IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, June 2024

Enhancing the Security of Digital Voting Systems: A Blockchain-Based Decentralized Approach for Future Electronic Voting Systems

Sree Ganesh M S[1], Karthik P Naik[2], Deekshith Acharya[3],
Naresh Maibam[4], Dr. Pushparani M K[5]
6th Sem, Department of Computer Science and Design[1,2,3,4]
Sr. Assistant Professor, Department of Computer Science and Design[5]
Alva's Institute of Engineering and Technology, Moodubidire, India
Affiliated to Visvesvaraya Technological University, Belagavi
4al21cg056@gmail.com, 4al21cg032@gmail.com
4al21cg016@gmail.com, nareshmaibam71@gmail.com, drpushparani@aiet.org.in

Abstract*:* *This paper introduces a blockchain-based electronic voting (e-voting) system aimed at improving voter turnout and ensuring robust security. Traditional offline elections often suffer from fairness and accuracy issues due to centralized control, which can lead to vote manipulation. The proposed system leverages blockchain technology to decentralize authority, reduce reliance on a single entity, and enhance transparency. It comprises four stages: setup, registration, voting, and result, each utilizing smart contracts to maintain an immutable record. Key features include secure voter and candidate registration, encrypted vote casting, and transparent result dissemination. By addressing critical security concerns such as vote uniqueness, mobility, coercion resistance, anonymity, and data integrity, this system offers a reliable and transparent solution for modern elections.*

Keywords: blockchain-based electronic voting

I. INTRODUCTION

As digitalization continues to infiltrate every facet of our lives, electronic voting (e-voting) has the potential o revolutionize traditional voting systems. The conventional offline elections are plagued by issues related of impartiality and accuracy, exacerbated by vulnerabilities from centralized control that may lead to vote manipulation and biased outcomes. The proposed e-voting system emphasizes enhancing voter turnout while ensuring robust security. Security is the most significant challenge facing any electronic service. However, leveraging blockchain technology can mitigate these challenges. This innovative approach decentralizes authority, reducing reiance on a single entity and promoting system transparency.

II. BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed, immutable ledger that facilitates the tracking of assets and recording of transactions within a business network. It operates as a decentralized database of records or digital events that are immutable and verified by a majority of participants. Each transaction is stored as a ”block” of data, which can represent any valuable item, tangible or intangible. These blocks are chronologically linked to form an unchangeable chain. The blocks are securely connected to prevent tampering and verify the exact timing and sequence of transactions. Blockchain technology offers numerous advantages, such as enhanced transparency, precise tracking, and the use of smart contracts.

III. EXISTING SYSTEMS

Many countries currently utilize digital systems for voting, with Estonia being the pioneer [1]. Every Estonian citizen receives a national ID, central to the voting process. Voters insert their ID cards into card readers and access the voting website on a connected computer. They are prompted to enter their PIN for authentication. Voters can cast their ballots

DOI: 10.48175/IJARSCT-18786

up to four times in the days leading up to election day. If a card reader is unavailable, they can use mobile devices to vote. This system employs three servers: the Vote Forwarding Server (VFS), the Vote Storage Server (VSS), and the Vote Counting Server (VCS). Votes are encrypted and stored until the end of the voting session, then transferred to the VCS for counting and decryption. Despite this system's advancements, it still faces security risks, such as potential vote manipulation by hackers and the inability of voters to confirm that their vote was counted correctly [2]. Another existing system [3] addresses authentication, transparency, anonymity, accuracy, autonomy, singularity, integrity, and mobility by incorporating blockchain and smart contracts. Voter data is stored as hashes on the blockchain, ensuring privacy and scalability. Smart contracts enhance security and speed up transactions using miners. The voting process is streamlined, and counting time is reduced through block-based vote counting [4].

IV. PROPOSED SYSTEM

The proposed e-voting system leverages blockchain technology to ensure the integrity, transparency, and security of the voting process. It comprises four main phases: Setup, Registration, Voting, and Result Phases. Each phase interacts with blockchain-based smart contracts to maintain a tamper-proof record of all voting activities.

4.1 Detailed Process Flow

1. Election Commission (EC): Initiates and supervises the election process.
2. Blockchain: Serves as a decentralized, immutable ledger for recording votes and election data.
3. Voter: Registers, authenticates, and casts their vote securely.
4. Crypto Server: Manages the encryption and decryption of votes to ensure security and privacy [6].
5. Result Phase: Handles vote counting and result publication, maintaining transparency and integrity.

V. SYSTEM ARCHITECTURE

5.1 Setup Phase

Ar1. Create Election: The EC initiates the election by establishing an election instance. 2. Generate Encryption Keys: Encryption keys are created to secure communication and data within the voting system, ensuring only authorized entities can decrypt votes. 3. Activate Election: The election is activated, allowing subsequent phases to commence. 4. Election Time: The election's duration is defined, specifying start and end times. 5. Vote Coins: Digital tokens (vote coins) are generated and distributed to eligible voters, necessary for casting votes [7]. During this phase, the EC sets up essential parameters and transfers keys to the blockchain system for further use.

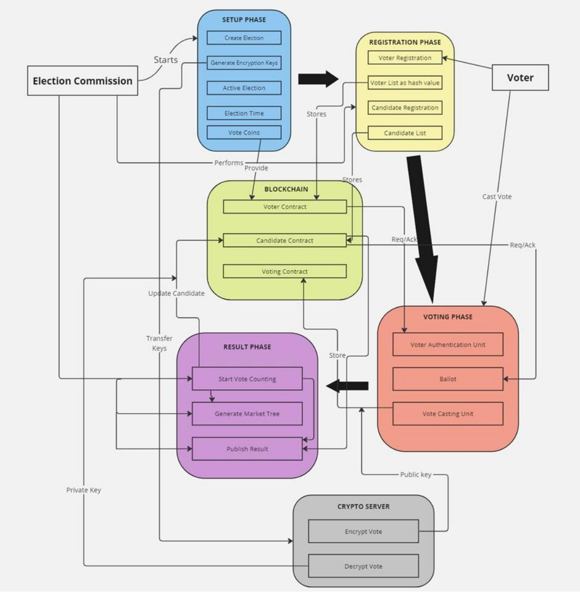

Figure 1: Fig. System architecture of digital voting using blockchain.

DOI: 10.48175/IJARSCT-18786

5.2 Registration Phase

1. Voter Registration: Eligible voters register, verifying their identities and storing their information as a hash value for privacy and integrity.
2. Voter List as Hash Value: A list of registered voters is maintained on the blockchain as a hash value, ensuring system immutability
3. Candidate Registration: Candidates register, providing details stored on the blockchain.
4. Candidate List: The list of registered candidates is maintained on the blockchain for reference during the voting phase [8].

5.3 Voting Phase

1. Voter Authentication Unit: Authenticates voters using their credentials, ensuring only registered voters can cast votes.
2. Ballot: Provides authenticated voters with an electronic ballot containing the list of candidates from the blockchain.
3. Vote Casting Unit: Voters cast their vote, encrypted using the public key from the Crypto Server before being stored on the blockchain. The encrypted vote is cast and stored on the blockchain, ensuring confidentiality and tamperproof records. A request and acknowledgment mechanism ensures successful vote recording [9].

5.4 Result Phase

1. Start Vote Counting: Once voting concludes, the vote counting process begins, retrieving encrypted votes from the blockchain. 2. Generate Merkle Tree: A Merkle tree is generated to verify the integrity of the votes, detecting any alterations in the vote data [10]. 3. Publish Result: Final results are computed and published, transparent and verifiable due to blockchain technology.

The Crypto Server decrypts votes using the private key. The blockchain is updated with the final results, ensuring the election outcome is immutable and publicly verifiable [11].

5.5 Blockchain Integration

The blockchain system includes three smart contracts:
1. Voter Contract: Manages voter registrations and ensures only eligible voters can vote.
2. Candidate Contract: Manages candidate registrations and maintains candidate information integrity.
3. Voting Contract: Manages the voting process, including vote casting and storage. These smart contracts interact with each other and various election phases, ensuring seamless and secure operations. Blockchain technology records all transactions in a decentralized, immutable ledger, providing high security and transparency [12].

VI. SECURITY

Security and trust are critical for electronic voting systems. Blockchain technology enhances security and privacy, preventing tampering by malicious parties and ensuring election integrity. The public key serves as the voter's network identity, ensuring voter anonymity. The Merkle tree ensures data integrity, detecting any changes in vote data. The system prevents coercion by ensuring that no one can determine a voter's intention [13]. Voters can cast their ballots from any location, ensuring accessibility [14]. Each voter can only cast one vote, included in the total count [15].

VII. CONCLUSION

The proposed e-voting system utilizes blockchain technology to create a secure, transparent, and reliable voting process. By integrating smart contracts and encryption mechanisms, the system ensures election integrity, protects voter privacy, and provides verifiable and immutable results. This methodology addresses common concerns in traditional voting systems, offering a robust solution for modern elections.

REFERENCES

[1]. Ahmed, M. R., Shamrat, F. J. M., Ali, M. A., Mia, M. R., Khatun, M. A. (2020). The future of electronic voting system using blockchain. International Journal of Scientific Technology Research, 9, 4131-4134.

IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, June 2024

[2]. Kumar, D. D., Chandini, D. V., Reddy, D., Bhattacharyya, D., Kim, T. H. (2020). Secure electronic voting system using blockchain technology. International Journal of Smart Home, 14(2), 31-38.

[3]. Kovic Marko, “Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system,” (2017)

[4]. Alvi, S. T., Uddin, M. N., Islam, L., Ahamed, S. (2022). DVTChain: A blockchain-based de centralized mechanism to ensure the security of digital voting system voting system. Journal of King Saud University-Computer and Information Sciences, 34(9), 6855-6871.

[5]. S. T. Alvi, M. N. Uddin and L. Islam, ”Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract,” 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 228-233, doi: 10.1109/IC-SSIT48917.2020.9214250.

[6]. Sourav Rajeev Rohan Varghese Mathew V. Arun, Aditya Dutta. E-voting using a decentralized ethereum application. 04 2019.

[7]. Samarth Shakya and Vivek Kapoor. A decentralized polling system using ethereum technology. Journal of Information Technology Management, 14 (Security and Resource Management challenges for Internet of Things): 1–8, 2022

[8]. Umair Khalid, Muhammad Asim, Thar Baker, Patrick Hung, Muhammad Adnan Tariq, and Laura Rafferty. A decentralized lightweight blockchain-based authentication mechanism for iot systems. Cluster Computing, 23, 09 2020.

[9]. The defiant. What is metamask? https://thedefiant.io/what-is-metamask/. the Independent. Blockchain could be the answer to fair voting in Bangladesh, a. http://www.theindependentbd.com/post/234648. the Independent. Significance of electronic voting machine in Bangladesh,

[10]. Mykletun, Einar, Narasimha, Maithili, Tsudik, Gene, 2003. Providing authentication and integrity in outsourced databases using merkle hash trees. UCI-SCONCE Technical Report.

[11]. Hsiao, T. C., Wu, Z. Y., Liu, C. H., Chung, Y. F. (2017). Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme. Advances in Mechanical Engineering, 9(1), 1687814016687194.

[12]. M. Gautam, S. Akthar, A. Basha and G. Dilip, ”Blockchain For Secure and Proper Management of Medical Data and Records,” 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2021, pp. 671-678, doi: 10.1109/ICECA52323.2021.9676078.

[13]. H. Ghavamipoor and M. Shahpasand, ”An anonymous and efficient e-voting scheme,” 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security, Kish Island, Iran, 2013, pp. 1-13, doi: 10.1109/ECDC.2013.6556734.

[14]. Jos´e Lu´ıs Pereira Jorge Lopes. Blockchain based e-voting system: A proposal. In Twenty-fifth Americas Conference on Information Systems, Cancun, 2019, 2019.

[15]. Jafar U, Aziz MJA, Shukur Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors. 2021; 21(17):5874.

DOI: 10.48175/IJARSCT-18786