Study of Cyber Security Approaches in Organizing Digital Voting

Nadiia Lobanchykova[1,2], Tetiana Vakaliuk[1,3,4], Viacheslav Osadchyi[5], Mykhailo Medvediev[6], and Ihor Pilkevych[7]

[1]Zhytomyr Polytechnic State University, 103, Chudnivsyka str., Zhytomyr, 10005, Ukraine
[2]PwC Nederland, Thomas R. Malthusstraat 5, 1066 JR Amsterdam, Netherlands
[3]Institute for Digitalisation of Education of the NAES of Ukraine, 9, M. Berlynskoho str., Kyiv, 04060, Ukraine
[4]Kryvyi Rih State Pedagogical University, 54, Gagarin ave., Kryvyi Rih, 50086, Ukraine
[5]Borys Grinchenko Kyiv University, 18/2, Bulvarno-Kudriavska str, Kyiv, 04053, Ukraine
[6]ADA University, School of Information Technologies and Engineering, Baku, AZ1008, Azerbaijan
[7]Korolov Zhytomyr Military Institute, 22, Prospect Myru, Zhytomyr, 10004, Ukraine

Abstract

The development of information technologies and digitalization are transforming society as a whole, which leads to the introduction of innovations and innovations at the state level. The issues of holding fair, democratic, and transparent elections using modern information technologies are the task of many countries of the world and Ukraine in particular. The experience of other countries in organizing digital elections creates opportunities for analysis, taking into account the vulnerabilities of the models used, and combining their advantages. Thus, within the framework of this publication, an analysis of known solutions for organizing digital voting and the possibility of its implementation in Ukraine by combining digitalization technologies of Ukrainian society and blockchain technologies was carried out. To ensure proper security, and increase the level of trust and transparency of elections, it is proposed to use a combination of methods and technologies, namely: Ethereum blockchain technology using some smart contracts to ensure the voter registration procedure, the voting procedure, and vote counting; cryptographic hashing methods to ensure anonymity and confidentiality of information The possibilities of using the application/portal "Diia" for organizing digital elections on the territory of Ukraine are considered. The proposed solutions are analytical and conceptual and require the development of a mathematical and algorithmic apparatus and a detailed analysis of the possibilities of physical implementation within Ukraine and Ukrainian legislation.

Keywords

Voting, blockchain, Ethereum, smart contracts, Diia, cybersecurity.

1. Introduction

Today, humanity is constantly transforming into a digital society. The development of information technology leads to the emergence of new technologies and their implementation in everyday life. Blockchain technology is rapidly developing and expanding the possibilities of its use. The advent of cryptocurrency has opened up new opportunities for the transition of society to digital finance. The cryptocurrency market is constantly expanding, it has certain fluctuations, like ordinary money.

With the advent of Ethereum, smart contracts were introduced. Based on blockchain technology, smart contracts have gained trust and expanded their use cases. Today they are used in financial structures, insurance, business, logistics companies, industry, etc.

A special place in the digital society is occupied by digital elections, which, using blockchain technology, would provide the desired trust, transparency, and confidentiality. This issue is very relevant in most countries that are

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine

EMAIL: lobanchikovanadia@gmail.com (N. Lobanchykova); tetianavakaliuk@gmail.com (T. Vakaliuk); poliform55@gmail.com (V. Osadchyi); miserablewisdom@ukr.net (M. Medvediev); igor.pilkevich@meta.ua (I. Pilkevych)
ORCID: 0000-0003-4010-0308 (N. Lobanchykova); 0000-0001-6825-4697 (T. Vakaliuk); 0000-0001-5659-4774 (V. Osadchyi); 0000-0002-3884-1118 (M. Medvediev); 0000-0001-5064-3272 (I. Pilkevych)

transforming into digital societies and have a particular potential for this. Holding democratic, independent, and impartial elections will allow the citizens of the countries to choose their leaders and will increase the credibility of the country's government.

The introduction of a digital voting system and electoral blockchain technology will increase the transparency and quality of vote counting, minimize the cost of elections, reduce voting offenses, and make the voting process more comfortable for people. These technologies support the paradigms of democracy. However, all technologies have some drawbacks and implementation difficulties, including the organization of digital elections using blockchain technology.

Some experts believe that paper voting is the only correct solution to ensure that every vote is counted, but the complexity of the organization process, the involvement of a large number of people, the truthfulness, and the duration of the count leaves much to be desired. Reduce trust and undermine the integrity and irregularities in the organization, vandalism at polling stations, fictitious voting, and monitoring problems. Recently, the trust in paper elections among the population is still declining, and losing the basic principles of democratic elections.

There are attempts to conduct Internet voting by several countries, including Estonia, Switzerland, the USA, Australia, Brazil, Belgium, the Netherlands, and other countries There are attempts to conduct Internet voting by several countries, including Estonia, Switzerland, the USA, Australia, Brazil, Belgium, the Netherlands, and other countries [1–5].

When organizing digital voting, ensuring cybersecurity is critical to avoid influence on the election process and internal and external manipulations.

Therefore, the purpose of this publication is:

- Analysis of known models and solutions for the use of digital voting systems using blockchain technology.
- The study of digital voting vulnerabilities.
- Identifying the shortcomings of blockchain technology to find ways to minimize them.

This article will be devoted to the study of cyber defense approaches in organizing digital voting.

2. Theoretical Background

Let's analyze the experience of implementing and using digital voting in some countries to form the requirements and prerequisites for implementing digital voting technologies in Ukraine.

So, thanks to the long and successful work on digitalization in Estonia [**Error! Reference source not found.**], in particular, the provision of digital identity cards to citizens in the form of a smart card (ID-card), which contains data for personal authorization, including cryptographic keys and certificates signing key; development of some normative legal documents; introduction of e-governance; citizens of the country can participate in early Internet voting since 2005. This technology reached its peak of popularity in 2019 when 43.8% of voters voted via the Internet [**Error! Reference source not found.**, 3]. Citizens have the right to participate in early voting directly at the polling station. The system will take into account the most recent identification of the person. In 2014, a vote verification mechanism was developed, through which voters could verify an individual cast and enrolled vote through a mobile application. However, the proposed Internet voting system acts as a partial digitalization in the electoral process and has faced some cyber defense issues. So, in 2017, a critical hardware vulnerability was discovered, which potentially made it possible to generate a private key with an ID-card public key. This problem was solved by updating the ID card certificates, but this should be taken into account when creating and using the e-voting system in Ukraine. In 2019, electoral blockchain technology was used in countries during voting.

Another example of the successful use of Internet voting is Switzerland, which began testing this technology in 2002 as a pilot project among students, and in 2003 three cantons, namely Zurich, Geneva, and Neuchâtelet, conducted Internet voting in a test mode for willing voters. In 2018, digital voting was piloted using blockchain technology, and in 2019, digital voting was used in 14 out of 26 Swiss cantons and took place 229 times [**Error! Reference source not found.**].

Also, the country practitioner is the Netherlands, which has been using digital voting technologies since the 90s of the last century. Currently, 448 out of 458 communes in the country vote using software systems for digital voting [**Error! Reference source not found.**].

The US experience in this process should also be noted. So, since 2015, digital voting technologies have been introduced in the United States using blockchain technologies on a platform with a Web 3.0 application. In the United States, optical scanning systems are widely used, which are used to process paper media and electronic voting systems, where voting takes place using special machines. Optical scanning systems require the correct mark on the ballots, which is then recognized by the system. The touch screens of an electronic machine work similarly to tablets or smartphones. Touch screens can be supplemented with physical buttons [5]. It is noted that Internet voting systems are characterized by such attacks as denial-of-service attacks, malware vulnerability, and substitution of the original software [6–8].

There are many other examples of the use and conduct of electoral processes using modern information technologies, but the most promising in this direction is the use of blockchain technology. Internet voting, conducted in some countries, was an alternative to using paper ballots.

The relevance of the issue of introducing and improving digital voting technology is emphasized by some studies by scientists. In particular, the authors Kvitka Sergiy and Gusarevych Nataliia [**Error! Reference source not found.**] analyzed the use of electoral blockchain technology in the digital voting system. The authors note that in today’s conditions, the most effective technology for implementing Internet voting is the electoral blockchain, which provides for the creation of “digital wallets of candidates”, and the voting process itself is reduced to sending a “coin” from any part of the world by a voter to the wallet of an elected candidate. The authors note that this will minimize electoral fraud and increase voter confidence. Kvitka Sergiy and Gusarevych Nataliia note the following positive aspects of using digital voting systems [**Error! Reference source not found.**]:

- Availability of voting regardless of location.
- Reducing the cost of organizing and holding elections by automating the processes of counting votes.
- Reduction of bureaucratization.
- Lack of possibility of external influence on voters.
- Reducing the time for counting votes and obtaining voting results.
- Ensuring maximum transparency of all stages of the electoral process.
- Reduction in the proportion of absentees.

Among the problems are:

- The hypothetical possibility of failure of equipment and software products, which will lead to false voting results.
- Violation of the confidentiality of the personal data of voters and their use for malicious purposes.
- Ensuring the secrecy of voting due to the need for authorization of voters in the system.
- The anonymity of the cast votes in the database on the server.
- The probability of repeated voting by the voter.
- The procedure for authenticating voters when registering via the Internet.

A rather interesting construction methodology was proposed in [3]. A group of authors proposes the use of blockchain technology to ensure the anonymity of voters by storing only a hash in the blockchain instead of information about voters. Fairness is ensured by the fact that the casting vote is stored in encrypted form until the end of the voting, which makes it impossible to receive any voting results before the end of the voting process. In the proposed methodology, it is proposed to implement the verification of the casting vote on the side of the voter. The use of smart contracts allows the implementation of the digital voting process and increases the level of the truthfulness of the election results, transparency through the publication of the results of the vote count and protection against fraud, and security through voter verification tools. An analysis of system performance was carried out based on security indicators and the cost of fees for transactions.

In [9], it is proposed to create a methodology for building a decentralized electronic voting system. It combines the following blockchain technologies: Dependency NPM (Node Package Manager); Truffle framework; Ganache; Metamask wallet; coding language; solidity, HTML, JavaScript, CSS. This system is decentralized with a fairly easy-to-use voting mechanism that provides an adequate level of security for identifying elections and transmitting and verifying data. The disadvantage of this methodology is not ensuring the anonymity of voters.

Other scientists [10] proposed an electronic voting system for using blockchain technology based on Ethereum smart contracts, and Metamask electronic wallet to connect to the blockchain network. It is proposed to create a code in the form of smart contracts that will be executed on the “nodes” of the blockchain network. The use of POW (Proof-of-Work) consensus is proposed. The authors propose the use of a method to prevent multiple entries of the same voter. The essence of the method is that after voting, his data is deleted from the database of voters, instead of creating another database. When they log in again, the user is notified that the authentication failed. With this approach, it is necessary to ensure the correctness of the voting procedure and take into account possible “failures” in the network. The main thing here is for the voter to complete the voting procedure, check whether his vote has been added, and only after that delete it.

The methodology for building an electronic voting system, presented in [11], uses blockchain technology as a service to create a distributed voting system. It includes two types of nodes, namely district (district) and boot. The problems with the proposed technology are the inability to provide an adequate level of voter confidentiality and the lack of automated vote-counting procedures.

The proposed technology for building an electronic voting system in [12] is based on the use of blockchain technology for machines used for voting. The chairman checks the unique identification and biometric data of the voter. After a successful authentication procedure, the voter votes. The next step is to create a hash using SHA-256 and send it to the chairperson. This approach improves the e-voting algorithm but requires increased security, privacy, and transparency.

A large number of works in this direction indicates the relevance of this problem and the prospects for research to find optimal technologies, methodology, and tools for building digital voting systems.

3. Results

In organizing elections, it is very important to observe democracy, honesty, and transparency. The main prerequisites for the introduction of electronic voting:

- Digitization of the society of the state.
- The developed structure of the Internet.
- Availability of mobile networks throughout the state.
- ICT literacy of society.
- A regulatory framework has been introduced.
- Solidarity and readiness for the electronic (digital) voting format of all political parties of the country.
- The financial viability of the state.

A special place in the organization of digital voting is occupied by the issue of cybersecurity. The analysis and the results of the research [2, 13–15] made it possible to formulate the requirements for the digital voting security system:

- Transparency of all stages of the electoral process with the ability to check your vote and take it into account for the elected candidate with complete confidentiality of information about the voter.
- The anonymity of voters during the voting procedure and vote counting.
- User authentication when registering and receiving voting keys.
- Data integrity during the voting process and after the end of the procedure, the impossibility of changing, or replacing the voting results.
- Security at all stages of the voting.
- Mobility.
- Fairness and the ability to verify the results of the voting to obtain an honest result that would be trusted.
- Is the optimal cost of the system?

The introduction of a digital voting system will allow voting anywhere in the world with the proper level of cybersecurity. In general, the following main components of digital voting can be seen:

- Voter registration.
- Voting procedure.
- Counting votes.

To ensure proper security, and increase confidence and transparency of elections, it is proposed to use a combination of methods and technologies, namely:

- Ethereum blockchain technology uses some smart contracts to ensure the procedure for registering voters, conducting the voting procedure, and counting votes.

- Cryptographic hashing methods to ensure the anonymity and confidentiality of information.

The methodology presented in [3, Fig. 1], needs to be adapted for use on the territory of Ukraine. The first component of the electoral process is the formation of voter lists, which are constantly criticized. From the side of cybersecurity, the possibility of an insider attack infecting the system is taken into account, which can lead to incorrect operation of the system and cast doubt on the voter lists. To form a register, voters need to register.

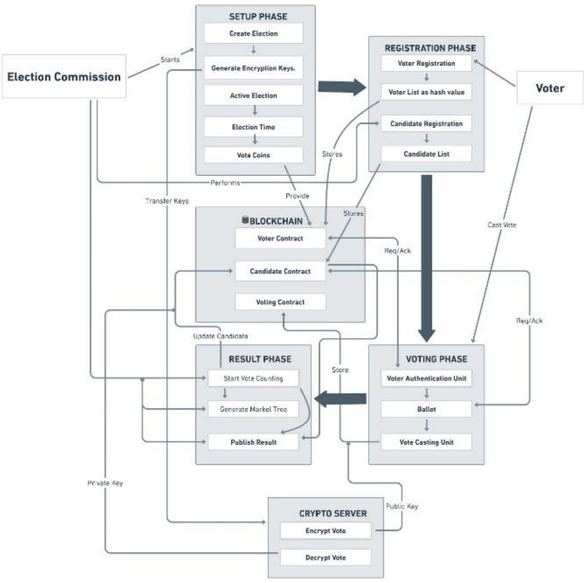

Figure 1: An example of the implementation of digital voting using smart contracts [3]

Modern electronic methods of personal identification introduced in Ukraine, the possibility of obtaining an electronic digital signature, the possibility of verification through a special service on the website of the State Register of Voters, and their presence in the electoral lists created a certain basis for the introduction of a digital voting system. However, the introduction of the “Diia” (State and Me) application, which is a mobile application, web portal, and brand of the digital state in Ukraine developed by the Ministry of Digital Transformation of Ukraine, makes digital voting possible.

“Diia” allows you to sign documents using an electronic digital signature, which can be obtained from an accredited key center. The application allows you to save internal and international passports, driver’s licenses, individual tax numbers, and other documents. All these documents can be used in everyday life, as well as when receiving banking services. Registration in the application is available using BankID, Mobile ID, or SmartID. 72 services are already available on the portal, and in the application, there are 9 services and 15 digital documents [16].

The use of the app/portal “Diia” requires the creation of appropriate software. Writing an additional module “voter registration” allowed citizens to register. To confirm your data and carry out authentication, you can use the verified documents uploaded to the application and fill in the fields required for registration, formed by the regulatory framework. Voters confirm the registration data by applying a digital signature. All data is recorded in the appropriate register. Registration data is provided by a certain smart contract that works on blockchain technology. At this stage, it is important to prevent fraud with documents for the formation of the list of voters. Responsibility for the formation of the list of voters is assigned in Ukraine to the Central Election Commission (CEC). Considering that digital elections will be an alternative to paper ones, especially in the early years, this would form a real voter base. So, for example, it is necessary to organize help points for registering citizens for elections, conduct training, record videos, etc. That is, it is necessary to form a new and up-to-date base of voters, which would not allow the abuse of register data and create the basis for the implementation of fair and transparent elections. With the combined use of voting technologies, it is necessary to create labels for those voters who decide to vote online. This will minimize the cost of producing the number of ballots and speed up the counting process. When registering voters, it is necessary to avoid repetition, and the possibility of gaining access to the register to change, forge, and gain unauthorized access. In addition, a significant role in simplifying this procedure will be played by a digital electronic signature, which is proposed to be used primarily to verify the voter. However, to date, the use of single-factor authentication is ineffective and will greatly weaken this system. This can be done by due diligence before adding data to the registry and confirmation of the information from several trusted sources. The use of smart contracts for voter registration and direct interaction with blockchain technology makes their use quite attractive while minimizing the influence of third parties.

After successful registration, the voter’s incoming data is hashed to ensure anonymity, and each voter receives a public and private key for voting in the app/portal “Diia”. To create keys and verify them, you should create a special cryptographic server and provide an appropriate level of cyber protection. After confirming the receipt of the keys, the hash value and the public key are added to the blockchain. After that, a message is sent to the voter about the successful registration procedure.

The concept of the candidate registration procedure, the creation and conduct of elections, the stages of voting, and the calculation of results and their publication are presented in [3]. As can be seen from Figure 1, the proposed methodology has three smart contracts, namely: a voter smart contract, a candidate smart contract, and a voting smart contract. The proposed methodology is based on the use of a secure Metamask e-wallet. As an alternative for Ukrainian society, it is possible to use the app/portal “Diia”. Creating a wallet within the specified application will allow the receipt of a “coin” for voting.

The advantage of this approach is to ensure anonymity since the identification of voters is not possible due to the use of hashing. During the voting process, the public key is used to identify the voter and recalculate the coin. The transaction (recalculation of the coin) is confirmed by the private key. Blockchain technologies make it possible to ensure the anonymity and integrity of data. No particular vote can be traced back to the voter, as the voter’s information is recorded on the blockchain as a hash, which is the unique identification of the voter and is the public key, and the hash value represents the voter’s choice. Integrity is ensured by the formation of the fundamental concept of the Merkle tree. The beginning at the end of voting is regulated by legal documents and is quite simply implemented programmatically. During the voting period, the vote-counting procedure is not carried out, which makes it impossible to coerce voters and increases the fairness of the electoral process. To ensure integrity, all votes are encrypted from the moment of voting until the end of the election. The voting phase is separate from the counting phase, which is again positive for fairness.

It is important to note that there are many different schemes and models of electronic elections using blockchain technology, and each of them can have its characteristics and advantages.

Cyberattacks on the blockchain can come in many types and forms, but the following deserve our attention:

51% Attack. This attack is aimed at the blockchain network, in which hackers are trying to seize (get) control over the majority of the network’s computing nodes. The goal of the attack is to control the process of creating new blocks and double costs.

Counteracting this attack is quite difficult. The main recommendation is to monitor the network. When using a private blockchain, which can be the case when organizing elections, it is important to check the nodes of the network and make sure that they are in trusted places. The choice of consensus protocol should respond to these kinds of attacks. For example, the Proof of Work has been updated.

Sybil attack. This attack is characterized by the creation by a hacker (a group of hackers) of a large number of nodes in the network to obtain their own “votes”. The more nodes, the greater the chance to gain control of the majority of the network’s votes and send false transactions, form blocks and add them to the blockchain chain sequence. This type of attack can be counteracted by monitoring the network and choosing the right consensus algorithm.

DDoS attack. Using a large number of computers to block the blockchain network. Thanks to the available technology, the hacker creates a lot of requests sent to the server and tries to overload it, thereby blocking the network. The kinds and types of these attacks are different. The decentralization aspect creates protection against this type of attack. Even if several nodes are attacked and cannot communicate or simply go offline, the blockchain can continue to work and verify transactions. Once the nodes are up and running, they can get back to work. To do this, it is necessary to re-synchronize the latest data that was picked up by the provided nodes that were violated. It is necessary to monitor the network and disable these nodes from block formation and transaction processing. Recognize them as erroneous and those that cannot be trusted so that requests from this node are not processed. The degree of protection of each blockchain from these attacks is related to the number of nodes and the network hash rate. The use of certain types of consensus can also protect nodes from such attacks, in particular the use of Proof of Work.

Smart Contract Exploits (Vulnerabilities of smart contracts). With the advent of this technology, accordingly, new cyberattacks have appeared. Considering that, in essence, a smart contract is a software product with source code running on a blockchain network, it may have vulnerabilities that hackers can exploit. Using vulnerabilities in smart contracts, an attacker can change access rights, “arrange” the verification of incoming data at an improper level and perform unwanted actions on the network. Therefore, the main recommendation is to check the code for vulnerabilities, use a hash to sign the original code, and test the code.

Phishing attacks. This type of attack is aimed at breaking access to an electronic wallet (wallet). To counter this type of attack, you must follow the recommendations for storing the private key. Raise digital literacy in society. To conduct explanatory work on cybersecurity and its main provisions.

Cybercriminals are actively monitoring blockchain vulnerabilities. Particular attention is focused on cryptocurrencies. As a result of the attack, attackers try to profit financially from their actions. When conducting elections, the expected desire of third parties to influence, violate the confidentiality, integrity, and availability of information. Therefore, when implementing a digital voting system, it is necessary to focus on the development of a system to counter attacks. This issue needs a detailed analysis and study, depending on the specific practical implementation of the digital voting system.

4. Discussions

Accordingly, the proposed solutions are analytical and conceptual and require the development of a mathematical and algorithmic apparatus and a detailed analysis of the possibilities of physical implementation within Ukraine and Ukrainian legislation.

The following questions require research:

- Protection of electronic registers of the population.
- Resistance to coercion.
- Counting of votes.
- Resistance to protest actions of voters.

Depending on the specific chosen technologies and schemes for the practical implementation of the study, protection against cyberattacks is required.

5. Conclusions

Within the framework of this study, an analysis was made of known solutions for organizing digital voting and the possibility of its implementation in Ukraine by combining digitalization technologies of Ukrainian society and blockchain technologies.

Based on the analysis, the main prerequisites for the introduction of electronic voting are determined and the requirements for the security system of digital voting are formed, and the main components of digital voting are determined.

To ensure proper security, and increase the level of trust and transparency of elections, it is proposed to use a combination of methods and technologies, namely: Ethereum blockchain technology using some smart contracts to ensure the voter registration procedure, the voting procedure, and vote counting; cryptographic hashing methods to ensure the anonymity and confidentiality of information

An assessment was made of the use of the application/portal “Diia” for organizing digital elections on the territory of Ukraine.

The concept of building a digital voting system in Ukraine is presented, and technologies, approaches, and algorithms for each stage of voting and the principles of implementation in today’s conditions for Ukraine are described.

The analysis is carried out and the main types of cyberattacks that can take place during the organization of digital voting are identified. Recommendations for their counteraction are offered.

6. References

[1] S. Kvitka, N. Gusarevych, Application of Electoral Blockchain Technology in the Digital Voting System, Pub. Adm. Asps. 10(2) (2022) 23–30. doi: 10.15421/152209

[2] A. Ibrahim, F. Gebali, Compact Modular Multiplier Design for Strong Security Capabilities in Resource-Limited Telehealth Iot Devices, J. King Saud Univ. Comput. Inf. Sci. 34(9) (2022) 6847–6854. doi: 10.1016/j.jksuci.2022.06.009

[3] S. Alvi, et al., DVTChain: A Blockchain-Based Decentralized Mechanism to Ensure the Security of Digital Voting System Voting System, J. King Saud Univ. Comput. Inf. Sci. 34(9) (2022) 6855–6871. doi: 10.1016/j.jksuci.2022.06.014

[4] O. Tokar-Ostapenko, Electronic Voting: Prospects for Implementation in Ukraine, 2021. URL: https://niss.gov.ua/sites/default/files/2021-02/tokar-1.pdf

[5] Britannica. Electronic Voting, 2022. URL: http://www.britannica.com/EBchecked/top

ic/1472946/electronicvoting/278912 /E-voting?anchor=ref1006102

[6] V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.

[7] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[8] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[9] S. Khan, et al. Implementation of Decentralized Blockchain E-Voting, EAI Endorsed Transactions On Smart Cities, 4(10) (2020). doi: 10.4108/eai.13-7-2018.164859

[10] R. Singh, R. Chaudhary, A. Tripathi, Electronic Voting System Using Blockchain, Int. J. Sci. Res. Eng. Manag. (IJSREM), 2021.

[11] F. Hjálmarsson, et al., Blockchain-Based E-Voting System, 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, 983–986. doi: 10.1109/cloud.2018.00151

[12] B. Shahzad, J. Crowcroft, Trustworthy Electronic Voting Using Adjusted Blockchain Technology, IEEE Access, 7 (2019) 24477–24488. doi:10.1109/ACCESS.2019.2895670

[13] P. Baudier, et al., Peace Engineering: The Contribution of Blockchain Systems to the E-Voting Process, Technol. Forecast. Soc Change, 162 (2021) 120397. doi: 10.1016/j.techfore.2020.120397

[14] H. Pranith, et al., End-to-End Verifiable Electronic Voting System Using Delegated Proof of Stake On Blockchain, SSRN Electronic J. 1 (2019) doi: 10.2139/ssrn.3511409

[15] C. Onur, A. Yurdakul, ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol, arXiv, 2022. doi: 10.48550/arxiv.2204.00057

[16] Government Services Online. URL: https://diia.gov.ua/