UDC 004.738.5:342.8+004.9+681.3.06+351.9

Kovtun Y.O., Ph.D student, specialty 281 Public Administration and Management
Supervisor: Matveieva O.Y., Candidate of Sciences in Public Administration, Associate Professor at the Department of Public Administration
(*Dnipro University of Technology, Dnipro, Ukraine*)

ADDRESSING SECURITY AND PRIVACY CONCERNS IN BLOCKCHAIN-BASED ELECTIONS

Blockchain technology has been proposed as a tool for modernizing elections, but before its adoption, significant security and privacy risks must be addressed. While blockchain offers decentralization and cryptographic protections, deeper analysis reveals vulnerabilities that could undermine election integrity.

Key security risks in blockchain voting:

1. Malware manipulation remains the most persistent threat. If voter devices are infected, votes can be altered before reaching the blockchain, potentially allowing large-scale manipulation by foreign actors [1].
2. The consensus mechanism itself presents risks:
   - A 51% attack could allow a group of nodes to control election outcomes [1].
   - Private, centrally managed blockchains create single points of failure [1].
   - Synchronization issues in distributed ledgers may lead to vote forgery [4].
3. Lack of physical audit trails: unlike traditional paper-based elections, blockchain systems do not inherently provide a way to conduct manual recounts or independent verification of results [1].

Although blockchain provides some anonymity, important concerns remain:

1. Deanonymization risks: voting transaction patterns can be analyzed to identify voters [3].
2. Linking voter identity and ballot choices: weak separation between registration and voting can compromise anonymity [6].
3. Decryption vulnerabilities: if multiple authorities share encryption keys, improper handling could expose votes [3].

A blockchain voting pilot in Oman integrated biometric authentication and smart contracts to enhance security. However, the project highlighted scalability issues, especially in preserving voter anonymity for large populations [5].

A combination of technological solutions and policy changes can enhance security. Table 1 describes the proposed technological solutions:

Table 1

Technological solutions

Solution	Purpose
Zero-knowledge proofs	Ensures vote verification without exposing voter identity [6]
Hybrid systems	Integrates blockchain with paper-based audits [1][2]
Elliptic curve cryptography	Strengthens voter authentication via digital signatures [4]
Decentralized key management	Prevents single points of decryption control [3][5]

For secure implementation, governments should consider the following policy recommendations:

- Mandate open-source election software for transparency.
- Establish international governance standards for blockchain voting nodes.
- Develop contingency plans for manual overrides in case of failures.
- Implement liability frameworks for voting technology providers.

While blockchain alone cannot fully secure elections, when combined with encryption and paper-based verification, it strengthens electoral integrity [3][5][6]. Future efforts should focus on real-world testing of hybrid models and quantum-resistant cryptography to ensure long-term security. Instead of dismissing blockchain, policymakers should strategically integrate it within multi-layered electoral security frameworks.

List of references

1. The Myth of "Secure" Blockchain Voting. (n.d.). *U.S. Vote Foundation.* URL: https://www.usvotefoundation.org/blockchain-voting-is-not-a-security-strategy

2. Blockchain Voting: An imminent threat to democracy. (n.d.). *U.S. Vote Foundation.* URL: https://www.usvotefoundation.org/blockchain-threat-to-democracy

3. Blockchain for Electronic Voting System - Review and Open Research Challenges. (2021). *PubMed Central*. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC8434614/

4. Securing e-voting based on blockchain in P2P network. (n.d.). *Deutsche Nationalbibliothek.* URL: https://d-nb.info/1200324145/34

5. Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in Oman. (n.d.). *F1000Research.* URL: https://f1000research.com/articles/14-223

6. Integrating Blockchain Technology for Privacy-Preserving and Tamper-Proof Electronic Voting in Modern Electoral Systems. (n.d.). *Infonomics Society.* URL: https://infonomics-society.org/wp-content/uploads/Integrating-Blockchain-Technology-for-Privacy-Preserving-and-Tamper-Proof-Electronic-Voting.pdf