SN Computer Science (2024) 5:921
https://doi.org/10.1007/s42979-024-03286-2

ORIGINAL RESEARCH

Enhancing Security and Transparency in Online Voting through Blockchain Decentralization

Inderpreet Singh[1] · Amandeep Kaur[1] · Parul Agarwal[2] · Sheikh Mohammad Idrees[3]

Received: 18 May 2024 / Accepted: 2 September 2024

Abstract

Most existing e-government services are centralized and rely heavily on human control. This centralized approach makes the system more susceptible to external attacks and compromises data integrity by rogue insiders. Additionally, relying on individuals to monitor and control workflows introduces errors and corruption risks. In order to guarantee security and transparency, this study proposes an automated and decentralized online voting system that makes use of blockchain technology. Compared to conventional voting techniques, it is more efficient and cost-effective, because it eliminates the need of intermediaries. The primary goal of this research is to use blockchain technology to develop a transparent and safe online voting system. In this paper, a decentralized voting system will be developed utilizing ethereum blockchain and smart contracts to ensure the voting process's integrity. The system can be evaluated with simulated voting data to reflect real-world scenarios, focusing on security, scalability, and user-friendliness. The study also explores potential future enhancements, such as incorporating biometric authentication to further improve accessibility and security. The insights provided will be valuable to policymakers, researchers, and practitioners involved in the development, implementation, and regulation of blockchain-based voting systems.

Keywords Blockchain · Cryptography · Electronic voting · Smart contracts

Introduction

Voting is the heart of democracy. Through voting, individuals exercise their right to voice their opinions, shape the direction of governance, and elect representatives who align with their values and aspirations. To guarantee fairness and credibility in every stage of the election process, we must ensure security and reliability [7]. In India, the electoral process initially relied on the use of ballot papers for voting. This traditional method involved distributing paper ballots to eligible voters, who then marked their choices by hand. Counting the votes cast on ballot papers was another meticulous process. The election process was significantly delayed as a result of the hand counting of the majority of these voting papers. Allegations of booth capture were made in various constituencies. Electronic voting machines (EVMs) were launched in the 1990s as a solution to the issues [2]. The election process is completed much faster thanks to electronic voting machines (EVMs), which show the entire number of votes cast for each candidate in a given area. EVM machines are brought to a safe area where the total votes are collected in front of the election commission and the political party representatives in order to achieve the final result. While there is ongoing discussion over the security mechanism of EVM machines [23].

Blockchain-powered decentralized internet voting platforms provide an open, safe, and effective electioneering environment [1]. By utilizing the decentralization and immutability that come with blockchain technology, these solutions seek to improve voting process integrity and confidence. Eligible voters can safely cast their ballots using cryptographic methods, and those votes are then documented as transactions. These solutions save expenses and simplify the voting process

✉ Amandeep Kaur
amandeep.gtbit@gmail.com

✉ Sheikh Mohammad Idrees
sheikh.m.idrees@ntnu.no

[1] Guru Tegh Bahadur Institute of Technology, New Delhi, India

[2] Department of Computer science, Jamia Hamdard, New Delhi, India

[3] Department of Computer Science (IDI), Norwegian University of Science and Technology, 2815 Gjøvik, Norway

Published online: 30 September 2024

by doing away with middlemen, increasing accessibility and inclusivity. Decentralized online voting systems have the potential to completely transform elections by guaranteeing democratic participation, security, and transparency even though there are still obstacles to overcome [1, 5, 22].

Early in the decade of the 2010s saw the introduction of decentralized online voting systems powered by blockchain technology [1, 6]. Around this time, the idea of using blockchain technology for voting started to gain traction. The rise of cryptocurrencies like Bitcoin demonstrated the transparency and security of blockchain technology [1, 5]. In 2014, Follow My Vote published a seminal paper introducing a blockchain-based voting platform, igniting further research and advancements in the field. Over the years, numerous studies and experiments have been conducted to evaluate the feasibility and efficacy of decentralized online voting systems [1].

In general, the importance of decentralized online voting systems based on Blockchain technology is in their ability to respect the values of inclusivity, security, transparency, and trust—thus fortifying democratic processes and guaranteeing impartial and trustworthy elections [25].

The primary goals of electronic voting technology are to decrease expenses related to manual vote tallying, expedite the ballot counting process, and increase voter inclusion for voters with disabilities. To accomplish this goal, a software platform for voter registration, voting in elections, compiling and tracking election results in real-time, and—most importantly—enabling remote voting can be designed and developed. To protect against external breaches, Blockchain technology will be utilized in this endeavor to examine and build a security strategy that guarantees the integrity and invulnerability of votes within the system [2, 6, 11].

This paper aims to provide a comprehensive analysis of the research landscape surrounding decentralized online voting systems. The evolution of these systems, the challenges they face, and the potential they hold for revolutionizing electoral processes has been examined. Additionally, this paper delves into recent developments, emerging trends, and future directions in this rapidly evolving field. By synthesizing existing literature, techniques and discussing key findings, it seeks to contribute to the ongoing discourse on the design, implementation, and regulation of blockchain-based voting systems. Through this analysis, the paper aims to provide insights that inform policymakers, researchers, and practitioners in their efforts to promote secure, transparent, and inclusive democratic practices.

Literature Review

A lot of research was conducted before starting the project, which includes numerous research papers. Electronic voting has become a hot topic for researchers and policymakers who want to improve the integrity and efficiency of elections. The use of blockchain technology in e-voting systems has gained attention because it can address security, transparency, and trust issues [1, 3, 11].

The research on blockchain-based voting Dapps is quite extensive, covering various aspects such as security, usability, scalability, transparency, trustworthiness, regulatory challenges, and privacy features [1]. In a nutshell, the Table 1 below provides a summary of important discoveries and approaches from different sources, giving the insights into the progress made, obstacles f. aced, and potential future developments in the fusion of blockchain technology and the electoral system.

The study focuses on security, usability, scalability, transparency, trustworthiness, impact on election integrity, review of existing voting Dapps, privacy features, and regulatory challenges of implementing blockchain in voting [8]. The authors have identified vulnerabilities in X voting Dapps, proposed security enhancements, and explored user concerns about complexity [8, 15]. They also assessed the scalability of blockchain for large-scale voting, identifying challenges in handling high transaction volumes and proposing scalability solutions [9, 10]. The study also examined the transparency and trustworthiness of blockchain voting systems, highlighting the need for complete anonymity [10, 12]. The study also examined the impact of blockchain on election integrity, demonstrating potential in preventing fraud and ensuring tamper-proof records. It further explored the privacy feature of blockchain in voting systems, highlighting the benefits but challenges in implementation [14]. The study concluded that blockchain provides enhanced privacy compared to traditional voting systems but faces challenges in implementation [15].

Proposed Methodology

Using Ethereum Blockchain technology, a decentralized voting system is to be developed as part of the suggested strategy [1]. The voting process will be managed and its integrity ensured using smart contracts. To replicate real-world events, the datasets used in this will be made up of simulated vote data. It will also contain a review of the system's usability, scalability, and security performance. In order to increase security and accessibility, biometric authentication may be integrated in future updates.

Through the integration of blockchain technology with e-voting, we propose multiple alternatives for the secure e-voting process. The voting events are created and managed by the online application [13].

To make this application, we use the Ethereum blockchain platform (Remix IDE). We will use the Solidity language to write all the logic and code. Solidity is a

Table 1 Summary of literature review

Ref. No.	Year	Objective /purpose	Methodology/approach	Key findings
[1]	2011	It aims to develop and evaluate an online voting system by integrating the Internet of Things (IoT) and the Ethereum blockchain	It involve integrating IoT devices for secure and verifiable voter authentication, deploying smart contracts on the Ethereum blockchain to facilitate the voting process, and testing the system's overall functionality and security	It highlight how IoT devices contribute to secure voter identification and how the Ethereum blockchain ensures the integrity and transparency of the voting process
[2]	2017	Investigating the impact of blockchain voting on election integrity	Comparative analysis of blockchain and traditional voting systems	Blockchain demonstrated potential in preventing fraud and ensuring tamper-proof records
[3]	2018	Investigation the feasibility and benefits of utilizing Ethereum's blockchain and smart contract capabilities	It includes creating and deploying Ethereum smart contracts to handle voting processes, ensuring the security and transparency of the system	It highlight the advantages and challenges encountered during the development process, emphasizing the impact of Ethereum smart contracts on the voting system
[4]	2018	Addressing challenges in traditional voting systems through the application of blockchain and cryptographic techniques	It involve designing and deploying smart contracts to facilitate the voting process, testing the application's functionality, and evaluating its performance in terms of security and user experience.	The study highlights the advantages of decentralized and tamper-resistant ledger systems in ensuring the integrity of the voting process
[5]	2018	Addressing challenges in traditional voting systems through the application of blockchain and cryptographic techniques	Include designing and testing the system, assessing its resilience to tampering, and evaluating the cryptographic techniques	Include the system's ability to ensure the integrity and confidentiality of votes, as well as the overall transparency achieved through blockchain technology
[6]	2019	It includes smart contract development, user interface design, and interaction with the Ethereum network	It includes smart contract development, user interface design, and interaction with the Ethereum network.	It tells insights of the development process of Ethereum Dapps
[7]	2019	It aims to implement and address security issues in a mobile voting decentralized application	It include testing the DApp's features, assessing its usability, and identifying and addressing security concerns.	It highlight challenges encountered during the implementation and provide recommendations or solutions to address security concerns in the context of mobile voting
[8]	2019	It aims to develop and demonstrate the feasibility of a transparent e-voting decentralized application using Waves blockchain and the RIDE programming language	It involve deploying smart contracts or utilizing the unique features of the Waves blockchain for secure and transparent voting.	It highlights the advantages and unique characteristics of the selected blockchain and programming language for electronic voting
[9]	2019	It aims to design and implement a decentralized e-voting portal utilizing blockchain technology.	It involve deploying smart contracts on a blockchain platform to secure and automate the voting process, testing the portal's functionality, and evaluating its performance in terms of security and transparency.	It highlight the advantages of using blockchain technology to ensure tamper-resistant records and automate various aspects of the voting process
[10]	2019	Examine the transparency and trustworthiness of blockchain voting system	Case studies and blockchain analysis	Blockchain enhanced transparency, but challenges with ensuring complete anonymity
[11]	2019	Evaluate the security of blockchain-based voting Dapps	Evaluate the security of blockchain-based voting Dapps	Identified vulnerabilities in X voting Dapp, proposed security enhancements
[12]	2020	Investigate the usability of blockchain in online voting systems	User surveys and usability testing	Users expressed concerns about complexity; suggested user-friendly interfaces

Table 1 (continued)

Ref. No.	Year	Objective /purpose	Methodology/approach	Key findings
[13]	2020	It aimed to measure the average expenses incurred by both voters and the election committee during transactions, using smart contracts and related technologies	The smart contract was deployed on the Ethereum platform. Several transactions were executed to evaluate real-time cost distribution. The cost analysis focused on the linear relationship between the election committee's expenses and the number of voters, revealing a constant voting cost	The study tells, linear increase in the election committee's costs proportional to the number of voters, while the voting cost remained consistent
[14]	2020	To develop and evaluate the feasibility of a decentralized E-voting system	Deployeing a decentralized E-voting system on a blockchain platform like Etherium	It demonstrated the advantages of a decentralized E-voting system, emphasizing the secure and transparent nature of the process facilitated by smart contracts
[15]	2020	To develop and assess the feasibility of an Electronic Voting System integrating Blockchain technology and Aadhaar, aiming to enhance the security, transparency, and inclusivity of the voting process	Implementing a prototype of the Electronic Voting System using a combination of Blockchain technology and Aadhaar authentication	It demonstrated the integration's effectiveness, highlighting the enhanced security features from blockchain and the unique identification capabilities provided by Aadhaar
[16]	2020	It aims to implement and evaluate a blockchain-based e-voting system using Ethereum and Metamask	It include designing and deploying smart contracts, testing the system's functionality, and evaluating its performance in terms of security and user experience	It includes insights into the effectiveness of using Ethereum and MetaMask in the e-voting system
[17]	2021	Assess the scalability of blockchain for large-scale voting	Assess the scalability of blockchain for large-scale voting	Blockchain faced challenges in handling a high volume of transactions; proposed scalability solutions
[18]	2021	Access the privacy feature of blockchain in voting system	Privacy impact assessments and blockchain analysis	Blockchain provided enhanced privacy compared to traditional voting systems, but challenges in implementation
[19]	2021	A blockchain-based voting system, focusing on enhancing security, transparency, and integrity in the voting process	Integrate blockchain technology, implement smart contracts, and employ security measures to create the BCT-voting system	The BCT-voting system demonstrates heightened security, improved transparency, and usability, showcasing the impact of blockchain technology on enhancing the voting process
[20]	2021	It aims to design and implement a decentralized voting platform based on the Ethereum blockchain	It involve developing and deploying smart contracts to handle the voting process, integrating user interfaces for interaction, and evaluating the system's performance in terms of security and transparency	It showcase improvements in security, transparency, and user engagement, demonstrating the advantages of utilizing Ethereum blockchain for electronic voting
[21]	2022	It aims to develop and evaluate a secure and anonymous voting decentralized application (D-App) that incorporates IoT embedded devices	It involve integrating IoT devices for secure voter identification and authentication, deploying smart contracts on the blockchain to ensure transparency and integrity, and evaluating the D-App's functionality and security	It explores how IoT devices contribute to secure and anonymous voter identification and how the blockchain ensures the transparency and tamper-resistance of the voting process
[22]	2022	Exploration of a voting decentralized application	Implementing a DApp for voting purposes, potentially involving blockchain technology, smart contracts, and user interfaces	It addresses security aspects related to the Voting DApp, covering potential vulnerabilities and proposing solutions to ensure the integrity and confidentiality of the voting process
[23]	2022	It aims to design and evaluate a secure electronic voting system based on various platforms	It could involve testing the system's security features, usability, and performance across different platforms to validate its effectiveness	The study presents the findings on the effectiveness of the electronic voting system, emphasizing its security measures and adaptability to various platforms
[24]	2023	Review existing blockchain based voting Dapp	Literature review and case analysis	Identified common features and challenges in existing voting Dapps; proposed future research directions

Table 1 (continued)

Ref. No.	Year	Objective /purpose	Methodology/approach	Key findings
[25]	2023	Explore the regulatory challenges of implementing blockchain in voting	Legal analysis and case studies	Identified legal and regulatory barriers; proposed policy recommendations

high-level, object-oriented language influenced by various programming languages and is designed to integrate with the Ethereum Virtual Machine (EVM). In Solidity, we write smart contracts, which are self-executing contracts similar to real-world contracts, but digital. Smart contracts enable secure and trusted transactions. They are stored on the blockchain, which ensures immutability and global distribution. Because they are immutable, if someone tries to alter a smart contract, it will be marked as invalid, making tampering almost impossible.

The Election Commision stores the information such as Adhaar Card number, Pan Card number, Voter Id, Voter Retina bytecode (Encrypted) etc. These details are carried in a dataset and maintained.

To check all the information of the voter, we use a government dataset. Government datasets contain information about citizens, such as their personal details, contact information, medical details, education details, and many more. These datasets contain a lot of information, and accessing all of this information at once can create redundancy and data leak problems. Therefore, for this application, the election commission will have access only to the necessary information of the voter, such as contact details, education details, and some private information like date of birth, name, age etc. We can also use biometric and fingerprint information for user authentication, such as verifying whether a voter is registered or eligible to vote or not. Biometric and fingerprint information are very sensitive data of the candidate. Therefore, we can use cryptographic techniques to maintain their integrity and security.

The voting events takes place through a web application, where the voter is allowed to cast a vote from anywhere. Firstly, the voter authentication and authorization takes place. For authentication, voter has to submit its details such as adhaar card number and other necessary information such as name, age, gender, date of birth. When voter submit this information security mechanism starts and takes the retina scan of the voter. This security mechanism makes the bytecode from the retina scan and then send it to the server from where the encrypted retina bytecode matches with already stored bytecode from the government dataset. If the bytecode matches, voter lands on the main page from where it can cast and polls the vote.

This solution's primary contribution is preventing duplicate polled votes by maintaining the voting data's confidentiality and storing it in blockchain blocks. Through the use of a web application, it creates data integrity, data immutability, and the ability to receive the most votes possible [18, 22].

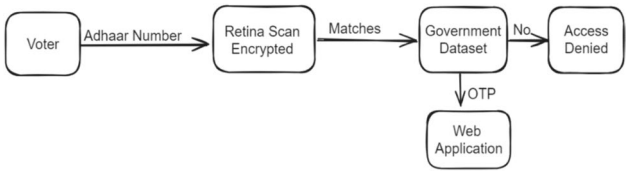

Fig. 1 Passing security mechanism

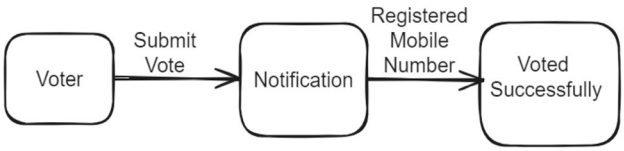

Fig. 2 Vote notification

Implementation

Stage 1–Passing Security Mechanism

Before participating in the voting process, candidates must pass the security mechanism. To pass the security mechanism, candidates must mention their identification ID (Aadhaar Card number, PAN Card number, Driving License). Then, the application will take a retina scan from the candidate's device and generate a bytecode. If this bytecode matches with the already stored bytecode in the government dataset, then an OTP will be sent to the user's registered phone number, and after entering it, the user will land on the Voting page. If the match is unsuccessful, further candidate access would be denied as shown in Fig. 1.

Stage 2–All Voters Cast Their Votes

Now the voters review the information provided about each candidate, which may include their names, affiliations, and brief descriptions like their education, experiences etc. Based on their preferences and opinions, voters select the candidate they wish to support and then voters submit their votes electronically. After submitting vote, voters will get a voting confirmation notification (Fig. 2).

Stage 3–Result Released by Election Commission Committee

After a successful vote-casting process, the counting of votes for the candidates will start. All candidates and voters will get notification from the Election Commission as soon as the results are known (Fig. 3).

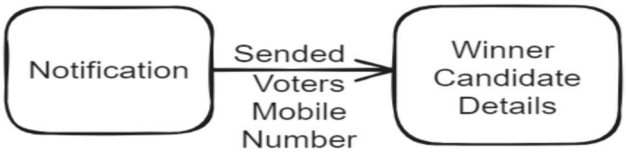

Fig. 3 Result notification

Table 2 Year wise distribution of literature review papers

0	Year of publication	Number of papers
1	2017	2
2	2018	4
3	2019	6
4	2020	6
5	2021	6
6	2022	1
7	2023	2

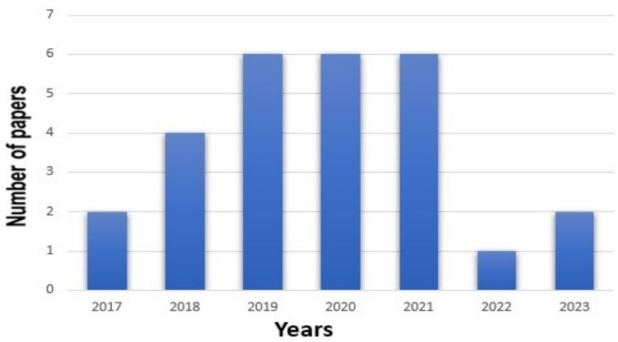

Fig. 4 Paper published as per year

Results and Discussions

The provided data in the Table 2 below presents the distribution of research papers related to blockchain-based voting systems over a period of seven years, from 2017 to 2023. The number of papers on blockchain-based voting systems has shown a generally increasing trend over the years, with a notable rise from 2018 onwards.

The highest number of papers were published in 2019, 2020, and 2021, indicating a peak period of research interest in this domain during these years. The surge in publications from 2018 to 2021 as shown in Fig. 4 below could be attributed to increased awareness and interest in blockchain technology and its potential applications in voting systems.

Blockchain technology finds application across various domains, offering solutions that enhance transparency, security, and efficiency. Specifically, its integration

into critical areas such as government elections, corporate governance, proxy voting, and decentralized organizations demonstrates its versatility and potential impact [1–3, 7, 14, 26]. The utilization of Blockchain technology, particularly Ethereum, in the creation and execution of an online voting system holds immense potential to transform the way elections are conducted. Smart contracts and the elimination of intermediaries, as revealed through extensive research, can enhance transparency and security while minimizing manipulation chances. Although the feasibility of this system has been demonstrated through simulated voting data, it is imperative to conduct real-world testing to comprehensively evaluate its performance. The evaluation of the system's security, scalability, and usability has successfully identified its strengths and areas that require further enhancement [24].

Challenges in Implementation

Even though smart contracts have numerous benefits, there are drawbacks including unanticipated events and coding weaknesses. This section examines the body of research on e-voting Dapps' ability to mitigate these issues [1]. Blockchain-based decentralized online voting systems have many benefits, but their successful deployment will require addressing a number of issues. The following are some major obstacles:

Scalability

When handling a high number of votes, the scalability of Blockchain technology may encounter challenges, particularly in public Blockchains. Finding strategies to keep things running as quickly and as well as possible when processing large transaction loads is essential [1].

Privacy

It might be difficult to strike a compromise between voter privacy and transparency. Voters' identities and preferences may be revealed by Blockchain, even if it guarantees transparency and immutability [14]. To protect voter privacy, privacy-preserving methods such as secure encryption and zero-knowledge proofs must be developed [3].

Adoption and Usability

It might be difficult to promote the widespread use and acceptance of decentralized online voting systems among voters, election officials, and other stakeholders. Gaining widespread acceptance requires educating consumers about the features, security precautions, and ease of use [3].

Security Risks

Even with the increased security offered by blockchain technology, no system is impenetrable to attackers. Ensuring the legitimacy of the voting process requires identifying and mitigating potential vulnerabilities like as 51% attacks, double-spending, or manipulation of smart contracts [1, 12, 27].

Voter Coercion and Bribery

Voter coercion or vote buying, in which voters are persuaded to cast a particular ballot, is a concern associated with online voting. Maintaining the integrity and fairness of elections requires the design of systems that are capable of identifying and stopping such activities [1, 11, 23].

Slow Development

Blockchain technology is complex, so building applications often requires extensive research, development, and validation. As a result, a lack of clarity about the requirements can create significant risks for users.

Conclusion and Future Enhancements

The analysis of the data on the publication of research papers related to blockchain-based voting systems reveals a dynamic landscape characterized by fluctuations in research output over the years. The findings indicate a notable increase in research interest and publications from 2018 to 2021. The initial surge in publications could be attributed to heightened awareness and enthusiasm surrounding blockchain technology and its potential applications in enhancing the security, transparency, and integrity of voting systems. Despite the fluctuations observed, the overall trajectory indicates sustained interest and potential for further exploration and innovation in blockchain-based voting systems. The decline in research output in recent years underscores the need for continued efforts to address challenges such as scalability, usability, regulatory barriers, and privacy concerns to foster the development and adoption of more robust and practical voting solutions based on blockchain technology.

Shifting towards blockchain platforms is currently not feasible due to their high costs and complexity of implementation. Additionally, moving entirely to blockchain-based e-voting is not currently possible. To achieve this, we need to take the first step of testing and implement these applications on a small scale. This will allow us to gather data for analysis and improve the technology over time. The main challenge is encouraging people to adopt these platforms and giving them the experience and power to control their privacy using blockchain technology. Since e-voting and

cryptocurrency are not the only applications of blockchain, there are many more to explore. These initial efforts will help the next generation advance to the next step.

Moving forward, future research endeavors should focus on addressing these challenges while also exploring emerging technologies and methodologies to advance the state-of-the-art in blockchain-based voting systems. By doing so, researchers, policymakers, and practitioners can contribute to the development of more secure, transparent, and inclusive electoral processes that uphold the principles of democracy and ensure the integrity of democratic institutions.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital).

Declarations

Conflict of interest The authors declare that they have no conflict of interest to declare.

Research Involving Human and /or Animals Not applicable.

References

1. Lee JH. Systematic approach to analyzing security and vulnerabilities of blockchain systems. Doctoral dissertation, Massachusetts Institute of Technology; 2019.
2. Riedlberger K. The impact of blockchain technology on the trustworthiness of online voting systems. http://hdl.handle.net/10362/106854
3. Zhang S, Wang L, Xiong H. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. Int J Inf Secur. 2020;19:323–41.
4. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress); 2017 (pp. 557–564). IEEE.
5. Hyvärinen H, Risius M, Friis G. A blockchain-based approach towards overcoming financial fraud in public sector services. Bus Inform Syst Eng. 2017;59:441–56.
6. Tanwar S, Gupta N, Kumar P, Hu YC. Implementation of blockchain-based e-voting system. Multimedia Tools Appl. 2024;83(1):1449–80.
7. Stach C, Gritti C, Przytarski D, Mitschang B. Assessment and treatment of privacy issues in blockchain systems. ACM SIGAPP Appl Comput Rev. 2022;22(3):5–24. https://doi.org/10.1145/3570733.3570734.
8. Gupta R, Sharma A, Prasad VS, Alatba SR, Singh DP, Shingadiya CJ. A voting system using block chain a deep survey. In: 2023 3rd international conference on advance computing and innovative technologies in engineering (ICACITE); 2023 (pp. 556–561). IEEE.
9. Abuidris Y, Kumar R, Yang T, Onginjo J. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI J. 2021;43(2):357–70.
10. Al-Madani AM, Gaikwad AT, Mahale V, Ahmed ZA. Decentralized E-voting system based on smart contract by using Blockchain Technology. In: 2020 international conference on smart innovations in design, environment, management, planning and computing (ICSIDEMPC); 2020 (pp. 176–180). IEEE.
11. Tyagi AK, Fernandez TF, Aswathy SU. Blockchain and aadhaar based electronic voting system. In: 2020 4th international conference on electronics, communication and aerospace technology (ICECA); 2020 (pp. 498–504). IEEE.
12. Varaprasada Rao K, Panda SK. Secure electronic voting (E-voting) system based on blockchain on various platforms. In: Computer communication, networking and IoT: proceedings of 5th ICICC 2022, Volume 2 (pp. 143–151). Singapore: Springer Nature Singapore.
13. Fusco F, Lunesu MI, Pani FE, Pinna A. Crypto-voting, a Blockchain based e-Voting System. In: KMIS; 2018 (pp. 221–225).
14. Shukla S, Thasmiya AN, Shashank DO, Mamatha H. Online voting application using ethereum blockchain. In: 2018 international conference on advances in computing, communications and informatics (ICACCI); 2018 (pp. 873–880). IEEE.
15. Othman AA, Muhammed EA, Mujahid HK, Muhammed HA, Mosleh MA. Online voting system based on iot and ethereum blockchain. In: 2021 international conference of technology, science and administration (ICTSA); 2021 (pp. 1–6). IEEE.
16. Patidar K, Jain S. Decentralized e-voting portal using blockchain. In: 2019 10th international conference on computing, communication and networking technologies (ICCCNT); 2019 (pp. 1–4). IEEE.
17. Toma C, Popa M, Boja C, Ciurea C, Doinea M. Secure and anonymous voting D-App with IoT embedded device using Blockchain Technology. Electronics. 2022;11(12):1895.
18. Faour N. Transparent E-voting dApp based on waves blockchain and RIDE language. In: 2019 XVI international symposium problems of redundancy in information and control systems (REDUNDANCY); 2019 (pp. 219–223). IEEE.
19. Kherlen N, Park JB, Park JS. A mobile voting DApp implementation and security issues. In: Proceedings of the Korean institute of information and commucation sciences conference; 2019 (pp. 290–292). The Korea Institute of Information and Commucation Engineering.
20. Rai A. Voting Dapp. PhD diss., SRM UNIVERSITY, 2022. (Thesis).
21. Raikar D, Vatsa A. BCT-voting: a blockchain technology based voting system. In: The 27 th international conference on parallel and distributed processing techniques and applications (PDPTA'21); 2021 (pp. 26–29).
22. Pramulia D, Anggorojati B. Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask. In: 2020 international conference on informatics, multimedia, cyber and information system (ICIMCIS); 2020 (pp. 18–23). IEEE.
23. Infante R. Building Ethereum Dapps: decentralized applications on the Ethereum blockchain. Simon and Schuster; 2019.
24. Chaudhary A, Chauhan N, Kumar A. Decentralized voting platform based on Ethereum blockchain. In: 2021 international

conference on advances in electrical, computing, communication and sustainable technologies (ICAECT); 2021 (pp. 1–4). IEEE.
25. Thanekar GS. Decentralized voting application using Ethereum smart contract (Doctoral dissertation, University of Mumbai) (Thesis).
26. Idrees SM, Aijaz I, Jameel R, Nowostawski M. Exploring the blockchain technology: issues, applications and research potential. Int J Online Biomed Eng. 2021;17(7):48–69.
27. Idrees SM, Nowostawski M, Jameel R, Mourya AK. Security aspects of blockchain technology intended for industrial applications. Electronics. 2021;10(8):951.