Blockchain-Empowered E-Voting: A Transparent and Scalable Solution

Tushar Gupta*, Anmol Gupta, Tushar Gupta, Chirag Chirag, Garima Singh
Department of Computer Science and Information Technology, Krishna Institute of Engineering & Technology (KIET), Ghaziabad, Delhi-NCR, Uttar Pradesh, India
tusharguptatg800@gmail.com*
Anmolguptaag8755@gmail.com
really.tushar835@gmail.com
Chirag741795@gmail.com
garima.singh@kiet.edu

Abstract. In the past few years, the government and other institutions across the world are keen on seeking a voting system that is secure, transparent and decentralized. With increasing cases of election frauds, cyberattack vulnerability and the lack of trust by voters towards the conventional and highly centralized electronic voting system (EVM) that entirely depend on a centralized and vulnerable to tamper system, it became essential to provide a more secure and robust system. To solve these issues, we suggest a blockchain-based e-voting system that introduces the process of combining a decentralized ledger-based technology with safe cryptographic technology. Our suggested system supports smart contracts that automate the election processes, homomorphic encryption to count the votes privately without knowing the mandate of the voter, and linkable ring signature to secure the identity of the voter and prevent double voting. We have both permissioned and permissionless blockchain models and can be optimized to work with performance and scalability across election environment. The experiments demonstrated promising performance, as the system processed 1000–2000 concurrent votes with minimal transaction latency of 2–3 seconds while maintaining security. By eliminating centralized sources of failure and providing an unalterable transparent and auditable registry of voting, this system provides a step towards a viable and reliable digital democracy.

Keywords: Blockchain, Cryptography, Smart Contract, Linkable Ring Signature, Homomorphic Encryption

1 Introduction

The transparency of elections, the equity of the electoral process, and the safety of the voters are the only keys to the flourishing and strong democracy and that is why it is vital to possess effective voting system [1]. Paper ballets and the conventional electronic voting machines continue to encounter the problem of human error, logistical inefficiency, slow results, resource consumption and probability of manipulation [2]. Additionally, most of the current electronic voting systems continue to fail to deliver end to end verification, voter privacy and reliable auditing [3]. The Blockchain technology has attracted massive interest owing to the property of decentralization and immutability and high cryptographic value, which has enabled it to emerge as a better alternative to ensure a secure and transparent electoral system [4]. These characteristics facilitate resistant to tampering records, shared confidence and are thoroughly transparent audits [5]. In spite of this potential, there are major challenges that implementing blockchain in real-world elections such as voter privacy, voting twice, confirmation of

M. Kaushik et al. (eds.), *Proceedings of the International Conference on Responsible, Risk-aware, and Regulated AI (RRRAI 2026)*, Advances in Intelligent Systems Research 210,
https://doi.org/10.2991/978-94-6239-723-1_8

privately cast votes and scaling to large scale elections [6]. Other issues like eligibility check, anti-manipulation, and open auditing are of high priority [7].

In order to solve these problems, our study suggests a blockchain derived voting mechanism that references homomorphic encryption to compute votes privately without revealing individual voting preferences, while smart contracts are employed to manage election processes in a secure and transparent way. The system will be deployed on both permissioned and open blockchain platforms. The first objective is defining, testing and assessing a secure, scalable and transparent electoral system that is appropriate to real electoral systems. Fig. 1 illustrates the transition from traditional insecure voting systems to a secure, transparent, and scalable blockchain-based voting system

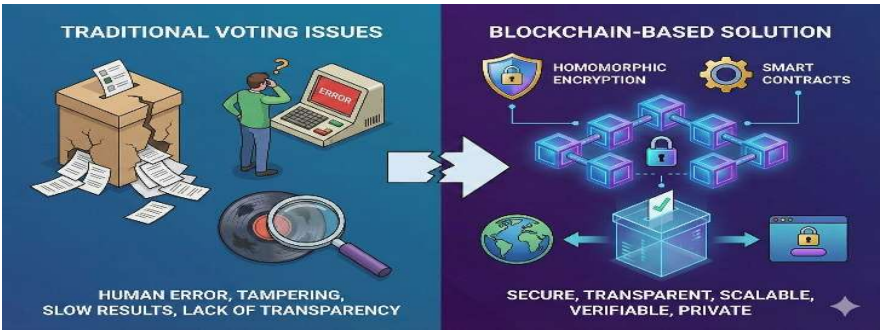

Fig. 1. An illustrative comparison of the change between the insecure nondetectable traditional form of voting to a secure, transparent, and scalable blockchain-based system.

2 Related Work

In recent years, blockchain technology has attracted significant research interest as a means to improve the security and transparency of electronic voting systems [8]. This interest is partly due to the problems that the conventional methods of voting have - such as suspicion of credibility, precision and privacy of voters [9]. To resolve these problems, many researchers have been trying to develop various cryptographical and system-based solutions to establish electronic voting systems [10]. Some experiments to combine blockchain with Shamir Secret Sharing were performed in the early research on this direction. The outstanding aspect was that the tallying of the votes was divided to a number of diverse parties as opposed to having it being divided to a single point [11]. Due to the advancement in research, more advanced methods were presented. Paillier homomorphic encryption allowed the votes to be added without decryption; and linkable ring signatures allowed the voters to be anonymous and prevent the voters to vote twice and Zero-knowledge proofs enable voters to verify that a vote has been cast correctly without disclosing the actual vote content [12]. Some researchers tried to focus on enhancing transparency and reliability with smart contracts [13]. For instance, a system focused on using smart contracts were used to automate election operations and reduce the risk of majority control attacks. Similarly, a conceptual model focused on decentralization and anonymity of elector, but this conceptual model was more theoretical rather than practical [14]. Other works were done on surveys and trend analysis [15]. The feasibility of using Ethereum for e-voting demonstrated improvement in

automation and trust offered by smart contracts, while a detailed review of different types of blockchain-based voting systems pinpointed key features such as voter eligibility verification, transparency and anonymity. One of the main problems constantly raised is scalability, how to efficiently handle millions of voters. A comparison of permissioned and permissionless blockchains showed that permissioned ones typically perform faster but decide to do so at the cost of some decentralization [16]. The idea of blockchain-as-a-service for voting also suggested a way to merge it with the principles of liquid democracy in a permissioned blockchain setup [17]. Even with all these innovations, most of the current systems still aren't ready for national-scale elections [18]. Many of them are designed for specific platforms like the Ethereum network, resulting in lack of interoperability and overall scalability [19]. There is also the ongoing challenge of keeping the votes private while still enabling the voting process to be verifiable [20].

To overcome such challenges, through our proposed system we could potentially develop a blockchain-agnostic framework that could scale to handle national elections. The design uses a combination of the encryption algorithm Paillier, linkable ring signatures, and zero knowledge-proofs under one system and features smart contracts that manage important election tasks automatically. This approach takes the best part of earlier studies, but addresses straight on the main technical and practical shortcomings.

Despite extensive research on blockchain-based e-voting systems, several fundamental challenges remain unresolved for real-world deployment.

- Scalability & Performance: The existing systems fail to manage high transaction costs, network overload and system overloads during large scale elections.
- Authentication & Security: There have been no known-scalable solutions to voter authentication and sybil attacks (where a single user impersonates many identities).
- Real-World Usability: Non-technical users find interfaces too complicated which presents adoption barriers.
- Regulatory & Legal: It remains highly unclear how these systems align with the current election laws and regulations.
- Theoretical vs. Practical: Only small lab demonstrations have been conducted on most research, with little available in the way of practical solutions to large and national-scale implementations.

3 Proposed Work

The primary aim of our Dapp (Decentralized voting system) is to ensure that the less secure and less transparent current voting systems which continue to have poor privacy are eliminated and to support the high amount of users simultaneously. Our Dapp is being used to support the voter dashboard in which registered voters only can vote to the candidate of their choice and simple users can get them registered after undergoing the validation by the group of admins. In this case, we are voting safely with the Ethereum based blockchain. The other point is that also registered voters sign their vote with the private key of their MetaMask wallet to accomplish the authentication process so that no other individual can represent another individual in the voting process. Solidity-based smart contracts are utilized to automate the work of the system and regulate

the voting regulations to ensure that no one can cheat with the records of votes since the records are stored in blockchain to provide reliable, trusty or more secure voting to the maximum possible.

3.1 System Architecture Overview

The architecture of the system will be described here. It consists of the following major parts: a) Voter Dashboard: It is in this place where ordinary citizens register, and actually cast their votes. The friendly interface is developed by applying web3.js framework in order to enable any person to use it. b) Admin Dashboard: This is where the election commission authority is in charge and will oversee elections, the votes that will be received and maintain the voter list. Both dashboard communicates with Ethereum blockchain, and all the rules (such as only authorized individuals can vote or no one can vote twice, etc.) are defined by smart contracts, and thus no one can simply ruin the voting system. Fig. 2 illustrates the proposed algorithm for the secure voting system.

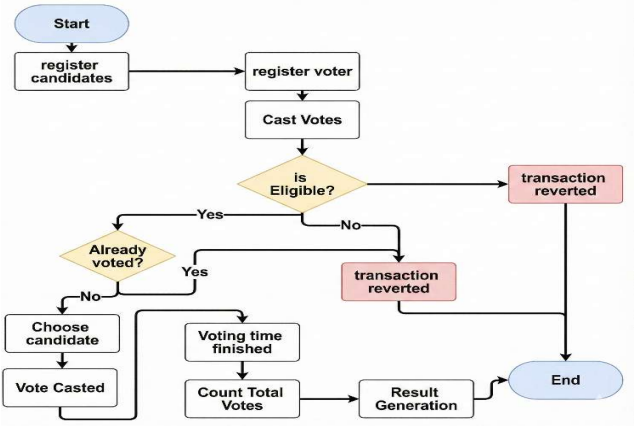

Fig. 2. The Proposed Algorithm

3.2 Main Components

a) Smart Contracts: These pieces of self-executable code handle the validation of the transact that any node of the blockchain produces and also it is stored on every node that exists within the system in case they are not valid otherwise reverted. It also makes sure that no one is able to tamper or defraud the records in the future.
b) Digital Wallets: Voters receive a MetaMask account, more of a safe stamp to demonstrate their actual identity and to demonstrate that they voted in reality. (but does not indicate who they voted).
c) Decentralized Storage: The entire transaction records of the votes, as well as the voter, is not stored at a single location in the blockchain, and thus, the hacking of one computer will not affect the rest of the network copies of the ledger.
Due to this architecture:

- Every vote is registered safely and no one will be able to tamper with the outcome of the vote.
- Anyone may look at the outcomes of election in real time, and know that

everything is really fine.

- All this is much time taking or much effort taking to hackers to crack and this is in addition to the fact that it is nearly impossible to alter past votes.

1. Registration and Authentication of voters: In order to ensure that only those people can cast a vote that should have the opportunity to do so, our system employs metamask wallets and decentralized manner of knowing who the people are.

Algorithm:

- On the Voter Dashboard, the user registers himself by giving information such as aadhar ID and mobile number.
- A smart contract then verifies whether they are actually registered as well as ensures, they have not already voted.
- A user then logs in with his/her MetaMask wallet to identify himself/herself.
- Once they have been validated, they are provided with a unique and encrypted token by the system and broadcast to all the nodes within the system so that they are not able to cheat by voting twice.
-

2. Election Setup (Admin Dashboard)

The election commission can have access to dashboard where they are worrying about registration of candidates, voting time and rules. They also have the ability of following the voting progress on without interfering with the privacy.

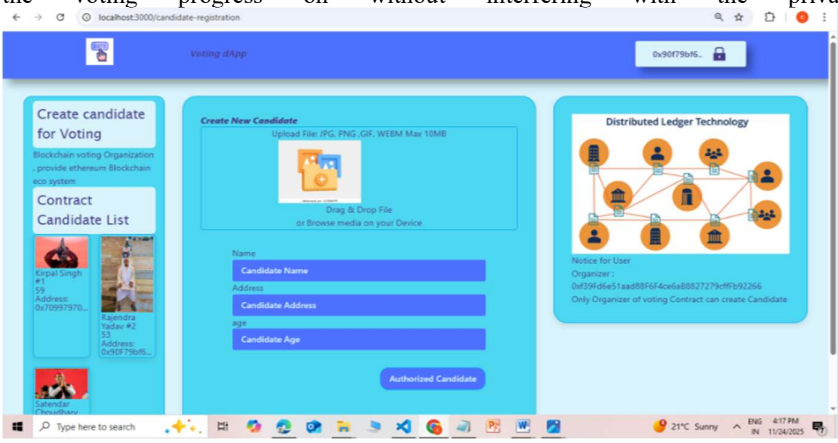

Fig. 3. Candidate registration and authorization interface based on blockchain and smart contract and distributed ledger technology.

Algorithm:

- The admin enters the information in order to choose the candidates, voting hours, and regulations.
- Then these details are locked by sending a smart contract to the blockchain.
- This information is stored on the blockchain forever thus it cannot be altered by anyone in future.

This system helps in ensuring that elections are not only transparent but also safe and easy not only to the voters themselves but also the admins (Fig. 3 Candidate registration and authorization interface) and this helps all trust the process much.

3. Vote Casting

It is possible to vote through the Voter Dashboard with ease and security. Here's how it actually works:

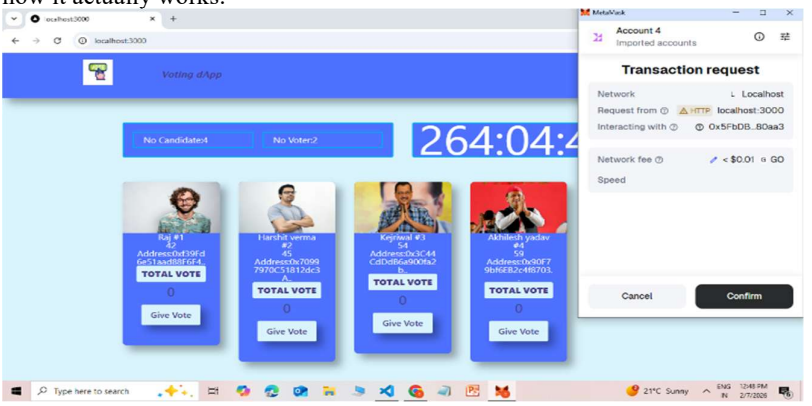

Fig. 4. Real-time blockchain-based voting interface showing candidate-wise vote casting, live tally updates, and smart contract–controlled election timing.

The candidate is selected by the voter who selects one of the candidates presented in the list on the dashboard as shown in Fig. 4.

Algorithm:

- They cast their digital votes using their digital wallet (MetaMask) and transmit the same to the blockchain network.
- The smart contract will ensure that the vote is authentic like the voter is not banned and has not already voted.
- The next step is storing the vote on the blockchain that cannot be manipulated, and only visible to the authentic individuals (voters and admins).

4. Vote Counting and Result Generation

The smart contract is able to tally the votes in real-time to present the results in a short period and in a just manner.

Algorithm:

- Whenever a vote is casted, it is securely stored in the blockchain.
- The smart contract automatically counts the votes of the candidate who is elected and nobody is obliged to count the votes manually.
- The smart contract then stores the outcome on blockchain after the voting process is completed after the votes cast on each candidate have been compared.
- Then they can be scrutinized and relied upon by any man.

5. Security Mechanisms (Preventing Fraud and Manipulation)

The system is struggling to ensure the safety of the votes and avoid any kind of hacking and cheating.

Algorithm:

- A signature is created with a personal key of MetaMask account on each vote.
- Votes are stored in a single copy of ledger that is available in each node therefore they

cannot be modified or erased.
- The blockchain is decentralized and it has no authority that can interfere with the votes.
- The system is able to notice any suspicious activity that is happening like an overloading of votes in a specific location and immediately alert it.

4 Implementation

Candidate Registration

```
function setCandidate(
    address _address,
    string memory _age,
    string memory _name,
    string memory _image,
    string memory _ipfs
) public {

    require(votingOrganizer == msg.sender,
    "Only organizer can authorize candidate");

    _candidateId.increment();
    uint256 idNumber = _candidateId.current();

    Candidate storage candidate = candidates[_address];

    candidate.age = _age;
    candidate.name = _name;
    candidate.candidateId = idNumber;
    candidate.voteCount = 0;
    candidate.image = _image;
    candidate._address = _address;
    candidate.ipfs = _ipfs;

    candidateAddress.push(_address);

    emit CandidateCreate(
        idNumber,
        _age,
        _name,
        _image,
        candidate.voteCount,
        _address,
        _ipfs
    );
}
```

Fig. 5. Code snippet for candidate registration in the voting smart contract.

Only voting organizer can create or register the candidates. Info like candidateId, name, image, age etc about the candidates is stored on the blockchain securely (as implementation shown in Fig. 5).

Voter Registration

```
function voterRight(
    address _voterAddress,
    string memory _name,
    string memory _image,
    string memory _ipfs
) public {
    require(votingOrganizer == msg.sender,
    "Only organizer can create voter");

    voterId.increment();
    uint256 idNumber = voterId.current();

    Voter storage voter = voters[_voterAddress];

    require(voter.voterallowed == 0, "Voter already exists");

    voter.voterallowed = 1;
    voter.votername = _name;
    voter.voterimage = _image;
    voter.voteraddress = _voterAddress;
    voter.voterId = idNumber;
    voter.votervote = 1000;
    voter.votervoted = false;
    voter.voteripfs = _ipfs;

    votersAddress.push(_voterAddress);

    emit VoterCreated(
        idNumber,
        _name,
        _image,
        _voterAddress,
        voter.voterallowed,
        voter.votervoted,
        voter.votervote,
        _ipfs
    );
}
```

Fig. 6. Code snippet for voter registration and storage of voter details on the blockchain

Only voting organizer can register the voter, each voter receives only one vote token such that fairness is ensured and voting rights are also stored on the blockchain (as implementation shown in Fig. 6).

- **Cast Vote**

```
function vote(address _candidateAddress, uint256 _candidateVoteId)
    external {
    Voter storage voter = voters[msg.sender];
    require(!voter.voter_voted, "you have already voted");
    require(voter.voter_allowed != 0, "You have no right to vote");
    voter.voter_voted = true;
    voter.voter_vote = _candidateVoteId;
    votedVoters.push(msg.sender);
    candidates[_candidateAddress].voteCount += voter.voter_allowed;
```

Fig. 7. Code snippet for casting a vote and updating the candidate vote count

After validating the vote given by the voter, vote is casted successfully to the chosen candidate while ensuring the immutability, privacy and security (as implementation shown in Fig. 7).

- **Result Generation**

```
const getWinner = async () => {
  if (window.ethereum) {
    try {
      const provider = new ethers.BrowserProvider(window.ethereum);

      await provider.send('eth_requestAccounts', []);
      const signer = await provider.getSigner();
      const add = await signer.getAddress();
      console.log("Signer Address:", add);

      const contract = new ethers.Contract(VotingAddress, VotingAddressABI, signer);

      const allCandidate = await contract.getCandidate();
      console.log("Candidate Data:", allCandidate);

      const updatedCandidates = await Promise.all(
        allCandidate.map(async (el) => {
          const singleCandidateData = await contract.getCandidatedata(el);
          console.log("Single Candidate Data:", singleCandidateData);
          return singleCandidateData;
        })
      );

      setCandidateArray(updatedCandidates);
      console.log("Updated Candidate Array:", updatedCandidates);

      const allCandidateLength = await contract.getCandidateLength();
      console.log("Candidate Length:", allCandidateLength);
      setCandidateLength(allCandidateLength);

      // Determine the maximum vote count
      let max = 0;
      updatedCandidates.forEach((el) => {
        if (el[4] > max) max = el[4];
      });

      // Collect all winners with max votes
      const winnerArray = updatedCandidates.filter((el) => el[4] === max);
      setWinners(winnerArray);

    } catch (error) {
      console.log("Error:", error);
    }
  } else {
    console.log("Connect to MetaMask or install MetaMask");
  }
};
```

Fig.8. Implementation of the getWinner function in the blockchain voting system: (a) retrieving candidate data from the smart contract, (b) determining the winner based on the maximum vote count.

The results or winner info is retrieved from the blockchain and displayed transparently to all node of system (as implementation shown in Fig. 8).

5 Results and Discussion

In order to test the concept of the e-voting system, we performed numerous experiments and simulations on different scenarios, in order to determine the effectiveness of our blockchain based system. Fig. 9 illustrates the performance and scalability of the proposed e-voting system under varying load conditions. Its main aim was to test its efficiency, reliability, scalability and user experience especially when dealing with a large number of voters. Performance & Scalability: The system demonstrated satisfactory performances in terms of high transaction rates (particularly on a permissioned block chain on 200 TPS) and high reliability during the stress test on 100 -100K voters. Security & Privacy: Simulations in the real world provided an adequate security against typical attacks. Ring signatures ensured voter anonymity and homomorphic encryption ensured the confidentiality of the ballots. User Experience: The user trials generated a success rate of 95 percent and positive user experience in terms of the user-friendly interface of the system and the provision of easy audit trails. In the left panel, it is depicted that permissioned network is five-fold faster than a public blockchain and can be utilized to conduct over 200 transactions per second. On the whole, the findings indicate a highly reliable, safe and transparent system which is a good candidate to be adopted in large scale applications of e-voting.

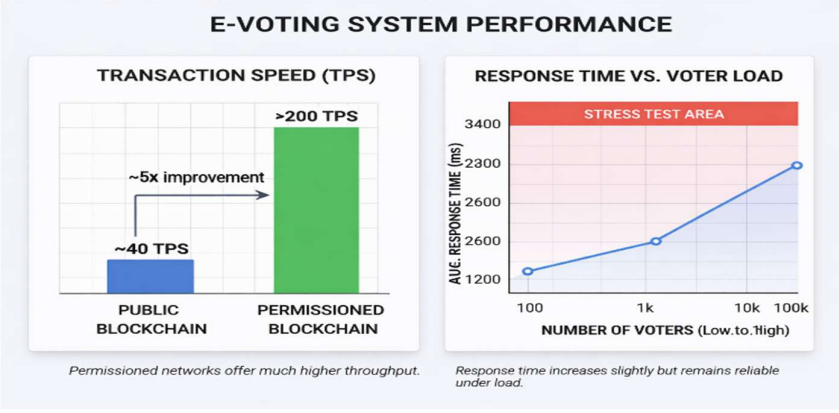

Fig. 9. Illustrating the performance characteristics of our e-voting system.

6 Conclusion

To sum it up, the present paper had the opportunity to develop and propose a blockchain-based electronic voting system with a decentralized structure and smart contracts. The system provides transparency and auditability by tallies that can be publicly verified, security and privacy with homomorphic encryption and ring signatures, and scalability and high load performance. Our review confirms that there is a great deal of success in functionality and usability and challenges like reliance on identity systems and expense will persist. All in all, this system gives a foundation to safe, verifiable and inclusive online voting. The overall objective is to build a developing system which is scalable, reliable and accessible. Future: The areas covered in the future are decentralized identity, biometric and multi-factor authentication, gas optimization with Layer-2

solutions, existing infrastructures interoperability, privacy with advanced cryptography, regulatory compatibility, user-centric, and real-life pilot deployments to test the system at scale.

References

1. Alvi, S.T., Uddin, M.N., Islam, L.: Digital voting: A blockchain-based e-voting system using biohash and smart contract. In: 3rd International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 228–233 (2020)
2. Taş, R., Tanrıöver, Ö.Ö.: A systematic review of challenges and opportunities of blockchain for evoting. Symmetry 12(8), 1328 (2020)
3. Al-Madani, A.M., Gaikwad, A.T., Mahale, V., Ahmed, Z.A.T.: Decentralized e-voing system based on smart contract by using blockchain technology. In: International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), pp. 176–180 (2020)
4. Garg, K., Saraswat, P., Bisht, S., Aggarwal, S.K., Kothuri, S.K., Gupta, S.: A comparative analysis on e-voting system using blockchain. In: 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1–4 (2019)
5. Alam, A., Rashid, S.M.Z.U., Salam, M.A., Islam, A.: Towards blockchain-based e-voting system. In: International Conference on Innovations in Science, Engineering and Technology (ICISET), pp. 351–354 (2018)
6. Farooq, M.S., Iftikhar, U., Khelifi, A.: A framework to make voting system transparent using blockchain technology. IEEE Access 10, 59959–59969 (2022)
7. Al-Maaitah, S., Qatawneh, M., Quzmar, A.: E-voting system based on blockchain technology: A survey. In: International Conference on Information Technology (ICIT), pp. 200–205 (2021)
8. Abuidris, Y., Kumar, R., Wang, W.: A survey of blockchain-based e-voting systems. In: 2nd International Conference on Blockchain Technology and Applications, pp. 99–104 (2019)
9. Hanifatunnisa, R., Rahardjo, B.: Blockchain-based e-voting recording system design. In:11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–6 (2017)
10. Khan, K.M., Arshad, J., Khan, M.M.: Secure digital voting system based on blockchain technology. International Journal of Electronic Government Research 14(1), 53–62 (2018)
11. Khan, K.M., Arshad, J., Khan, M.M.: Investigating performance constraints for blockchain-based secure e-voting system. Future Generation Computer Systems 105, 13–26 (2020)
12. Ayed, A.B.: A conceptual secure blockchain-based electronic voting system. International Journal of Network Security and Its Applications 9(3), 1–9 (2017)
13. Alvi, S.T., Uddin, M.N., Islam, L., Ahamed, S.: DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system. Journal of King Saud University – Computer and Information Sciences 34(9), 6855–6871 (2022)
14. Huang, J., He, D., Obaidat, M.S., Vijayakumar, P., Luo, M., Choo, K.K.R.: The application of blockchain technology in voting systems: A review. ACM Computing Surveys 54(3), 1–28 (2021)
15. Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system—review and open research challenges. Sensors 21(17), 5874 (2021)
16. Fusco, F., Lunesu, M.I., Pani, F.E., Pinna, A.: Crypto-voting, a blockchain-based e-voting system. In: International Conference on Knowledge Management and Information Systems (KMIS), pp. 221–225 (2018)
17. Adiputra, C.K., Hjort, R., Sato, H.: A proposal of blockchain-based electronic voting system. In: 2nd World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 22–27 (2018)
18. Berenjestanaki, M.H., Barzegar, H.R., Ioini, N.E., Pahl, C.: Blockchain-based e-voting systems: A technology review. Electronics 13(1), 17 (2024)
19. Yu, B., Liu, J.K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., Au, M.H.: Platform-independent secure blockchain-based voting system. In: International Conference on Information Security, pp. 369–386 (2018)
20. Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M., Hjálmtýsson, G.: Blockchain-based e-voting system. In: IEEE International Conference on Cloud Computing (CLOUD), pp. 983–986 (2018)