to verify the results. The Blockchain principles will ensure the immutability of votes, avoiding the possibility of their alteration or deletion.

4.2. The system's components

The blockchain-based electronic voting system includes:

1. Validator nodes: The main participants that confirm and verify votes in the system. Each has its own copy of the Blockchain.
2. Voting processing module: An important part of the validator that checks the validity of votes, processes data, and registers votes on the Blockchain.
3. Connector node: An intermediary that provides connectivity between validator nodes by maintaining up-to-date information.
4. Blockchain: A distributed database that stores votes. Ensures data is inaccessible and immutable.
5. Voters: Users who vote through a web-based interface.
6. Web user interface: A user-friendly interface for registration and voting.
7. PBFT-based consensus: Interaction of nodes to decide whether to include a block in the Blockchain.

The developed e-voting system based on Blockchain uses this complex set of components and elements to ensure security, reliability, and anonymity of voting. The use of Blockchain in the system helps to ensure the immutability and authenticity of votes, making it reliable and secure for electronic voting [14].

4.3. Processes in the system

The processes in a Blockchain-based e-voting system include:

1. User registration: The administrator creates a registration transaction with the user's public key.
2. Creating a poll: The administrator creates a vote creation transaction with questions and answers.
3. User voting: Users select answer options, create and confirm voting transactions.
4. Vote counting: The system counts the votes by looking at the vote transactions in the Blockchain.
5. User vote verification: Users check the status of their transactions to confirm their vote.
6. Adding a new node: A new validator confirms its legitimacy, synchronizes the Blockchain, and notifies other participants.

Each process ensures the security, integrity, and anonymity of the vote.

5. Development of an electronic voting system based on blockchain

5.1. Choosing technologies and tools for development

The following technologies and tools were used to develop the prototype e-voting system:

1. Golang: For the backend with high performance and efficient memory management.
2. Vue.js 3: For the development of a dynamic web interface.
3. Docker and Railway: For containerization and efficient application deployment.
4. IntelliJ IDEA Ultimate: An integrated development environment with a powerful code editor.
5. Postman: A tool for testing and developing APIs with support for HTTP and WebSocket.
6. Agile development: An iterative approach for flexible and efficient development.
7. Jira: A project management system for planning and tracking tasks.
8. Git and GitHub: For version control and code collaboration.
9. GitHub Copilot: An intelligent assistant for auto-complete code based on artificial intelligence.

The choice of these technologies is aimed at ensuring the efficiency, reliability, and speed of system development and operation.

5.2. Implementation of individual system modules

5.2.1. Node Connector

A node connector in an electronic voting system is responsible for connectivity between different nodes. Its API has two main requests: GET /nodes to get a list of active nodes and POST /nodes to notify when a new node is available. By providing constant communication checks using WebSockets, it quickly updates the list of active nodes. Information about nodes is stored in RAM and the file system for quick access and preservation between system starts [15]. The node connector is used as an intermediary between validators and web clients, providing them with up-to-date information about active nodes and ensuring efficient interaction.

5.2.2. Validator

A validator plays a key role in an e-voting system by accepting, validating, and creating blocks. They check the validity of transactions, group them into blocks, and create new blocks based on consensus rules. Validators distribute the blocks across the network and make decisions about their addition. The applied consensus model resembles Byzantine fault tolerance, ensuring the security and integrity of the network. The number of validators to validate a block depends on the configuration file, and the decision-making process takes into account the importance of consensus and support from many participants. The system uses polls and validators signatures to ensure distributed decision-making and reliability of the block addition process.

5.2.3. Web-client

To implement the web client of the electronic voting system, we used several development technologies were used to implement the web client. The main platform for the frontend was Vue.js, which provided powerful tools for creating interactive and aesthetic user interface (Figure 4).

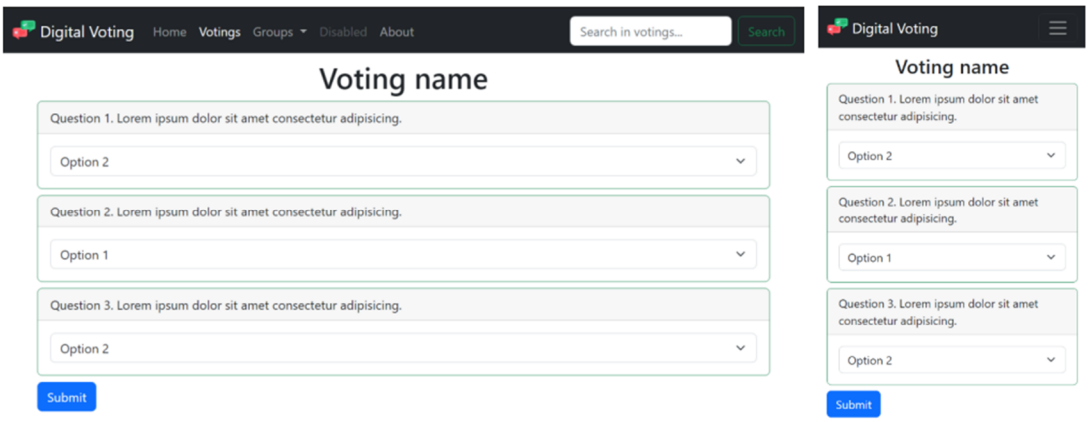

Figure 4: User interface on screens with different resolutions.

The e-voting system uses the Bootstrap v5 library for speed and flexibility of design. The backend uses the Golang programming language to process cryptography and validation logic. The use of validator packages guarantees the security and accuracy of transaction processing. Golang supports modules, which facilitates easy package reuse and dependency management. Operations related to users' private keys are performed locally, ensuring a high level of security. The user's private key is stored encrypted in the file system, which increases protection against possible attacks. This approach using Golang ensures efficient processing and security of operations in the e-voting system.

6. Testing and evaluation of the developed system

6.1. Conducting testing

During the testing process, each of the developed test scenarios was executed, the results were collected and analyzed. Scenarios related to administrator registration, user registration, creating a survey, voting by the user and viewing voting results were successfully completed. The system responded to each of these scenarios in accordance with expectations, which demonstrates its reliability and efficiency. The results confirm that the developed system is reliable and effective. This indicates that the system is ready for implementation in real conditions.

6.2. Analysis of system efficiency

The e-voting system meets the requirements of decentralization, ensuring security and transparency. The user interface is intuitive and adaptive [16]. The cost of the system depends on the number of validators and the length of the Blockchain. The system uses PBFT consensus, ECDSA for signatures and provides a high level of security. Prevents 51% attacks on keys, nodes, unauthorized use, and client substitution. Only the administrator creates votes and uses cryptographic algorithms to ensure data security. It is noted that the system is not completely impenetrable, and continuous improvements are needed.

6.3. The system's prospects

High-load testing of the system is planned to monitor and optimize the response during intensive use. The possibility of integrating the voting system with the Diia project and other government programs for the digitalization of civic participation is being considered. The development of electronic voting systems and cooperation with scientific institutes will contribute to the creation of a modern and innovative system for a decent future for Ukrainian citizens. It is emphasized that the digital transformation of voting is an important step towards a transparent, democratic and strong Ukraine.

7. Conclusions

Based on the research, it can be stated that the developed Blockchain-based voting system using PBFT consensus consensus has proven to be effective and reliable. The code can be found in the repositories GitHub [17, 18].

Traditional voting systems face problems such as vote manipulation, lack of transparency, accessibility issues, high costs, and the risk of counting errors.

The developed Blockchain-based voting system using the PBFT consensus voting system effectively solves these problems. It ensures security and transparency of voting, guarantees the reliability of decision-making, and prevents vote fraud.

The system also solves the problem of accessibility by allowing voting from from any location. Using Blockchain and distributed consensus ensures that each vote is recorded and stored securely.

The developed system can be implemented in practice in various areas, including local elections or corporate voting. It can also be used in other areas where transparency and reliability of voting is required.

In the process of developing this system, a number of modules were created that perform different roles in the context of validation and the voting process.

The implemented system is of great importance in the context of research on how such systems are built, how similar systems are built. During the implementation process, the team faced a number of challenges that had to be addressed both in the choice of technologies and the selection of algorithms to be applied.

The work opens up new opportunities for research in the field of Blockchain and e-voting systems, and also contributes to the technical improvement of electronic voting technologies. From the socio-economic side, the system can contribute to the efficiency of voting by ensuring transparency and saving resources.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, In: S. Shukla, A. Unal, J. Varghese Kureethara, D.K. Mishra, D.S. Han (Eds.), Data science and security, volume 290 of Lecture Notes in Networks and Systems, Springer, Singapore, 2021, pp. 258–265. doi: 10.1007/978-981-16-4486-3_28.

[2] R. Kostyrko, T. Kosova, L. Kostyrko, L. Zaitseva, O. Melnychenko, Ukrainian market of electrical energy: Reforming, financing, innovative investment, efficiency analysis, and audit, Energies 14 (16):5080 (2021). doi: 10.3390/en14165080.

[3] O. Suprun, N. Savorona, Decentralized electronic voting system based on blockchain technology, in: Proceedings of International scientific and technical conference "Intelligent technologies of linguistic analysis", NAU, Kyiv, 2022, p. 39.

[4] T. M. Buchsbaum, E-Voting: International Developments and Lessons Learned, 2022. URL: https://tinyurl.com/37fxpkhf.

[5] U. Jafar, M. J. Ab Aziz, Z. Shukur, Blockchain for Electronic Voting System-Review and Open Research Challenges, 2021. URL: https://doi.org/10.3390/s21175874.

[6] B. Adida, Helios: Web-based Open-Audit Voting, 2022. URL: https://tinyurl.com/2edssk9v.

[7] D. Springall, T. Finkenauer, Z. Durumeric, et al., Security Analysis of the Estonian Internet Voting System, 2023. URL: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.

[8] S. Popereshnyak, O. Suprun, O. Suprun, T. Wieckowski, Intrusion detection method based on the sensory traps system, in: Proceedings of XIV-th International Conference on Perspective

Technologies and Methods in MEMS Design (MEMSTECH), IEEE, Lviv, Ukraine, 2018, pp. 122–126. doi: 10.1109/MEMSTECH.2018.8365716.
[9] L. C. Bollinger, M. A. McRobbie, D. Baltimore, et al., Securing the Vote: Protecting American Democracy, The National Academies Press, 2018.
[10] J. Zsigmond, Creating a Blockchain from Scratch. Level Up Coding, 2020. URL: https://levelup.gitconnected.com/creating-a-blockchain-from-scratch9a7b123e1f3e.
[11] P. Kravchenko, B. Skryabin, O. Dubinina, Blockchain and decentralized systems: a textbook [for students of higher education institutions]: in 3 parts. Part 1, Kharkiv, PROMART, 2019.
[12] P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina, : a textbook [for students of higher education institutions]: in 3 parts. Part 3, PROMART, Kharkiv, 2020.
[13] O. Kurbatov, P. Kravchenko, O. Shapoval et al., Anonymous Decentralized E-Voting System, in: Proceedings of International Workshop on Conflict Management in Global Information Networks, 2019, pp. 12–22.
[14] Wang G. SoK: Understanding BFT Consensus in the Age of Blockchains [Electronic resource] / Gang Wang. - 2021. - Mode of access to the resource: https://eprint.iacr.org/2021/911.pdf.
[15] K. Cox-Buday, Concurrency in Go, Sebastopol, CA: O'Reilly Media, Inc., 2017.
[16] Railway documentation, 2023. URL: https://docs.railway.app/.
[17] A. O. Balykov, R. V. Volchetskyi, N. V. Savorona, Repositories with the code of the described system, 2023. URL: https://github.com/orgs/Digital-Voting-Team/repositories.
[18] O. Ponomarenko, O. Suprun, A. Ponomarenko, N. Savorona, V. Nechyporuk, Information Capacity of Traffic Parameters of the Wireless Network of Critical Application in: Proceedings of 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), IEEE, Kyiv, Ukraine, 2022, pp. 273–276. doi: 10.1109/ATIT58178.2022.10024246.