Blockchain Technology and Election Transparency: An Application of E-Voting Mechanism

Dr. Vishal Kumar Singh
Assistant Professor,
School of Management Sciences (SMS),
Varanasi, India
E-mail id-vishalkrsingh@fmsbhu.ac.in

Aditya Keshari
Assistant Professor,
University School of Business,
Chandigarh University,
Chandigarh, India
E-mail id- adityakeshari@fmsbhu.ac.in

Divya Singh
Doctoral Fellow,
Institute of Management,
Banaras Hindu University,
Varanasi, India
E-mail id- divyasingh@fmsbhu.ac.in

Dr. Pravin Chandra Singh
Assistant professor,
MSMSR, MATS University,
Raipur, India
E-mail id- pravinchandrasingh@fmsbhu.ac.in

Prof. Amit Gautam
Professor,
Institute of Management,
Banaras Hindu University,
Varanasi, India
E-mail id-amitgautam@fmsbhu.ac.in

Abstract

This manuscript discusses the potential of blockchain technology in electronic voting systems. It begins by examining previous studies and experimentation with e-voting, particularly in Estonia, Switzerland, and Norway. The manuscript highlights the success of e-voting in Estonia and Switzerland, but also acknowledges the discontinuation of e-voting in Norway due to security concerns and lack of impact on abstention rates. It emphasizes the need for national-scale testing of e-voting in actual settings, which is currently lacking in blockchain-based solutions.

The manuscript then delves into the legal and political concerns associated with electronic voting. It discusses the fundamental legal standards that any electronic voting system must adhere to, including inclusivity, impartiality, non-restriction, and secrecy. It recognizes the challenges of ensuring fairness, unique votes, and voter authentication in electronic voting compared to traditional paper voting. The manuscript also highlights the importance of confidentiality and how blockchain technology can address this requirement. However, it acknowledges that regulatory framework evolution is necessary for countries seeking to implement e-voting systems.

Furthermore, the manuscript explores the political factors that need to be considered when deploying e-voting. It emphasizes the importance of transparency in the voting system and the role of public oversight in ensuring legitimacy. It also acknowledges the financial consequences of creating and deploying e-voting technology and the need to strike a balance between cost-effectiveness and system reliability. The role of private enterprises in the execution of e-voting systems is also discussed.

Technical factors for electronic voting are then addressed, focusing on the restrictions that e-voting applications must meet. These include ensuring privacy and confidentiality, accessibility for all voters (including those with limited internet access), protection against attacks and system malfunctions, and verification of voter identity to prevent duplicate votes. The manuscript highlights the ongoing efforts of the EU in piloting trustworthy and secure e-voting systems.

The conclusion of the manuscript emphasizes the potential benefits of blockchain technology in revolutionizing election administration. It highlights how blockchain can provide a tamper-evident record of every vote cast, ensuring transparency and security. The manuscript discusses the potential of remote voting through mobile devices, simplifying the voting process and increasing participation. However, it also acknowledges the challenges that need to be addressed, such as security concerns and voter privacy.

In terms of future scope, the manuscript suggests that while blockchain-based electronic voting systems hold promise, there is still a need for extensive testing and addressing potential vulnerabilities. It proposes the possibility of using blockchain as an addition to existing voting methods, rather than a standalone solution. Additionally, it explores the potential of blockchain in improving participation for isolated individuals in countries with expansive territories.

Overall, this research identifies the research gap in the field of blockchain and electronic voting, highlighting the need for further study and development. The manuscript provides insights into the challenges and potential benefits of implementing blockchain-based electronic voting systems, setting the stage for future research in this area.

Keywords: Blockchain, Distributed network, Electronic Voting, Tranparency, Security, Hash Function.

Introduction

The increasing popularity of remote electronic voting, commonly known as e-voting, is due to its ability to enhance voter participation by allowing individuals to cast their ballots from the convenience of their homes. Firstly, it is important to note that the rate of abstention has been steadily increasing, partially because voters must travel a distance to cast their ballots. On the other side, in many nations, electoral openness is being questioned and opposed increasingly commonly (P. Li & Lai, 2019). Therefore, adopting blockchain technology to secure e-voting sounds like an exciting solution to address these challenges(Garg et al., 2019).Although Internet voting has previously been utilised in a number of nations for small-scale elections, it is still in its infancy(Panja et al., 2020).Such voting techniques cannot currently be considered for national elections owing of the significant attack risk and insufficient scalability. For a person who has the right to vote but lacks power or control over the electoral process, ensuring transparency and the ability to verify the system pose significant obstacles similar to those faced in traditional paper voting. Blockchain technology presents itself as a promising route for overcoming these issues(Pawlak & Poniszewska-Marańda, 2021).In this study, we study the most insightful blockchain-based electronic voting systems to better comprehend their distinctive qualities and what benefits they offer over conventional voting.

In place of the paper ballot system and EVM system, electronic voting has gained popularity since the late 1990s/early 2000s. Electronic voting (e-voting) has been extensively studied by scholars, resulting in the development and deployment of different systems at different times(Al-Madani et al., 2020). The kiosk hardware system that is installed at polling places frequently makes electronic voting easier. Voters may usually cast their ballots via an interactive touch screen interface on these machines. Despite several issues with auditing and legitimacy, electronic voting is still quite common. In democratic countries, an election system that is characterised by robustness is highly valued. This system ensures the protection of privacy and the promotion of openness. But there are some shortcomings. Voting may be altered or seen by trojan horse software. These result in a loss of privacy and make counting more challenging.The election might be tainted by insider assaults and automated vote buying. Election transparency can be undermined by spoofing, which can be started from anywhere by downloading malware.

Literature Review

The emergence of blockchain technology as a new technical foundation has brought attention to its potential to be used as the fundamental framework for various

Information Technology (IT) applications, such as apps for electronic voting, in order to take advantage of the benefits that it offers(Benabdallah et al., 2022).The democratisation of blockchain technology has contributed to the current rise in popularity of electronic voting, despite the fact that the concept of electronic voting has been around for a very long time(Maldonado-Ruiz et al., 2021). The challenges faced by that electronic voting programmes included privacy problems, a lack of supporting data, resistance to fraud, user friendliness, scalability, speed, and cost(Yang et al., 2020). It is also found that while blockchain technology can provide some security benefits, it also has vulnerabilities that could be exploited (Larriba et al., 2021).To make voting more accessible and transparent, the study suggested a blockchain-based electronic voting system for remote elections. The authors also discussed the potential security and privacy risks associated with such a system (Shejwal et al., 2020).A case study of a blockchain-based electronic voting system that was implemented in a local government election in China. The authors found that the system was successful in increasing voter turnout and reducing the risk of fraud (W. Zhang et al., 2018).

Blockchain Technology

Blockchain represents a type of decentralised record-keeping system where individuals can directly store and trade information without needing to know each other or have mutual trust beforehand. This is achieved by consolidating data records into cryptographically verified blocks, therefore preventing any form of tampering. An important step is to generate a hash of the past entries and include it in the next block's header. As a result, each block depends on the one before it, thus any effort to modify a record in the chain will be seen in the changes to the hashes of following blocks. In order to produce valid sequences of records and maintain the accuracy of data, it is crucial for participants in a blockchain to reach a consensus, which requires agreement on a procedural framework (Park et al., 2021).

The Proof-of-Work consensus is used by the Bitcoin blockchain. Within the framework of transactional compensation, every miner strives to calculate the hash value of previous transactions in a reverse manner. The task of creating a hash that is universally agreed upon poses a significant difficulty, requiring computational power that surpasses 50% of the total processing capacity of miners. Reversing a hash requires significant computer resources, but validating it is very simple(Larriba et al., 2021). With the Proof-of-Stake system, miners are chosen at random based on how many coins they commit to mining. This protocol does not require a lot of processing power. These monies are saved and accessible again(Taş & Tanrıöver, 2020). The greatest currency holders might centralise the blockchain, too, as mining power would likewise rise with wealth (Krimmer et al., 2021).The hosting networking's consensus mechanism creates trustworthy applications. The study includes a table that compares various consensus techniques based on their tolerance for rogue nodes. (Xu & Cao, 2020). A blockchain is said to as public when anybody can read it and permissionless when these same entities may write on it. Permissions/centralization and scalability are typically trade-offs(Shejwal et al., 2020). The data authentication in blockchain is left to a small group of credible nodes, and its read/write policy is restricted, typically demonstrates improved efficiency compared to a public and permissionless blockchain, due to the quick achievement of consensus (Vivek et al., 2020).The researcher (Soud et al., 2020) suggest an analysis of the different novel applications of blockchain 3.0, including electronic voting, where the technology provides unique solutions regarding the issue.

Conceptual Framework

E-voting using Blockchain

There are basic five steps considered for election mechanism as shown in Figure 1.

Initialization (Phase 1): At this point, the voter list is integrated into the smart contracts, candidate list, and voting rules. These initial smart contracts must be followed for any further modifications to this phase. This step is when voter registration and confirmation applications are processed (Sadia et al., 2020).

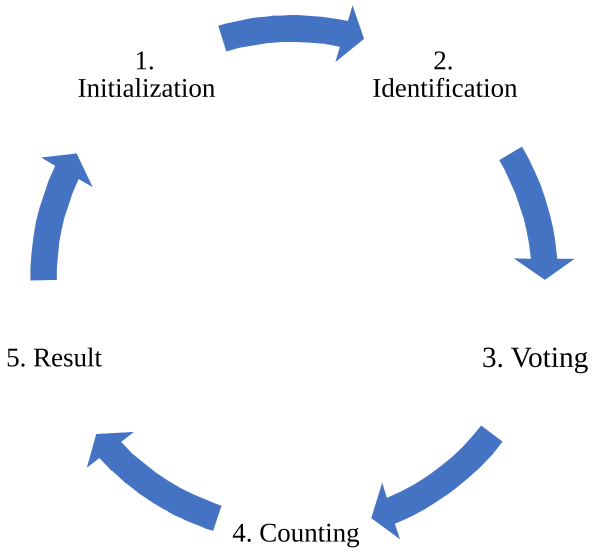
Identification (Phase 2): On election day, users connect and identify themselves using the various authentication methods. A specific website or application may occasionally be utilised (Pawade et al., 2020).

Voting (Phase 3): After thorough identification, the voter selects one or more candidates in accordance with the voting procedures. After that, a cryptographic technique is used to hash or encrypt the vote. Finally, the hashed or encrypted vote is recorded on the blockchain. The voter may cancel their ballot before the cutoff time using the electronic voting programme (Y. Li et al., 2020). It is not possible to decrypt a broadcast ballot containing a vote until the voting phase concludes and a sibling block is broadcast. (Killer et al., 2020).

Counting (Phase 4): Once the election is over, it is impossible to modify or add votes.The current result must not be made public if the counting is done concurrently with voting in order to protect voters who have not yet cast their ballots. Any audits to verify there hasn't been any fraud are conducted at this period.

Results (Phase 5): The results are fully disclosed and made available to everyone over a secure channel.The solutions' consensus procedure is a crucial component.

Figure 1: Steps of Election Voting



Source: Literature Review

Thesmart contracts are used to both record and count votes and function similarly to a public ledger. They ensure anonymity and can accommodate unique encryption techniques.As an alternative, smart contracts built on Hyperledger Fabric could facilitate 100,000 transactions per second. (Chaieb & Yousfi, 2020; Dimitriou, 2020). The existence of a central authority conducting the vote cannot entirely be eliminated by the deployment of blockchain technology.

Additionally, scalability difficulties would make it difficult for a public blockchain to manage a national election. There are several options that provide a decentralised blockchain. Three node levels are used in the architectural approach: national, constituency, and local(Bellini et al., 2020). Constituency nodes form links with national-level nodes, which have the task of uploading blocks onto the blockchain and keeping a portion of local station data. In this approach, every candidate has their own personalised blockchain. The first transaction in the blockchain records the candidate's name, while following transactions represent votes cast in their support (Al-Madani et al., 2020; Alvi et al., 2020). Every block can be roughly interpreted as a transaction in addition to including the hash of the Merkle tree root and its antecedent block. An all-encompassing transaction requires the inclusion of the voter's identification, signature, vote, and timestamp.

Voter Identification method

A biometric authentication mechanism for the voter is to be used at the time of voting. The solution offered by this idea to the aforementioned key exchange issue does actually look quite intriguing(Shahzad & Crowcroft, 2019). The subject's fingerprint or iris image is used to generate a hash key that is unique to them, making it more secure than an email code. This significantly lowers the possibility of fraud and assures that the identity of a user is ture while casting a vote. The fundamental issue, however, continues to be the massive logistical challenges this entails,that to ensure that every voter has access to the device necessary to transmit their biometric data, it is currently looking challenging. (Braghin et al., 2019).

Voting Encryption/Hash function

In order to keep the user's anonymity intact, his vote must be added to the blockchain after identification. Vote encryption/hashing algorithms step in at this stage to assure the security and legitimacy of transactions throughout the election(Srivastava et al., 2018). Vote hashing and encryption functions are common, with SHA-256 being among the most widely used. (Ansong et al., 2019). The Secure Hashing Algorithm (SHA) algorithm produces a hash value of 256 bits, which is composed of 64 hexadecimal characters. It was created by the United States National Security Agency. The new hash algorithm SHA 256 does not have issues with collusion and appears to be trustworthy for now (Almeida et al., 2019).

Resistance to attack

It goes without saying that a voting system's resilience to outside threats is crucial. Although it is difficult to claim that an application is entirely safe against all assaults, several of the articles we have read suggest the potential of repelling particular attacks. Indeed, it would be extremely difficult to foresee all potential hazards if such an application has not been well tested(Benabdallah et al., 2022). This is why we will limit our discussion to papers that have taken measures to ensure that their applications are secured from attacks in this domain. Alternately, several publications highlight the flaws in certain applications while facing these similar threats(Bartolucci et al., 2018).DDoS (Distributed Denial of Service) attacks are one of the biggest problems that cyber assault professionals are now experiencing. This sort of assault is allegedly faced by several blockchain-based electronic voting apps(Zheng et al., 2017).

In such an assault, the perpetrator circumvents the peer-to-peer network's reputation mechanism by generating a huge number of identities and utilising them to exert disproportionate influence—dramatic influence in the event of a vote(Park et al., 2021; S. Zhang et al., 2020).

Security

The property that can be verified by voters improves the audit property. Verification of the correct entry and tally of a user's vote is required. Attacks that the audit property cannot find can be detected by it. Consider the possibility that a hacker could vote in someone else's name if he finds their private key.; however, the audit property would not be able to detect this, and the only person who could do so would be the voter himself. It is known as the Forgiveness Property, and it also makes resistance to compulsion weaker since a coercer cannot be certain that the forced person won't modify his vote(Hsiao et al., 2018).

Blockchain technology has the inherent characteristic of data integrity.It ensures that data cannot ever be mistakenly or purposefully changed while being sent or processed. People may select a password that has already been exposed, which would allow a hacker to register from a compromised terminal or steal their identity. Additionally, it is vital to maintain the secrecy of each vote's associated data(Shejwal et al., 2020).The confidentiality property is one of the most crucial ones.Never should a voter's vote be used to identify them. A vote will always be encrypted, allowing it to be possible to find out who voted for whom if a vote could be linked to their vote. (Pawade et al., 2020).

Discussion

E-Voting Experimentation

E-voting was a common practise before blockchain in Europe and other parts of the world. In Estonia, Switzerland, and Norway, several electronic voting systems have been put into place that do not utilise blockchain technology. E-voting has had excellent results in Estonia and Switzerland, but it was discontinued in Norway in 2014 due to security concerns and the fact that it did not significantly lower the abstention rate. Nevertheless, Estonia saw a record 44% of votes cast online in the most recent parliamentary elections of 2019, demonstrating the public's acceptance of this voting technique.

Regardless of whether these tests were successful or not, they enabled for the national-scale testing of e-voting in actual settings, which is not the case with blockchain currently. They have drawn attention to the system's potential flaws, which are unacceptable for problems like these. Furthermore, it's critical to note that these solutions remain centralised and are therefore susceptible to the disadvantages that the blockchain's decentralised structure enables it to alleviate. But first, let's look more closely at the factors to take into account when determining if an e-voting programme is running properly.

Legal and Political Thoughts about Electronic Voting

Legal Concerns

Various nations' norms and regulations deny the necessity of paper or online voting. Any application for electronic voting must, according to the research, first adhere to the fundamental legal standards. For this reason, a secret ballot must be private, inclusive, impartial, and unrestricted. The other three criteria must be taken into account, with the exception of the free vote criterion, which does not seem to be severely endangered by the e-vote. Comparing the electronic vote to the paper vote, it is also much harder to guarantee the fairness of the electronic vote, or that each voter has a unique vote. It is in fact quite difficult to accurately confirm a voter's identity when they cast a ballot remotely.Nothing establishes that the voter is who he or she says he or she is. As a result, the issue of the voter's authentication method is crucial, and Finally, one of the core voting concepts that is protected by legislation is confidentiality.This criteria heavily depends on how well the electronic voting system is implemented and constructed. We'll examine how blockchain notably satisfies this restriction. The authors of the report (Almeida et al., 2019)assert that nations wishing to implement an electronic voting system will still need to evolve their regulatory frameworks, regardless of whether an electronic voting solution meets these criteria or not.

Political Factors

Political ramifications of the decision to deploy e-voting must be included in the study. For the results of an election to be regarded as legitimate, all voters must have confidence in the voting mechanism. Therefore, while selecting a voting technology, the fundamental issue of the voting system's transparency must be taken into consideration.The actual ballot counting, which is overseen and guaranteed by the public, provides the transparency in paper voting. However, this transparency criteria is compromised in non-democratic nations when the votes are tabulated in secret from the populace. Consequently, electronic voting should address this issue and provide voters with transparency regarding the results of the vote tallying process and the functioning of the system. E-voting through blockchain also appears to especially respect this restriction.Because it uses public funds, creating and deploying such voting technology has financial consequences that should not be overlooked. As a precaution against the system's impending failure, the cost-effectiveness balance needs to be thoroughly examined. Finally, a significant problem with this system's execution is the role that private enterprises play (Khan et al., 2018).

Technical Factors for Electronic Voting

After the political and legal constraints have been defined, we can now ignore the technological constraints that an e-voting app must comply with(Perez & Ceesay, 2018). There are two basic categories of these limitations, those relating to people and those relating to technology.Ensure people' privacy and confidentiality so that their votes stay secret and cannot be used to identify them.By allowing voters to use their own devices to cast their ballots electronically, you are not discriminating against those who cannot or will not have access to the Internet.Voting needs to be possible for those persons who now have bad internet connections.There are corrective measures needed for avoid any attack, system malfunction, or connection issue. Further, it is requiered to verify the voter identity and also avoid duplicate votes.

Among these restrictions, the availability of universal broadband internet connection or the potential for a paper alternative have less to do with the voting application and more to do with the government body in charge of the election. However, the e-voting application is largely in charge of ensuring that all other requirements are met. As seen, for instance, by the elections in Estonia, certain e-voting software appear to respect some of these limitations. For the purpose of implementing a trustworthy and secure e-voting system, the EU pilot initiatives are also underway in this area. [83]. This essay examines whether or whether the blockchain can handle these limitations more successfully than more established e-voting solutions.

Conclusion

Election administration might undergo a change thanks to blockchain technology, which would also guarantee the validity of the voting process. Blockchain-based electronic voting systems might make voting and vote counting more transparent and secure while doing away with paper ballots and human vote counting. Blockchain technology can offer a tamper-evident record of every vote cast, which is one of the main advantages of utilising it for electronic voting. Data stored on a blockchain cannot easily be changed or deleted since blockchains are spread over a network of computers and decentralised. This makes it far more difficult for anyone to rig an election. Another benefit of adopting blockchain for electronic voting is that it can speed up and simplify the voting process. For instance, voters might cast their ballots remotely using their cellphones or other devices, eliminating the need to visit a polling place. Election participation may become simpler as a result, particularly for individuals who are physically unable to visit a voting place because of illness or a handicap.

But before blockchain-based electronic voting systems are widely used, there are still a lot of obstacles to be addressed. These include concerns about the security of the voting machines itself and issues relating to voter privacy. As they seek to build and deploy blockchain-based electronic voting systems, developers and legislators must carefully take these concerns into account. An intriguing aspect is the implementation of blockchain technology as the method of voting. The blockchain industry is dynamic, with new entrants and established players both regularly changing the landscape by entering and exiting. In fact, electronic voting systems based on the blockchain are being proposed in an increasing number of scholarly articles. However, none of the proposed solutions have actually been implemented, and even fewer have been thoroughly tested. Therefore, it is quite challenging to draw the conclusion that blockchain today offers a completely secure alternative to holding a national election. Despite the security of the blockchain's underlying principles, a number of assaults can still target e-voting software. It becomes extremely challenging to guarantee the integrity of an election when the stakes are this high. There are additional possibilities for the application of blockchain in future elections, though. Even if it appears impossible right now to arrange a vote only using blockchain, it is conceivable to think about its usage as an addition to existing methods. Furthermore, in countries with large territories, individuals who were previously cut off from participating in political process due to their isolation can now be more actively involved through a blockchain-based voting app for smartphones, in addition to physical polling booths.

References

- Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, 176–180.
- Almeida, R. L., Ricci, L., & Camarinha-Matos, L. M. (2019). votechain: Community based scalable internet voting framework. *Doctoral Conference on Computing, Electrical and Industrial Systems*, 70–80.
- Alvi, S. T., Uddin, M. N., & Islam, L. (2020). Digital voting: A blockchain-based e-voting system using biohash and smart contract. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 228–233.
- Ansong, E. D., Appiah, J., & Odoi-Lartey, B. (2019). Digital Voting Systems Deploying the use of Blockchain Technology. *International Journal of Computer Applications*, *975*, 8887.
- Bartolucci, S., Bernat, P., & Joseph, D. (2018). SHARVOT: Secret SHARe-based VOTing on the blockchain. *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, 30–34.
- Bellini, E., Ceravolo, P., Bellini, A., & Damiani, E. (2020). Designing process-centric blockchain-based architectures: A case study in e-voting as a service. *International Symposium on Data-Driven Process Discovery and Analysis, International Symposium on Data-Driven Process Discovery and Analysis*, 1–23.

- Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access*, *10*, 70746–70759. https://doi.org/10.1109/ACCESS.2022.3187688
- Braghin, C., Cimato, S., Cominesi, S. R., Damiani, E., & Mauri, L. (2019). Towards blockchain-based E-voting systems. *International Conference on Business Information Systems*, 274–286.
- Chaieb, M., & Yousfi, S. (2020). LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol. *European, Mediterranean, and Middle Eastern Conference on Information Systems*, 151–168.
- Dimitriou, T. (2020). Efficient, coercion-free and universally verifiable blockchain-based voting. *Computer Networks*, *174*, 107234.
- Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019). A comparitive analysis on e-voting system using blockchain. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1–4.
- Hsiao, J.-H., Tso, R., Chen, C.-M., & Wu, M.-E. (2018). Decentralized E-voting systems based on the blockchain technology. *International Conference on Ubiquitous Information Technologies and Applications, International Conference on Computer Science and Its Applications*, 305–309.
- Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research (IJEGR)*, *14*(1), 53–62.
- Killer, C., Rodrigues, B., Scheid, E. J., Franco, M., Eck, M., Zaugg, N., Scheitlin, A., & Stiller, B. (2020). Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system. *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, 172–183.
- Krimmer, R., Duenas-Cid, D., & Krivonosova, I. (2021). New methodology for calculating cost-efficiency of different ways of voting: Is internet voting cheaper? *Public Money & Management*, *41*(1), 17–26.
- Larriba, A. M., Cerdà i Cucó, A., Sempere, J. M., & López, D. (2021). Distributed Trust, a Blockchain Election Scheme. *Informatica*, *32*(2), 321–355.
- Li, P., & Lai, J. (2019). LaT-Voting: Traceable anonymous E-voting on blockchain. *International Conference on Network and System Security*, 234–254.
- Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A blockchain-based self-tallying voting protocol in decentralized IoT. *IEEE Transactions on Dependable and Secure Computing*.
- Maldonado-Ruiz, D., Torres, J., El Madhoun, N., & Badra, M. (2021). An innovative and decentralized identity framework based on blockchain technology. *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–8.
- Panja, S., Bag, S., Hao, F., & Roy, B. (2020). A smart contract system for decentralized borda count voting. *IEEE Transactions on Engineering Management*, *67*(4), 1323–1339.
- Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From internet voting to blockchain voting. *Journal of Cybersecurity*, *7*(1), tyaa025.
- Pawade, D., Sakhapara, A., Badgujar, A., Adepu, D., & Andrade, M. (2020). Secure online voting system using biometric and blockchain. In *Data Management, Analytics and Innovation* (pp. 93–110). Springer.
- Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing & Management*, *58*(4), 102595.
- Perez, A. J., & Ceesay, E. N. (2018). Improving end-to-end verifiable voting systems with blockchain technologies. *2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1108–1115.
- Sadia, K., Masuduzzaman, M., Paul, R. K., & Islam, A. (2020). Blockchain-based secure e-voting with the assistance of smart contract. In *IC-BCT 2019* (pp.

161–176). Springer.

- Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, *7*, 24477–24488.
- Shejwal, P., Gaikwad, A., Jadhav, M., Nanaware, N., & Shikalgar, N. (2020). E-voting using block chain Technology. *International Journal of Scientific Development and Research (IJSDR)*, *4*(5), 583–588.
- Soud, M., Helgason, S., Hjálmt?sson, G., & Hamdaqa, M. (2020). TrustVote: On elections we trust with distributed ledgers and smart contracts. *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 176–183.
- Srivastava, G., Dwivedi, A. D., & Singh, R. (2018). Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. *ICETE (2)*, 674–679.
- Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry*, *12*(8), 1328.
- Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., & Namratha, M. (2020). E-voting systems using blockchain: An exploratory literature survey. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, 890–895.
- Xu, Z., & Cao, S. (2020). Efficient privacy-preserving electronic voting scheme based on blockchain. *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 190–196.
- Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Future Generation Computer Systems*, *112*, 859–874.
- Zhang, S., Wang, L., & Xiong, H. (2020). Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. *International Journal of Information Security*, *19*(3), 323–341.
- Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A., & Huang, S. (2018). A privacy-preserving voting protocol on blockchain. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 401–408.
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564.