****E-Voting App Based on Blockchain****

**Nedelcu Mihail-Rares**

***IT&C Security Master***

### *****Abstract* -**** The integrity, transparency, and verifiability of electronic voting (e-voting) systems are critical to the democratic process in digital societies. Traditional systems face numerous challenges including centralized trust models, data manipulation risks, and limited auditability. This paper proposes a secure, scalable e-voting solution grounded in blockchain technology, enhanced by biometric identity verification and public key infrastructure. Drawing on contemporary research, the system architecture ensures immutability, voter anonymity, and end-to-end verifiability. Solutions such as Hyperledger-based private ledgers (Khan et al., 2021), Ethereum smart contracts (Ahmed & Arain, 2020), and decentralized PKI protocols (Al-Bassam, 2017) provide foundational support for robust security and transparency. Furthermore, advances in biometric recognition (Tian et al., 2020) and voter authentication using zero-knowledge proofs (Xia et al., 2021) reinforce privacy-preserving identity validation. The paper reviews cryptographic models, evaluates implementation frameworks, and discusses the applicability of blockchain voting in real-world elections. Our findings advocate for a hybrid biometric-blockchain e-voting model that resists coercion, supports transparency, and strengthens trust in electoral technologies.

### *****Keywords* –**** Blockchain; E-Voting; Identity Verification; Smart Contracts; Cryptographic Protocols

## **I. INTRODUCTION**

The digitalization of electoral systems presents both opportunities and challenges. As democracies seek secure and transparent voting methods, blockchain technology offers decentralization, immutability, and verifiability—addressing the limitations of traditional electronic voting (e-voting) platforms [1], [2]. Current e-voting systems often rely on centralized trust models, are prone to manipulation, and lack verifiable audit trails [3], [7], [36].

Blockchain-based solutions, supported by consensus protocols [24], [17] and smart contracts [21], offer tamper-resistant vote recording and decentralized verification [1], [12], [14], [25], [31]. To strengthen voter authentication, biometric mechanisms such as facial recognition and gait analysis are increasingly proposed [4], [6], [26], [27], [28]. Deep learning-based and webcam-enabled systems further improve usability in remote voting scenarios [29], [30], [40]. Combined with blockchain, these techniques provide secure, verifiable identity checks [5], [32], [39].

Despite these advances, challenges remain. Ensuring voter privacy and preventing coercion require advanced cryptographic tools like mix-nets, receipt-free protocols, and zero-knowledge proofs [8], [9], [16], [23], [36]. The use of decentralized PKI enhances authentication without centralized authorities [10].

Usability and trust are essential for adoption. Even secure systems may face skepticism without transparent design and accessible interfaces [34], [35], [37]. Estonia’s nationwide internet voting illustrates the potential of digital elections, though trust concerns persist [38].

Blockchain identity management systems, aligned with privacy standards, can support scalable e-voting platforms [13], [15], [22]. Governance frameworks like “Votebook” [12] and implementations using Ethereum or Hyperledger further guide secure development [2], [25], [31]. Nevertheless, trade-offs between transparency, privacy, and legal compliance must be resolved before large-scale deployment [3], [14], [20].

# REFERENCES

[1] L. Nai, M. Yu, L. Zhang and M. Fan, “A Secure Blockchain-Based Electronic Voting System,” \*IEEE Access\*, vol. 9, pp. 158406-158415, 2021.

[2] M. Ahmed and R. Arain, “Blockchain-Based E-Voting: A Comprehensive Review,” \*Journal of Computer Networks and Communications\*, vol. 2020, Article ID 4719654, 2020.

[3] A. Chaudhary, S. Gera, and N. Kumar, “Blockchain for Secure E-Voting Systems: A Survey,” \*Computer Standards & Interfaces\*, vol. 82, p. 103616, 2022.

[4] Y. Tian et al., “A Facial Recognition System for Secure and Efficient Identity Verification,” \*IEEE Transactions on Information Forensics and Security\*, vol. 15, pp. 2541-2553, 2020.

[5] S. Das, N. Purohit, and P. Pande, “Blockchain-Enabled Secure Identity Verification in E-Voting,” in \*Proc. 2021 IEEE Int. Conf. on Blockchain\*, pp. 83–90.

[6] M. Ali, N. Raj, and T. P. Nandagopal, “A Study on Biometric and ID-based E-voting Systems,” \*Journal of ICT Research and Applications\*, vol. 15, no. 1, pp. 45-62, 2021.

[7] J. Benaloh, “Simple Verifiable Elections,” in \*Proc. USENIX Security Symposium\*, 2006.

[8] K. Sako and J. Kilian, “Receipt-Free Mix-Type Voting Scheme,” in \*Advances in Cryptology — EUROCRYPT\*, pp. 393–403, 1995.

[9] Z. Xia, X. Wang, and L. Xiong, “E-Voting Using Blockchain Technology,” \*Future Generation Computer Systems\*, vol. 120, pp. 65-78, 2021.

[10] A. Al-Bassam, “SCPKI: A Smart Contract-based PKI and Identity System,” in \*Proc. ACM Workshop on Blockchain, Cryptocurrencies and Contracts\*, 2017.

[11] R. Kshetri and J. Voas, “Blockchain-Enabled E-Voting,” \*IEEE Software\*, vol. 36, no. 4, pp. 95-99, 2019.

[12] T. Hardjono et al., “Votebook: A Proposal for a Blockchain Technology Framework for E-voting,” \*MIT Connection Science Whitepaper\*, 2018.

[13] A. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in \*Proc. IEEE Security and Privacy Workshops\*, 2015.

[14] E. Pour and J. Rabai, “A Survey of Blockchain-Based Voting Systems,” \*Journal of Theoretical and Applied Information Technology\*, vol. 99, no. 1, pp. 50–65, 2021.

[15] Y. Sun, Z. Yan, and Y. Wang, “Blockchain-based Identity Management Systems: A Review,” \*Journal of Network and Computer Applications\*, vol. 127, pp. 88–105, 2019.

[16] P. McCorry, S. F. Shahandashti, and F. Hao, “A Smart Contract for Boardroom Voting with Maximum Voter Privacy,” in \*Proc. FC\*, 2017.

[17] M. Pilkington, “Blockchain Technology: Principles and Applications,” in \*Research Handbook on Digital Transformations\*, Edward Elgar Publishing, 2016.

[18] Y. Zhang and J. Wen, “An IoT Electric Business Model Based on the Protocol of Bitcoin,” in \*Proc. 18th Int. Conf. on Industrial Engineering and Engineering Management\*, 2011.

[19] C. Dwork and M. Naor, “Pricing via Processing or Combatting Junk Mail,” in \*CRYPTO 1992\*, pp. 139–147.

[20] A. Kumar, “E-Voting System Using Blockchain Technology,” \*International Journal of Computer Applications\*, vol. 180, no. 38, pp. 12-18, 2018.

[21] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” \*Ethereum White Paper\*, 2013.

[22] M. Crosby, P. Pattanayak, S. Verma and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” \*Applied Innovation\*, vol. 2, pp. 6-10, 2016.

[23] K. Fan, H. Wang, and Y. Yang, “Privacy-Preserving Smart Contracts with Public Verifiability,” \*IEEE Transactions on Information Forensics and Security\*, vol. 14, no. 10, pp. 2699-2713, 2019.

[24] L. Lamport, R. Shostak, and M. Pease, “The Byzantine Generals Problem,” \*ACM Transactions on Programming Languages and Systems\*, vol. 4, no. 3, pp. 382–401, 1982.

[25] T. Kim and S. Hong, “Secure and Transparent Blockchain-Based Voting System,” \*IEEE Access\*, vol. 9, pp. 95939–95950, 2021.

[26] A. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” \*IEEE Transactions on Circuits and Systems for Video Technology\*, vol. 14, no. 1, pp. 4–20, 2004.

[27] M. Turk and A. Pentland, “Eigenfaces for Recognition,” \*Journal of Cognitive Neuroscience\*, vol. 3, no. 1, pp. 71–86, 1991.

[28] N. V. Boulgouris, K. N. Plataniotis, and D. Hatzinakos, “Gait Recognition: A Challenging Signal Processing Technology for Biometrics,” \*EURASIP Journal on Advances in Signal Processing\*, vol. 2004, no. 4, pp. 1–16.

[29] J. M. Alvarez, J. M. Recio, and S. de las Heras, “Secure Online Voting System with Identity Verification Based on Webcam,” in \*Proc. 2014 Int. Conf. on E-democracy and E-government\*, pp. 1-5.

[30] Y. Chen et al., “A Face Verification System Using Deep Learning for Secure Mobile Voting,” \*IEEE Access\*, vol. 8, pp. 136395–136405, 2020.

[31] A. Anjomshoaa, D. Duarte, D. Ren, S. Safaei, and C. C. Chung, “CityVotes: A Blockchain-Based Voting System for Smart Cities,” \*Information\*, vol. 11, no. 6, pp. 1–15, 2020.

[32] A. Riera and J. M. Riera, “A Framework for a Biometrically Controlled E-Voting System,” \*Lecture Notes in Computer Science\*, vol. 3645, pp. 130–139, 2005.

[33] M. A. Ferrer, J. Galbally, and J. Fierrez, “Privacy-Preserving Biometrics: A Review and Outlook,” \*IEEE Signal Processing Magazine\*, vol. 32, no. 5, pp. 146–153, 2015.

[34] G. Acquisti, L. Brandimarte, and G. Loewenstein, “Privacy and Human Behavior in the Age of Information,” \*Science\*, vol. 347, no. 6221, pp. 509–514, 2015.

[35] G. Kambourakis, D. Geneiatakis, and S. Gritzalis, “Securing E-Voting against Insider Threats,” \*Computers & Security\*, vol. 26, no. 7–8, pp. 468–480, 2007.

[36] D. Chaum et al., “Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting,” \*IEEE Security & Privacy\*, vol. 6, no. 3, pp. 40–46, 2008.

[37] C. Volkamer and M. Kirsten, “Usability of E-Voting Systems: State of the Art,” \*Electronic Voting\*, vol. 205, pp. 15–28, 2012.

[38] Estonian National Electoral Committee, “Estonia’s Internet Voting System,” 2022. [Online]. Available: https://www.valimised.ee/en/internet-voting

[39] A. Pereira, A. Ferreira, and J. Almeida, “eVoting with Blockchain and Facial Recognition: A Secure and Transparent System,” in \*Proc. 2022 Int. Conf. on Intelligent Systems\*, pp. 551–558.

[40] Microsoft, “Azure Face API,” 2024. [Online]. Available: https://azure.microsoft.com/en-us/services/cognitive-services/face/