Meta-analysis of blockchain-powered electronic voting systems

Vijaya Kittu Manda[1*], and *Madhu* Bhukya[2]

[1]BEST Innovation University, Gorantla, India
[2]KG Reddy College of Engineering & Technology, Hyderabad, India

Abstract. Electronic voting systems are increasingly becoming popular globally for political and non-political purposes. The three key constraints for lack of trust in e-voting systems are security, transparency, and voter privacy. Blockchain is a promising technology that addresses these needs. This study uses a meta-analysis approach to identify key themes, trends, and considerations from current blockchain-based electronic voting system research. The study lists topics that are of potential future research interest and benefit various stakeholders, including researchers, government agencies, election commissions, and electoral bodies.

1 Introduction

Electronic Voting Systems, or e-voting systems, are increasingly being adopted by various countries globally. Countries like Germany, Russia, Estonia, and Switzerland have already begun using them in mainstream political elections, while several other countries have plans at various stages for such implementations. E-voting systems are mission-critical applications [1], having applications not just in political elections (such as national and local elections) but also in social media in the form of opinion polls and surveys, in jury voting in legal circles, by shareholders in corporate decision-making, in decentralized finance (DeFi) systems such as Decentralized Insurance in claim adjudication, governance proposals and pool allocation, and in decentralized governance applications like Decentralized Autonomous Organizations (DAO).

Electronic voting has several advantages: increased convenience and accessibility, faster and more accurate results, reduced costs, increased transparency, improved accessibility for voters with disabilities, and reduced invalid votes. The flip side of this includes security concerns leading to social concerns (such as interference by foreign powers, unauthorized voting, or voter disenfranchisement [2]), lack of transparency and audit-ability (end-to-end verification), digital divide, vulnerability to malware and disruption, the potential for voter coercion, loss of tradition, and tactile experience. Some critical considerations on electronic voting include the type of voting system used (online, kiosk, amongst others), needs, resources, regulations of different countries and regions, and public trust and confidence in

* Corresponding author: vijaykittu@hotmail.com

the systems. Such systems should be thoroughly tested for cybersecurity and data privacy parameters.

Blockchain technology has features that can significantly enhance the traditional voting system by reducing barriers [3] and thereby protecting privacy and voting bias. Blockchain system's decentralization and shared database features can thwart database manipulation attempts. Secure voting systems are one of blockchain's most widely proposed use cases [4]. With the Internet of Things (IoT) and 5G technology, blockchain-based voting systems will be critical in smart cities [5]. This literature review summarizes the existing academic research literature on technological concepts with beneficial social implications.

1.1 Background and Rationale

The rationale for taking up this study revolves around three reasons:
1. Traditional e-voting systems face concerns regarding security, transparency, and voter privacy.
2. With its unique features like decentralization, immutability, and transparency, blockchain technology has the potential to address these concerns in e-voting.
3. The growing adoption of e-voting systems globally and the potential benefits of blockchain suggest exploring the effectiveness of blockchain-based e-voting systems.

1.2 Research Questions

The study attempts to address the following research questions:

1. What is the current state of research on the effectiveness of blockchain-based e-voting systems in addressing security, transparency, and voter privacy concerns?
2. To what extent do existing studies demonstrate the positive or negative impacts of blockchain-based e-voting systems on these aspects?
3. Are there specific characteristics of blockchain-based e-voting systems that contribute to their effectiveness?

1.3 Inclusion/Exclusion Criteria

1.3.1 Inclusion:

1. Studies investigating the effectiveness of blockchain-based e-voting systems.
2. Studies focusing on security, transparency, and voter privacy aspects.
3. Studies published in peer-reviewed academic journals or conference proceedings.
4. Studies published within a defined timeframe (e.g., past 5 years).

1.3.2 Exclusion

1. Studies focus on other aspects of blockchain-based e-voting not related to security, transparency, or voter privacy.
2. Studies not published in peer-reviewed academic sources.
3. Opinion pieces, editorials, or book chapters.

2 Methods

2.1 Literature Search Strategy

Considering the research objective, the literature search strategy included the following:

1. **Academic Databases**: Scopus, Web of Science, IEEE Xplore, ACM Digital Library, Dimensions.ai, Google Scholar.
2. **Search Terms**: The search term "blockchain electronic voting" is used. The rationale behind the search term is that it combines terms related to "blockchain" (e.g., blockchain, distributed ledger, smart contracts) with terms associated with "e-voting" (e.g., electronic voting, online voting, digital elections). Synonyms and alternative phrases are also used to ensure broader coverage. Further refinement (in later stages) was done to include three areas of concern - security, transparency, and voter privacy.
3. **Boolean Operators**: Boolean operators like "AND" and "OR" are used to refine search results within the context of blockchain-based e-voting systems.
4. **Date Range**: Our search focused on studies published within the past five years, from 2019 to 2023, ensuring that recent advancements and developments are captured.
5. **Grey Literature**: Additionally, conference proceedings, pre-print repositories, and relevant websites of government agencies and research institutions are considered to identify potentially relevant grey literature not indexed in academic databases. This became necessary because the topic is still evolving.

2.2 Study Selection Process

A two-stage screening process is undertaken as follows:

1. **Stage 1 (Title and Abstract Screening)**: Two independent reviewers screened titles and abstracts based on pre-defined inclusion criteria. The studies had to (i) investigate blockchain-based e-voting systems, (ii) address at least one of the three key concerns (security, transparency, or voter privacy), and (iii) be published in peer-reviewed journals, conference proceedings, or reputable reports.
2. **Stage 2 (Full-Text Screening)**: Disagreements from Stage 1 were resolved through discussion. The remaining studies underwent full-text review by both reviewers to confirm they fully met the inclusion criteria and provided relevant data for analysis.

2.3 Data Extraction and Coding

Each included study extracted relevant data using a pre-defined data extraction form. This form captured information on the following parameters. The form data is exported to a spreadsheet for further analysis.

1. Author information (year, publication venue)
2. Research methodology (study design, sample size)
3. Voting system characteristics (specific type of blockchain used, security mechanisms, privacy-enhancing techniques)
4. Outcome measures related to security, transparency, and voter privacy (e.g., incidence of vote manipulation, transparency of vote counting process, anonymity of individual votes)
5. Any limitations or biases identified by the study authors

The extracted data is then coded using Zotero and MAXQDA qualitative coding software, categorizing information based on pre-defined themes and frameworks relevant to our research question and key concerns.

2.4 Quality Assessment of Studies

To assess the quality of included studies, the researchers evaluated the potential risk of bias in study design, data collection, analysis, and reporting before continuing further.

2.5 Meta-analysis Methods

While the research question primarily seeks a qualitative synthesis of current research, a dimension of meta-analysis techniques is applicable for studies that present comparable quantitative data on specific outcomes related to security, transparency, or voter privacy (e.g., the proportion of successful attacks on the voting system).

3 Results

3.1 Characteristics of Included Studies

1. **Studies included**: Table 1 shows the quantum of research studies that have been done on the topic over the years. Both Table 1 and Figure 1 show that the topic is increasingly becoming an area of research interest. Considering the availability of full papers and several other inclusion and exclusion criteria, 88 papers were selected and used in the study. Figure 2 displays connected papers generated using Litmaps.

Table 1. Search trends for the keyword "Blockchain Electronic Voting."

Academic Database	2019	2020	2021	2022	2023
Scopus	94	117	123	140	176
Web of Science	47	55	61	55	51
IEEE Xplore	47	52	67	89	108
ACM Digital Library	7107	8061	9402	8455	9517
Dimensions.ai	2877	3705	5006	6337	8022
Google Scholar	7780	9270	11100	13900	10900

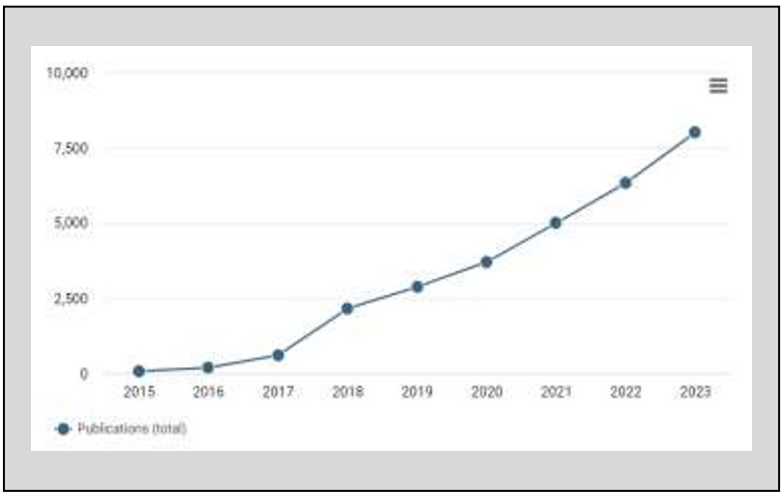

Fig. 1. Publication trends for the keyword "blockchain electronic voting" in dimensions.ai

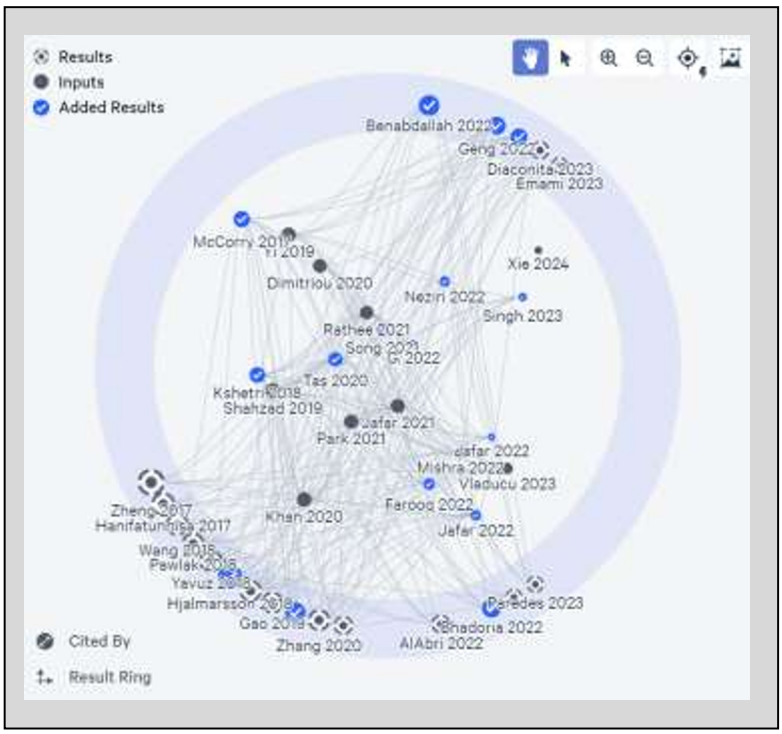

Fig. 2. Connected papers generated using Litmaps.

Table 2 lists leading researchers in the area and their affiliations. Table 3 shows the type of research publications that happened. Table 4 shows a list of leading journals that published manuscripts related to the topic.

Table 2. Leading Researchers and their affiliation

Name of Researcher	Affiliation
Andreja Pucihar	University of Maribor, Slovenia
Roger W H Bons	FOM University of Applied Sciences for Economics and Management, Germany
Mirjana Kljajic Borstnar	University of Maribor, Slovenia
Palanisamy, Balaji	University of Pittsburgh, Pittsburgh, United States
Li, Chao	Beijing Jiaotong University, Beijing, China
Mohammed Nasir Uddin	Jagannath University, Bangladesh
Neeraj Kumar	Thapar University, India
Pascal Ravesteijn	Utrecht University, Utrecht, Netherlands
Abdulah, Wan Auzan Bin W.	Universiti Teknologi MARA, Shah Alam, Malaysia
Juergen Seitz	Baden-Württemberg Cooperative State University, Stuttgart, Baden-Württemberg, Germany

Table 3. Leading Publication Types

Type of Publication
Conference Proceedings
Research Articles
Edited Book

Table 4. Leading/Influential Journals List

Name of Journal
MDPI
Journal of Information Processing Systems
IEEE Explore
International Journal of Scientific & Technology Research
Future Generation Computer Systems
Advances in Intelligent Networking and Collaborative Systems (Springer)
International Journal of Smart Home
ACM International Conference Proceeding Series
Security And Communication Networks
AIP Conference Proceedings

2. **Publication years**: The study finds that many of the research publications on the topic started in 2015 or 2017 and have rapidly gained pace since then. While early publications focused on electronic voting as a replacement for traditional general election voting, as in democratic voting, modern research papers also focused on emerging dimensions – such as decentralized finance and governance.
3. **Study design**: Most researchers use the predominant study designs, conceptual/theoretical papers, simulations, and prototypes, followed by experimental designs. Further, these studies focussed on addressing the three key issues of the electronic voting process.
4. **Geographic scope**: No geographical bias or selective coverage is being taken. Table 5 shows the list of leading countries/regions where the research is primarily done.

Table 5. Leading countries of research

List of countries/regions
People's Republic of China
India
Slovenia
United States
United Kingdom
Malaysia
Canada
Bangladesh
Indonesia
South Korea

5. **Blockchain platforms**: The study finds that Ethereum, Hyperledger Fabric, Solana, Algorand, and Voatz are the leading platforms for electronic voting infrastructure on blockchain networks. While some Governments, such as Australia, Germany, Norway, Sierra Leone, and Switzerland, use commercial systems to conduct the elections, a few other governments, such as Estonia, Russia, South Korea, and the United States (Washington D.C.) are using their proprietary systems [6].
6. **Consensus mechanisms**: Consortium blockchains are popular implementations and give the convenience of ownership to governing bodies, such as the election commission [7]. The most common consensus mechanisms followed are Consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or Byzantine Fault Tolerance (BFT) algorithms [8]. In some works, a hybrid consensus model (PSC-Bchain) composed of Proof of Credibility and Proof of Stake works mutually to address the problems of securing e-voting systems [9].
7. **Privacy-enhancing techniques (PETs)**: The study finds Blind signatures, Homomorphic encryption, Zero-knowledge proofs, Ring signatures, and Mixnets are the top PETs being used in blockchain e-voting systems.

8. **Outcome measures**: Briefly mention the outcome measures used to assess security, transparency, and voter privacy in the studies.

4 Discussion

4.1 Technical considerations

While the blockchain system handles transparency requirements, a pseudonym mechanism can be used for identity privacy, while homomorphic encryption technology can be used for ciphertext vote counting. Some implementations use a double signature in which one is used to sign the voting ciphertext and then a pseudonym to ensure the voter's identity and the vote's legitimacy [10]. Threshold blind signatures are used in a few cases, especially in voter registration, because they are better than linkable ring signatures for large group sizes [11].

With other technologies, such as face authentication techniques using Haar cascade and Support Vector Machine Algorithms, a blockchain-based voting system can address trustlessness, privacy, and security [4]. Some systems use a user credential model based on elliptic curve cryptography (ECC) to provide authentication and non-repudiation [12]. Certain protocols were designed to operate without a centralized tallying authority. In these systems, votes are submitted along with comprehensive validity proofs and deposited publicly in an encrypted format. A novel encryption mechanism ensures the confidentiality of votes while enabling anyone to verify their validity and the final tally, leveraging the homomorphic properties of the encryption scheme. This transparency empowers public verification of election results [13].

A distributed application (dApp) on an Ethereum network is an ideal setup for the e-voting system. Smart contracts built on Solidity can be used to cast votes. A Truffle framework can be used to test the deployment of smart contracts to the blockchain. Upon being examined on Ganache, the smart contract can be deployed on Ethereum platforms using tools like Geth. Wallets such as Metamask can be used for the transaction.

The voting system needs help from privacy-preserving technologies. Zero-knowledge proofs allow voters to prove their votes' validity without revealing sensitive information. Homomorphic encryption enables vote aggregation and counting on encrypted data, preserving privacy while ensuring verifiability [8].

Typical limitations of a blockchain-based voting system include accessibility and digital divide, security and vulnerabilities, privacy and anonymity, scalability and throughput, governance and consensus, legal and regulatory frameworks, voter education and trust, system audit-ability and transparency, technical expertise, and maintenance, adoption, and transition [8].

A study utilizing expert interviews from election observers and blockchain professionals highlights the crucial role of trust and human factors within the voting process despite the strengths and weaknesses inherent to blockchain technology [14]. Several expected features from a typical electronic voting system can be achieved with technology upgrades. However, certain things, such as receipt-freeness, in-coercibility, and universal verifiability, are much harder to implement, which, fortunately, some blockchain implementations claimed to have addressed [15].

4.2 Practical and Policy Implications

Six practical and policy implications arise from the findings of the study:

1. Regulatory bodies and authorities (such as Governments and election commissions) could explore implementing blockchain-based electronic voting systems to address existing security, transparency, and privacy concerns with traditional e-voting. There is clear evidence that blockchain's decentralized nature makes tamper with vote data difficult.

2. Technical standards and best practices need to be developed for blockchain e-voting systems. Areas like cryptography methods, consensus algorithms, and protocols for authentication, privacy, and verifiability require guidance.

3. Legal and regulatory frameworks must be updated to allow for new forms of e-voting and address issues like voting eligibility, system certification, auditing requirements, and dispute resolution. Existing laws may need modifications.

4. Voter education will be essential to build trust in new technologies. Pilot programs and social media/awareness campaigns can help voters understand how blockchain e-voting works and why it improves over previous e-voting methods.

5. International cooperation is important as many studies are conducted globally. Standardization efforts and guidelines developed across different administrations can help the proliferation of best practices.

6. Accessibility still needs to be addressed as the digital divide remains. Alternative voting methods may still be required for those unable to vote online/digitally. Hybrid online-offline models could help enhance inclusion.

4.3 Future Research Directions

Researchers highlight five potential areas that have scope for future research. These include:

1. **Scalability and Performance**: The scalability and performance of a blockchain system can be measured in the dimensions of block generation rate, transaction speed, and block size [16]. Limitations that arise from the current blockchain technology may negatively impact when the system is used for large-scale elections, such as that of India, where there are 945 million voters as of January 1, 2024, as per Election Commission of India (ECI) data. The limitations arise due to limited transaction throughput and processing power. Future research should explore scalability solutions like layer-2 protocols, sharding, or hybrid blockchain-traditional voting system approaches.

2. **Privacy-Enhancing Techniques**: While blockchain offers transparency, ensuring individual voter privacy remains crucial. Future research can explore some advances in cryptographic techniques, such as zero-knowledge proofs, ring signatures, and homomorphic encryption, to strengthen privacy guarantees without compromising verifiability.

3. **Usability and Accessibility**: Integrating blockchain with existing voting infrastructure and systems and ensuring user-friendliness is important. This is because the application will be used by a diverse population with little or no technical knowledge of the implementation and operational aspects. The concept of the user interface for distributed applications (dApps) is still in its infancy. Research should focus on intuitive interfaces, accessibility for voters with disabilities, and integration with existing voter authentication mechanisms.

4. **Standardization and Regulations**: Clear standards and regulations are needed for secure and consistent implementation across different jurisdictions. Research should explore collaborative efforts to develop interoperable standards, define legal frameworks for e-voting, and address data protection concerns. This also requires debates and amendments to existing laws.

5. **Long-Term Security and Maintenance**: Blockchain systems require ongoing maintenance and upgrades to address evolving security threats and technological advancements. Flaws in internet and polling systems on one side and the blockchain's need for software architecture and managerial expertise on the other are considered leading deterrents [17]. Hence, research should explore sustainable funding models, secure maintenance procedures, and long-term security guarantees for blockchain-based voting systems.

5 Conclusion

This literature review analyzed and synthesized prior research that went into developing and applying the concept of electronic voting systems using blockchain technology. The study identified various blockchain-based approaches and their ability to enhance security, transparency, and voter privacy. However, as the study finds, additional research is still needed to realize the full potential of the use case/application. In particular, scalability and performance must be improved to handle large-scale elections. More work is also required to develop advanced privacy-enhancing techniques, intuitive user interfaces, and international standardization efforts. Long-term maintenance and ongoing security also present challenges that future research could help address. As the technology progresses, blockchain has the potential to improve trust and participation in electronic voting worldwide substantially. Further research pursuing these open directions would help strengthen democratic processes globally.

References

1. J. C. L. A. De Farias, A. Carniel, J. De Melo Bezerra, and C. M. Hirata, “Approach based on STPA extended with STRIDE and LINDDUN, and blockchain to develop a mission-critical e-voting system,” *Journal of Information Security and Applications*, vol. 81, p. 103715, Mar. 2024, doi: 10.1016/j.jisa.2024.103715.
2. S. Park, M. Specter, N. Narula, and R. L. Rivest, “Going from bad to worse: from Internet voting to blockchain voting,” *Journal of Cybersecurity*, vol. 7, no. 1, p. tyaa025, Feb. 2021, doi: 10.1093/cybsec/tyaa025.
3. R. Ahmed, “The Future of Electronic Voting System Using Blockchain,” *International Journal of Scientific & Technology Research*, vol. 9, no. 02, 2020.
4. J. Anitha, M. S. L. Priya, and V. V. Chamundeeswar, “E-voting system with secure blockchain alert on data tampering,” in *Artificial Intelligence, Blockchain, Computing*

and Security Volume 2, 1st ed., 2023, p. 5. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781032684994-87/voting-system-secure-blockchain-alert-data-tampering-anitha-julian-lekshmi-priya-vijaya-chamundeeswari

5. G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities," *IEEE Access*, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.
6. M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," *IEEE Access*, vol. 11, pp. 23293–23308, 2023, doi: 10.1109/ACCESS.2023.3253682.
7. B. Shahzad and J. Crowcroft, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019, doi: 10.1109/ACCESS.2019.2895670.
8. M. K. Sahu, A. Mohite, M. M. Khakhi, M. A. Bagde, and M. K. Karale, "BlockVote: Harnessing Blockchain for Transparent E-Voting," vol. 10, no. 05, 2023.
9. Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *ETRI Journal*, vol. 43, no. 2, pp. 357–370, Apr. 2021, doi: 10.4218/etrij.2019-0362.
10. W. Xie, W. Li, and H. Zhang, "Electronic Voting Privacy Protection Scheme Based on Double Signature in Consortium Blockchain," in *Artificial Intelligence Security and Privacy*, vol. 14509, J. Vaidya, M. Gabbouj, and J. Li, Eds., in Lecture Notes in Computer Science, vol. 14509. , Singapore: Springer Nature Singapore, 2024, pp. 548–562. doi: 10.1007/978-981-99-9785-5_38.
11. B. Gong, "Advancements in public-key cryptography : crafting novel constructions to address emerging demands," Department of Computing, Hong Kong Polytechnic University, 2023. [Online]. Available: https://theses.lib.polyu.edu.hk/handle/200/12766
12. H. Yi, "Securing e-voting based on blockchain in P2P network," *J Wireless Com Network*, vol. 2019, no. 1, p. 137, Dec. 2019, doi: 10.1186/s13638-019-1473-6.
13. [13] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," *Future Generation Computer Systems*, vol. 112, pp. 859–874, Nov. 2020, doi: 10.1016/j.future.2020.06.051.
14. P. Baudier, G. Kondrateva, C. Ammi, and E. Seulliet, "Peace engineering: The contribution of blockchain systems to the e-voting process," *Technological Forecasting and Social Change*, vol. 162, p. 120397, Jan. 2021, doi: 10.1016/j.techfore.2020.120397.
15. T. Dimitriou, "Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting," *Computer Networks*, vol. 174, p. 107234, Jun. 2020, doi: 10.1016/j.comnet.2020.107234.
16. K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, Apr. 2020, doi: 10.1016/j.future.2019.11.005.
17. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874.