Blockchain-Based E-Voting Systems

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Mohammad Hajian Berenjestanaki, Hamid R. Barzegar, Nabil El Ioini, Claus Pahl

The employment of blockchain technology in electronic voting (e-voting) systems is attracting significant attention due to its ability to enhance transparency, security, and integrity in digital voting. Blockchain technology has been recognized as a potential solution for secure and transparent e-voting systems. By leveraging the decentralization, immutability, and transparency of blockchain technology, e-voting systems can prevent fraud and manipulation, improve voter anonymity, and increase trust in the electoral process. Moreover, blockchain-based e-voting systems can reduce the cost and time associated with traditional voting systems.

Keywords: blockchain ; digital transformation ; e-voting systems ; security ; scalability

1. Background

1.1. Blockchain Technology

A blockchain is a decentralized and distributed ledger made of a sequence of blocks linked to each other. Each block contains a list of transactions, and each transaction is a record of an event or action. The block header, which includes the previous block hash, timestamp, nonce, and Merkle root, identifies each block. The previous block hash links the current block to the previous one. The timestamp verifies the data in the block and assigns a time or date of creation for digital documents. The nonce, a number used only once, is a central part of the proof of work in the block. The Merkle root, a type of data structure frame for different blocks of data, stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. This structure provides assurance that once data are recorded in a block, they cannot be altered in the future without modifying all subsequently recorded blocks, making blockchain transactions immutable and secure. **Figure 1** represents an overview of the blockchain structure with the chain of blocks that encapsulate the transactions and secure them with hashes and other data. These blocks are broadcasted and replicated across a network of peers. This method is characterized by its robust security measures through cryptographic principles, which effectively mitigate the risks of manipulation and fraudulent activities. The decentralized nature of blockchain enables universal accessibility of the distributed database to all participants in the network, which is governed by a consensus algorithm. Therefore, blockchain data are immutable; it additionally traces and validates transactions based on their origins. This technique makes digital transactions transparent, secure, and tamper-proof. Considering these unique characteristics, blockchain is an appropriate mechanism for integration with e-voting systems.

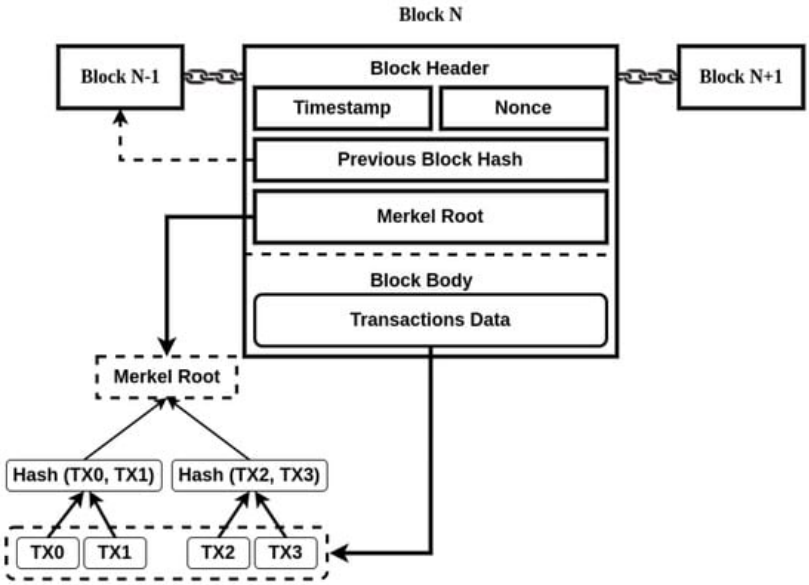

Figure 1. The blockchain structure.

1.2. Blockchain Applications across Domains

Blockchain technology has emerged as a revolutionary trend across various domains, and whereas blockchain technology application in e-voting systems attracts interest in enhancing electoral integrity and transparency, it is equally valuable in other domains, each with distinct requirements and objectives. This section aims to provide a comparison and analysis of blockchain applications in different domains such as healthcare, financial services, supply chain management, cloud computing, education, and IoT (Internet of Things) [1], highlighting their parallels and contrasts with their use in e-voting systems.

- Blockchain in healthcare: In healthcare, blockchain is employed for secure data sharing, patient privacy, and interoperability among different healthcare systems [2]. Its application in healthcare shares some aspects of e-voting, such as the emphasis on data security and privacy. However, whereas blockchain in healthcare deals with continuous data flow and personal health records, in e-voting, it addresses the singular event of casting and recording votes.

- Blockchain in financial services: In financial services, blockchain technology revolutionizes transactions and trust mechanisms. Similar to e-voting, where blockchain brings transparency and verifiability to the voting process, in financial services, it introduces a new concept of trust and efficiency in transactions [3]. The key difference lies in blockchain's role in handling continuous financial transactions as opposed to the discrete event of voting.

- Blockchain in supply chain management: blockchain technology in supply chain management focuses on improving transparency, reducing fraud, and enhancing efficiency [4], whereas both supply chain management and e-voting systems benefit from blockchain's immutability and transparency, supply chain management uniquely utilizes blockchain for continuous tracking of goods and transactions, in contrast to the periodic nature of elections.

- Blockchain in cloud computing: In cloud computing, blockchain enhances security, data provenance and creates new service models like Blockchain-as-a-Service (BaaS). The integration of blockchain in cloud computing shares similarities with e-voting in terms of improving security and reliability. However, the use cases in cloud computing are more varied and continuous, focusing on service enhancement and data integrity across diverse cloud-based applications [5].

- Blockchain in education: Blockchain technology in education mainly focuses on enhancing data security, credential verification, traceability, and record management. Through its immutable feature, blockchain technology not only ensures the integrity of educational records and certificates, consequently creating trust in academic credentials, additionally, it effectively secures and tracks the progress of academic patents, copyrights, and research innovations, significantly enhancing the management and protection of property within the educational domain [6][7][8]. Compared to its application in e-voting, where blockchain ensures vote integrity and transparency, in education, it serves to preserve academic achievements and automate administrative processes.

- Blockchain in IoT: Blockchain technology in IoT includes enhancing security, scalability, and trustworthiness in diverse applications like smart cities. The decentralized nature of blockchain in IoT addresses issues similar to those in e-voting, like ensuring security and scalability [9]. However, IoT applications deal with a broader range of data types and greater scalability challenges than electronic voting systems.

1.3. Related Work

Studies exploring potential applications of blockchain technology in the domain of e-voting aim to evaluate its feasibility, security, and efficiency in enhancing the transparency and integrity of the election process.

Taş and Tanrıöver [10] reviewed in 2020 the state of blockchain-based voting research, identifying potential challenges and forecasting future directions. They presented a conceptual description of the desired blockchain-based e-voting application and conducted a review of 63 research papers. The articles that were examined were categorized into five main categories: general, integrity, coin-based, privacy, and consensus. They concluded that, whereas blockchain-based voting systems can prevent data manipulation and integrity issues, the most frequently highlighted issues are scalability, cost-effectiveness, authentication, privacy, and security in blockchain-based e-voting systems.

Jafar et al. [11] presented a conceptual description of a blockchain-based e-voting application in addition to an introduction to the blockchain's fundamental structure and characteristics in relation to e-voting. They mentioned that whereas blockchain systems could help solve some of the issues that currently affect election systems, the authors conclude that

the most frequently mentioned issues in blockchain applications are scalability, user identity, transactional privacy, energy efficiency, immatureness, acceptableness, and political leaders' resistance.

In [12], Pawlak et al. indicated the remaining problems like security attacks, coercion, cost efficiency, and privacy that still need to be solved. The paper serves as a valuable resource for understanding the current trends and challenges in blockchain-based electronic voting systems.

Huang et al. [13] in 2021 provided a comprehensive review of blockchain-based voting systems, discussing their advantages, challenges, and technical innovations. They also provide a taxonomy of blockchain and identify key challenges in blockchain-based voting systems such as authentication, anonymity, coercion-freeness, and auditability.

Jafar and Ab Aziz in [14] emphasized the benefits and challenges of blockchain-based e-voting systems, providing useful details on probable future applications of this technology with regard to democratic processes. They demonstrated how blockchain technology offers security, transparency, and a reduced risk of fraud. However, they brought up issues with scalability, transactional privacy, and immaturity for these systems.

Devi and Bansal [15] provided a comprehensive review of the security requirements and potential threats in e-voting systems. They discuss various cryptographic techniques that can be used to secure these systems.

Benabdallah et al. [16] presented a comprehensive analysis of blockchain solutions for e-voting. They discussed the challenges faced by e-voting systems and how blockchain technology can address these issues. They also provide a comparison of several blockchain-based e-voting solutions, identifying their strengths and weaknesses. The paper also addressed the limitations and issues raised by this technology, such as scalability, unpredictable attacks, weakness of the identification system, new issues raised using blockchain technology, efficiency and decentralization, the digital divide, and vulnerabilities in smart contracts.

Jafar et al. in their systematic literature review [17] discussed the challenges and solutions for scalable blockchain-based electronic voting systems, in addition to anticipating future developments. To evaluate cost and time, they identified well-known proposals, their implementations, verification methods, and various cryptographic solutions in previous research. They analyzed performance parameters, the primary benefits and limitations of different systems, and the most common approaches to blockchain scalability.

In [18], Vladucu et al. provided a thorough overview of blockchain-based e-voting systems currently in use by various countries and companies, as well as those proposed for academic research. The authors discussed the challenges that blockchain e-voting systems face and identified areas for future research to improve their trustworthiness. Furthermore, they included a detailed explanation of the terminology used in blockchain-based e-voting systems, such as consensus algorithms, cryptography, and system characteristics.

1.4. Implementations of Blockchain-Based E-Voting Systems

In the following, the researchers present several projects that are currently being developed or have already implemented e-voting on blockchain.

- Luxoft: Luxoft Holding Inc., a global IT service provider of technology solutions, is developing an e-voting infrastructure that will enable the world's first consultative vote on blockchain in Zug, Switzerland. Hyperledger Fabric was used to create an authorized blockchain that included a network, applications, and algorithms. In order to allow voters to cast their ballots, Zug's digital ID registration app based on Ethereum was authorized through uPort. Luxoft announces its intention to open source this technology and creates a Government Alliance Blockchain to encourage blockchain use in public institutions [19].

- Votem: A company specializing in election management, its main product is the CastIron platform. This platform is built on blockchain technology and offers several distinctive features, including a distributed database, immutability, permission-based access, and an audit trail. Votem has successfully handled over 13 million voters, serving both government elections and various associations in the United States and around the world. Notably, their track record boasts zero instances of fraud, compromise, attacks, or hacking, highlighting the security and reliability of their system [20].

- Voatz: A blockchain-based mobile voting tool that was launched in 2018 in West Virginia for overseas military voters participating in the 2018 midterm elections in the United States. Voatz includes biometric validation, such as

fingerprints or retinal scans, so that voters validate their applicants and themselves on the application. A recent study found Voatz has major security flaws that allow attackers to monitor votes and edit or block ballots in large amounts [21].

- POLYAS: In the summer of 1996, Finland held the first POLYAS online election, with 30,000 voters participating in three languages. The company uses blockchain technology to offer an electronic voting system to the public and private sectors. Germany's Federal Office for Information Security granted the first online election certification in 2016. The online voting system satisfies anonymity, accuracy, singularity, verifiability, and auditability. In Europe and the USA, several important companies employ POLYAS to manage their electronic voting systems [22].

- Polys: An online voting system that increases confidence in the voting process and results. Because it is based on blockchain technology, it is secure and transparent. Both the voting procedure and the results are immutable. Transparent cryptographic techniques are employed on the top of the blockchain to protect voter anonymity. Voters can check at any moment to ensure that their vote is valid and unmodified [23].

- DecentraVote: A blockchain-based solution for virtual meetings was originally developed by a team at the iteratec location in Vienna. DecentraVote uses a public Ethereum network based on Proof of Authority consensus with permissioned validator nodes. The smart contract constructed a Merkle tree of all voting rights on-chain, and the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) generated a proof for every voting right off-chain. DecentraVote does not address national political elections [24].

2. Benefits and Challenges

2.1. Benefits of Blockchain-Based E-Voting Systems

- Security: a major benefit of blockchain-based e-voting systems, where subcategories highlight a unique perspective:
  - Integrity: holistic assurance of security aligned with the design [25].
  - Immutability: once a vote is recorded, it cannot be altered, ensuring the voting process's finality [26].
  - Durability: robust against data loss and ensures the permanency of stored data.
  - Stability: Resistance to disruptions or manipulations like hacking. Stability is enhanced by strong encryption systems, often inherent in blockchain technology [27].
  - Non-repudiation: a voter cannot dispute the validity of their cast vote [28].
- Transparency: The blockchain-based e-voting system's inherent design encourages open voting, recording, management, and counting procedures. It facilitates independent audits [29] and ensures that all transactions (votes) on the blockchain are visible to all participants and can be independently verified.
- Privacy: the ability of blockchain-based e-voting systems to protect voters' personal information and the confidentiality of their voting choices.
  - Anonymity: protecting a voter's identity [30].
  - Confidentiality (secrecy): the voters' choices are private, and outcomes are not presented ahead of time [31].
  - Untraceability: prevent the tracing of a vote back to its individual voter [30].
  - Pseudoanonymity: voters' actual identities are masked, but their voting activities are linked to unique identifiers similar to pseudonyms or addresses [32][33].
- Verifiability: the ability to confirm that votes have been cast as intended, stored, and counted.
  - Public verifiability: the ability of all to verify the entire election process [34].
  - Individual verifiability: the ability for every voter to verify that their vote was precisely recorded and counted [34].
- Auditability: ensure the voting process accuracy and truthfulness [35].
- Accessibility: provide every eligible voter with an equal opportunity to participate in the voting process.

    - Availability: blockchains generally ensure that voters are able to cast their votes anytime within the stipulated period without facing any issue.
    - Broad turnout: technology allows substantial participation of eligible voters.
    - Universal access: the ability of the system to be used effectively by all eligible voters.
- Decentralization: Refers to the distribution of voting system authority, responsibility, and operations across a network compared to a central entity. This property is fundamental to blockchain technology and is essential for enhancing confidence among citizens by minimizing control of a potentially corrupt third party [16].
- Usability: facilitate an extensive number of voters casting votes in accordance with their choices in an effective way while being satisfied with the process [36].
    - Simplicity: how simple and straightforward the system is to operate.
    - Understandability: clarity in system operation ensures that voters cast their votes as intended.
- Efficiency: ability of an e-voting system to allow voters to cast votes in a swift and inexpensive manner.
    - Cost efficiency: The system's capacity to carry out voting operations at a cost that is affordable. This can involve a lower-cost setup and maintenance, material distribution, and human expenses.
    - Time efficiency: the system's ability to speed up voting and vote tallying.
    - Performance efficiency: the ability to handle massive amounts of data (votes), process, and count votes accurately, securely, and swiftly.
- Trustworthiness: Secure, transparent, and fair system that ensures the accurate tracking and integrity of each vote. It is a balance of rigorous security measures, prompt results, and scalability, all of which are critical to preserving trust in the voting process [37].
    - Eligibility: only eligible voters can participate [38].
    - Fairness: election results are not exposed before the voting process finalizes [38].
    - Accountability: ability to determine whether or not the official vote record is inaccurate is facilitated by the blockchain [39].
    - Uniqueness: each eligible voter merits one and only one vote.
    - Accuracy: each vote is precisely accounted for, ensuring there is no modification, omission, or unauthorized inclusion [40].
    - Credibility: how much voters, politicians, and the general public trust and believe in the e-voting system.
    - Reliability: the system's consistency in performance through time ensures accurate, error-free function and availability [41].
- Compatibility: ability of the e-voting system to operate in conjunction with various types of hardware, software, protocols, and legislation.
    - Adaptability: ability of an e-voting system to alter or adjust in order to accommodate various circumstances or necessities that may emerge [42][43].
    - Flexibility: ability to adapt to different frameworks, election types, voting methods, and voter interfaces.
- Resistance to coercion: capacity of an e-voting system to shield voters from potential manipulations or coercions [16][44].

2.2. Challenges in Blockchain-Based E-Voting Systems

Despite the properties of blockchain technology and the benefits it offers, these systems are not inherently applicable across all voting contexts due to some barriers. The objective is an understanding of the obstacles and challenges

associated with using blockchain technology for e-voting systems, specifically identifying properties that traditional e-voting systems have but blockchain-based ones do not.

1. Enhanced privacy: Recent advances in cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, blind signatures, ring signatures, and mix networks, have significantly enhanced the privacy aspect of blockchain-based e-voting systems. These methods enable the verification of votes without revealing the voter's private information, simultaneously balancing privacy with the necessary transparency and auditability.

2. Enhanced security: In response to security challenges, there have been significant developments in both blockchain architecture and cryptographic defenses. In addition, enhanced consensus algorithms, like Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), have been implemented to counteract various blockchain-specific attacks. Additionally, the integration of advanced security protocols and mechanisms could become standard methods, improving these systems against cyber threats.

3. Scalability improvement: To address scalability issues, innovative solutions such as off-chain transactions, sharding, optimized consensus protocols, and layer-2 scaling solutions like Lightning Networks have been introduced. These technologies have proven effective in increasing transaction throughput, allowing for more scalable e-voting systems.

4. Technical improvement: to address the technical complexities, approaches for optimizing the chosen consensus algorithm for efficiency, simplifying technical complexities, ensuring hardware platform compatibility, ensuring interoperability with existing systems and protocols, implementing automation for configuration, and constantly seeking feedback for refinement are some of the steps taken or that need further research to evolve the system.

5. Energy and cost efficiency: The shift towards more energy-efficient consensus mechanisms, like Delegated Proof of Stake (DPoS), has notably reduced the operational costs and energy consumption of blockchain networks. Further, ongoing research into optimizing blockchain infrastructure and in other layers (on-chain and non-chain) can lead to the economic feasibility of blockchain-based e-voting systems.

6. Increasing acceptability: Experimental projects and real-world evaluations can play an important role in building trust and demonstrating the viability of blockchain-based e-voting systems. By developing educational resources and engaging stakeholders, this technology can be accepted and understood by a broader audience.

7. User-friendly interfaces: Significant efforts can be made to develop interfaces that are both simple for voters and secure. These interfaces often include guiding instructions and reliable verification mechanisms to ensure a seamless and secure voting experience.

8. Provide coercion-resistant: To achieve this aim in a blockchain-based e-voting system, there are several methods in the literature: implementing strong end-to-end encryption, utilizing zero-knowledge proofs, enforcing receipt-freeness, using blind signatures, employing multi-step authentication, securing physical components, maintaining a transparent blockchain, implementing auditing and monitoring, and ensuring user-friendly interfaces. Together, these strategies ensure the integrity of the voting process, prevent coercion, and enable voters to participate freely and without fear of repercussions.

9. Accuracy and reliability enhancements: By adopting robust cryptographic techniques and providing a decentralized ledger with transparent, auditable transactions, accuracy and reliability can be enhanced. By using identity verification mechanisms and smart contracts to ensure fairness, double voting can be prevented, whereas decentralized oracles and on-chain storage of critical data can reduce reliance on centralized sources. Consensus mechanisms and regular security testing are key to overall reliability. In all these cases, blockchain-based e-voting systems become more accurate and reliable.

10. Improved accessibility: Efforts to expand accessibility include developing offline voting mechanisms and protocols in mobile voting apps and establishing remote voting centers in areas with limited internet access. These centers can be equipped with the necessary technology to ensure that mobile voting applications are accessible to voters. Provide features for people with disabilities, such as screen readers, voice-guided interfaces, etc. Consider having backup plans in place in case of technical failures or disruptions in areas with limited internet access.

11. Regulatory compliance and governance: establishing legal frameworks and standards is a key focus, ensuring that these systems comply with the regulatory challenges associated with blockchain-based e-voting.

12. Decentralization and consensus mechanism optimization: customized consensus mechanisms that adjust to the unique requirements of e-voting systems can enable achieving a balance between speed, security, and decentralization.

3. Security and Privacy Technologies and Implementation of Blockchain-Based E-Voting Systems

1. Zero-Knowledge Proofs (ZKPs): a cryptographic technique that enables one party to prove to another party the truthfulness of a statement or claim without disclosing any extra information [13][45].

2. Homomorphic Encryption (HE): a cryptographic technique that facilitates computations to be executed on encrypted data without the need for decryption [46][47][48].

3. Blind Signature (BS): a cryptographic method that enables a party to receive a valid signature on a message without disclosing the message's contents to the signer [49].

4. Ring Signatures: A cryptographic technique that offers anonymity and unlinkability to the signer within a group (ring) of potential signers. In the context of cryptographic protocols, a ring signature allows the signer to generate a signature on a specific message, thus convincing the verifier that the message was signed by an entity within a specific group while at the same time obscuring the true identity of the singer [50].

5. Shamir's Secret Sharing Scheme (SS): a cryptographic method that enables the division of a secret into multiple shares that are distributed among participants [51].

6. Quantum Key Distribution (QKD): a method of establishing secure cryptographic keys between two parties that makes use of the concepts of quantum physics [52][53].

7. Mix Network (MN): This technique is used to protect the privacy of voters and the secrecy of votes. Through serving as a channel between voters and the authority responsible for counting the votes [54][55].

8. Time-lock encryption (TLE): in this technique, a time-based delay is added to the encoding of encrypted data [55].

9. Machine Learning (ML): By integrating machine learning and blockchain technology, along with deep learning algorithms, significant enhancements can be achieved in biometric ID authentication. This involves utilizing machine learning methods to analyze facial features and verify the identities of users [56][57].

10. Circle Shuffle (CS): this method relies on a circular arrangement of votes, wherein each vote is assigned to a particular place in the circular structure [51].

11. Reputation-Based PayOff algorithm (RoPO): An incentive mechanism that is used in different decentralized systems to motivate players based on their reputation or performance history [58].

12. Proxy Multi-Signature Scheme (PMS): a variant of the common multi-signature method that includes the idea of a proxy or delegate to make signing on behalf of multiple individuals [59].

13. Bit Commitment (BC): a cryptographic technique in which one party (the committer) makes a commitment to another (the verifier) about a value without initially disclosing that value to the verifiers until the committer decides to reveal the committed value at a later time [60].

14. Differential Privacy (DP): It intends to maintain voters' sensitive data private while still allowing effective aggregate voting data analysis. It provides a structure for protecting voters' anonymity by adding random noise or perturbations to the data in a controlled manner [61].

15. Provenance-Based solution (PB): this solution involves tracking the origin and transformations of data (provenance) within the blockchain [62].

References

1. Kong, X.; Wu, Y.; Wang, H.; Xia, F. Edge Computing for Internet of Everything: A Survey. IEEE Internet Things J. 2022, 9, 23472–23485.

2. Arbabi, M.S.; Lal, C.; Veeraragavan, N.R.; Marijan, D.; Nygård, J.F.; Vitenberg, R. A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions. IEEE Commun. Surv. Tutorials 2023, 25, 386–424.
3. Ali, O.; Ally, M.; Dwivedi, Y. The state of play of blockchain technology in the financial services sector: A systematic literature review. Int. J. Inf. Manag. 2020, 54, 102199.
4. Du, M.; Chen, Q.; Xiao, J.; Yang, H.; Ma, X. Supply Chain Finance Innovation Using Blockchain. IEEE Trans. Eng. Manag. 2020, 67, 1045–1058.
5. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain Meets Cloud Computing: A Survey. IEEE Commun. Surv. Tutorials 2020, 22, 2009–2030.
6. Steiu, M. Blockchain in education: Opportunities, applications, and challenges. First Monday 2020, 25.
7. Hu, J.; Zhu, P.; Qi, Y.; Zhu, Q.; Li, X. A patent registration and trading system based on blockchain. Expert Syst. Appl. 2022, 201, 117094.
8. Zhu, P.; Hu, J.; Li, X.; Zhu, Q. Using blockchain technology to enhance the traceability of original achievements. IEEE Trans. Eng. Manag. 2023, 70, 1693–1707.
9. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions. Electronics 2022, 11, 630.
10. Taş, R.; Tanrıöver, Ö.Ö. A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry 2020, 12, 1328.
11. Jafar, U.; Ab Aziz, M.J.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors 2021, 21, 5874.
12. Pawlak, M.; Poniszewska-Marańda, A. Trends in blockchain-based electronic voting systems. Inf. Process. Manag. 2021, 58, 102595.
13. Huang, J.; He, D.; Obaidat, M.S.; Vijayakumar, P.; Luo, M.; Choo, K.-K.R. The application of the blockchain technology in voting systems: A review. ACM Comput. Surv. (CSUR) 2021, 54, 1–28.
14. Jafar, U.; Ab Aziz, M.J. A state of the art survey and research directions on blockchain based electronic voting system. In Proceedings of the Second International Conference, ACeS 2020, Penang, Malaysia, 8–9 December 2020; Revised Selected Papers 2. Springer: Singapore, 2021.
15. Devi, U.; Bansal, S. Secure e-Voting System—A Review. In Proceedings of the Hybrid Intelligent Systems, Olten, Switzerland; Porto, Portugal; Vilnius, Lithuania; Kochi, India, 12–14 December 2023; Springer Nature: Cham, Switzerland, 2023; pp. 1209–1224.
16. Benabdallah, A.; Audras, A.; Coudert, L.; El Madhoun, N.; Badra, M. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. IEEE Access 2022, 10, 70746–70759.
17. Jafar, U.; Ab Aziz, M.J.; Shukur, Z.; Hussain, H.A. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors 2022, 22, 7585.
18. Vladucu, M.-V.; Dong, Z.; Medina, J.; Rojas-Cessa; R.Vladucu, M.-V.; Dong, Z.; Medina, J.; Rojas-Cessa, R. E-Voting Meets Blockchain: A Survey. IEEE Access 2023, 11, 23293–23308.
19. Luxoft. Available online: https://www.luxoft.com/ (accessed on 18 November 2023).
20. Votem. Available online: https://votem.com/ (accessed on 20 November 2023).
21. Voatz. Available online: https://voatz.com/ (accessed on 20 November 2023).
22. Polyas. Available online: https://www.polyas.com/ (accessed on 21 November 2023).
23. Kaspersky Box. Available online: https://box.kaspersky.com/f/e68a161d8e7241909ea3/ (accessed on 21 November 2023).
24. Decentra.Vote. Available online: https://decentra.vote/ (accessed on 25 November 2023).
25. Harley, K.; Cooper, R. Information Integrity: Are We There Yet? ACM Comput. Surv. 2021, 54, 1–35.
26. Çabuk, U.C.; Adiguzel, E.; Karaarslan, E. A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems. arXiv 2020, arXiv:2002.07175.
27. Kugusheva, A.; Yanovich, Y. Ring Signature-Based Voting on Blockchain. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 9–11 December 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 70–75.

28. Haiyan, X.; Lifang, W.; Yuechuan, W. A New Fair Electronic Contract Signing Protocol. In Proceedings of the Advances in Intelligent Networking and Collaborative Systems (INCoS-2019), Oita, Japan, 5–7 September 2019; Springer International Publishing: Cham, Switzerland, 2020; pp. 289–295.
29. Hjálmarsson, F.Þ.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjálmtýsson, G. Blockchain-Based E-Voting System. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 983–986.
30. Kumar, M.; Katti, C.P.; Saxena, P.C. A secure anonymous e-voting system using identity-based blind signature scheme. In Proceedings of the 13th International Conference, ICISS 2017, Mumbai, India, 16–20 December 2017; Springer International Publishing: Cham, Switzerland, 2017.
31. Russo, A.; Anta, A.F.; Vasco, M.I.G.; Romano, S.P. Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 417–424.
32. Ikundi, O.; Nwosu, K.C.; Abdulgader, M. LegitVote: A Blockchain-Based System to Facilitate E-Voting Process. In Proceedings of the 2022 International Conference on Computer and Applications (ICCA), Cairo, Egypt, 20–22 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
33. Fusco, F.; Lunesu, M.; Pani, F.; Pinna, A. Crypto-voting, a Blockchain based e-Voting System. In Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2018)—Volume 3: KMIS, Seville, Spain, 18–20 September 2018; pp. 223–227.
34. Vivek, S.K.; Yashank, R.S.; Prashanth, Y.; Yashas, N.; Namratha, M. E-Voting Systems using Blockchain: An Exploratory Literature Survey. In Proceedings of the 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 15–17 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 890–895.
35. Mello-Stark, S.; Lamagna, E.A. The Need for Audit-Capable E-Voting Systems. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 535–540.
36. Hsu, J.; Bronson, G. E-Voting Technologies Usability: A Critical Element for Enabling Successful Elections. In Emerging Challenges in Business, Optimization, Technology, and Industry, Proceedings of the Third International Conference on Business Management and Technology, Vancouver, BC, Canada, 13–17 March 2017; Springer International Publishing: Cham, Switzerland, 2018.
37. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488.
38. Sheer Hardwick, F.; Gioulis, A.; Naeem Akram, R.; Markantonakis, K. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. In Proceedings of the 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), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1561–1567.
39. Küsters, R.; Müller, J. Cryptographic security analysis of e-voting systems: Achievements, misconceptions, and limitations. In Proceedings of the Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, 24–27 October 2017; Springer International Publishing: Cham, Switzerland, 2017.
40. Anane, R.; Freeland, R.; Theodoropoulos, G. E-voting requirements and implementation. In Proceedings of the the 9th IEEE International Conference on E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), Tokyo, Japan, 23–26 July 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 382–392.
41. Conti, V.; Taş, R.; Tanrıöver, Ö.Ö. A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. Secur. Commun. Networks 2021, 2021, 6673691.
42. Borras, J. Overview of the Work on E-Voting Technical Standards; Cabinet Office, UK Government: London, UK, 2002.
43. Prajapati, P.; Dave, K.; Shah, P. A review of recent blockchain applications. Int. J. Sci. Technol. Res. 2020, 9, 897–903.
44. Kho, Y.-X.; Heng, S.-H.; Chin, J.-J. A Review of Cryptographic Electronic Voting. Symmetry 2022, 14, 858.
45. Fatrah, A.; El Kafhali, S.; Haqiq, A.; Salah, K. Proof of Concept Blockchain-Based Voting System. In Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT ’19), Rabat, Morocco, 23–24 October 2019; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–5.
46. 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, 323–341.

47. Gupta, S.P.; Tripathi, A.M. E-Voting using Blockchain. J. Physics Conf. Ser. 2021, 1911, 1–14.
48. Qu, W.; Wu, L.; Wang, W.; Liu, Z.; Wang, H. A Electronic Voting Protocol Based on Blockchain and Homomorphic Signcryption. Concurr. Comput. Pract. Exp. 2022, 34, e5817.
49. Carcia, J.C.P.; Benslimane, A.; Boutalbi, S. Blockchain-based system for e-voting using Blind Signature Protocol. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 01–06.
50. Kurbatov, O.; Kravchenko, P.; Poluyanenko, N.; Shapoval, O.; Kuznetsova, T. Using Ring Signatures For An Anonymous E-Voting System. In Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 18–20 December 2019; IEEE: Piscataway, NJ, USA, 2022; pp. 187–190.
51. Bartolucci, S.; Bernat, P.; Joseph, D. SHARVOT: Secret SHARe-Based VOTing on the Blockchain. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB '18), Gothenburg, Sweden, 27 May 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 30–34.
52. Verma, G. A Secure Framework for E-Voting Using Blockchain. In Proceedings of the 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 8 September 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
53. Gupta, S.; Gupta, A.; Pandya, I.Y.; Bhatt, A.; Mehta, K. End to End Secure E-Voting Using Blockchain & Quantum Key Distribution. Mater. Today Proc. 2023, 80, 3363–3370.
54. Chaieb, M.; Yousfi, S. LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol. In Proceedings of the Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, 25–26 November 2020; Springer International Publishing: Cham, Switzerland, 2020.
55. Golnarian, D.; Saedi, K.; Bahrak, B. A decentralized and trustless e-voting system based on blockchain technology. In Proceedings of the 2022 27th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Islamic Republic of Iran, 23–24 February 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
56. Cheema, M.A.; Ashraf, N.; Aftab, A.; Qureshi, H.K.; Kazim, M.; Azar, A.T. Machine Learning with Blockchain for Secure E-voting System. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 177–182.
57. Parmar, A.; Gada, S.; Loke, T.; Jain, Y.; Pathak, S.; Patil, S. Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
58. Li, M.; Luo, X.; Sun, W.; Li, J.; Xue, K. AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 4751–4756.
59. Luo, T. An Efficient Blockchain Based Electronic Voting System Using Proxy Multi-signature. In Proceedings of the 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 10–12 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 513–516.
60. Doost, M.; Kavousi, A.; Mohajeri, J.; Salmasizadeh, M. Analysis and Improvement of an E-voting System Based on Blockchain. In Proceedings of the 2020 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran, 4–6 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–4.
61. Xu, Z.; Cao, S. Efficient Privacy-Preserving Electronic Voting Scheme Based on Blockchain. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 190–196.
62. Khan, K.M.; Arshad, J.; Khan, M.M. Empirical Analysis of Transaction Malleability within Blockchain-Based E-Voting. Comput. Secur. 2021, 100, 102081.