Possibilities of Implementing E-Voting System in Ukraine

KATERYNA O. PAVSHUK, BOHDAN S. MOKHONCHUK, PAVLO V. ROMANIUK, OLEKSII O. LIUBCHENKO AND ALINA O. MURTISHCHEVA

sciendo

Politics in Central Europe (ISSN 1801-3422)
Vol. 21, No. 2
DOI: 10.2478/pce-2025-0009

Abstract: There are constant risks and threats to fair elections against the background of the current crisis of democratic civic engagement and the global pursuit of convenience in the digital age. The political and institutional context in Ukraine, including wartime displacement, occupation of territories and a large diaspora abroad, requires innovative digital tools to ensure that all eligible voters can participate in elections. Therefore, the article aims to analyse the adherence to the principles of secret ballot and personal voting through alternative voting methods, such as e-voting. A four-level e-voting system is identified, having the legal, organisational, procedural and technological components. Moreover, the modern ways of securing, guaranteeing and ensuring the principles of secret ballot and personal voting in e-voting at these levels in Ukraine and abroad are clarified. To this end, the authors analyse legal approaches and electoral practice of foreign countries to determine how the substantive law is implemented in electoral procedures. It is established that the main problem of their unacceptability is the weak protection of confidentiality and the high probability of unauthorised interference with the voting procedure. However, it is possible to prevent such violations through a decentralised blockchain-based e-voting system. The article discusses the main advantages and disadvantages of using various platforms for e-voting, in particular Ethereum and the Hyperledger Fabric platform. Furthermore, the law of Ukraine is analysed concerning the possibility of using digital technologies in testing e-voting in elections and referendums.

Keywords: ***electoral principles, secret ballot, personal voting, electronic electoral process, Ethereum platform, Hyperledger Fabric platform***

Introduction

In 2021, a petition was submitted to the president of Ukraine to create a voting mechanism based on blockchain technology (Electronic Petitions 2021). This petition proposed the possibility of introducing such a mechanism into the electoral system and providing the citizens of Ukraine with unique identification keys. Accordingly, such a system would make it impossible to fake, toss votes or use the voices of 'dead souls'. Apart from that, the author of the petition emphasised the possibility of using this system not only for the needs of the national vote, but also in certain regions and cities in order to resolve issues of local importance. However, this petition was not supported, gaining only 515 votes out of the 25,000 necessary. This indicates not only the citizens' lack of awareness about the opportunities offered by modern technologies, but also a certain distrust of electronic facilities that can simplify traditional methods and approaches to organising state processes.

In this regard, even in the most developed democracies of the world, where legitimate power institutions are trusted, the first concern is confidentiality. It is not only about citizens' daily activities, but also about exercising the right to vote. Given that electoral procedures include several levels (legal, organisational, procedural, technological), the starting point in their implementation is the legal level. It provides for compliance with the principles of electoral law, ensuring confidence in elections as a democratic instrument of a legitimate transfer of power. It includes international and national standards for voting (Spanos & Kantzavelou 2024).

While the traditional method of voting has a well-established universal set of principles, the e-voting alternative provokes discussion and concerns on the part of traditionalists. Thus, Kliuchkovskyi (2018) considers the role and problems of ensuring the principles of secret ballot and personal voting within electoral law to guarantee free elections. He claims that alternative voting methods weaken the guarantees of secret balloting in favour of the right to vote.

The use of blockchain for voting has attracted significant attention from foreign researchers because it increases the openness, safety and honesty of remote voting. Thus, Hajian Berenjestanaki et al. (2024) conducted a study of the advantages, challenges and impact of such systems. Moreover, they identified future areas of research. Furthermore, Horbenko et al. (2020) analysed the technical aspect of blockchain technology usage for voting. They identified a four-level system for organising and conducting e-voting. The scholars suggested, investigated and tested the two-level architecture (lower and upper levels) of the electronic blockchain voting system by physical prototyping. It was based on the research carried out by scientists from the United States, aiming to ensure protection from external interference of third-party users while operating the system (Pass, Seeman & Shelat 2017).

Moreover, Johnson (2019) argued that the potential for blockchain technologies to uphold the legitimacy of the US and EU constitutional orders is based on their accessibility, transparency, decentralisation and security. In particular, e-voting based on blockchain technology could serve as a platform for civic engagement, public debate and democratic competition, thereby reinforcing the legitimacy of the constitutional orders in question. In connection to this, Tokar-Ostapenko (2022) explored the legal and technical aspects of the Ukrainian version of e-voting.

Given the identification of a four-level system of e-voting, the purpose of this article is to establish ways to guarantee and ensure the implementation of the principles of secret ballot and personal voting in remote e-voting from the regulatory and technological perspectives in Ukraine and foreign countries. In accordance with the purpose, a scope of research objectives is set as follows:

- to define the architecture of blockchain voting,
- to determine whether such a system is able to protect the anonymity of e-voting,
- to analyse the prospects and threats posed by blockchain in order to comply with fundamental democratic principles related to the realisation of the right to vote and public involvement in decision-making.

Methodological framework

The first part of the study is focused on examining the electoral principles of secret ballot and personal voting. Therefore, the history of alternative voting methods is analysed. The legal and technical sides of electronic technologies application during elections is considered. Moreover, the development of the electoral law of Ukraine is analysed regarding the likelihood of using electronic technologies to prevent violations of these principles and international standards of democratic voting. In this regard, the norms enshrined in the Electoral Code of Ukraine (Verkhovna Rada of Ukraine 2020), Law of Ukraine No. 1135-IX 'On the all-Ukrainian referendum' (Verkhovna Rada of Ukraine 2023), and other legal documents regulating e-voting are considered.

The normative legal analysis involves the study of the Committee of Ministers of the Council of Europe and the Venice Commission's recommendations on the legal, functional and technical norms of e-voting, their conclusions on overcoming challenges of e-voting, compliance with international electoral principles and ensuring security when using digital technologies (Council of Europe 2005; European Parliament and the Council 2016; European Parliament and the Council 2019; Venice Commission 2004, 2018). In this context, one of the problems is to guarantee the reliability and safety of the digital means of voting. Therefore, it is important to consider the relationship among the functional, legal and technical characteristics of e-voting. To avoid massive falsifications of

voting results, a study of the lower and upper levels of the blockchain e-voting system is conducted.

In the second phase of the research, taking into account the legal, organisational, procedural and technological levels of e-voting, the ways of fixing, guaranteeing and ensuring the principles of secret ballot and personal voting in e-voting in Ukraine and foreign countries are clarified. To study the problems of using electronic technologies at all levels of the electoral process, the analysis of a decentralised blockchain-based voting system is carried out. In addition, an e-voting system on the Ethereum platform is considered. Apart from that, the analysis method was applied to specify the principles and algorithms by which the system solves the legal problem of protecting privacy using the Hyperledger Fabric platform. Moreover, the comparative method facilitates establishing the difference between these platforms, as well as their advantages and shortcomings regarding their implementation in e-voting.

A doctrinal legal analysis is applied to determine the legal and technical aspects of implementing the right to vote electronically, ensuring a blockchain-based personal and secret ballot system. Apart from that, the functional legal analysis is applied to prototype the main components of the two-level architecture of blockchain voting. Given the possibility of using automated information and telecommunication systems by the Central Election Commission of Ukraine (hereinafter – CEC), the procedure for administering the referendums and elections is difficult due to the insufficient regulation of its use. Thus, the regulatory impact analysis is employed to define problems and prospects for applying blockchain in referendums and elections in Ukraine. These methods allow for the further application of electronic technologies in the electoral process in Ukraine.

Results and discussion

Normative regulation of e-voting in the EU

There are hundreds of interpretations of democracy. Therefore, the processes of democratisation vary across different national contexts. There is no singular, universal approach to reforming former totalitarian systems that aim to establish genuine democratic institutions grounded in the rule of law (Barabash &berchenko 2019). The development of democracy as well as the standards of its observance are believed to be influenced by information and technical progress.

In this regard, alternative ways of voting, in particular postal vote, e-voting using special voting devices or remote voting through an application, are actually a victory of convenience over security. However, it is impossible to recognise the results of such a vote if the regulatory component does not provide a system

of guarantees, including technical ones, to prevent violations of generally recognised electoral principles. Otherwise, there can be no talk of any democracy (De Farias et al. 2024). Mechanical voting devices were introduced in the 19th century. Computers were introduced in the 1960s, while Direct Recording Electronic (DRE) systems were created in the 1990s and internet voting appeared after 2000 (Maurer 2020). Accordingly, Maurer (2020) notes that normative regulation of internet voting has evolved rapidly.

Thus, in Austria, it was recognised that the regulation of internet voting violated the constitution because it was not sufficiently detailed to allow members of election commissions to carry out their tasks without technical assistance. Since such regulation was not and could not be updated to meet the constitutional requirements, the implementation of online voting in Austria cannot yet be foreseen. In Switzerland, the analysis of the long experimental phase and the first-generation regulatory framework introduced in 2002 provoked an important update of the legal framework regulating e-voting in 2013. Thus, the second-generation regulation introduced new provisions that reflected a better understanding of digital technologies, namely: risk policies, verification requirements, broad control by independent and expert bodies, strict data protection, transparency requirements, etc. (Razali et al. 2024).

The recommendations of the Council of Europe on electronic voting (2005) were developed according to a similar scenario. Recent experiences in applying new regulatory provisions on e-voting in Switzerland and Estonia show the need for their further improvement in order to resolve the issue of verification or transparency. Such dynamics are interesting in the context of searching for other digital solutions. Accordingly, the EU adopted several normative documents that are related to cybersecurity and the protection of personal data in the electoral process such as Convention 108 + (Council of Europe 2018) and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (European Parliament and the Council 2016a). Paragraph 30 of Regulation (EU) 2016/679 determines that it is possible for natural persons to be associated with online identifiers provided by a variety of devices, applications, tools and protocols. These identifiers may include, but are not limited to, internet protocol addresses, cookie identifiers and other identifiers such as radio frequency identification tags. Such data may result in the retention of digital footprints that can be used to create profiles and identify individuals when analysed with other data, such as unique identifiers and information obtained by servers (European Parliament and the Council 2016a). This stipulation may be employed to establish profiles of individual entities and ascertain their identity when coupled with distinctive identifiers and supplementary information procured from remote servers.

Furthermore, the European Parliament approved Directive (EU) 2016/1148 (European Parliament and the Council 2016b) in July 2016. In 2019, Regula-

tion (EU) 2019/881 (Cybersecurity Act) (European Parliament and the Council 2019) was adopted. Paragraphs 3 and 4 of this Cybersecurity Act prescribe taking all the required actions to improve cybersecurity in the EU to provide better protection against cyber threats to systems, digital products, communication networks, services and resources used by the general public, organisations and enterprises, i.e. small and medium-sized enterprises (SMEs). In addition, the European Agency for Network and Information Security (ENISA) was created by Regulation of the European Parliament and the Council (EU) No. 526/2013 (European Parliament and the Council 2019). Consequently, enhancing cybersecurity in the EU for SMEs and startups should involve providing the public with the access to relevant information.

Legal framework of e-voting in Ukraine

According to the degree of automation, e-voting systems can be divided into three types:

1. systems that use electronic devices to read marks from paper ballots and count votes,
2. systems that use voting machines with electronic displays and buttons (or touch-sensitive displays) instead of paper ballots, while the voting results are stored in the memory of the voting machine,
3. systems that implement remote voting via the Internet using cryptographic protocols (Horbenko et al. 2020).

The first and second types for e-voting are indicated in Article 18 of the Electoral Code of Ukraine (Verkhovna Rada of Ukraine 2020) as a pilot project for using innovative technologies in the electoral process that may relate to voting at a polling station using technical means and software (machine voting). They can also be used to count votes by means of technical means for electronic vote counting. Moreover, they can be applied to prepare protocols on vote counting and voting results using an information and analytical system. However, the legislator warns that the conduct of these experiments should not create a false impression among voters about replacing the election procedures provided for by the Code with the procedures of the experiment or the pilot project. All other norms of the Electoral Code of Ukraine (Verkhovna Rada of Ukraine 2020) are related to the traditional method of voting and do not provide any legal basis for ensuring the principles of electoral law during e-voting.

In contrast, the Law of Ukraine No. 1135-IX 'On the all-Ukrainian referendum' (Verkhovna Rada of Ukraine 2023) enshrines the possibility of exercising the right to vote electronically. In particular, Article 13 of this law determines that at a particular all-Ukrainian referendum each voter can exercise the right to vote only once and only at one polling station by submitting a ballot paper or

by e-voting. The law states that in order to prepare e-voting and count votes at the all-Ukrainian referendum, a special e-voting station is created on a temporary basis (Part 2 of Article 38). The law also establishes that a voter can apply for one's inclusion in the voter list of a special e-voting station to the body of the State Register of Voters five days prior to the date of the election. Such an application can be submitted by the voter personally in paper form or in electronic form by means of an automated information and telecommunication system. The application in electronic form is created using a qualified electronic signature (Article 57) (Verkhovna Rada of Ukraine 2023). Thus, it is possible to claim that the procedure for holding the all-Ukrainian referendum includes the possibility of e-voting. However, it is only outlined in general terms and does not specify the technical aspect of its implementation, the principles of cybersecurity, secret ballot or personal voting.

An initial regulatory framework was created in Ukraine for further development of the legal framework of the e-voting procedure. Accordingly, the Law of Ukraine No. 2155-VIII 'On electronic identification and electronic trust services' (Verkhovna Rada of Ukraine 2017a) enshrines the possibility of introducing modern electronic methods of identification in Ukraine, including Mobile ID. Moreover, the Law of Ukraine No. 2163-VIII 'On the basic principles of ensuring cybersecurity of Ukraine' (Verkhovna Rada of Ukraine 2017b) delineates the primary objectives, strategic orientations and fundamental tenets that inform the government's approach to cybersecurity. It also defines the authorities and responsibilities of state institutions in this area. Apart from that, the Law of Ukraine No. 698-V 'On the state register of voters' (Verkhovna Rada of Ukraine 2007) specifies that the State Register of Voters is maintained in electronic form, while the application for inclusion of a person having the right to vote into the Register may be sent by him/her to the body of the Register in electronic form with a digital signature.

In addition, the Ministry of Digital Transformation of Ukraine has been operating since 2019, which developed the Diia mobile application. This application provides access to administrative services, allows tax payments, and displays digital documents. Apart from that, it is used to conduct nationwide polls. However, in 2024, Diia crashed due to overload during voting in the finals of the national selection for Eurovision, which demonstrated the technical inability to process a significant number of requests simultaneously. This experience shows another advantage of decentralised blockchain technology, which has a large bandwidth for processing user requests (Tokar-Ostapenko 2022).

Although such modern technologies increase the efficiency of voting, they involve offline voting, i.e. with voters visiting the polling station. On the contrary, remote e-voting provides an opportunity to vote without visiting a polling station. While highlighting the pros and cons of remote voting using electronic technologies, it is important to emphasise the need to combat cybersecurity threats, prevent cyber-attacks and maintain voter anonymity (Balicki & Preisner 2007).

Challenges and threats posed by e-voting

In its recommendations on the subject of e-voting, the Council of Europe makes it clear that any system of this nature must adhere to the principles that underpin democratic elections and referendums. E-voting systems must meet the same reliability and security standards as those employed in democratic elections and referenda, which do not utilise electronic means (Council of Europe 2005). Such a position would seem unambiguous if not for the various existing methods of implementing the e-voting procedure, which ensures the principles of democratic elections, with secret and personal voting being the key ones. Their violations can lead to falsification of voting results.

It should be mentioned that compared to other alternative voting methods, remote voting is more difficult to implement because it is necessary to guarantee the confidentiality and integrity of data transmitted on the Internet. In the modern world, human beings are being constantly monitored, with their actions and movements recorded: telephone conversations, communication in social networks and video surveillance in public spaces. This means that the use of the latest forms of state control should be implemented, taking into account digital technologies and violations of privacy. This is also directly related to electronic procedures for organising elections and referendums.

Voting anonymity in its electronic format can be violated because while casting a vote a voter is identified. Therefore, hypothetically, it is technologically possible to fix the content of the cast vote, constituting a direct violation of the principles of secret ballot and personal voting. From a technical perspective, there is no connection between the voter as the subject of the electoral process and the content of his/her vote. It is noteworthy that in the Netherlands, public concern about compliance with the principles of secret ballot and personal voting when using e-voting caused a refusal to use e-voting devices in 2006. Up to now, Denmark and Germany have refused to introduce e-voting technologies (Kliuchkovsky 2018).

The practice of the Russian Federation is one of the most illustrative examples of the dangers of e-voting. When introducing online voting for regional elections in Moscow, numerous violations of the principles of free expression of will and transparency were recorded. Therefore, in the Russian context, digital platforms become a tool not for expanding citizen participation but rather for control and manipulation by the authorities, which undermines the legitimacy of the electoral process (Toepfl 2016). In 2019, the Russian authorities presented an e-voting system based on blockchain technology. However, on election day, significant technical failures were recorded, while independent experts identified critical vulnerabilities in the system's security. Thus, researchers from France were able to hack into the system, recreate the encryption keys and de-anonymise voters, which contradicts the secret ballot principle (Gaudry & Golovnev 2020).

Unlike Russia, where digital tools are often used as a repressive means, Ukraine demonstrates a different attitude towards e-voting, despite the fact that the Ukrainian Internet Association also warns against the precocious implementation of e-voting. Thus, it is claimed that online elections will lead to a loss of anonymity due to possible hacking. As a result, it may cause leaks of the base of citizens' votes from the system. E-voting also poses a threat of controlling voting results by third parties, leading to a complete distortion of the results and undermining the electoral system due to loss of confidence in it (UIA 2024). In this regard, it is worth recognising that the development of the Diia application, the introduction of digital signatures and BankID create the preconditions for a more secure and legitimate introduction of e-voting in Ukraine.

Exploring the problem of ensuring the implementation of the principles of secret ballot and personal voting, Kliuchkovskyi (2018) proves that the relationship between them is unlikely to exist. Thus, voting by proxy is not personal, but the requirement of secret ballot is ensured. On the contrary, although some alternative ways of voting are personal, they do not guarantee its secrecy. In this context, it can be stated that while personal voting does not ensure secrecy, maintaining a secret ballot does not guarantee that this choice was made by the specific citizen registered as voter. The vote must be secret, but the voter must be identified. In this context, the relationship between the principles of secret ballot and free elections is traceable.

The fundamental tenet of free and fair elections is built on the principles of the freedom of expression and true vote. This is accomplished through the implementation of the principles of the secret ballot, impartial and transparent electoral procedures, fair and accurate vote counting and the subsequent declaration of the elected candidates (Mokhonchuk & Romaniuk 2019). This is done through the use of asymmetric cryptography, in particular digital signature algorithms and directed encryption (Zhan et al. 2024). To ensure complete anonymity, blind signature algorithms and homomorphic encryption are used. Such encryption does not require deciphering individual votes when counting (Horbenko et al. 2020).

Furthermore, any method of remote voting in an uncontrolled state environment creates risks for bribery and violation of the secret ballot. One of the most well-known methods of electoral fraud in the post-Soviet countries involves taking an unfilled ballot outside the voting premises and transferring it to a representative of a candidate or party. The representative would then fill out the ballot and ask other voters to throw it into the voting booth and take out a blank ballot for undue benefit. Thus, according to the circular principle, control is ensured over the voting results when bribing voters. In this case, remote voting will allow dishonest voters to vote under the direct control of the person who commits bribery.

One of the possible methods of guaranteeing the secret ballot and combating voter bribery may be the approach used in the Estonian elections. In Estonia, e-voting is possible along with traditional voting. Although during the last elections to the Riigikogu (the Estonian parliament), more than half of voters voted online, i.e. 312,181 out of 610,320 ballots cast (Vahtla 2023). In the period preceding voting, the voter is required to enter the system with either an ID card or a mobile ID, after which voting may commence. The voter's identification is eliminated from the ballot prior to its submission to the National Election Commission for the purpose of vote counting. This process is implemented with the intention of ensuring anonymity for the voter. Voters in Estonia are permitted to utilise the online portal to cast as many votes as they wish in the established pre-voting period. In accordance with the system's operational parameters, each vote is automatically canceled upon the submission of a new vote. Thus, voters are afforded the opportunity to modify their choice at any point during voting (Slinko et al. 2021). Since 2021, voters may modify their vote on voting day when digital lists of voters are introduced (Wright 2021). However, resistance to controlled e-voting will depend on the effectiveness of public surveillance and mechanisms of state control. In other words, the creation of a dependable, adaptable, transparent and secure voting system that also offers a reasonable cost-to-value ratio is a pressing necessity.

Blockchain-based voting: Principles, advantages and platforms

While modern e-voting systems raise concerns related to cybersecurity and are therefore unsuitable for use in public elections, offline voting entails considerably higher costs. Accordingly, e-voting based on blockchain technology, which is decentralised in its organisation and operation, appears. By applying blockchain technology to voting, it is possible to guarantee transparency and confidentiality as voter's data and aggregated information are maintained separately.

The distributed nature of blockchain renders it more secure than existing online voting systems that rely on a central server (Ahn 2022). In this regard, Ahn (2022) analyses the problem of fraudulent voting and suggests improving the safety and integrity of e-voting through the Ethereum system. Ethereum is a cryptocurrency, but its 'smart contracts' can be used in various financial areas where protection from unauthorised interference is required. It is possible to safely conduct business with an unknown entity, as long as the terms are explicitly defined in a blockchain-based smart contract (Bloomberg 2016).

Furthermore, a team of Indian scholars (Hajian Berenjestanaki et al. 2024) carried out research on the use of blockchain technology during e-voting. They emphasised that the principal advantages of blockchain-based voting systems are their capacity to enhance security, transparency and decentralisation. In contrast, aspects such as confidentiality, verifiability, effectiveness, trustworthiness

and audit capability are not essential. Furthermore, the researchers observed a paucity of emphasis on key factors such as availability, suitability and ease of use. While recognised, a comprehensive analysis of these aspects has not been undertaken to the same extent as that of the principal advantages inherent to the suggested solutions for e-voting systems based on blockchain. Meanwhile, their solutions for blockchain-based e-voting systems are designed with a focus on enhancing safety, openness, privacy and scalability through the utilisation of blockchain technology (Hajian Berenjestanaki et al. 2024).

Jayakumari et al. (2024) put forth a novel approach to online voting, proposing the use of blockchain technology in a hybrid cloud environment. This system was designed to address the limitations of the existing voting system. It was carried out in three stages – registration, voting and vote counting. The timestamp-based authentication protocol verifies voters and candidates digitally at the registration and voting stages. The use of smart contracts prevents third parties from intervening, while transactions are protected on the blockchain network. Further, to ensure trustworthy voting results, a Practical Byzantine Fault Tolerance (PBFT) is used, which prevents the voice from being changed or tossed. The results demonstrated a notable improvement in the performance of the system in comparison to the existing one. The subsequent analysis of performance was conducted with regard to the following factors: authentication delay, voice change, response time and delay.

Ukrainian developers of the technical component of decentralised e-voting argue that the physical prototyping allows asserting thoroughness and balance of the two-level architecture. They confirm its ability to ensure the fulfillment of the fundamental norms of e-voting and the security and integrity of digital technologies (Horbenko et al. 2020). The blockchain voting architectural model may be said to enhance public confidence in the veracity of services, a factor particularly salient to government institutions. Furthermore, this approach will result in a reduction in both time and expenses. In addition, such a system would effectively prevent any possibility of corrupt actions from being committed by centralised institutions. Finally, this will result in a notable enhancement to the credibility of information storage and the quality of the services.

Hence, in Ukraine, the lower (first) level of this system facilitates ensuring the implementation of all components of the electronic identification process using existing technical means and legal measures (for example, BankID, MobileID, digital signature, etc.). This will guarantee the compatibility of the voting system, the continuity of established national information systems and technologies (such as the national electronic trust services system), and the replicability of the outcomes from physical blockchain voting prototypes. The upper (second) level is designed to cast one's vote and count votes. This should guarantee the principles of democratic elections (approved by the Venice Commission), namely: independent control over the correctness of the voter

lists compilation; the potential for voting anonymously; immutability and irrefutability of voting results; easy and transparent verification of vote counting correctness, etc. (Horbenko et al. 2020).

During the full-scale armed aggression of the Russian Federation against Ukraine, e-voting can become a key tool for ensuring a comprehensive and fair electoral process. In particular, one of the main advantages of e-voting is the millions of Ukrainian citizens abroad exercising their right to vote. According to the Ministry of Foreign Affairs of Ukraine, more than 6 million Ukrainians were internally displaced or temporarily residing abroad as of June 2023 (Ukrinform 2025). According to the UN, more than 6 million Ukrainians had temporary protection in European countries as of the end of September 2024 (Zanuda 2024). However, the number of officially registered voters in a foreign constituency is much lower as people fleeing the war and trying to adapt to new realities are the last to think about elections. Traditional mechanisms of voting at consular offices or embassies are logistically complicated, slow and cover only a small part of the electorate.

E-voting based on modern digital identification technologies (e.g. Mobile ID, Bank ID, digital signature) can provide convenient and secure access to voting for citizens abroad without the need for physical presence at polling stations. This will increase the level of participation and ensure real representation of citizens in the political process, regardless of their location. Apart from that, e-voting can be a partial solution to the problem of holding elections in the temporarily occupied territories where physically opening polling stations is impossible. Although the full implementation of such a scenario requires additional measures for verification, security and prevention of external interference, blockchain technologies can offer mechanisms to control the integrity of the results through anonymous and one-time votes stored in a decentralised environment. In this context, it is worth considering the model of distribution of functions between the main government institutions for the implementation of e-voting in Ukraine (see Table 1).

The anonymity of blockchain-based e-voting and privacy protection is ensured by the use of one-time traceable ring signatures and a stealth address using the application-level protocol. This protocol serves as the basis for the CryptoNote family of anonymous cryptocurrencies. In this regard, Li et al. (2023) argue that the ring signature only allows the verifier to check the authenticity of the ballot and cannot reveal the voter's identity, thus protecting the voter's privacy. The essential function of a one-time traceable ring signature is to provide an immutable image that can be employed to address the issue of multiple voting and to guarantee the principle of 'one person, one vote'. A stealth address methodology concurrently creates an anonymous address through the voter's public key, consequently encrypting the data and trajectory of the ballot. Only after the conclusion of the electoral process is the voter able

Table 1: Functions of the main state institutions in the implementation of e-voting in Ukraine

Government institutions	Functions
Verkhovna Rada of Ukraine	legislative consolidation of the regulatory framework for e-voting, definition of electoral procedures and guarantees
Central Election Commission of Ukraine	organisation and administration of the elections, management of technical infrastructure and verification of security systems
Ministry of Digital Transformation of Ukraine	technical implementation of digital identification components (Mobile ID, digital signatures, Diia), development of a mobile/web interface for voting
State Service for Special Communications and Information Protection of Ukraine	system security certification, audit and protection against cyber threats
National Security and Defense Council	risk management and rapid response to cybersecurity threats during elections
Civil society organisations and international observers	ensuring transparency, independent monitoring and increasing public trust in e-voting

Source: Authors

to disclose their private key for the purpose of verifying a specific candidate. Furthermore, blockchain technology provides a means of ensuring fairness and impartiality. Moreover, the blockchain provides transparency and security for the voting process, ensuring that each ballot is open and protected from forgery. In order to implement this voting system, the Hyperledger Fabric platform was employed (Li et al. 2023).

It is also possible to use the aforementioned Ethereum platform. Yet, there are differences between the Hyperledger Fabric and Ethereum platforms. Ethereum Blockchain is a fully transparent and completely decentralised network with crypto tokens, while Hyperledger Fabric is a network for dealing with regulations in a corporate environment, where data privacy, scaling, high transactional throughput and access control are required (Zfort Group 2019). Given the platform's technical characteristics and the modern need to ensure the electoral principles of secret ballot and personal voting, Hyperledger Fabric holds significant advantages for organising and conducting e-voting, as it is subject to preliminary preparation and testing. This position is supported by Stan, Barac and Rosner (2021) who regard Hyperledger Fabric as a permissive, easily customisable and integration-oriented implementation of the blockchain. In addition, this platform provides basic security aspects (for example, Sybil attack resistance) and performance measurements (for instance, block size, database performance). The difference with other platforms consists in a simple but safe architectural form that is focused on isolation and distribution of functions.

The key Council of Europe document that sets standards for e-voting is Recommendation CM/Rec(2017)5 of the Committee of Ministers to Member States on standards for e-voting. This document, approved on 14 June 2017, updated the previous Recommendation of 2004 and sets legal and technical requirements for e-voting systems. As a member of the Council of Europe, Ukraine has the opportunity to adapt its national policy in the field of e-voting in accordance with the provisions of this Recommendation. They include mandatory requirements to ensure the anonymity, integrity, transparency, verifiability, accessibility and reliability of e-voting (Martínek et al. 2024).

In this regard, when developing blockchain-based e-voting systems, it is important to ensure compliance with the criteria set out in Recommendation CM/Rec(2017)5. Although blockchain systems can implement the principles of transparency and immutability, they raise questions about privacy, technical complexity and compliance with legal criteria. In this context, the choice between public and private blockchains is particularly relevant. Public blockchains like Ethereum have an open architecture where anyone can view data and interact with the system. It increases transparency but poses serious challenges to preserving voter anonymity and personal data. In this case, it is necessary to answer a number of questions related to the legal status of voters, the management and verification of the system, and the compliance of procedures with democratic norms (Cucurull et al. 2019).

In contrast, private blockchains, such as Hyperledger Fabric, offer a more flexible model where only certain nodes are authorised to validate transactions. Choosing this approach allows for more precise customisation of the system in accordance with national legislation and international standards. However, it requires identifying institutions that will support these nodes. In such a model, it is advisable to envisage that the nodes will be supported by independent state institutions (e.g. CEC, SSSCIP), international observers and possibly civil society to guarantee independence, transparency and compliance with democratic standards (Martínek & Malý 2024). Thus, for the effective implementation of blockchain-based e-voting in Ukraine, it is necessary to take into account technical aspects and ensure full compliance with legal and democratic criteria.

Conclusions

In the light of globalisation and general trends in the crisis of civic activity, which may pose a threat to the fundamental principles of constitutionalism, the struggle against traditionalism and the transition to a technological society, reevaluating the approaches to organising, administrating and conducting elections is inevitable, as they are the most important institutions of democracy.

Ukraine today faces new challenges caused by Russian full-scale aggression. In the post-war elections, the state will not have enough time to introduce e-vot-

ing, regarding its legal, organisational, procedural and technological aspects. However, the electoral and referendum legislation of 2020–2021 established the regulatory base for the possibilities of introducing digital technologies for elections.

Given the general trend towards digitalisation, Ukrainian electoral realities must correspond to such trends. The national electoral legislation, the creation of virtual user rooms, the widespread use of the Diia application and the introduction of a digital signature indicate not only technical progress, but also a desire and willingness to make operations and transactions more convenient and less expensive for Ukrainian citizens. Therefore, it is possible to assert that in Ukraine the issue of choosing an accessible and reliable platform for e-voting will become acute in the future.

The analysis shows that ensuring secret ballot, protection from cyber-attacks of voting results with personal and one-time implementation of electoral law according to the principle 'one person – one vote' are important for many countries before the implementation of e-voting. All the alternative methods of voting have sufficient shortcomings, containing risks of violation of compliance with electoral principles.

At the same time, electoral procedures should be flexible to modern realities and achievements. Based on blockchain platforms, a decentralised, secure and confidential voting procedure can be built. The Hyperledger Fabric platform can be a reliable platform for e-voting, provided that the financial and technical capabilities of the government are taken into account.

References

Ahn, B. (2022): Implementation and Early Adoption of an Ethereum-Based Electronic Voting System for the Prevention of Fraudulent Voting. *Sustainability,* 14(5), article number 2917.

Balicki, R. & Preisner, A. (2007): E-Voting – Opportunities, Possibilities, Threats. In: Grabowska, S. & R. Grabowski (eds.): *Międzynarodowa Konferencja Naukowa nt.: Alternatywne Sposoby Głosowania a Aktywizacja Elektoratu [International Scientific Conference: Alternative Ways of Voting and Activation of the Electorate]*. Rzeszow: Uniwersytet Rzeszowski, 50–73.

Barabash, Y. & Berchenko, H. (2019): Freedom of Speech under Militant Democracy: The History of Struggle against Separatism and Communism in Ukraine. *TalTech Journal of European Studies,* 9(3) 3–24.

Bloomberg (2016): This Is Your Company on Blockchain. *Bloomberg Businessweek*, 25 August, <accessed online: https://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain>.

Council of Europe (2005): *Legal, Operational and Technical Standards for E-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum*. Strasbourg: Council of Europe Publishing.

<accessed online: https://www.eods.eu/library/CoE_Recommentaion%20on%20Legal,%20Operational%20and%20Technical%20Standards%20for%20E-voting_2004_EN.pdf>.

Council of Europe (2018): Convention 108 + Convention for the protection of individuals with regard to the processing of personal data. *European Parliament,* <accessed online: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf>.

Cucurull, J., Rodríguez-Pérez, A., Finogina, T. & Puiggalí, J. (2019): Blockchain-Based Internet Voting: Systems' Compliance with International Standards. *International Conference on Business Information Systems,* 339, 300–312.

De Farias, J. C. L. A., Carniel, A., de Melo Bezerra, J. & Hirata, C. M. (2024): Approach Based on STPA Extended with STRIDE and LINDDUN, and Blockchain to Develop a Mission-Critical E-Voting System. *Journal of Information Security and Applications,* 81, article number 103715.

Electronic Petitions (2021): Petition No. 22/125898-ep "Voting through the Diia application". *Electronic Petitions*, <accessed online: https://petition.president.gov.ua/petition/125898>.

European Parliament and the Council (2016a): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). *European Union,* <accessed online: http://data.europa.eu/eli/reg/2016/679/oj>.

European Parliament and the Council (2016b): Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. *European Union,* <accessed online: http://data.europa.eu/eli/dir/2016/1148/oj>.

European Parliament and the Council (2019): Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *European Union,* <accessed online: http://data.europa.eu/eli/reg/2019/881/oj>.

Gaudry, P. & Golovnev, A. (2020): Breaking the Encryption Scheme of the Moscow Internet Voting System. *International Conference on Financial Cryptography and Data Security,* 12059, 32–49.

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N. & Pahl, C. (2024): Blockchain-Based E-Voting Systems: A Technology Review. *Electronics,* 13(1), article number 17.

Horbenko, I. D., Onoprienko, V. V., Horbenko, Y. I., Kuznetsov, O. O., Isirova, K. V. & Rodinko, M. Y. (2020): Problems, Construction Principles and Development Prospects of the National Electronic Voting System in Ukraine. *Radio Engineering,* 1(200), 85–97.

Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A. & Jawahar, M. (2024): E-Voting System Using Cloud-Based Hybrid Blockchain Technology. *Journal of Safety Science and Resilience,* 5(1), 102–109.

Johnson, D. (2019): Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values? *European Journal of Risk Regulation,* 10(2), 330–358.

Kliuchkovskyi, Y.B. (2018): *Principles of Electoral Law: Doctrinal Understanding, Status and Prospects of Legislative Implementation in Ukraine*. Kyiv: Vaite.

Li, Y., Li, Y., Hong, T. & Chen, Z. (2023): Design and Implementation of Blockchain-based Anonymous Electronic Voting System. In: *2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*. Beijing: BMSB, 1–6.

Martínek, T. & Malý, M. (2024): Evaluation of the I-Voting System for Remote Primary Elections of the Czech Pirate Party. *Acta Informatica Pragensia,* 13(3), 395–417.

Martínek, T., Pelikán, M., Tyrychtr, J. & Konopásek, J. (2024): Implementation of a Secret and Verifiable Personal Remote Electronic Election of an Agrarian Organization per the Recommendation of the Council of Europe. *AGRIS on-line Papers in Economics and Informatics,* 16(3), 59–73.

Maurer, A. D. (2020): *Digital Technologies in Elections: Issues, Conclusions and Prospects*. Strasbourg: Council of Europe Publishing House. *Council of Europe*, <accessed online: https://rm.coe.int/publication-digital-technologies-regulations-ukr/16809e8040>.

Mokhonchuk, B. & Romaniuk, P. (2019): Towards a Legal Framework that Protects Freedom of Expression in Electoral Processes. *Baltic Journal of European Studies,* 9(3), 43–62.

Pass, R., Seeman, L. & Shelat, A. (2017). Analysis of the Blockchain Protocol in Asynchronous Networks. In: Coron, J.S. & Nielsen, J. (eds.), *Advances in Cryptology – EUROCRYPT 2017. Lecture Notes in Computer Science.* Cham: Springer, 643–673.

Razali, M.H., Jamal, A.A., Fadzli, S.A., Zakaria, M.D., Wan Nik, W.N.S. & Hassan, H. (2024): E-Voting on Ethereum Blockchain. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 50(2), 186–194.

Slinko, T., Reznik, O., Kravchuk, M., Serohin, V. & Strelianyi, V. (2021): Use of Information and Communication Technologies in the Election Process: Ukrainian Realities and Foreign Experience. *Journal of Legal, Ethical and Regulatory Issues,* 24(1), 1–7.

Spanos, A. & Kantzavelou, I. (2024): EtherVote: A Secure Smart Contract-Based E-Voting System. *Wireless Networks,* 30(6), 1–8.

Stan, I.-M., Barac, I.-C. & Rosner, D. (2021): Architecting a Scalable E-Election System Using Blockchain Technologies. In: *Proceedings – RoEduNet IEEE International Conference*. Iasi: IEEE, 1–6.

Toepfl, F. (2016): Innovating Consultative Authoritarianism: Internet Votes as a Novel Digital Tool to Stabilize Non-Democratic Rule in Russia. *New Media & Society,* 20(3), 956–972.

Tokar-Ostapenko, O.V. (2022): Implementation of the Electronic Voting System in Ukraine: Current State and Legal Regulation. *Strategic Panorama,* 1, 26–41.

UIA (2024): Ukrainian Internet Association's Position on Electronic Voting. *UIA,* <accessed online: https://inau.ua/komitety/z-pytan-zakhystu-prav-lyudyny-ta-svobody-slova/pozytsiya-inau-shchodo-elektronnoho>.

Ukrinform (2025): The Number of Ukrainians and Their Migration Abroad due to the War. *Ukrinform*, <accessed online: https://www.ukrinform.ua/rubric-ato/3732355-kilkist-ukrainciv-ta-ih-migracia-za-kordon-cerez-vijnu.html>.

Vahtla, A. (2023): Online Votes Make Up Two-Thirds Of Reform, Less Than Third Of EKRE Votes. *Err.ee,* <accessed online: https://news.err.ee/1608906014/online-votes-make-up-two-thirds--of-reform-less-than-third-of-ekre-votes>.

Venice Commission (2004): Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe. *Venice Commission*, <accessed online: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2004)012-e>.

Venice Commission (2018): Compilation of Venice Commission Opinions and Reports Concerning Digital Technologies in the Electoral Process. *Venice Commission,* <accessed online: https://venice.coe.int/webforms/documents/?pdf=CDL-PI(2018)011-e>.

Verkhovna Rada of Ukraine (2023): Law of Ukraine No. 1135-IX "On the all-Ukrainian referendum". *Verkhovna Rada of Ukraine*, <accessed online: https://zakon.rada.gov.ua/laws/show/1135-20/ed20230331#Text>.

Verkhovna Rada of Ukraine (2020): Electoral Code of Ukraine. *Verkhovna Rada of Ukraine,* <accessed online: https://zakon.rada.gov.ua/laws/show/396-20/ed20231231#Text>.

Verkhovna Rada of Ukraine (2017a): Law of Ukraine No. 2155-VIII "On electronic identification and electronic trust services". *Verkhovna Rada of Ukraine,* <accessed online: https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

Verkhovna Rada of Ukraine (2017b): Law of Ukraine No. 2163-VIII "On the basic principles of ensuring cybersecurity of Ukraine". *Verkhovna Rada of Ukraine,* <accessed online: https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

Verkhovna Rada of Ukraine (2007): Law of Ukraine No. 698-V "On the state register of voters". *Verkhovna Rada of Ukraine,* <accessed online: https://zakon.rada.gov.ua/laws/show/698-16#Text>.

Wright, H. (2021): E-Votes Can Be Canceled By Voting At Polling Stations On Election Day. *Err.ee.* <accessed online: https://news.err.ee/1608359610/e-votes-can-be-canceled-by-voting-at--polling-stations-on-election-day>.

Zanuda, A. (2024): Escape from War or Deliberate Departure. How Migration from Ukraine Has Changed and What will be its Consequences. *BBC*. <accessed online: https://www.bbc.com/ukrainian/articles/c93px84133jo>.

Zfort Group (2019): Ethereum vs Hyperledger: Which Platform to Choose? *Zfort,* <accessed online: https://www.zfort.com.ua/blog/ethereum-vs-hyperledger-kakuyu-platformu-vybrat>.

Zhan, Y., Zhao, W., Zhu, C., Zhao, Z., Yang, N. & Wang, B. (2024). Efficient Electronic Voting System Based on Homomorphic Encryption. *Electronics,* 13, 286.

Kateryna O. Pavshuk *holds a PhD in Law and is an Associate Professor of the Department of Constitutional Law of Ukraine of Yaroslav Mudryi National Law University, Kharkiv, Ukraine. Her research interests include electoral law, democracy, and constitutionalism. E-mail: k.o.pavshuk@nlu.edu.ua; ORCID: 0000-0003-0588-4178.*

Bohdan S. Mokhonchuk *holds a PhD in Law and is an Associate Professor of the Department of Constitutional Law of Ukraine of Yaroslav Mudryi National Law University, Kharkiv, Ukraine. His research interests embrace election law and process, electoral dispute resolution, electoral systems and collective decision-making, constitutional law as a branch of law, sources of constitutional law, constitutional and legal responsibility, democracy, and rule of law. E-mail: bmokhonchuk@gmail.com; ORCID: 0000-0002-8945-0731.*

Pavlo V. Romaniuk *holds a PhD in Law and is an Associate Professor of the Department of Constitutional Law of Ukraine of Yaroslav Mudryi National Law University, Kharkiv, Ukraine. He is also a Coordinator of the Election Law Center and a Deputy Head of the Council of Young Scientists, functioning at Yaroslav Mudryi National Law University. He is a member of the International Council of Experts on Investigation of Crimes Committed in the Context of Armed Conflict at the Office of the Prosecutor General of Ukraine. His research interests involve election law, election dispute resolution, impact of special legal regimes on the electoral process, liability for electoral offenses, electoral systems, democracy. E-mail: p. v.romanyuk@nlu.edu.ua; ORCID: 0000-0002-0571-9490.*

Oleksii O. Liubchenko *holds a PhD in Law and is an Associate Professor of the Department of Constitutional, Administrative, Environmental, and Labor Law of Poltava Law Institute of Yaroslav Mudryi National Law University, Poltava Ukraine. He teaches Constitutional Law of Ukraine, Parliamentary Law; Human Rights; Electoral Law and Electoral Process. E-mail: oleksiy.lyubchenko@gmail.com; ORCID: 0000-0002-8068-5665.*

Alina O. Murtishcheva *holds a PhD in Law and is an Associate Professor of the Department of State Building of Yaroslav Mudryi National Law University, Kharkiv, Ukraine. She is also a Head of the Council of Young Scientists at Yaroslav Mudryi National Law University. Her research interests include problems of state-building processes, the constitutional and legal status of state authorities and local self-government bodies in Ukraine and foreign countries, and the responsibility of governmental structures. E-mail: a.o.murtischeva@nlu.edu.ua; ORCID: 0000-0001-6520-7297.*