Cluster Computing (2025)28:132
https://doi.org/10.1007/s10586-024-04709-8

Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges

Henry O. Ohize[1,2] · Adeiza James Onumanyi[3] · Buhari U. Umar[4] · Lukman A. Ajao[4] · Rabiu O. Isah[4] · Eustace M. Dogo[4] · Bello K. Nuhu[4] · Olayemi M. Olaniyi[5] · James G. Ambafi[1] · Vincent B. Sheidu[1] · Muhammad M. Ibrahim[1]

Received: 27 May 2024 / Revised: 16 September 2024 / Accepted: 19 September 2024

Abstract

Electronic voting (e-voting) systems are gaining increasing attention as a means to modernize electoral processes, enhance transparency, and boost voters' participation. In recent years, significant developments have occurred in the study of e-voting and blockchain technology systems, hence reshaping many electoral systems globally. For example, real-world implementations of blockchain-based e-voting have been explored in various countries, such as Estonia and Switzerland, which demonstrates the potential of blockchain to enhance the security and transparency of elections. Thus, in this paper, we present a survey of the latest trends in the development of e-voting systems, focusing on the integration of blockchain technology as a promising solution to address various concerns in e-voting, including security, transparency, auditability, and voting integrity. This survey is important because existing survey articles do not cover the latest advancements in blockchain technology for e-voting, particularly as it relates to architecture, global trends, and current concerns in the developmental process. Thus, we address this gap by providing an encompassing overview of architectures, developments, concerns, and solutions in e-voting systems based on the use of blockchain technology. Specifically, a concise summary of the information necessary for implementing blockchain-based e-voting solutions is provided. Furthermore, we discuss recent advances in blockchain systems, which aim to enhance scalability and performance in large-scale voting scenarios. We also highlight the fact that the implementation of blockchain-based e-voting systems faces challenges, including cybersecurity risks, resource intensity, and the need for robust infrastructure, which must be addressed to ensure the scalability and reliability of these systems. This survey also points to the ongoing development in the field, highlighting future research directions such as improving the efficiency of blockchain algorithms and integrating advanced cryptographic techniques to further enhance security and trust in e-voting systems. Hence, by analyzing the current state of e-voting systems and blockchain technology, insights have been provided into the opportunities and challenges in the field with opportunities for future research and development efforts aimed at creating more secure, transparent, and inclusive electoral processes.

Keywords Architectures · Blockchain · Decentralize · E-Voting · Electronic · I-Voting · Survey · Voting

1 Introduction

Electronic voting (e-voting) is a modern approach to the traditional paper-based voting system, leveraging digital technologies to facilitate the casting and counting of votes in elections [1]. As societies embrace technological advancements, e-voting systems are a potential solution to streamline the electoral process, improve accessibility, and enhance the overall efficiency and accuracy of elections [2]. The concept of e-voting encompasses a wide range of technologies and methodologies, each with its own set of advantages, challenges, and considerations. From internet-based voting platforms accessible from personal devices to specialized e-voting machines deployed at polling stations, the landscape of e-voting is diverse and continuously evolving [3]. Despite these benefits, the adoption of e-voting systems raises various technical, legal, and societal considerations. Concerns surrounding cybersecurity

Extended author information available on the last page of the article

Published online: 26 November 2024

vulnerabilities, privacy protection, accessibility for marginalized populations, and the digital divide necessitate careful planning and implementation of e-voting initiatives.

In advancing e-voting systems, the incorporation of blockchain technology is being explored as a transformative solution to the limitations of existing e-voting systems. Blockchain is known for its decentralized, immutable, and transparent nature, and it offers a paradigm shift in how electoral processes can be conducted securely and reliably. By harnessing the unique properties of blockchain technology, e-voting systems can then stand to overcome longstanding challenges and instill greater confidence in democratic elections. The integration of blockchain technology in e-voting thus represents a significant step forward in democratizing electoral processes. By leveraging decentralization, immutability, and transparency, blockchain-based e-voting systems hold the potential to revolutionize how elections are conducted, ensuring fairness, integrity, and inclusivity for all participants [4].

In this regard, the rapidly and ever growing body of knowledge in blockchain technology and e-voting systems necessitates the need for trending, comprehensive, and systematic evaluation of the state-of-the-art developments in this domain. However, there is a limited availability of a thorough synthesis in survey literature regarding major architectural frameworks that integrate blockchain technologies. Consequently, in this article, we present a comprehensive survey of e-voting systems, focusing on key aspects such as architectural frameworks, advancements in blockchain technology, performance constraints, and strategies to address emerging concerns. In particular, this survey emphasizes the technological innovations that blockchain introduces to e-voting systems, including advanced cryptographic techniques, decentralized ledger architectures, and improved consensus mechanisms. These innovations are critical in addressing the inherent challenges of security, scalability, and transparency in e-voting, which offers new pathways to enhance the reliability and trustworthiness of electoral processes. By exploring the evolving landscape of e-voting, this survey aims to provide insights into the current state-of-the-art, as well as future directions for research and development in this critical domain. In light of this, the contributions of the present survey can be summarized as follows:

1. We present a survey of e-voting systems, focusing on key aspects such as architectural frameworks, advancements in blockchain technology, performance constraints, and strategies to address emerging concerns. This includes an in-depth analysis of how blockchain's decentralized and immutable properties can be leveraged to create more secure and transparent voting systems.
2. We explore the integration of blockchain technology in e-voting systems, analyzing recent developments, and innovations in leveraging distributed ledger technology to enhance security, transparency, and verifiability. Particularly, we discuss how recent advancements in cryptographic methods, such as homomorphic encryption and zero-knowledge proofs, are being used in conjunction with blockchain to ensure end-to-end vote integrity and auditability.
3. We highlight performance constraints inherent in e-voting systems, including scalability, efficiency, and usability considerations. As e-voting platforms strive to accommodate growing populations and increasingly complex election processes, optimizing performance becomes paramount to maintaining the integrity and efficiency of the electoral process. Additionally, this survey identifies innovative blockchain-based solutions that address these constraints, which ensures that e-voting systems can scale effectively while maintaining security and user accessibility.

An outline of the rest of this article is given as follows: Sect. 2 provides a discussion of related survey articles as a means of distinguishing the present article from existing survey articles. Section 3 describes the methodology used in designing and conducting this survey work, Sect. 4 gives a broad overview of e-voting process and systems, while Sect. 4.3 focuses on traditional architectures. In Sect. 5, we discuss blockchain-based e-voting systems while Sect. 6 dives into research endeavours in blockchain for e-voting. Section 7 highlights the technical challenges and concerns and Sect. 8 lists future research directions, while the conclusion is presented in Sect. 9.

2 Related survey articles

There are many survey articles on e-voting systems that cover various aspects of the system. However, the goal of this section is to highlight the gap covered in our survey. Furthermore, we have documented additional survey references in Table 1 for readers interested in exploring other facets of e-voting systems.

Specifically, Table 1 presents a summary of related survey works focusing on various aspects of e-voting systems and their integration with blockchain technology. For example, the survey in [4] concentrates on e-voting systems with emphasis on blockchain, and offering structured solutions aimed at enhancing security, transparency, privacy, and scalability. In another survey [5], the authors

Table 1 Related survey papers

References	Year	Main focus	Specific details
[4]	2023	e-voting systems with emphasis on blockchain	• Structured solutions for blockchain-based e-voting systems with specific interest in security, transparency, privacy, and scalability
[5]	2023	e-voting systems with cryptography techniques	• Trends in blockchain technologies in e-voting system integrated with IoT, • E-voting systems in an IoT environment and sensor network
[6, 7]	2022	Decentralization of authority in electoral processes	• Development of Ethereum framework which primarily uses Solidity as a language • Roadmap for blockchain technologies developing in e-Voting
[8–10]	2022	Secured e-voting framework that uses blockchain technology	• Emphasis on potential benefits and concerns in e-voting systems • Introduction of e-voting framework • Comparative study of different e-voting systems
[11]	2022	Review of literature in blockchain technology between 2011 to 2020	• Blockchain technology were studies that include smart contracts, Zcash platform, blockchain programmed from scratch, and blockchain depending on digital signature • Features and limitations of Blockchain
[12, 13]	2020	Application of blockchain technology on e-voting	• Emphasis on challenges of e-voting systems • Implementation of voter systems architecture
[9, 14, 15]	2022	Systematic review of literature in blockchain technology on e-voting	• A systematic study that summarizes the current research in e-voting, with blockchain technology • Background information on current e-voting systems, the blockchain concept and its applications are introduced • Gaps and solutions to current e-voting systems, potentials of the blockchain concept to improve e-voting
[16]	2022	State-of-the-art review of blockchain-based e-voting system	• A systematic review of e-voting system • Introduction to TrustVote system • Gaps and solutions to current e-voting systems
[17]	2021	Review of implementations in distributed ledger voting technology	• Review of e-voting systems based on blockchain technology • Identification of countries that have implemented e-voting technology
[18]	2021	Comparative analysis of various blockchain techniques	• Address the challenges associated with traditional voting systems • Comparative review of e-voting systems based on blockchain technology
[19–21]	2020	Application of blockchain technology on e-voting	• Survey of e-voting systems across the globe • Developments in blockchain-based e-voting systems • Comparison of several blockchain-based e-voting schemes
[22]	2021	Review of blockchain-based voting systems and classification	• Comprehensive review of blockchain-based voting systems • Classification based on a number of features • Identification of limitations and research opportunities
[23]	2023	Review of some decentralized e-voting systems	• Proposed an e-stamping technique in digital voting system • Proposed an Android application for E-voting system using Blockchain and Cloud Server
[24]	2023	Review on Blockchain-based e-voting systems	• Properties of a robust e-voting system • Emphasis on some cryptography techniques such as zero-knowledge proofs, zk-SNARKs, ring signatures, blind signatures, homomorphic encryption, mix-networks, secret sharing scheme, and elliptic curve • Comprehensive review of some blockchain-based e-voting systems with their strengths and weaknesses

explored e-voting systems incorporating cryptography techniques, highlighting trends in blockchain technologies integrated with IoT and their application in sensor networks. In [6], the decentralization of authority in electoral processes was discussed, further proposing the development of an Ethereum framework primarily utilizing the Solidity programming language. Additionally, they

provided a roadmap for the development of blockchain technologies in e-voting.

In [7], the focus was on secured e-voting frameworks leveraging blockchain technology. The authors emphasized the benefits and concerns associated with e-voting systems, and also introduced an e-voting framework, while conducting a comparative study of different e-voting systems. Similarly, the authors in [11] conducted a comprehensive review of blockchain technology between 2011 and 2020. Their review encompassed studies on smart contracts, the Zcash platform, blockchain programmed from scratch, and blockchain relying on digital signatures. They also discussed the features and limitations of blockchain technology.

Although the survey works mentioned in Table 1 are worthwhile, nevertheless, for effective planning, development, and implementation of e-voting systems, several foundational aspects require thorough examination beforehand. From an engineering perspective, this involves determining the most suitable architecture, ensuring efficient integration with e-voting applications and services, and addressing scalability concerns. There challenges constitute a noticeable absence in most survey articles, thus highlighting a gap that warrants attention for the contemporary reader or researcher interested in exploring the subject matter. Consequently, the specific topics explored in this article were formulated based on critical inquiries discussed in the methodology adopted for this survey.

Additionally, Table 2 reveals the limited presence, if any, of broad survey papers on contemporary e-voting design architectures, as far as the authors are aware. The legend in Table 2 implies that the relevant item was covered in the survey paper. Each label is described as follows: BB = Blockchain-based means approaches, systems, or methodologies that are built on or utilize blockchain technology were discussed. CT = Cryptography Techniques: the survey covered the use of cryptographic methods and protocols to secure data and communications. D = Decentralization techniques: The techniques that distribute control and decision-making away from a central authority, promoting a decentralized network or system were covered. SF = Security Focus: the survey emphasized aspects related to the protection of data, systems, and networks from unauthorized access, attacks, or vulnerabilities. CA = Comparative Analysis: the authors compared and contrasted different methods, systems, or technologies to evaluate their relative strengths, weaknesses, and performance. RM = Review Methodology: authors described the systematic approach used to review and analyze existing literature, studies, or technologies. AD = Architecture described: Indicates that the structural design or framework of a system, technology, or process was explained or detailed. CB = Country-based: authors discussed studies, data, or analysis that are specific to or based on individual countries or regions. BE = Blockchain Evolution: the survey discussed the development, advancements, and historical progression of blockchain technology over time. We highlight the gaps in the survey literature in Table 2 showing the relevance the current survey article. Thus, following the findings of Table 2, the primary objective of this article is to provide a more robust review of trends and advancements in e-voting system focusing on blockchain integration from an architectural perspective.

Table 2 Gaps in related surveys

References	Year	BB	CT	D	SF	CA	RM	AD	CB	BE
[12, 13]	2020	✓	X	X	✓	X	X	X	X	X
[19–21]	2020	✓	X	X	X	✓	X	X	X	X
[17]	2021	✓	X	X	X	X	X	X	X	X
[18]	2021	✓	X	X	X	✓	X	X	X	X
[22]	2021	✓	X	X	X	✓	X	X	X	X
[6, 7]	2022	✓	X	✓	X	X	X	X	X	X
[8–10]	2022	✓	X	X	✓	✓	X	X	X	X
[11]	2022	✓	X	X	X	X	X	X	X	X
[9, 14, 15]	2022	✓	X	X	X	✓	✓	X	X	X
[16]	2022	✓	X	X	X	X	✓	X	X	X
[4]	2023	✓	X	X	✓	X	X	X	X	X
[5]	2023	✓	✓	X	X	X	X	X	X	X
[23]	2023	✓	X	✓	X	X	X	X	X	X
[24]	2023	✓	✓	X	X	X	✓	X	X	X
Current	2024	✓	X	✓	✓	✓	✓	✓	✓	✓

BB blockchain-based, *CT* cryptography techniques, *D* decentralization techniques; *SF* security focus, *CA* comparative analysis, *RM* review methodology, *AD* architecture described, *CB* country-based, *BE* blockchain evolution

3 Survey methodology

This section describes the methodology used in this survey based on the approach reported in [25, 26]. The steps of the methodology are presented in Fig. 1. Firstly, we observed that the development and deployment of e-voting systems is of increasing importance in many democratic governments globally. Therefore, in order to conduct a survey in this regard, we constructed research questions using carefully selected e-voting related keywords. This was then followed by an appropriate article search and selection approach, evaluation, and synthesis of the materials discovered, and reporting of our survey article. The evaluation followed the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) guidelines, which guarantee a rigorous and transparent methodology for the synthesis of available research data. The PRISMA protocol is a reporting guideline designed to aid researchers in the

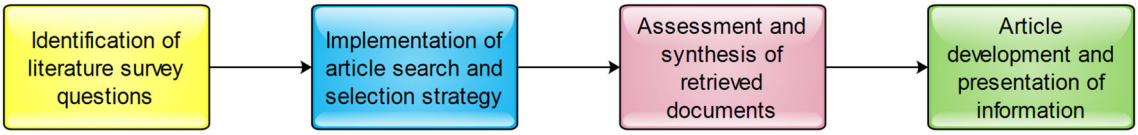


Fig. 1 Survey methodology [25]

preparation and documentation of systematic review and meta-analysis protocols [27]. The details of the adopted approach are presented in the subsequent subsections.

3.1 Literature survey questions

In order to understand e-voting systems, it is essential to grasp the concept of its components. To achieve this, we conducted a search of the scholarly literature to identify existing survey studies on e-voting systems and their constituent components. The results of our search are detailed in this section. Although many survey articles exist, we found minimal synthesized information on three critical components, namely the suitable architectures for e-voting system deployment, the latest advancements in blockchain-based e-voting, and security solutions for e-voting systems. These gaps thus prompted our further exploration of the subject matter leading to the following research questions:

1. What are the most feasible architectures for establishing e-voting systems, including their advantages and disadvantages?
2. How are these architectures implemented for blockchain-based e-voting systems?
3. What are the fundamental components and current improvements in blockchain technology necessary for the effective implementation of e-voting systems?
4. What are typical threats, goals, and solutions associated with the successful implementation of e-voting systems?
5. What are the research challenges and possible future prospects for the development/enhancement of architectures and security concerns in e-voting systems?

After developing these questions, we conducted a second literature search to determine whether these questions had been appropriately answered and synthesized in other related survey publications. Upon finding that these questions were either sparsely covered or not addressed, we proceeded to the article search and selection phase.

3.2 Search and selection strategy

Our article selection criteria centered on research works dealing with architectures, e-voting, blockchain, and security in e-voting systems. The following is an explanation of the approach used to determine the selected papers:

1. We searched for articles using the Scopus, ACM Digital Library, IEEE Xplore, SpringerLink, and Google Scholar databases. We considered the Scopus database for its high-quality indexing and computer science-related information. Similarly, IEEE Xplore, which focuses mostly on computer science, engineering, and electronics, received similar consideration. Due to their magnitude and potential to locate relevant papers, we also analyzed the ACM, MDPI, and Springer databases. Following our exploration of these databases, we performed a final double-check using the Google Scholar database to minimize the chance of missing articles.
2. Next, we identified terms that define our area of interest, namely "architectures", "e-voting", "i-voting", "blockchain", and "security". These keywords were derived from a preliminary literature search to locate survey publications that had previously addressed the same issues. In addition, we generated a list of search strings that combine the operators "AND" and "OR" with keywords and the term "e-voting".
3. These keywords and phrases were used to search databases mentioned above such as Scopus and Google Scholar, among others considered.
4. The search yielded more than 22,000 results, which were then narrowed down based on the time span covered within the previous two decades. Furthermore, these results were refined based on the following key categories: "architectures", "e-voting", and "blockchain". These keywords were used to manually reduce the number of articles to 250. The excluded articles were those that did not directly contribute to our area of interest. While 250 articles were carefully considered during the survey process, only 165 of these were ultimately cited after thorough evaluation for their direct relevance to the focus of this paper.
5. Furthermore, survey papers located within this list were filtered and evaluated to determine the uniqueness of our present article; our findings have been discussed in the related literature survey in Sect. 2. After obtaining the initial documents based on search

process, we then evaluated their quality and began the reading and synthesis of the acquired articles.

3.3 Assessment and synthesis of information

To assess the quality of the retrieved documents, we established specific inclusion and exclusion criteria to refine our methodology. These specifications are outlined as follows:

3.3.1 Inclusion criteria

1. All articles must have been published in academic journals or conference proceedings.
2. Relevant survey articles must be highly specific and directly related to the components of e-voting systems.
3. The discovered articles aligned with the provided keywords must have discussed these keywords extensively rather than simply mentioning them.

3.3.2 Exclusion criteria

1. Articles without full text were excluded.
2. Articles that only mentioned the keywords without substantial discussion were ignored.
3. Preprints, reports, lecture notes, and proposals were discarded from consideration since they provided little accessible details void of the peer review process.

After applying these inclusion and exclusion criteria to filter the identified articles, we further assessed their quality by:

1. Generating a set of questions and answers to evaluate the contextual information of each article.
2. Determining whether the article discusses the questions raised in Sect. 3.1. If yes, the article was considered for further analysis. If not, we assessed whether the discussion was comprehensive enough to warrant further study.
3. We employed the same assessment questions for each keyword to ensure the relevance of the retrieved articles for further synthesis.

With the goal of constructing a traditional literature review article, we meticulously examined each of the articles. We then synthesized the information within each article in relation to the research questions and provided an overview of the contextual information gathered.

3.4 Article development and presentation of information

After gathering and synthesizing pertinent contextual information around each keyword and research question, we proceeded to refine and improve the structure of our article. To achieve this, the following strategy was adopted:

1. Following the popular PRISMA framework, we constructed the outline for our manuscript. Given our objective to present a traditional literature survey article, the body of the manuscript was divided into six main sections based on the title and keywords. This approach helped clarify the scope of our article. However, in the absence of separate results and discussion sections, we incorporated summaries for each section, along with a conclusion addressing research challenges and future directions within the body of work.
2. The synthesized information was organized into clusters based on how each article related to the research questions. Subsequently, each section was expanded to include an analysis of the advantages and disadvantages of different e-voting-related methods.
3. The final draft of our manuscript underwent revision to ensure alignment with the overarching purpose, which was to provide a comprehensive overview of e-voting, architectures, and security to facilitate the development of viable e-voting systems.

Consequently, the process of structuring and refining the article while maintaining coherence and readability was ensured so that we present a comprehensive overview of e-voting systems and related components.

4 Overview of the e-voting process, system components, and architectures

4.1 Overview of the e-voting process and system components

Generally, a typical e-voting process consists of key stages including registration, authentication and authorization, vote casting, vote counting, and vote verification [28–30]. Figure 2 depicts this process showing the electronic devices for voting and registration, a registration agent, a voting manager, an encrypted database, and an electronic election bulletin board. The process is briefly discussed as follows:

4.1.1 Voter registration

The process begins with the voter interacting with a registration agent. The registration agent is responsible for

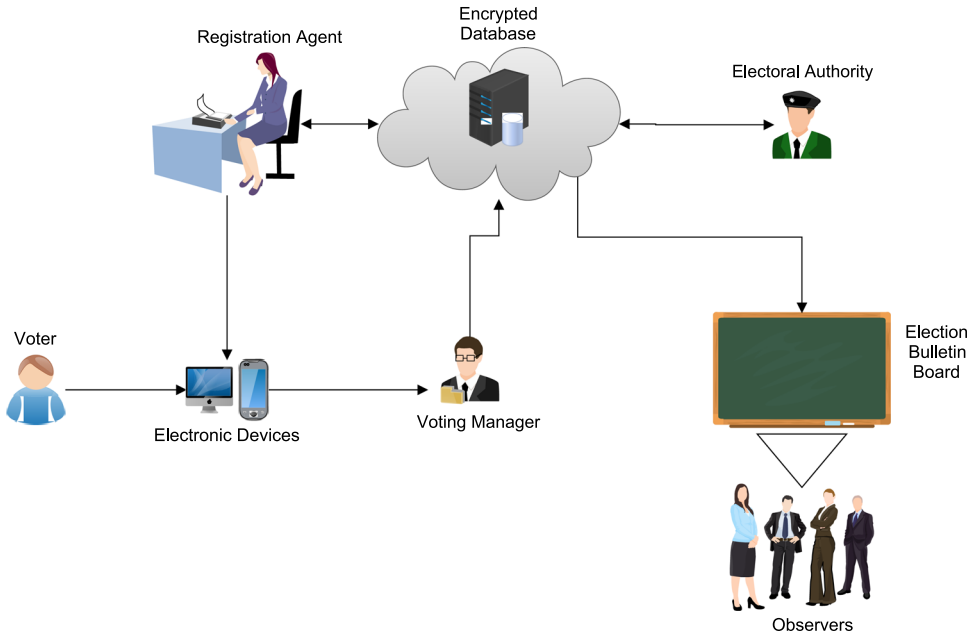


Fig. 2 Typical e-voting process

verifying the identity of the voter and ensuring they are eligible to participate in the election. Once the voter's identity is verified, the voter is registered in the encrypted database. This database securely stores the information necessary to authenticate the voter during the voting process.

4.1.2 Casting of vote

The registered voter proceeds to use an electronic device to cast their vote. This device could be a voting machine located at a polling station or a personal device used for internet-based voting. The voter's choices are encrypted to ensure the confidentiality and integrity of their vote. This encryption prevents unauthorized parties from viewing or altering the vote.

4.1.3 Vote verification and counting

The voting manager is responsible for managing the collection and initial processing of the votes. This role includes ensuring that all votes are properly encrypted and posted to the bulletin board. The voting manager decrypts and verifies the voter's authenticity using biometric data, RFID, etc. The voting manager then retrieves the ballot for eligible candidates and after authentication, voters can use the voting console to cast their votes. The voting manager further stores votes in the encrypted database and electronic bulletin board, providing a voting receipt to each voter. On the other hand, the electoral authority oversees the entire election process. This authority has access to the tools and methods required to decrypt the votes for counting while maintaining voter anonymity. The encrypted vote is then sent to the election bulletin board. This bulletin board acts as a public ledger where all encrypted votes are posted. The bulletin board ensures transparency and allows voters and observers to verify that votes have been recorded correctly. Observers can monitor the election bulletin board to ensure the election process is conducted fairly and transparently. The electronic bulletin board, consisting of vote repositories and a counting unit, also stores encrypted ballots. Consequently, the election representatives and observers provide their private keys post-election and then the counting unit, armed with these keys, begins counting votes and sends results to the election bulletin board.

4.1.4 Announcement of results

Once the votes have been verified and counted, the results are announced. This process involves decrypting the votes in a manner that ensures individual voter choices remain confidential.

Throughout the entire process, the system incorporates various security measures to protect against fraud and tampering. Encryption ensures that votes cannot be altered once cast, and the public nature of the election bulletin board allows for independent verification of the process. The presence of observers adds an additional layer of oversight, ensuring that the election is conducted in a fair and transparent manner. Thus, the e-voting process described is a traditional one involving secure voter registration, encrypted vote casting, public posting of encrypted votes, monitored vote verification and counting,

and secure announcement of results, all overseen by an electoral authority and observed by independent parties to ensure transparency and integrity. In the next section, we will discuss the architectures that ensure that such security measures can be realized.

4.2 Key components of an e-voting system

Understanding the key components of an e-voting system is crucial for effectively realizing the voting process because it ensures the system's integrity, security, and transparency. By comprehensively grasping each element from voter registration and authentication to vote casting, encryption, and final tallying, stakeholders can design, implement, and manage a system that upholds fair democratic principles. Knowledge of these components helps in identifying potential vulnerabilities, ensuring robust security measures, and facilitating a transparent process that voters can trust. Additionally, understanding these components aids in compliance with legal standards, enhancing accessibility, and improving overall efficiency, thus fostering a reliable and inclusive electoral process. We mention some of these key components of an e-voting system as follows:

- Voter interface: This component provides the interface through which voters interact with the e-voting system. It can include various options such as web-based portals, mobile applications, or dedicated voting machines located at polling stations [30]. The voter interface should be intuitive, accessible, and user-friendly to ensure widespread adoption and participation.
- Authentication and authorization: Before casting their votes, voters need to be authenticated to verify their eligibility and authorization to participate in the election. Authentication mechanisms often involve the use of unique identifiers such as voter IDs, biometric data, or cryptographic keys to ensure the integrity and security of the voting process [31].
- Ballot generation and presentation: The e-voting system generates digital ballots based on the specific election and candidates or issues to vote on. These ballots are presented to voters through the voter interface, allowing them to make their selections securely and privately [32]. The presentation of the ballot should be clear and understandable to prevent confusion or errors in voting.
- Vote casting and encryption: Once voters have made their selections, the e-voting system securely records and encrypts their votes to maintain confidentiality and integrity. Encryption techniques are employed to prevent tampering or interception of votes during transmission and storage. Additionally, cryptographic protocols may be used to ensure that each voter's identity remains anonymous while still allowing them to verify that their vote was accurately recorded.
- Vote storage and aggregation: The encrypted votes are stored securely in a central database or distributed ledger, depending on the architecture of the e-voting system. These votes are aggregated and tallied to determine the overall outcome of the election. Strong security measures, such as access controls and audit trails, should be implemented to protect the integrity of the vote storage and aggregation process [33].
- Auditing and verification interface: E-voting systems typically incorporate mechanisms for auditing and verifying the integrity of the voting process. Independent third parties, election officials, and even voters themselves may have access to tools or protocols to verify that votes were cast and counted correctly [34]. Auditing procedures help detect and mitigate any potential vulnerabilities or discrepancies in the system.
- Resilience and redundancy: To ensure the reliability and availability of the e-voting system, redundancy and resilience measures are often implemented. This may include backup servers, redundant data storage, failover mechanisms, and contingency plans for handling technical failures or cyberattacks during the election process [35]. The above components are listed pictorially in Fig. 3.

4.3 Architectures of e-voting systems

An e-voting architecture refers to the structure and interconnection of the key components of an e-voting system used to facilitate the secured casting and counting of votes in elections. For the success of any e-voting system, the necessity of an architecture is crucial because it aims to

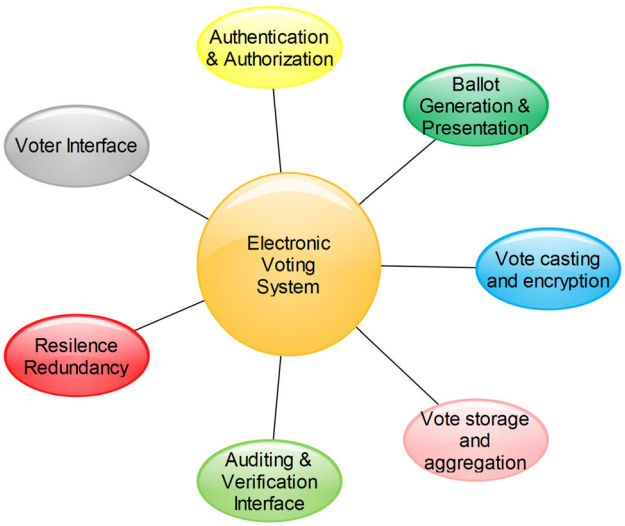


Fig. 3 Key components of an e-voting system

provide a secure, efficient, and accessible means for citizens to participate in democratic processes [36]. Consequently, the study of e-voting architectures is important and their structure can vary depending on the specific components, implementation, and technological advancements thereof. Furthermore, understanding the different fundamental architectures of e-voting systems is crucial to assess their strengths and weaknesses. Therefore, in this section, we discuss the different architectures of e-voting systems, focusing on their advantages and disadvantages and their comparative analysis. Generally, e-voting architectures can be categorized into two broad types; the centralized and the distributed architectures discussed as follows:

4.3.1 Centralized architecture

The structure of the centralized e-voting architecture consists of a central server, which coordinates and manages the multifaceted dimensions of the electoral process as shown in Fig. 4. This architecture necessitates voters' engagement through designated terminals or voting machines, fostering a controlled environment conducive to critical functions such as voter registration, ballot casting, and result aggregation.

The centralized e-voting architecture is designed to manage the entire e-voting process from a central authority, ensuring efficiency, security, and transparency. It consists of a central server, managed by the Electoral Authority, which is the core component of the system. The authority oversees the entire voting process, from voter registration to the final tallying of votes. It ensures the integrity and security of the election. The central server is responsible for handling the registration of voters. Essentially, the identities of the voters are verified and securely stored in the encrypted centralized database, which ensures that only eligible voters can participate in the election.

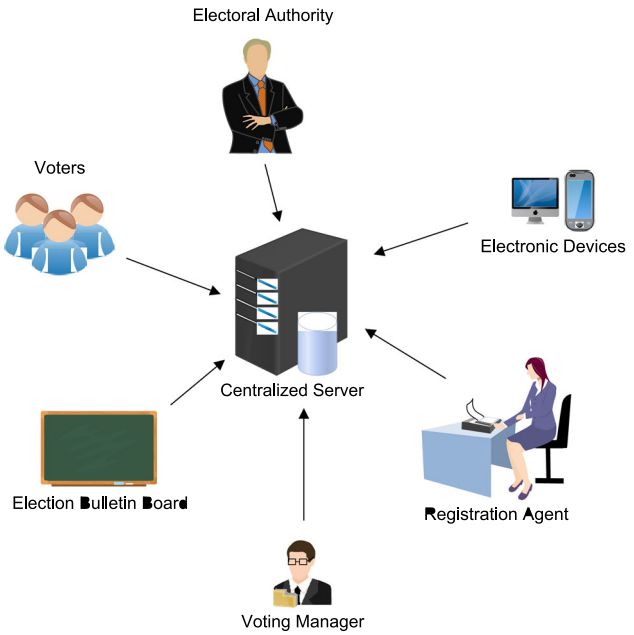


Fig. 4 Centralized architecture

The architecture also consists of the voting devices used by voters to cast their votes. They can be specialized e-voting machines located at polling stations or personal devices such as computers or smartphones for internet-based voting. These voting devices are connected to the central server to receive voter authentication and submit encrypted votes. The central database then securely stores all the encrypted votes cast by the voters. The encryption used ensures that the votes remain confidential and tamper-proof until they are decrypted for counting. The database also ensures that votes cannot be altered or accessed by unauthorized parties. One approach to achieving this is by using blockchain technology, which will be discussed in more detail.

The centralized architecture incorporates some level of security to protect against fraud and tampering, including using encryption and secure databases, which allows for verification of the voting process by observers and the public. However, it has its advantages and disadvantages highlighted as follows:

Advantages of centralized architecture:

1. A single authority manages the entire process, thus reducing the complexity and potential for errors associated with decentralized systems.
2. It simplifies the coordination and administration of the voting process.
3. They can be more easily monitored and secured as there are fewer points of vulnerability compared to distributed architecture.
4. Easier to scale up for larger elections without the need for significant additional infrastructure.
5. Centralized databases reduce the risk of data inconsistencies and can improve data integrity by providing centralized logging mechanisms, and unified data management and repository systems.

Disadvantages of centralized architecture:

1. A single point of failure is created, which can be compromised and the election process could be disrupted.
2. It can be an attractive target for cyber-attacks due to the concentration of critical data at a centralized location.
3. Concerns about transparency and fairness of the process can arise if the central authority is not fully trusted by the public.

4. Large-scale centralized systems can require significant resources, especially during peak voting periods.
5. Performance bottlenecks can arise under high voter turnout if the central infrastructure is not adequately robust.

4.3.2 Decentralized architecture

In the decentralized e-voting architecture, the management and operation of the voting process are distributed across multiple nodes rather than relying on a single central authority. This architecture leverages blockchain technology or other distributed ledger systems to ensure transparency, security, and trustworthiness in the electoral process as shown in Fig. 5. Each node (i.e., electronic device, bulletin board, database) in the decentralized network maintains a copy of the voting ledger, allowing for a highly resilient and tamper-resistant system. Decentralization mitigates the risks associated with a single point of failure and enhances the robustness of the voting system against cyber-attacks and technical failures. In the decentralized e-voting architecture, the main components include voter registration nodes, voting nodes, a distributed ledger, and verification nodes. Voter Registration Nodes are responsible for validating the identity of voters and ensuring they meet eligibility criteria. Once validated, voter information is securely recorded on the distributed ledger. Voting Nodes are used by voters to cast their votes. These nodes can be personal devices such as computers or smartphones, or specialized voting terminals located at polling stations. Votes are encrypted and recorded on the distributed ledger in real-time, ensuring immediate and verifiable logging of each vote.

The security of a decentralized e-voting system is largely derived from its distributed nature. With multiple nodes participating in the network, the system is highly resistant to tampering and fraud. Blockchain technology ensures that once a vote is recorded, it cannot be altered without the consensus of the network, making the voting process immutable and transparent. Each transaction (vote) is cryptographically secured, and its integrity is continuously validated by consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS). This consensus ensures that all nodes in the network agree on the state of the ledger, preventing any single entity from unilaterally altering the results.

One of the significant advantages of decentralized e-voting architectures is the transparency it offers. The distributed ledger is publicly accessible, allowing any stakeholder, including voters, election observers, and auditors, to verify the authenticity and accuracy of the recorded votes. This transparency builds trust in the electoral process, as stakeholders can independently verify that votes have been counted correctly and that the election is

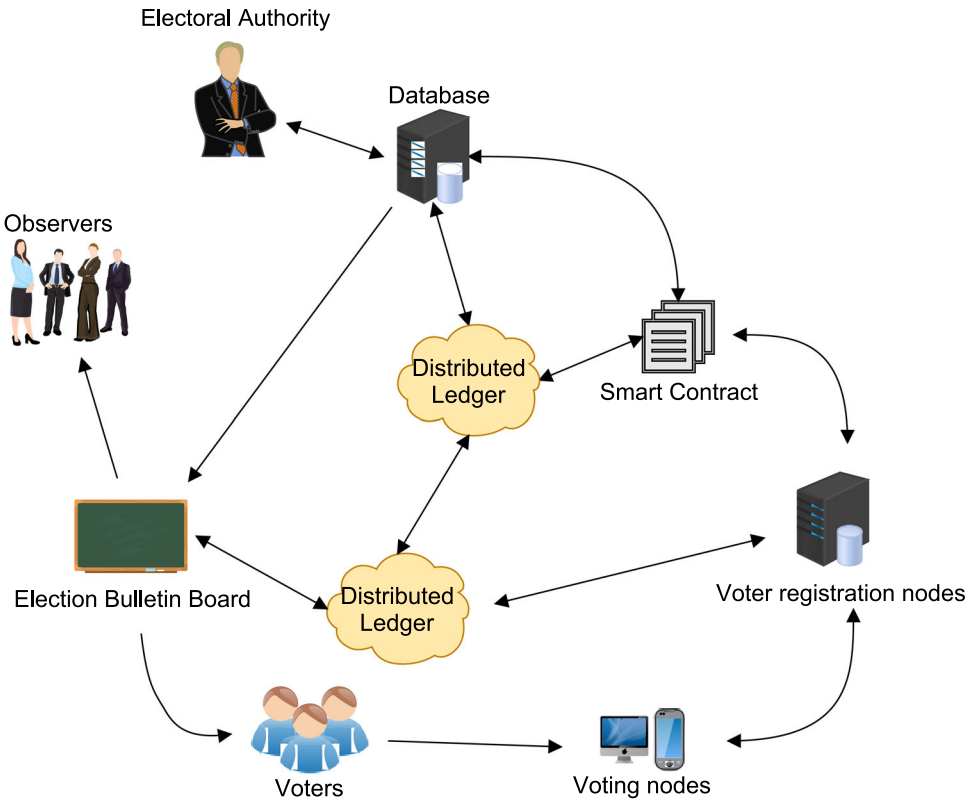


Fig. 5 Decentralized architecture

conducted fairly. Furthermore, decentralized systems empower voters by providing them with direct evidence of their participation and the inclusion of their votes, enhancing confidence in the democratic process. This approach to e-voting fosters a more open, accountable, and resilient electoral system. However, it has its advantages and disadvantages highlighted as follows:

Advantages of decentralized architecture:

1. The decentralized nature of the architecture makes it highly resistant to tampering and fraud since consensus of multiple nodes is needed to alter data.
2. The distributed ledger is publicly accessible, thus allowing voters, observers, and auditors to verify the authenticity and accuracy of the recorded votes.
3. Being decentralized, there is no single point of failure, thus ensuring that the failure of one or a few nodes does not compromise the entire voting process.
4. The architecture is resilient to attack as attacking a single node or small group will not disrupt the entire system.
5. Enhances voters' confidence since records can be verified, which makes it highly transparent.

Disadvantages of decentralized architecture:

1. It is highly technical and complex to implement, which can make it challenging to deploy and coordinate.
2. It can face scalability issues since high voter turnout can lead to performance bottlenecks, slowing down the voting and counting process.
3. Consensus mechanisms like PoW can be resource-intensive, thus requiring significant computational power and energy.
4. The implementation process will entail regulatory and legal challenges since it crosses multiple jurisdictions, thus introducing inconsistencies and complicated regulations required in the smart contract development process. We summarize by presenting a comparison of both architectures in Table 3.

5 Blockchain-based e-voting systems

Being a popular and widely deployed distributed ledger system, in this section, we synthesize the literature regarding the use of blockchain technology in e-voting systems. Firstly, we provide a background to blockchain as technology, and then we discuss its basic working principles as well as the different types of blockchain-based architectures. Thereafter, we present reasons to decide between blockchain and non-blockchain voting architectures. Focus is then placed on the research efforts and evolution in blockchain systems for e-voting, and case studies of its use globally.

5.1 Blockchain technology

The concept of blockchain technology is well documented in the literature, however, in this section, we provide a brief overview of blockchain, discussing what is blockchain, why we need blockchain and we proceed to provide some basic blockchain characteristics that make the technology useful for e-voting systems. Nevertheless, for further in-depth discussions of blockchain technology, readers can access the following foundational materials in [37–39] and references therein.

5.1.1 Overview of blockchain

Blockchain technology is a decentralized and distributed digital ledger system that records transactions across a network of computers in such a way that the recorded transactions cannot be altered retroactively, making it highly secure and transparent [40]. By being decentralized, this means that the control and storage of data are distributed across multiple nodes in a network, rather than being managed by a single central authority, which leads to greater security, transparency, and resistance to manipulation. In blockchain, a transaction is referred to as block, and it is linked to the previous one through cryptographic hashes, which creates an immutable chain of records. This approach thus eliminates the need for a central authority, because consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) can be used to validate and confirm transactions across the network [37]. Furthermore, the decentralized nature of blockchain enhances security by reducing the risk of single points of failure and it ensures transparency as all participants can verify the transactions. These characteristics make blockchain suitable for applications requiring high levels of trust and security, such as in financial services, supply chain management, and notably, in securing e-voting systems where the integrity, privacy, and transparency of votes are critical. Many recent studies have highlighted the potential of blockchain to revolutionize traditional systems by providing a secure and verifiable method for recording and auditing transactions or votes, which then helps to enhance trust in the processes it supports [37–40].

Blockchain technology is essential in many modern systems because it addresses key challenges related to security, transparency, and trust in digital transactions. Most traditional systems often rely on centralized authorities, which makes them vulnerable to single points of failure and potential corruption. Thus, the decentralized nature of blockchain technology eliminates this

Table 3 Comparison of centralized and decentralized e-voting architectures

Feature	Centralized	Decentralized
Control	Managed by a single central authority	Distributed control among multiple nodes
Data Management	Centralized database	Distributed ledger (e.g., blockchain)
Security	Centralized security protocols; vulnerable to single point of failure	Enhanced security; resistant to tampering and fraud due to consensus mechanisms
Transparency	Managed by the central authority; transparency depends on the authority	High transparency; publicly accessible ledger allows for independent verification
Fault Tolerance	Vulnerable to single point of failure	High fault tolerance; no single point of failure
Scalability	Easier to scale for larger elections but may face performance issues under high load	Scalability can be challenging; performance bottlenecks possible, especially with consensus mechanisms
Complexity	Simpler to implement and manage	Technically complex; requires advanced knowledge of blockchain and distributed systems
Maintenance	Easier to maintain and upgrade	Maintenance and upgrades are challenging due to the need for coordination among multiple nodes
User Accessibility	Generally more user-friendly; less dependent on individual technical capability	Can be less accessible; requires users to have access to and understanding of the necessary technology
Trust	Trust depends on the central authority	High trust due to transparency and independent verification
Regulatory Compliance	Easier to comply with existing laws and regulations	May face legal and regulatory challenges; existing frameworks may need to be updated

vulnerability by distributing control across multiple nodes, ensuring that no single entity can alter the transaction records without consensus from the network, thereby significantly enhancing security [40]. Additionally, blockchain provides an immutable ledger where all transactions are transparently recorded and cannot be altered retroactively, thus fostering trust among participants since all can independently verify the integrity of the records [38]. This transparency is valuable in applications like supply chain management, where stakeholders need to trace the provenance and authenticity of goods, or in financial services, where ensuring the integrity of transactions is paramount [39]. Furthermore, blockchain prevents fraud and double-spending, which refers to the fraudulent act of using the same digital currency or token more than once, effectively creating a duplicate transaction that illegitimately increases the amount of currency in circulation. This ensures that all transactions are legitimate and agreed upon by the majority of the network, which is crucial in systems like electronic voting where the integrity and security of votes must be guaranteed [37]. Consequently, blockchain technologies have found widespread patronage in many application areas, for example, they have been considered in the development of currencies for central banks [41], in the development of different cryptocurrencies [41], finding hidden patterns in covert communication systems [42], and interestingly for self-tallying e-voting systems with public traceability [43]. Additionally, blockchain has been utilized to improve the commute experience for private car users through blockchain-enabled multitask learning [44], orchestrate service function chains across multiple domains [45], and enable dynamic network function provisioning for industrial applications [46]. These examples illustrate the diverse and innovative applications of blockchain technology across various fields, further underscoring its potential to revolutionize modern systems.

5.1.2 Key characteristics of blockchain

The core characteristics of blockchain technology that makes it suitable for enhancing the security, transparency, and trustworthiness of e-voting systems are as follows:

- Decentralization: Unlike traditional systems that rely on a central authority, blockchain operates on a decentralized network of nodes. Each node maintains a copy of the ledger, ensuring that no single entity has control over the entire network. This decentralization is crucial in preventing fraud and ensuring that the e-voting process remains tamper-resistant.
- Immutability: Once a transaction (or in the case of e-voting, a vote) is recorded on the blockchain, it cannot be altered or deleted. This immutability guarantees the integrity of votes, as each vote is securely recorded and cannot be changed once cast.
- Transparency: Blockchain provides a transparent system where all participants can view the recorded transactions. In e-voting systems, this transparency allows voters, candidates, and observers to verify that

votes have been recorded and counted correctly, enhancing trust in the electoral process.

- Security: Blockchain uses advanced cryptographic techniques to secure transactions. Each block in the blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data. This structure makes it extremely difficult for malicious actors to alter the recorded data, as doing so would require changing every subsequent block in the chain.
- Consensus mechanisms: Blockchain relies on consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate and confirm transactions. In the context of e-voting, these mechanisms ensure that votes are accurately recorded only after they are validated by a majority of the network nodes, preventing double voting and other fraudulent activities.

5.1.3 Application in e-voting systems

The application of blockchain in e-voting systems is driven by its ability to provide a secure, transparent, and decentralized platform for electoral processes. By leveraging blockchain, e-voting systems can address many of the challenges faced by traditional voting systems, including:

- Voter authentication and registration: Blockchain can be used to create a tamper-proof voter registry, ensuring that only eligible voters can participate in the election. Each voter's identity is securely recorded on the blockchain, preventing duplicate registrations and unauthorized access.
- Secure vote casting: Votes are recorded on the blockchain in an encrypted form, ensuring that voter privacy is maintained. Once cast, a vote is securely recorded on the blockchain and cannot be altered or deleted, ensuring the integrity of the electoral process.
- Transparency and auditability: Blockchain allows for real-time auditing of the voting process. Stakeholders can monitor the blockchain to verify that all votes have been accurately recorded and counted. This transparency helps to build trust in the electoral process.
- Decentralized vote counting: Blockchain enables decentralized vote counting, where votes are tallied across multiple nodes in the network. This decentralization reduces the risk of manipulation and ensures that the results are accurate and reflect the will of the voters.

In conclusion, blockchain technology offers a robust framework for enhancing the security, transparency, and efficiency of e-voting systems. By leveraging the key characteristics of blockchain, e-voting systems can overcome many of the limitations and challenges associated with traditional voting methods, paving the way for more secure and trustworthy elections.

5.2 Basic working principles

In terms of how blockchain works, first, it is essential to note that it is made up of several basic components as depicted in Fig. 6. These basic components are the nodes, which are users or computers in the blockchain network, and the transaction, which is a unit of records in the blockchain network. Other important components are the block, which is a collection of data that is used to complete network transactions and distributed to all nodes. The miners on the blockchain play a very important role in the approval of transactions on the network. While a chain refers to a sequence of blocks in a specific order and consensus is a group of instructions that work together to complete blockchain procedures [7].

The technology adopts a consensus protocol, which serves as a fault tolerant mechanism and a means of reaching agreement among all members of the blockchain to achieve consensus [47, 48]. The consensus protocol is used to ensure the integrity of the data recorded on the blockchain. Examples of this technology include the Bitcoin and other mining-based cryptocurrencies, which use PoW on every node for verification purposes. Further details on PoW and its functionality can be gleaned in [49]. However, the PoW process is slow and consumes extensive electricity, which can be limiting in underdeveloped regions or causing heavy billing cost to users [50]. On the other hand, there is the Ethereum-based alternative, which works using the Proof-of-Stake (PoS), which is a more energy-efficient consensus protocol compared to PoW. The

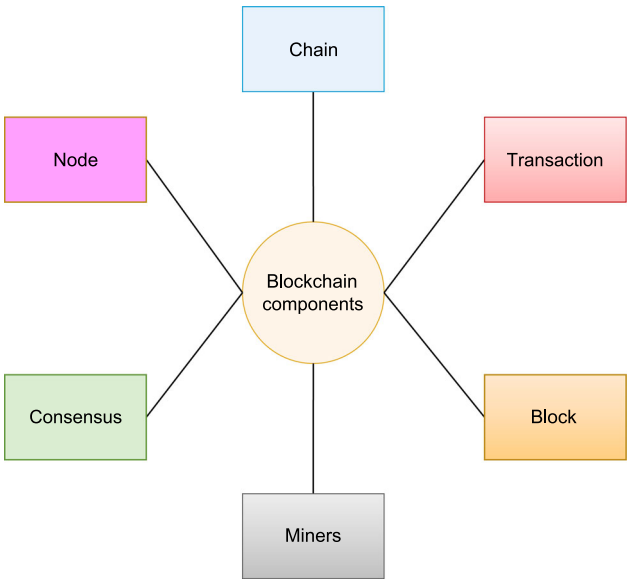


Fig. 6 Different key blockchain components

PoS works by randomly selecting a block and delegates to it the authority to contribute to the blockchain. Lastly, there is another approach termed the Proof-of-Authority (POA) algorithm, which is employed for its ability to deliver fast transactions through identity-based consensus mechanisms.

Using the blockchain architecture and its different consensus protocols depends primarily on two types of nodes, namely:

1. District node: This node represents each voting district, equipped with a software agent autonomously interacting with the "bootnode" and managing the smart contract's life cycle. The bootnode refers to a preconfigured node that helps new nodes to discover and connect to the network [51]. Then, after the ballot smart contract has been created, district nodes can interact with each of the corresponding ballot smart contact. When the voter has cast his vote from his smart contract, the vote data is being verified by all of the corresponding district nodes and every vote they agree upon are appended on the blockchain [52].
2. Bootnode: Specifically, the bootnode is hosted by institutions with access permission. The bootnode serves as a discovery and coordination service that facilitates communication between district nodes. The bootnode do not keep any state of the blockchain and they are configured on an static IP so that the district nodes can find their peers faster [52].

After establishing a secure and private blockchain, the next step involves defining and deploying a smart contract that represents the e-voting process. The smart contract design encompasses three essential components: election roles, the election process, and voting transactions. Each voter interacts with a ballot smart contract specific to their district, ensuring the privacy and security of individual votes [50]. Furthermore, in the decentralized e-voting system, zero-knowledge proof is utilized, which is a cryptographic method ensuring information verification without revealing underlying data. Zero-knowledge proofs provide a secure means of communication between entities on the internet without disclosing sensitive information. Generally, the common implementation details include the use of smart contracts written mostly in Solidity for Ethereum blockchain, the integration of zero-knowledge proofs, and a novel approach to voting with coins [53]. For additional details, the authors in [53] have discussed the advantages and challenges associated with zero-knowledge proofs and smart contracts.

5.3 Key blockchain technologies for e-voting

The key blockchain technologies necessary in any e-voting system are discussed in this section. They include:

1. Consensus algorithm: This algorithm realizes the process of bringing together members of a ledger to agree on an entity. By member of a ledger, it refers to the individual participants or nodes in the blockchain network while an entity typically refers to a block or a transaction that needs to be agreed upon by the members. In centralized networks, a control unit can determine the correct entities and broadcast them to the entire network [54]. However, in distributed ledgers, nodes must collaborate to reach an agreement without relying on a centralized authority. Some nodes may attempt to compromise the system by supporting a consensus that benefits themselves rather than reflecting the truth. Consensus-based blockchains eliminate the need for third parties while ensuring that participants agree on true and legitimate events [55]. The solution lies in protocols that operate based on predefined guidelines for standardizing the consensus mechanism. In a peer-to-peer network, the problem of consensus can still arise even if all peers are trustworthy. A common issue, known as a "fork," occurs when several blocks are added concurrently by different miners due to delays in block propagation across the network [32, 56]. A consensus rule called the "longest chain" distinguishes legitimate blocks from fraudulent ones. When a miner acknowledges the legitimacy of an existing path, the path is extended, signaling consensus on that particular path. This means that the longer a path is, the more computation has been invested in building it [32, 57].
2. Smart contract: A smart contract refers to a self-executing contract embedded in blockchain-managed computer code, facilitating communication and decision-making between parties [58]. It establishes a framework for efficient control over tokenized assets and access rights. Blockchain serves as an immutable database, and smart contracts expand and leverage its capabilities. Smart contracts self-verify conditions through data interpretation, with each network node ensuring the proper execution of individual contracts, thus eliminating the need for centralized tracking [58–60]. The contracts automate legal obligations, thus enabling the blockchain system to be mapped into automated processes. Contract execution can be triggered automatically, for instance, by an expiration date [54]. Smart contracts can also contribute to the evolution of smart governance [61].
3. Digital signature: A digital signature is a cryptographic tool used in a trustless environment like blockchain. In blockchain, each block is given a pair of keys: a private key (known only to the owner) and a public key (visible to everyone in the network). The private key acts as a secure password, while the public key allows

access to the signed transaction [32, 62]. The digital signatures thus ensure that only the rightful owner of a private key can authorize a transaction. This cryptographic mechanism ensures that transactions are tamper-proof and verifiable by all network participants, hence enabling trustless and decentralized operations.

4. Privacy-preserving techniques: These techniques enable blockchains to process and verify transactions without revealing sensitive information, ensuring that transaction details remain confidential while maintaining the integrity and transparency of the blockchain [48]. Examples of these techniques include zero-knowledge proofs, homomorphic encryption, and ring signatures, which can be integrated into blockchain-based e-voting systems. These techniques enable vote verification without revealing the voter's identity or vote content [55]. A brief discuss of these techniques is as follows:
   a The Homomorphic model is a probabilistic encryption scheme allowing voters to encrypt and publish their votes [63]. These encrypted votes are then added up to form the final tally without revealing individual votes. The model relies on algebraic properties of encryption, where messages are encrypted using mathematical operations. Election authorities decrypt the final tally cooperatively after the voting period ends, ensuring accuracy. The model ensures accuracy, privacy, fairness, robustness, and universal verifiability, though it may require voters to run specific code for proof of vote validity [32].
   b Blind signatures are used in online voting to ensure voter vote secrecy. Similar to sealed envelopes, voters encrypt their votes, blind them, and present them to a validating authority for verification [64]. After validation, voters unblind the encrypted votes, receiving validated votes that cannot be linked to the original messages. These protocols are simple, manageable, and computationally efficient, supporting "write-in" ballots.
   c Zero-knowledge proofs are cryptographic protocols used to prove the validity of a secret to a verifier [65]. In homomorphic voting, where encrypted votes require proof without decryption, zero-knowledge proofs play a vital role. However, this may require voters to run special-purpose code on their computers to generate proof of vote validity [55].
5. Immutable record (blockchain): The immutability of the blockchain ensures that once a vote is recorded, it cannot be altered or deleted. This feature enhances the integrity of the e-voting system, preventing fraud or manipulation of the vote count. Researchers have extensively studied the immutability aspect of blockchain. For instance, [66] introduced a solution for preventing double-spending without relying on trusted third parties, using a blockchain-based timestamping system and proof-of-work consensus to ensure immutability. Also, authors in [67] introduced biometric modalities (such as fingerprint and facial recognition), which were used for voter authentication, while the Hyperledger Fabric framework was used to ensure secure, transparent, and tamper-evident voting records.
6. Tokenization: Tokenization involves representing the right to vote as a digital token on the blockchain. This ensures that only eligible voters possess the necessary tokens to participate in the election. Tokenization can also facilitate the transfer of voting rights in proxy voting scenarios. This has been applied in several research works, for example, the authors in [68] developed an e-voting Decentralized Application (DApp) on the Ethereum blockchain using smart contracts. Here, each voter receives a digital wallet containing a single token representing one vote. When a user casts a vote, the corresponding token is transferred to the candidate's account, ensuring transparency and security. The blockchain-based system enhances vote visibility, real-time tracking, and anonymity while preventing tampering.
7. Open source platforms: Open-source platforms and frameworks tailored for e-voting on the blockchain provide customizable solutions for election authorities. These platforms often include built-in features such as voter registration, ballot creation, and result tabulation. Such open-source tools have been identified, for example in [69], the authors proposed SecureBallot, an open-source e-voting system that completely decouples the voter identification and voting phases using proven cryptographic technologies. It ensures privacy, secrecy, anonymity, integrity, uniqueness, and authenticity of votes while maintaining trust in the voting process. Similarly, in [70], a decentralized e-voting system using blockchain technology was proposed that leverages Ethereum's smart contracts, it guarantees protection for voters' identity, data transfer privacy, and verifiability through an open and transparent voting process.

5.4 Types of blockchain-based e-voting architectures

In deploying blockchain technology for e-voting, there are specific architectures that play a crucial role in determining the effectiveness of such systems. In this regard, four

primary blockchain architectures are noted, namely private, public, consortium, and hybrid architectures. Understanding these architectures is crucial for designing robust and effective e-voting platforms that meet the needs of diverse stakeholders while ensuring security, transparency, and accessibility. Thus, we describe them as follows:

5.4.1 Private blockchain architecture

A private blockchain architecture is a distributed ledger system where access is restricted to a specific group of authorized participants, providing enhanced control, privacy, and security within a closed network [71]. The private architecture depicted in Fig. 7 leverages Hyperledger Fabric to create a secure, controlled, and efficient environment for digital voting. The blockchain manager is the core administrative component that oversees the entire blockchain network within the Hyperledger Fabric. It is responsible for managing network policies, participant permissions, and overall blockchain operations. This centralization in a private blockchain environment typically presents enhanced control and governance by a single organization or a consortium.

The authorized nodes in Fig. 7 are the specific blockchain nodes authorized by the central authority to participate in the network. In a private blockchain, such nodes are usually known and trusted entities. These nodes might perform various functions such as transaction validation, consensus participation, and maintaining the ledger's state. The manager has the capabilities to configure or control how these nodes operate within the network. The voting logic in the voting system represents the application layer where the rules and procedures for the voting process are defined and executed. It includes the algorithms that handle the logic of vote casting, validation, counting, and any other related processes. This could also involve smart contract implementations, where the voting logic is encoded into self-executing contracts on the blockchain. On the other hand, the voting database is the storage component that maintains records of votes and possibly voter identities, depending on the privacy design of the system. Being part of a blockchain setup, the integrity and immutability of the voting data are maintained, ensuring that once a vote is recorded, it cannot be altered.

In terms of the workflow of Fig. 7, the data flow begins at the blockchain manager, which distributes configurations or permissions to the authorized nodes. Each node participates in the network according to the stipulated configurations. In this case, when a vote is cast, the transaction is processed through the nodes where the voting logic is applied to validate and record the vote into the Voting database. Given the private nature of the blockchain, all transactions would be validated by the authorized nodes to ensure they meet the pre-defined rules before they are immutably recorded. Generally, the private blockchain setup aims to restrict network access to authorized entities only, thus reducing exposure to malicious activities compared to public blockchains.

5.4.2 Public blockchain architecture

Public blockchain architecture refers to a decentralized and open ledger system where anyone can participate, validate transactions, and contribute to the consensus process [72]. It ensures transparency, security, and immutability through distributed consensus mechanisms, allowing for a trustless and inclusive network. In Fig. 8, a public blockchain architecture is presented designed for a voting system using the Ethereum blockchain. The nodes are the individual participants in the public blockchain network. Each node maintains a copy of the entire blockchain and participates in validating and propagating transactions across the network. The voting smart contract based on Ethereum is a self-executing contract deployed on the Ethereum

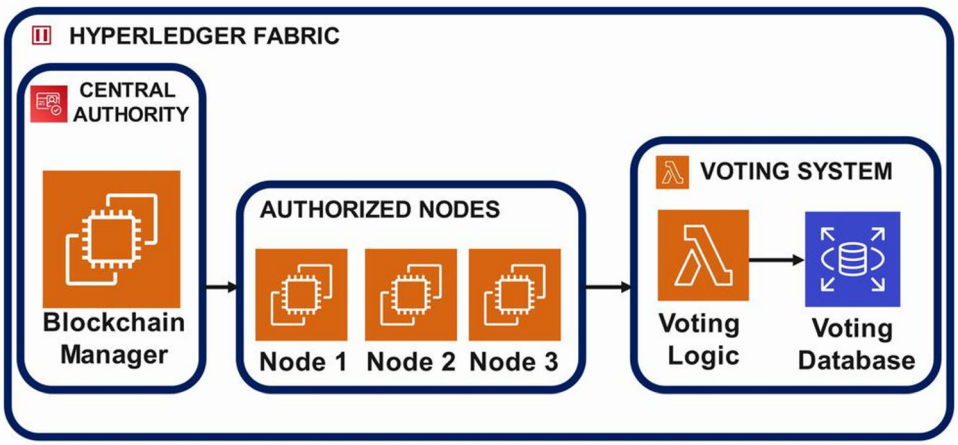


Fig. 7 Private blockchain architecture

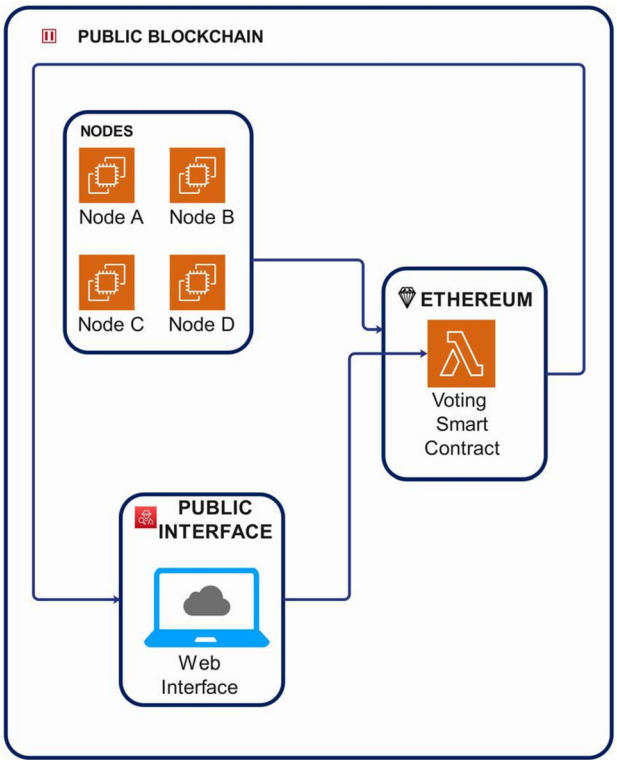


Fig. 8 Public blockchain architecture

blockchain. It contains the rules and logic for the voting process, ensuring that votes are cast, recorded, and counted in a transparent and tamper-proof manner. Finally, the web interface serves as the user-facing part of the voting system. It allows voters to interact with the blockchain through a user-friendly interface, facilitating actions such as casting votes and viewing results.

In using public blockchain architecture for e-voting, the voting process begins with the deployment of the voting smart contract on the Ethereum blockchain. This contract is programmed with the necessary voting rules and procedures. Voters then use the web interface to cast their votes. The web interface interacts with the Ethereum blockchain by sending transactions that invoke the methods defined in the voting smart contract. Once a vote is cast via the web interface, it is propagated to the nodes (e.g. Node A, Node B, Node C, Node D in Fig. 8) in the public blockchain network. Each node validates the transaction according to the consensus protocol used by Ethereum (e.g., Proof of Work). After validation, the transaction is added to a new block, which is then appended to the blockchain. The consensus mechanism ensures that all nodes agree on the state of the blockchain. Once a block containing the voting transaction is confirmed, it becomes immutable, ensuring that the vote cannot be altered or deleted. Because the blockchain is public, anyone can view the transactions and verify the voting results. This transparency builds trust in the voting process, as the data is available for public audit.

5.4.3 Consortium blockchain architecture

Consortium blockchain architecture is a type of blockchain where the consensus process is controlled by a group of pre-selected nodes, typically representing multiple organizations [73]. Unlike public blockchains, access and permissions in a consortium blockchain are restricted to these selected participants, ensuring both decentralization and control within a trusted group [74]. A consortium blockchain architecture is illustrated in Fig. 9 for a voting system using the Quorum platform. From Fig. 9, the trusted organizations are the participating entities in the consortium blockchain. Each organization represents a member of the consortium and has a role in the governance and operation of the blockchain network. The decentralized nodes are operated by the trusted organizations. They participate in the consensus process, validate transactions, and maintain a copy of the blockchain ledger. On the other hand, the smart contract is deployed on the Quorum blockchain. It contains the logic and rules for conducting the voting process, ensuring that votes are casted, recorded, and counted in a transparent and secure manner. Finally, the consortium interface hosts the member access portal, which is the user-facing component that allows members of the consortium to interact with the blockchain. Through this portal, members can access the voting system, cast votes, and view results.

Essentially, the consortium blockchain ensures that all participating organizations have visibility into the voting process, enhancing transparency and trust. It maintains security through restricted access and the use of smart contracts, which enforce the rules and prevent tampering with the voting data [75]. In terms of e-voting applications, it leverages the Quorum platform to create a secure, transparent, and collaborative voting system managed by multiple trusted organizations. By combining the benefits of decentralization with controlled access, it ensures that the voting process is both reliable and trustworthy, while allowing for efficient governance and decision-making among the consortium members.

5.4.4 Hybrid blockchain architecture

Hybrid blockchain architecture combines elements of both public and private blockchains, leveraging the strengths of each to provide a more versatile and effective solution [76]. In a hybrid blockchain, certain data and processes are made public and accessible to anyone, while other parts are restricted to authorized participants only. This approach allows for enhanced security, privacy, and control, while

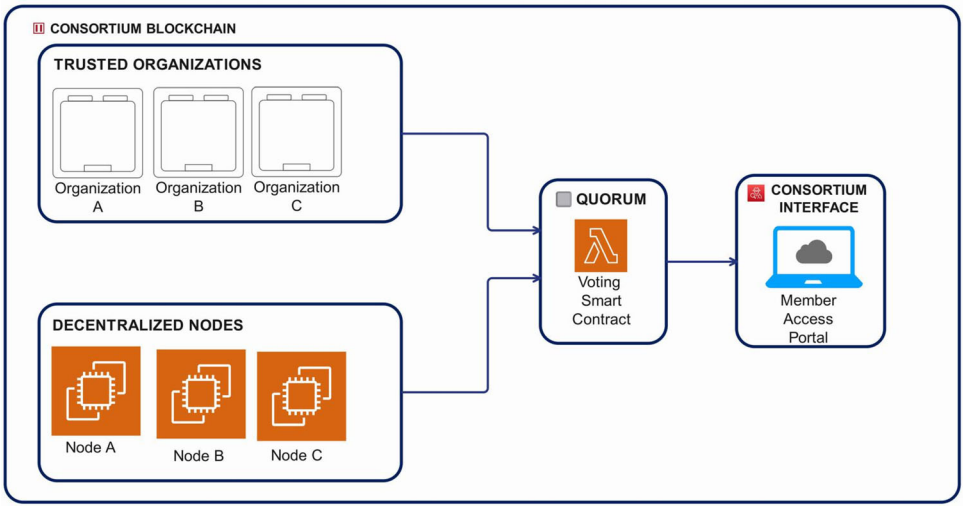


Fig. 9 Consortium blockchain architecture

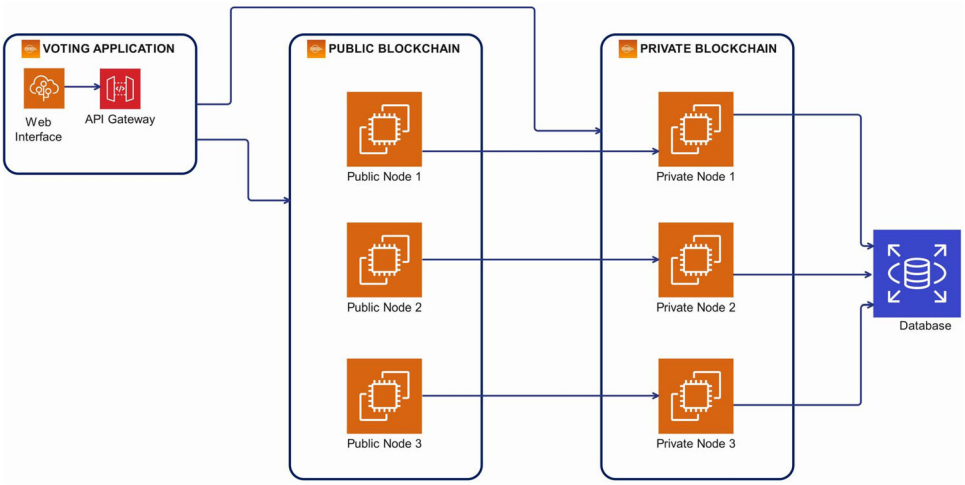


Fig. 10 Hybrid blockchain architecture

still maintaining transparency and decentralization where needed. Figure 10 illustrates a hybrid blockchain architecture that can be leveraged for e-voting purposes. For example, the web interface can represent the front-end component that allows users to interact with the voting system. Voters can cast their votes and view election-related information through this interface.

The voters interact with the web interface to cast their votes. The web interface provides a user-friendly platform for accessing the voting application. The application programming interface (API) serves as the middleware that handles communication between the web interface and the blockchain nodes. It ensures secure and efficient data transfer, routing requests from the web interface to the appropriate nodes in the blockchain network. Depending on the nature of the data, the API gateway directs the transaction either to the public or private blockchain nodes.

The public blockchain, represented by public nodes (Node 1, Node 2, Node 3) in Fig. 10, handles transactions that are meant to be transparent and publicly accessible, such as general election information or public audit trails. These nodes validate and record transactions on the public ledger, ensuring that the data is immutable and transparent. On the other hand, the private blockchain, represented by private nodes (Node 1, Node 2, Node 3), handles sensitive transactions that require privacy and restricted access, such as individual vote details or voter authentication information. These nodes validate and record transactions on the private ledger, ensuring data security and restricted access. The database component collects and integrates data from both the public and private blockchain networks. It ensures that all relevant information is stored securely and can be accessed as needed for the voting process.

Essentially, the hybrid blockchain architecture combines the transparency and trust of public blockchains with the privacy and control of private blockchains. The architecture ensures that sensitive voting data is securely handled by private nodes, while public nodes provide transparency

Table 4 Comparison of the different blockchain-based architectures

Architecture	Description	Key features	Advantages	Limitations	Example
Private blockchain	• A centralized authority manages the blockchain network and governs the voting process • Access restricted to authorized nodes	• Centralized • Single governing authority • Private • Controlled	• Faster transaction times • Increased privacy	• Centralized control • Potential single point of failure	• Hyperledger Fabric/Proof-of-authority or Practical-Byzantine-Fault-Tolerance [61, 80]
Public blockchain	• Open-source code • Publicly accessible blockchain like Bitcoin or Ethereum • A decentralized network of nodes validates and records votes on a public blockchain, without a central authority	• Decentralized • Open to public • Transparent • Voter anonymity	• High security • Transparency	• Scalability issues • Slow transaction times	• Bitcoin or Ethereum/ Proof-of-work or Proof-of-stake [80–82]
Consortium blockchain	• A group of trusted organizations or entities collaborate to manage and govern the blockchain network and voting process • Decentralized nodes verify transactions • Access restricted to consortium members	• Hybrid • Decentralized • Member controlled • Distributed trust	• Balanced security and privacy • Faster transaction times	• Complex implementation • Limited scalability	• Quorum/Practical-Byzantine-Fault-Tolerance [10, 59, 83]
Hybrid blockchain	• Combines public and private blockchain • Decentralized nodes verify transactions • Access restricted to authorized nodes	• Combination of permissionless and permissioned • Centralized voter registration • Decentralized vote recording	• Flexible • Scalable	• Complex implementation • Potential security risk	• Hyperledger sawtooth/ Delegated Proof-of-stake [14, 84, 85]

for less sensitive information. This approach leverages the best of both worlds, providing a robust, secure, and transparent voting system.

However, the integration of public and private blockchains in a hybrid architecture introduces complexity in terms of interoperability and synchronization between the different layers. To address these challenges, hybrid blockchain systems employ sophisticated consensus mechanisms and cross-chain communication protocols to ensure seamless data exchange and consistency across both blockchain types [77]. Additionally, resilience to synchronization issues is achieved through the use of sidechains or relay chains, which act as intermediaries to facilitate communication between public and private chains while maintaining the integrity and security of the overall system [78]. These measures are critical for maintaining the efficiency and reliability of the voting process in hybrid blockchain architectures, especially in large-scale deployments. Thus, by carefully managing these aspects, hybrid blockchain systems are able to effectively balance the need for security, privacy, and transparency, while maintaining the overall efficiency and reliability of the e-voting process. We have provided a summary of these architectures via a comparison documented in Table 4.

5.5 Traditional e-voting vs. blockchain-based architectures

Deciding between the choice of either a traditional or blockchain-based architectures significantly impacts the overall design, security, and transparency of the electoral process. This remains a debate in the literature and hence this section briefly highlights a comparative analysis of these two architectural paradigms.

5.5.1 Traditional e-voting architectures

Generally, traditional e-voting systems typically rely on centralized databases and client–server models. In this approach, a central authority manages the entire election

process, from voter registration to result tallying. The key characteristics of traditional architectures include [79]:

1. Centralized control: One central entity, often an Election Authority, oversees and controls the entire election process.
2. Vulnerabilities: Centralized systems are susceptible to single points of failure. Malicious actors could attack the central server to manipulate votes or disrupt the election process, making them vulnerable to hacking, fraud, or manipulation.
3. Limited transparency: The lack of a transparent and immutable ledger makes it challenging to verify the authenticity of votes and ensure the integrity of the electoral process.
4. Dependence on trust: Voters and stakeholders must place implicit trust in the central authority, as the entire process hinges on the integrity of a single entity.
5. Familiarity and accessibility: Traditional models are often well-established and familiar to voters, making them accessible and easily understandable.

The traditional architecture has weaknesses, and some include:

1. Security concerns: Centralized control is marred with challenges such as phishing attacks on sites, attack on data centers, fraudulent increment of votes by intercepting the votes [86]. All of this makes this system less secure and more prone to hackers.
2. Limited transparency: The lack of a transparent and immutable ledger hampers the ability to verify votes independently.

5.5.2 Blockchain-based architectural model

On the other hand, the blockchain-based architectural model is a decentralized model with the following strengths [79]:

1. Decentralization: The decentralized nature of the blockchain enhances security by distributing control across nodes, reducing the risk of single points of failure.
2. Transparency and immutability: The use of a tamper-resistant ledger ensures transparent and auditable records of the entire electoral process. Where votes can be easily tracked, checked, and associated by a wide range of sources while maintaining voter privacy [86].

The weaknesses of the blockchain-based architectural model include:

1. Learning curve: The adoption of blockchain technology may pose a learning curve for stakeholders unfamiliar with decentralized systems due to its complexity of implementation.
2. Scalability challenges: While advancements are being made, certain blockchain architectures may face scalability challenges in handling large-scale elections. The increased number of users on the network leads to increased cost and time consumption for the transaction [86]. We provide in Table 5 a summary of the comparison between the architectural model of the traditional e-Voting system and blockchain-based e-Voting system

6 Trends in blockchain systems for e-voting

In terms of blockchain research for e-voting purposes, this section provides a chronological overview of the key developments shaping the evolution of blockchain in e-voting and then focuses on research innovations in integrating blockchain techology for e-voting purposes. We conclude with an examination of different case studies of blockchain implementation in different countries around the world.

6.1 Evolution of blockchain in e-voting

The use of blockchain networks for voting has gained increased attention following the 2016 US presidential elections, during which e-voting systems were suspected to have been compromised by foreign hackers [56]. Since then, the evolution of blockchain technology in the context of e-voting has experienced a transformative journey marked by innovation and adaptation to address obvious challenges in traditional voting systems. This is because blockchain technology offers a solution to the transparency, security, and confidentiality challenges faced by e-voting systems. Its unique and secure architecture implies that interference is fundamentally improbable when implemented correctly, as blockchain networks are inherently transparent, consensus-based, and decentralized [82, 87]. We brifely highlight this evolution as follows:

1. In the pre-2010s era, blockchain technology began to garner attention for its potential applications beyond cryptocurrency. Researchers and technologists explored its use in creating secure and transparent e-voting systems [40, 88].
2. As the technology progressed, various challenges and criticisms emerged beyond 2010 era such as scalability, privacy concerns, and the lack of user-friendly interfaces hindered widespread adoption [89, 90].

Table 5 Comparative analysis of architectural model

Criteria	Traditional	Block chain
Data storage	Centralized server	Distributed ledger
Transparency and accountability	Limited transparency; voters rely on central entity for verification	High transparency; voters can independently verify votes on blockchain
Privacy and confidentiality	Voter privacy can be compromised if central entity is compromised	Enhanced privacy through anonymization techniques
Security vulnerabilities	Single point of failure	Tamper-resistant
Scalability	Highly scalable	Faces scalability issues in handling large-scale elections
Cost and complexity	Lower initial costs	Requires robust infrastructure and technical expertise
Familiarity and accessibility	More accessible and more familiar	Not very familiar as it is an emerging technology

3. Despite these challenges, research and development efforts persisted between 2010 and 2020s, focusing on enhancing security and efficiency in blockchain-based e-voting systems. This involved improving consensus algorithms, implementing privacy-preserving techniques, and enhancing smart contract functionalities [91, 92].
4. Towards the late 2010s and into the 2020s, there were instances of small-scale experiments and pilot projects where blockchain technology was implemented in e-voting scenarios [92].
5. Thereafter, discussions revolved around regulatory frameworks and standards for blockchain-based e-voting, aiming to address concerns about security, legality, and inclusion [14, 81].
6. Currently, both the public and private sectors have shown an increased interest in blockchain solutions for secure and transparent elections, recognizing the potential of blockchain technology to address long-standing issues in traditional voting systems [93].

6.2 Recent innovations towards improving blockchain-integrated voting technologies

Blockchain-integrated voting systems blend traditional and blockchain-based elements to enhance privacy and transparency while complying with regulations. Permissioned blockchains, such as private or semi-private networks, control access, ensuring only authorized entities participate in the consensus process [94]. To resist quantum computer attacks, post-quantum cryptography is integrated into blockchain-based e-voting systems, maintaining security. User-friendly interfaces are essential for widespread adoption. Cross-chain interoperability enables seamless asset and information transfer, fostering a more connected voting infrastructure. Blockchain facilitates immutable and transparent voter registration, minimizing fraudulent registrations or tampering with voter rolls. Tamper-evident audit trails ensure transparent and verifiable vote records, safeguarding election integrity. However, successful implementation requires considering legal, regulatory, and social factors, alongside ongoing research and development.

Blockchain-based e-voting technology offers an open-source, peer-to-peer, decentralized, and independently verifiable system, fostering confidence among voters and organizers [57, 95]. The immutability and security of blockchain content make it advantageous for online voting systems. By utilizing a public hash blockchain, governments can provide a straightforward and secure voting environment. Citizens provide their ID number and username to an external identity verifier, submit their distinct ballots to the blockchain-powered ballot box, and audit election results using open-access blockchain data after voting.

While blockchain security is generally robust, Grover's algorithm and other approaches still pose limitations [96]. This is because preserving the chain's integrity involves replacing blocks using hash search parameters. Thus, accelerating nonce generation can change hashes, jeopardizing blockchain integrity. Efforts to enhance e-voting include guaranteeing user identity, data availability, security against DoS attacks over the public network, optimizing speed, and reducing computational overhead.

Quantum cryptography explores quantum mechanics' influence on cryptographic techniques [97]. The Quantum Key Distribution (QKD) protocol generates a random bit stream between parties to encrypt a secret message using a one-time pad (OTP), secured by quantum principles [98].

The Quantum No-cloning theorem asserts that individual quantum particles' signal cannot be cloned without introducing noticeable defects. QKD, despite limitations, is rapidly evolving, with emerging concepts like "Quantum Bitcoin" and quantum bit commitment protocols as digital signature systems [99].

6.3 Global trends in blockchain-based e-voting systems

This section explores notable trends of blockchain-integrated e-voting systems globally, shedding light on successes, challenges, and lessons learned. For example, in Nigeria, the feasibility analysis for replacing traditional voting systems with blockchain-based solutions has shown promising results. According to [100], the implementation of a Blockchain-Enhanced Voting (BEEV) System, combined with a qualitative SWOT and PEST analysis, reveals significant potential for promoting peace, stability, and development. However, the early stage of blockchain development in Nigeria presents security concerns, software bugs, and a lack of legal frameworks as major challenges.

In Turkey, [101] illustrated the enhanced security and privacy assurance provided by blockchain technology in voting systems. Key features include improved efficiency in outcome announcements and trustworthy elections with enhanced security measures. Continuous monitoring of security threats and addressing physical threats to voting machines remain challenges. The successful implementation of timely updates on election results demonstrated the effectiveness of blockchain in improving the electoral process. Future efforts should focus on real-world application validation, exploring global adaptation considering diverse legal frameworks, and further enhancing security measures. Sierra Leone's case study, as detailed in [102], emphasizes the digitization and blockchain storage of votes, transactional digital identities, and a proof of concept for blockchain-based voting. The successful implementation of a fully verifiable online e-voting protocol using blockchain and consistent election results highlight the potential of this technology. However, policy and political issues, public relations risks, and perceived redundancy pose challenges. Addressing policy considerations and managing public perception will be crucial for future success and broader acceptance.

In the United States, the Voatz application, referenced in [103], showcased the integration of blockchain immutability, end-to-end encryption, and biometric authentication in the voting process. Enhanced accessibility and real-time verification are significant successes. However, security vulnerabilities and a lack of transparency are critical challenges. Developing robust security measures and ensuring transparency and auditing are essential future improvements to build trust and credibility in blockchain voting applications.

The Moscow Active Citizen Program, as described in [104], leverages blockchain-enabled voting on the Ethereum platform to increase convenience and government trust. Positive outcomes and increased democratic participation are notable successes. Nonetheless, scalability concerns for widespread usage remain a challenge. Future improvements should focus on expanding usage and addressing scalability issues to accommodate a larger voter base effectively. In the United Arab Emirates, the authors in [105] highlighted the adoption of blockchain in political elections, peer-to-peer communication in voting systems, and the use of a private blockchain platform. Enhanced security features, including an immutable ledger, and the successful implementation of a private blockchain voting system are key successes. However, security and privacy challenges of traditional voting systems and stakeholders' concerns about blockchain application need to be addressed. Future research and planning should focus on scalability in the blockchain voting system and enhancing isolation in blockchain developments to ensure deterministic transactions.

The European Union's 2020 Electoral Process, discussed in [106], emphasizes the architecture of a national e-voting system on blockchain technology, dealing with COVID-19 pandemic challenges, and fine-tuning for scalability. Key successes include the use of Hyperledger Fabric for quick response and scalability, Estonia's success in internet voting, and the introduction of user tokens and digital identity verification. Ensuring a balance between anonymity and security, improving authentication mechanisms, and exploring alternative methods to enhance voter privacy are critical future improvements.

In Morocco, the authors in [107] described a blockchain-based e-voting system using the Solana blockchain, a multilayered system design, and remote voting options. The system's successes included mitigating fraud, offering remote and on-site voting, reducing physical travel, and providing transparent and immutable records. However, initial skepticism towards blockchain adoption, infrastructural diversity, and diverse electoral needs present challenges. Future improvements should focus on architecture refinement, addressing remote voting complexities, optimizing consensus node rotation, and conducting educative public campaigns to increase acceptance.

Finally, South Africa's case study, as highlighted in [36], showcases a blockchain e-voting architecture using Hyperledger Fabric v2.0 and a zero-knowledge protocol for voter authentication. The system has successfully prevented security attacks, internal vote manipulation, and promoted transparency. However, weaknesses in voter

validation, security of architecture, and attacks on smart contracts are significant challenges. Future improvements should focus on voter validation, diversifying stakeholder groups, improving standardization efforts, and conducting public awareness campaigns to enhance the system's effectiveness.

These case studies summarized in Table 6 collectively demonstrate the transformative potential of blockchain technology in voting systems, while also highlighting the importance of addressing security, scalability, and public perception challenges to achieve widespread adoption and success.

7 Challenges and concerns in e-voting systems

In this section, we examine technical challenges in implementing blockchain for e-voting purposes.

7.1 Challenges in implementing blockchain-based technology

Implementing blockchain-based technology, including applications in areas like e-voting, faces several challenges [54]. While blockchain technology offers various benefits, it is essential to be aware of and address these challenges for successful deployment. Here are some common technical challenges associated with implementing blockchain-based developments:

1. Scalability challenges: Scalability is a critical issue in public blockchains, affecting performance and efficiency in different applications [108]. The high adoption of cryptocurrency further exacerbates scalability issues in public blockchains [109]. For example, Bitcoin with 13, 000 daily transactions, faces bulkiness due to its inefficient proof-of-work (PoW) consensus mechanism, leading to longer transaction latency and over 10, 000 transactions awaiting verification [55]. Bitcoin's transaction throughput is capped at 7 TPS, far below the VISA's standard of 400 TPS. On the other hand, Ethereum's limited block size results in longer transaction latency, with block interval latency in public blockchains reaching up to 10 minutes. As transactions increase, storage capacity needs to scale accordingly, with Bitcoin currently at 305.23 GB, Ethereum at 667.110 GB, and LiteCoin at 28.45 GB [32, 54]. The combination of low throughput, high latency, storage demands, and energy consumption degrades the performance of public blockchain decentralized applications, making them unsuitable for large-scale implementation in time-critical or real-time applications like e-voting. However, in the context of e-voting, practical solutions can be considered to address scalability, such as the implementation of Layer 2 solutions such as state channels and sidechains [110, 111]. These techniques allow off-chain transactions while still leveraging the security of the main blockchain, thereby improving transaction throughput and reducing latency. Additionally, sharding, which involves dividing the blockchain into smaller, manageable segments, can also be explored to enhance scalability in e-voting systems without compromising security [112, 113].
2. Interoperability: Interoperability refers to the seamless communication and information sharing among different blockchain networks. In blockchain-based developments, achieving interoperability presents challenges due to the existence of multiple platforms with varied protocols and standards. This challenge becomes pertinent when integrating systems or facilitating data transfer across disparate blockchains [59]. However, there are proposals for token-based access approaches, privilege-based mechanisms, and data-driven strategies. These methods aim to ensure secure interoperability across diverse systems and infrastructures. Nevertheless, they have struggled to support end-to-end interoperability for supply chain systems with differing policies, governance structures, and operational procedures. There are various solutions that have been proposed in other application areas to address interoperability challenges, which may be leveraged in e-voting systems. For instance, a blockchain-based privacy-preserving payment mechanism was suggested for vehicle-to-grid (V2G) networks, enabling data sharing while safeguarding sensitive user information. However, this solution falls short in detecting threats arising from stakeholders' business processes. Another approach involves a tokens-based mechanism called MOSChain Identity (MID), designed to track product names and quantities, yet it lacks comprehensive end-to-end interoperability among departments. Specifically for e-voting systems, interoperability is crucial when integrating multiple voting platforms or ensuring cross-chain communication between public and private blockchains. One practical solution is the use of cross-chain bridges, which facilitate communication and data transfer between different blockchain networks [114, 115]. Furthermore, the implementation of standardized protocols, such as the Inter-Blockchain Communication (IBC) protocol [116], which can enhance interoperability, by allowing different blockchain systems to work together seamlessly in a unified e-voting process.

Table 6 Summary of global trends in blockchain-based integrated systems

References	Country	Key features	Challenges	Success	Future improvements
[100]	Nigeria	• Feasibility analysis for replacing traditional voting systems • Qualitative SWOT and PEST analysis • Blockchain-Enhanced Voting (BEEV) System Analysis • Need for government investment and private partnerships	• Early stage of blockchain development in Nigeria • Security concerns, software bugs, legal frameworks	• Early adoption in banking and financial sectors • Potential for peace, stability, and development	• Investment in resources and collaboration with fintech • Gradual adoption, mixed approach with existing systems
[101]	Turkey	• Enhanced security through blockchain • Privacy assurance for individual voters • Improved efficiency in outcome announcements	• Continuous monitoring of security threats • Addressing physical threats to voting machines	• Trustworthy Elections with Enhanced Security Measures • Timely update on the results to improve the electoral process	• Real-World Application for Validation and Improvement • Exploring Global Adaptation Considering Diverse Legal Frameworks
[102]	Sierra Leone	• Digitization and blockchain storage of votes • Transactional digital identities • Proof of concept	• Policy and political issues • Public relations risks • Perceived redundancy	• Successful implementation of a fully verifiable online e-voting protocol using blockchain • Consistent results	• Address policy considerations • Manage public perception
[103]	Voatz (US)	• Blockchain immutability • End-to-end encryption • Biometric authentication	• Security vulnerabilities • Lack of transparency	• Enhanced accessibility • Real-time verification	• Develop robust security • Ensure transparency and auditing
[104]	Moscow (Active Citizen Program)	• Blockchain enabled voting (BEV) on Ethereum • Increased convenience and government trust	• Scalability concerns for widespread usage	• Positive outcomes • Increased democratic participation	• Expand usage • Address scalability
[105]	United Arab Emirates	• Adoption of blockchain in political elections • Peer-to-peer communication in voting system • Private blockchain platform for voting system	• Security and privacy challenges of traditional paper voting systems • Stakeholders' concerns about blockchain application	• Enhanced security features, including an immutable ledger • Implementation of a private blockchain voting system • Implementation with the receptiveness of stakeholders	• Further research and planning for scalability in the blockchain voting system • Enhance isolation in blockchain developments to ensure deterministic transactions

Table 6 (continued)

References	Country	Key features	Challenges	Success	Future improvements
[106]	European Union (2020 Electoral Process)	• E-election system over blockchain technology • Dealing with COVID-19 pandemic challenges • Architecture of the national e-voting system on blockchain • Fine Tuning and Scalability	• Ensuring balance between anonymity and security • Authentication and authorization system, digital identity linkage • Overseeing ballot ingestion, potential single point of failure	• Hyperledger fabric for quick response and scalability • Recognition of the need for digitalization, Estonia's success in internet voting • Use of private keys and certificates for digital identity • Introduction of user tokens, revoke tokens, and delegation	• Explore more remote voting possibilities, improve digitalization globally • Improve authentication mechanisms, explore alternative methods, and try to enhance voter privacy • Explore endorsement policy, optimize database technology, and refine transaction processing
[107]	Morocco	• Blockchain-based e-voting system utilizing Solana blockchain • Multilayered system design • DPLT layer for data verification and validation • Remote voting options • Logging method on Solana for historical transaction information	• Initial skepticism towards blockchain adoption • Infrastructural diversity • Diverse electoral needs • Resistance to technology • Low technology accessibility • Interplay of law and politics	• Mitigated fraud • Remote and on-site voting • Mitigated physical travel • Demonstrated feasibility • User-friendly interfaces • Reduced cost • Transparent and immutable records, faster processing, and increased accessibility	• Architecture refinement • Remote voting complexities • Alternate blockchain solutions • Optimize consensus node rotation to prevent centralization • Address socio-political factors • Educative public campaigns • Investigate advanced cryptographic techniques
[36]	South Africa	• Blockchain e-voting architecture • Application Service Layer, Blockchain Layer, IEC Data Storage Layer • Hyperledger Fabric v2.0 • Zero-knowledge protocol for voter authentication	• Weaknesses in voter validation and security of architecture • Attacks on smart contracts • Lack of standardization	• Prevented security attacks, internal vote manipulation, and promoted transparency • Hyperledger Fabric ensured security • Zero-knowledge protocol provided privacy protection	• Voter validation improvement • More diversified stakeholder group • Improve standardization efforts • Public awareness campaigns

3. Privacy concerns: While blockchain provides transparency and immutability, maintaining privacy can be challenging. In e-voting, ensuring the secrecy of individual votes while maintaining transparency in the overall process is crucial. Techniques like zero-knowledge proofs and homomorphic encryption address privacy concerns, but effective implementation can be complex [55]. Academic research in e-voting focuses on ensuring privacy in shared data exchanges through blockchain technology. This involves integrating IoT-based solutions like RFID, NFC, and QR codes with products to create Smart Tags (ST), which track products throughout their supply chain lifecycle. The solution, based on distributed ledger technology (DLT), offers decentralized, privacy-preserving, and verifiable management of Smart Tags. Also, Ethereum blockchain facilitates stakeholder interaction during product exchange, allowing stakeholders and consumers to verify product authenticity during voting without revealing their identity. However, this solution assumes that ST generators and other stakeholders provide authentic data, which may not always be the case [59]. To address privacy concerns in e-voting, advanced cryptographic techniques like homomorphic encryption, which allows computations on encrypted data without decrypting it, can be employed. This

ensures that votes remain confidential while still being verifiable. Zero-knowledge proofs can also be used to confirm the validity of a vote without revealing any details about the vote itself, preserving voter anonymity while ensuring election integrity. These methods, though complex, are feasible for enhancing privacy in real-world e-voting implementations.

4. Security threats: Blockchain technology, notably Bitcoin, is renowned for its distributed nature and security features. However, the increasing value of cryptocurrencies has made them susceptible to attacks, particularly identity theft. The security of the Bitcoin network relies on a combination of public and private keys, which are stored in various types of wallets. While hardware and paper wallets are considered more secure, they do not fully prevent private key theft as may be highly required in voting applications. Ethereum, another cryptographic currency, offers solutions such as password protection for private keys, mitigating the risk of data being stolen if the key is compromised. Two-factor security involves sharing private keys between two devices, ensuring successful transaction execution. Eclipse attacks, proposed by Heilman, Kendler, Zohar, and Goldberg in 2025 [117], exploit multiple IP addresses to monopolize connections through a victim node. These attacks can target consensus systems during, thus facilitating double-spending, or enabling selfish mining. Countermeasures to mitigate these attacks include disabling incoming connections and selectively choosing outgoing connections, such as miners, to be included in a whitelist. The most notable threats are 51% attacks and double spending attacks, which can have severe consequences such as altering transaction data, manipulating mining, or halting the blockchain network for transaction verification. Measures to prevent these attacks include disabling incoming connections and carefully selecting outgoing connections for inclusion in the whitelist [49, 60, 118]. In e-voting systems, ensuring security against such threats is paramount. Multi-signature schemes, where multiple keys are required to authorize a transaction, can add an additional layer of security, making it harder for attackers to compromise the system [119]. Additionally, decentralized oracles can be employed to verify off-chain data, ensuring that external information used in the voting process is accurate and has not been tampered with [120]. These solutions can be practically implemented to enhance the security and resilience of blockchain-based e-voting systems.
5. Energy consumption: Proof-of-Work (PoW) serves as a primary consensus mechanism in public blockchains like Bitcoin, but its high energy consumption has raised environmental concerns, which becomes a challenge in voting scenarios. In response, the blockchain community has explored alternative consensus mechanisms, such as Proof-of-Stake (PoS). PoS selects validators to create new blocks based on their cryptocurrency holdings and willingness to "stake" as collateral, thereby reducing the energy footprint associated with blockchain operations. This energy efficiency helps lessen the environmental impact of blockchain networks by eliminating the need for miners to perform intensive computations. Additionally, PoS introduces a more democratic and inclusive approach to block creation, distributing decision-making power more evenly. However, critics argue that reliance on stake may lead to an oligarchic system, where the wealthy gain disproportionate influence. Despite these challenges, ongoing research and development aim to address concerns and enhance the robustness of PoS as a viable alternative to PoW [54]. The exploration of alternative consensus mechanisms, like PoS, represents a significant step towards mitigating the environmental impact of blockchain technology. In the specific context of e-voting, transitioning from PoW to PoS can reduce the environmental footprint of blockchain-based voting systems, making them more sustainable. Additionally, exploring hybrid consensus mechanisms, which combine PoS with other energy-efficient techniques, could offer a practical solution for large-scale e-voting deployments that require both security and scalability.
6. Smart contract security: Smart contracts are self-executing programs on the blockchain, and vulnerabilities in these contracts can lead to security breaches. Ensuring the security of smart contracts for the voting authority itself is crucial, as any flaws in the code could be exploited, potentially compromising the integrity of the entire blockchain system. In this regard, the role of transparent observers becomes highly significant. For e-voting, smart contracts must be rigorously audited and tested before deployment to ensure they function as intended. Formal verification, a mathematical approach to checking the correctness of smart contracts, can be used to prove that a contract behaves as expected under all possible conditions [121]. This practice helps to prevent vulnerabilities that could be exploited during an election, ensuring that the voting process remains secure and trustworthy.
7. Costs and resources: The development and maintenance of blockchain-based systems present a significant challenge due to their resource-intensive nature. The costs associated with hardware, software, and ongoing maintenance must be carefully weighed, impacting the financial considerations of implementing

blockchain solutions for e-voting purposes. The need for robust infrastructure, often involving specialized hardware configurations and powerful computing resources, adds to the investment required. Furthermore, the demand for skilled developers and blockchain experts can contribute substantially to overall expenses, as their expertise is crucial for the successful design, implementation, and ongoing optimization of blockchain systems. Navigating these financial considerations is paramount for organizations looking to leverage blockchain technology effectively while managing resources judiciously. To address these costs, organizations may explore the use of blockchain-as-a-service (BaaS) platforms, which provide the necessary infrastructure and maintenance support, reducing the need for in-house resources [122]. Additionally, consortium blockchains, where multiple organizations share the costs and governance of a blockchain network, can also be a cost-effective approach for implementing e-voting systems.

8. Legacy system integration:Integrating blockchain into existing systems poses a unique set of challenges, particularly when dealing with legacy infrastructure. The compatibility of blockchain technology with traditional databases and systems demands meticulous planning and execution to ensure seamless integration without disrupting existing operations. Legacy systems often lack inherent features that facilitate straightforward integration with blockchain, necessitating careful consideration of data migration, system interoperability, and potential workflow adjustments. Successful integration requires a strategic approach, focusing on preserving data integrity, minimizing downtime, and maximizing the benefits of blockchain technology without compromising the functionality of established systems [123]. As organizations strive to modernize their operations, careful navigation of legacy system integration complexities becomes imperative for the successful adoption of blockchain solutions [124]. In the context of e-voting, middleware solutions that bridge the gap between blockchain systems and legacy infrastructure can be developed to ensure smooth integration. These solutions can handle data translation and interoperability between old and new systems, allowing organizations to adopt blockchain technology without completely overhauling their existing infrastructure [125]. Additionally, adopting a phased integration approach, where blockchain components are gradually introduced and tested alongside legacy systems, can help mitigate risks and ensure a successful transition [126].

7.2 Concerns with e-voting systems

There are significant social, legal and educative concerns that must be addressed in deploying blockchain technology for e-voting. This section highlights key areas of concern surrounding e-voting systems and discusses their implications for electoral integrity and building public trust.

1. Transparency and auditability: Transparency and auditability are crucial for the credibility of electoral processes, especially in e-voting systems. Ensuring accurate vote recording and counting independently is vital for public trust and democratic integrity. E-voting systems often lack end-to-end verifiability, raising concerns about the reliability of results compared to traditional paper-based systems. In Pennsylvania, they mostly use DRE systems without paper trails, hampering error detection. The 2014 crash of DRE machines in Virginia revealed vulnerabilities, alarming officials. Proprietary software and hardware in e-voting systems make independent audits difficult due to restricted access [127]. Although mechanisms like voter-verifiable paper audit trails (VVPATs), risk-limiting audits (RLAs), and zero-knowledge proofs enhance transparency, they face implementation challenges. Concerns about VVPAT reliability arose in India. RLAs depend on reliable paper trails, which may not always be available [21]. Real-world cases, like Estonia's i-voting system, highlight transparency issues. Verifiability is essential for the correctness and integrity of the elections. The widespread use of e-voting systems emphasizes the urgency of addressing transparency and auditability concerns [128].
2. Voter authentication and identity verification: Proper voter authentication and identity verification are critical for electoral integrity, especially in e-voting systems with their inherent vulnerabilities. These mechanisms ensure only eligible voters participate, reducing fraud and unauthorized access. E-voting systems employ various authentication methods like voter ID cards, biometrics, and knowledge-based authentication. Yet, each method has its challenges and vulnerabilities [129]. Identity theft or impersonation is a significant risk in e-voting systems, especially in remote or online voting setups. Compromised biometric data poses long-term security risks. Implementation of authentication systems is crucial. Poorly designed protocols can lead to failures, as seen in elections in Namibia and Nigeria in 2014 and 2015 [130]. Centralized voter databases introduce single points of failure, vulnerable to cyber attacks. Concerns about system integrity were evident in the 2016 US election, with accusations of Russian interference

[131]. Ensuring proper authentication is vital for electoral credibility, particularly in e-voting systems with complex security requirements. A comprehensive approach balancing security, usability, and accessibility is necessary, leveraging advanced technologies and best practices. Continued research, testing, and collaboration among experts, policymakers, and stakeholders are essential to mitigate risks and build confidence in the electoral process.

3. Legal and ethical implications: The adoption of e-voting systems raises crucial legal and ethical considerations, impacting the integrity, fairness, and democratic principles of elections. These implications encompass data privacy, accessibility, transparency, and potential biases or discrimination. Legally, e-voting systems must comply with national and international laws, ensuring adherence to election regulations, data protection, and citizen rights [132]. Non-compliance risks legal challenges, undermining election legitimacy and disenfranchising voters. Protecting the privacy of the voter and the confidentiality of personal data is paramount. In this regard, the authors in [133] explored the development of a secure blockchain-based e-voting system that prioritizes confidentiality and voter anonymity. They proposed a novel framework that integrates cryptographic techniques and decentralized ledger technology to ensure the integrity and privacy of the voting process. Their findings suggest that the proposed solution effectively addresses common security vulnerabilities in e-voting systems, providing a robust mechanism for confidential and anonymous elections. Following their work, it is important that e-voting systems handle sensitive information, requiring robust security measures and compliance with data protection laws to prevent unauthorized access or misuse, safeguarding against voter suppression or coercion [134]. Equal access and non-discrimination for all eligible voters are imperative, aligning with civil rights and the right to vote. Transparency and auditability, essential for free and fair elections, carry legal and ethical weight. Opaque systems may breach transparency laws and face legal challenges. The use of proprietary software raises ethical concerns about vendor lock-in and lack of accountability [134]. Advocates call for open-source software to ensure scrutiny and integrity. Accessibility issues in India highlight concerns about marginalized communities' rights. Addressing these implications necessitates collaboration among experts, policymakers, and civil society. Clear legal frameworks, robust security measures, and ethical adherence are vital for e-voting legitimacy, failure of which risks undermining democracy and eroding public trust.
4. Social acceptance and trust: E-voting systems aim to increase voter turnout and streamline the electoral process, however, their success depends on widespread social acceptance and public trust. Without trust in their integrity and security, adoption may face obstacles, threatening electoral legitimacy and democratic principles. Social acceptance and trust hinge on factors like transparency, ease of use, and perceived reliability. Complexity and opacity in e-voting systems can breed suspicion, especially among non-experts and the elderly. Accessibility issues may further alienate segments of the population, exacerbating societal divides [130]. Concerns about integrity and security, fueled by incidents like alleged hacking and foreign interference, deepen public skepticism. Addressing these concerns requires transparency, education, and inclusive engagement. Independent auditing, clear communication, and voter education campaigns can build confidence. Estonia's successful internet voting is attributed to its emphasis on digital literacy. Prioritizing transparency and accessibility is essential for e-voting's acceptance and long-term sustainability. Failure to do so risks perpetuating skepticism and undermining electoral legitimacy [57].
5. Potential misuse of blockchain technology: Blockchain technology is lauded as a potential solution for enhancing transparency, security, and auditability in e-voting systems. However, its implementation poses risks and potential misuse scenarios, requiring careful consideration to safeguard the integrity of the electoral process. One concern is the risk of immutable errors or bugs in blockchain systems. While designed to prevent tampering, the immutability of blockchain can pose challenges if errors are introduced, potentially undermining the accuracy of election results. Another concern involves manipulation of the consensus mechanism, critical for agreement among participants. Attack vectors like Sybil attacks or collusion could compromise the integrity of the voting process, enabling manipulation or censorship. Integration of blockchain may introduce new vulnerabilities, exposing entry points for malicious actors. Inadequate security measures could nullify transparency and auditability benefits. Blockchain's complexity may unintentionally exclude certain voters, undermining inclusivity. In the 2018 West Virginia midterm elections, a blockchain-based voting app faced criticism over security vulnerabilities, prompting investigation [103]. Addressing blockchain misuse requires rigorous security audits, testing, and multidisciplinary expertise. Robust contingency plans and ongoing collaboration are essential to harness blockchain benefits while minimizing risks.

6. Scalability: Blockchain technology is effective for small-scale applications, but challenges arise when it is applied to large-scale elections. As the number of users increases, transaction processing becomes slower and more costly, exacerbated by the growing number of nodes in the blockchain network. Scalability is already a significant concern in elections, and integrating e-voting further complicates the issue [135, 136]. One potential solution to enhance blockchain scalability is sharding, a technique that involves partitioning data horizontally into smaller parts, or shards. This allows for parallel processing of transactions, increasing concurrency and throughput. Several techniques in the literature address blockchain scalability issues. These include Segregated Witness (Segwit), which separates transaction signatures from transaction data to increase block size efficiency, sharding, as previously mentioned, and adjustments to consensus protocols to improve transaction throughput [137–139]. While blockchain offers promise for secure and transparent elections, scalability issues must be addressed for its effective implementation in large-scale voting scenarios. Techniques such as sharding and protocol adjustments are being explored to overcome these challenges and ensure the integrity and efficiency of e-voting systems [140, 141].
7. Security: Security emerges as a paramount concern in the dynamic landscape of blockchain technology implementation. While blockchain brings forth a revolutionary paradigm with its decentralized and tamper-resistant characteristics, the pursuit of a secure and robust system demands a nuanced understanding of the specific considerations and challenges within this ecosystem. Blockchain's appeal lies in its ability to enhance data integrity, reduce the risk of fraud, and establish transparent and accountable transactions. However, the intricate nature of security in blockchain involves navigating various complexities to fortify the overall resilience of the system. In this context, it becomes imperative to delve into key security considerations, recognizing both the inherent strengths and potential vulnerabilities, to craft and implement blockchain solutions that not only capitalize on the technology's benefits but also stand resilient against evolving threats and risks [142]. Some key security considerations in the context of blockchain include the various consensus mechanism.

   Blockchains are vulnerable to 51% attacks when a group or entity controls over 50% of the network's mining power [143]. To prevent or mitigate these attacks, security measures are crucial. The consensus mechanism, which approves and verifies transactions, is characterized as proof-based or voting-based. Proof-based is commonly used in public or permissionless blockchains, but it has high energy consumption and requires specialized hardware. Proof-of-stake (PoS) is another proof-based mechanism, faster but vulnerable to risks like Agency issues. Ethereum gradually implements PoS reduced energy consumption and better scalability. Voting-based consensus models are typically used in private blockchains, such as PBFT [144].

8 Future directions and emerging trends

As e-voting systems evolve rapidly, blockchain technology are also expected to undergo significant changes, driven by advances in various fields such as artificial intelligence, IoT, consensus protocols, cryptography, distributed systems, and user experience design. These developments offer potential solutions to existing challenges and we discuss them in this section.

8.1 Cryptography

Advanced cryptographic techniques such as homomorphic encryption and zero-knowledge proofs aim to ensure end-to-end verifiability, guaranteeing accurate vote recording while maintaining secrecy [145]. These methods also bolster the security and auditability of tallying processes, reducing the risk of manipulation. Integrating blockchain with advanced cryptography may address concerns regarding auditability, privacy, and tampering. In [145], the authors advocate for the integration of crypto-blockchain technology into electronic voting systems. Their paper emphasizes secure authentication using unimodal fingerprint biometrics, blockchain transparency, and privacy-preserving techniques to enhance the integrity and trustworthiness of e-voting systems. Furthermore, in [15], the authors advocate for the use of cryptography in e-voting systems. They describe various e-voting approaches, including mix-net-based e-voting, homomorphic e-voting, blind signature-based e-voting, blockchain-based e-voting, post-quantum e-voting, and hybrid e-voting. Further exploration of these cryptographic primitives will be necessary in ensuring security, privacy, and integrity within e-voting systems.

8.2 AI, machine learning, and deep learning

Artificial Intelligence (AI) is a field that encompasses a broad range of computational techniques aimed at creating systems capable of performing tasks that typically require human intelligence. Within AI, machine learning is a

subset that involves training algorithms on data to make predictions or decisions without explicit programming [146]. Deep learning is therefore a further subset of machine learning, in which neural networks with many layers are used to model complex patterns in data [146]. These distinctions are crucial in understanding their application in blockchain-based e-voting systems.

Specifically, AI and machine learning hold promise for enhancing the security, accessibility, and efficiency of e-voting platforms. These systems can improve voter verification and authentication, detect and prevent fraud, and ensure inclusivity. For instance, machine learning algorithms analyze voter data to detect anomalies and flag suspicious registrations for review, significantly reducing the risk of fraudulent voting [147–153]. Additionally, AI can identify users with disabilities and provide tailored voting options, ensuring that the voting process is inclusive and accessible.

Deep learning, which is distinguished by its use of artificial neural networks, excels at processing and interpreting complex, unstructured data. This makes it particularly effective for applications like biometric voter verification, where neural networks analyze intricate patterns in biometric data such as facial features, voice patterns, and iris scans to ensure highly accurate and reliable voter authentication [4, 154]. Furthermore, deep learning's advanced pattern recognition capabilities are invaluable for fraud detection and voting behavior analysis. By analyzing large volumes of voting data, deep learning algorithms can identify suspicious patterns or irregularities indicative of fraudulent activities, such as vote tampering or ballot stuffing [155].

In the age of social media and online information, deep learning can also help combat misinformation and fake news that may influence voter behavior by analyzing text, images, and videos for patterns associated with false information [156]. Additionally, deep learning can enhance the accessibility and user experience of e-voting platforms by analyzing user behavior to suggest personalized interfaces, ensuring an inclusive voting experience for all eligible voters, including those with disabilities.

While deep learning shares similarities with traditional machine learning in its ability to learn from data and make predictions, its capacity to process and extract insights from complex, unstructured data sets it apart, making it particularly effective for tasks like biometric authentication, fraud detection, and misinformation analysis [68].

8.3 Internet of Things (IoT)

The Internet of Things (IoT) refers to a network of interconnected devices wherein data is shared to facilitate timely decision-making. Integrating IoT devices and distributed ledger technologies with blockchain-based e-voting systems can significantly transform the voting process by enhancing accessibility, security, and transparency [157]. For example, IoT devices can serve as secure voting terminals, which will allow for voting from various smart devices like smartphones, tablets, and wearables, potentially increasing voter turnout and inclusivity [158]. These devices can also integrate secure biometric authentication methods, such as fingerprint or facial recognition, to verify voter identity and prevent fraud, while tamper-proof mechanisms and encrypted communication channels ensure data integrity and confidentiality [159].

Other potential areas including the integration of distributed ledger technologies (DLTs) with blockchain-based e-voting systems, which can enable cross-chain interoperability for simplifying voting across multiple jurisdictions or organizations and reducing administrative complexities [160]. Moreover, blockchain's ability to provide a transparent and immutable record of votes allows for enhanced auditability and accountability, ensuring that the electoral process is resistant to tampering and fraud. Future research should explore the potential of integrating blockchain with emerging IoT technologies, such as edge computing, to further enhance the efficiency and security of e-voting systems [161]. There should also be further developments in the integration of blockchain, AI, and IoT systems to create highly robust decentralized voting systems, where secure IoT devices can record votes on an immutable blockchain ledger, with AI algorithms analyzing voting data to improve security and efficiency [162, 163]. In particular, the integration of blockchain with AI-driven IoT devices can provide real-time analysis and fraud detection during elections, further bolstering the integrity of the voting process [164]. Additionally, blockchain-based smart contracts can be used to automate actions based on voting results, such as declaring winners or initiating recounts, thereby reducing manual intervention and enhancing transparency and hence more research will be required in this regard. By exploring these lines of research works, e-voting systems can be made more accessible, secure, and transparent, which will foster stronger public trust and democratic participation.

8.4 Integration with emerging consensus mechanism

The integration of novel consensus mechanisms with blockchain-based e-voting systems shows promise in addressing challenges faced by traditional models like proof-of-work (PoW) and proof-of-stake (PoS). Scaling blockchain networks to handle high transaction volumes requires more sophisticated solutions than simply adjusting

block size or hash complexity. The proof-of-history (PoH) mechanism, utilized by the Solana network, offers an innovative approach to these issues [165]. PoH provides a verifiable timestamping system, ensuring transparency and integrity in the voting process. It enables high transaction throughput crucial for large-scale elections while consuming significantly less energy compared to PoW, thus promoting sustainability [166]. Despite its potential benefits, PoH is still in its early stages, requiring further research and real-world testing to fully understand its capabilities and limitations [61, 107].

9 Conclusion

This survey has provided an overview of e-voting, covering various systems, architectures, advancements in blockchain technology, performance constraints, concerns, and potential solutions. We have synthesized the integration of blockchain technology as a promising solution to enhance the security, transparency, and integrity of e-voting systems, alongside related literature emphasizing the relevance of blockchain for e-voting purposes. We provided insights into the current state of e-voting systems and blockchain technology, touching on future research and development efforts focused on creating more secure, transparent, and inclusive electoral processes. Our survey encompasses the major components of e-voting systems, along with architectures, and case studies of blockchain-based e-voting systems. We also discussed technical constraints, including scalability issues and concerns related to voter privacy and accessibility, and propose emerging solutions such as parallelization techniques and consensus mechanism improvements. By highlighting both opportunities and challenges inherent in e-voting and blockchain technology, our survey serves as a foundation for future research and development endeavors. Collaboration among researchers, policymakers, and stakeholders is essential to balance innovation with robust security measures and uphold the fundamental principles of democratic elections. With further research, e-voting systems can leverage blockchain technology to fortify the foundations of modern democracies.

Acknowledgements The authors would like to acknowledge the support of the Tertiary Education Trust Fund (TETFund), Nigeria, under the National Research Fund (NRF) Intervention with Project ID REF: TETF/ED/DR&D-CE/NRF2021/SETI/SAE00147/VOL.1

Author contributions All authors H.O.O, A.J.O, B.U.U, L.A.A, R.O.I, E.M.D, B.K.N, O.M.O, V.B.S, M.M.I contributed equally to this work. Conceptualization, H.O.O., A.J.O, B.U.U, L.A.A; Methodology, H.O.O., A.J.O., R.O.I; Validation, A.J.O., E.M.D., O.M.O.; Formal analysis, E.M.D., O.M.O.; Investigation, V.B.S., M.M.I., B.K.N.; Resources, H.O.O; Data curation, V.B.S., M.M.I, B.U.U, B.K.N, R.O.I; Writing—original draft preparation, V.B.S., M.M.I, H.O.O, A.J.O.; Writing—review and editing, H.O.O, A.J.O.; Visualization, L.A.A., B.U.U, H.O.O, A.J.O; Supervision, H.O.O., E.M.D.; O.M.O.; Project administration, H.O.O; Funding acquisition, H.O.O. All authors have read and agreed to the published version of the manuscript.

Funding Open access funding provided by Council for Scientific and Industrial Research. Open access publication funding provided by the Council for Scientific and Industrial Research (CSIR), South Africa.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no Conflict of interest.

Ethical approval Not applicable

References

1. Vonnahme, G.: Electronic Voting Systems. Oxford University Press, Oxford (2019). https://doi.org/10.1093/obo/9780199756223-0259
2. Ikrissi, G., Mazri, T.: Electronic Voting: Review and Challenges, pp. 110–119. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-53824-7_11
3. Damgård, I., Groth, J., Salomonsen, G.: The Theory and Implementation of an Electronic Voting System. Springer, Cham (2003). https://doi.org/10.1007/978-1-4615-0239-5_6
4. Hajian Berenjestanaki, M., Barzegar, H.R., El Ioini, N., Pahl, C.: Blockchain-based e-voting systems: a technology review. Electronics **13**(1), 17 (2023). https://doi.org/10.3390/electronics13010017
5. Geng, T., Njilla, L., Huang, C.-T.: A survey of blockchain-based electronic voting mechanisms in sensor networks. In: Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems. SenSys '22, pp. 1222–1228. Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3560905.3568181
6. Viji, D.C., Kumar, A., Noorayen, A., Amjad, H., Abrar, M.: Blockchain voting: a comparative analysis. Int. J. Res. Appl. Sci. Eng. Technol. **10**(3), 1886–1890 (2022). https://doi.org/10.22214/ijraset.2022.41005
7. Varaprasada Rao, K., Panda, S.K.: Secure electronic voting (e-voting) system based on blockchain on various platforms. In: Computer Communication, Networking and IoT: Proceedings of

5th ICICC 2021, vol. 2, pp. 143–151. Springer (2022). https://doi.org/10.1007/978-981-19-1976-3_18
8. Verma, G.: A secure framework for e-voting using blockchain. In: 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), pp. 1–5. IEEE (2022). https://doi.org/10.1109/iccsea54677.2022.9936073
9. Soni, Y., Maglaras, L., Ferrag, M.A.: Blockchain based voting systems. In: European Conference on Cyber Warfare and Security, pp. 241–248. Academic Conferences International Limited (2020)
10. Shahzad, B., Crowcroft, J.: Trustworthy electronic voting using adjusted blockchain technology. IEEE Access **7**, 24477–24488 (2019). https://doi.org/10.1109/access.2019.2895670
11. Salman, S.A.-B., Al-Janabi, S., Sagheer, A.M.: A review on e-voting based on blockchain models. Iraqi J. Sci. (2022). https://doi.org/10.24996/ijs.2022.63.3.38
12. Sekar, S., Vigneshwar, C., Thiyagarajan, J., Narayanan, V.S., Vijay, M.: Decentralized e-voting system using blockchain. Int. J. Eng. Technol. (2020). https://doi.org/10.32628/ijsrset2310216
13. Sadia, K., Masuduzzaman, M., Paul, R.K., Islam, A.: Blockchain-based secure e-voting with the assistance of smart contract. In: IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology, pp. 161–176. Springer (2020). https://doi.org/10.1007/978-981-15-4542-9_14
14. Taş, R., Tanrıöver, Ö.Ö.: A systematic review of challenges and opportunities of blockchain for e-voting. Symmetry **12**(8), 1328 (2020). https://doi.org/10.3390/sym12081328
15. Kho, Y.-X., Heng, S.-H., Chin, J.-J.: A review of cryptographic electronic voting. Symmetry **14**(5), 858 (2022). https://doi.org/10.3390/sym14050858
16. Soud, M., Helgason, S., Hjálmtỳsson, G., Hamdaqa, M.: Trustvote: On elections we trust with distributed ledgers and smart contracts. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 176–183. IEEE (2020). https://doi.org/10.1109/brains49436.2020.9223306
17. Sahib, R.H., Al-Shamery, E.S.: A review on distributed blockchain technology for e-voting systems. J. Phys. Conf. Ser. **1804**, 012050 (2021). https://doi.org/10.1088/1742-6596/1804/1/012050
18. Sabharwal, A., Saifullah, M., Grover, P., Batra, N.: Comparative study of blockchain techniques in electronic voting. System (2021). https://doi.org/10.2139/ssrn.3884390
19. Xiao, S., Wang, X.A., Wang, W., Wang, H.: Survey on blockchain-based electronic voting. In: Advances in Intelligent Networking and Collaborative Systems: The 11th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2019), pp. 559–567. Springer (2020)
20. Singh, S., Wable, S., Kharose, P.: A review of e-voting system based on blockchain technology. Int. J. New Pract. Manag. Eng. **10**(04), 09–13 (2021). https://doi.org/10.17762/ijnpme.v10i04.125
21. Singh, A., Chatterjee, K.: SecEVS: secure electronic voting system using blockchain technology. In: 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 863–867. IEEE (2018). https://doi.org/10.1109/gucon.2018.8675008
22. 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) **54**(3), 1–28 (2021). https://doi.org/10.1145/3439725
23. Marath, R., Sachin, C., Sanjay, S., Sagar, D., Annigeri, S.F., Abhinav, R., Bangalore, D.: A review on e-stamping in digital voting system using block chain and cloud server. Int. J. Inno. Sci. Res. Tech. **8**(1), 1851–1855 (2023). https://doi.org/10.5281/zenodo.7628522
24. Majeed, N.A.: Review on blockchain based e-voting systems. Konferenzband zum Scientific Track der Blockchain Autumn School **2021**(004), 001–008 (2021)
25. Alenoghena, C.O., Onumanyi, A.J., Ohize, H.O., Adejo, A.O., Oligbi, M., Ali, S.I., Okoh, S.A.: eHealth: a survey of architectures, developments in mHealth, security concerns and solutions. Int. J. Environ. Res. Public Health **19**(20), 13071 (2022). https://doi.org/10.3390/ijerph192013071
26. Alenoghena, C.O., Ohize, H.O., Adejo, A.O., Onumanyi, A.J., Ohihoin, E.E., Balarabe, A.I., Okoh, S.A., Kolo, E., Alenoghena, B.: Telemedicine: a survey of telecommunication technologies, developments, and challenges. J. Sens. Actuator Netw. **12**(2), 20 (2023)
27. Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Syst. Rev. (2021). https://doi.org/10.1186/s13643-021-01626-4
28. Pawlak, M., Poniszewska-Marańda, A., Kryvinska, N.: Towards the intelligent agents for blockchain e-voting system. Procedia Comput. Sci. **141**, 239–246 (2018). https://doi.org/10.1016/j.procs.2018.10.177
29. Angsuchotmetee, C., Setthawong, P., Udomviriyalanon, S.: Blockvote : An architecture of a blockchain-based electronic voting system. In: 2019 23rd International Computer Science and Engineering Conference (ICSEC), pp. 110–116 (2019). https://doi.org/10.1109/ICSEC47112.2019.8974826
30. Qadah, G.Z., Taha, R.: Electronic voting systems: requirements, design, and implementation. Comput. Stand. Interfaces **29**(3), 376–386 (2007). https://doi.org/10.1016/j.csi.2006.06.001
31. Sridharan, S.: Implementation of authenticated and secure online voting system. IEEE (2013). https://doi.org/10.1109/icccnt.2013.6726801
32. Kumar, D.A., Begum, T.U.S.: Electronic voting machine—a review. In: International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), pp. 41–48. IEEE (2012)
33. Habibu, T., Sharif, K., Nicholas, S.: Design and implementation of electronic voting system. Int. J. Comput. Organ. Trends **7**(4), 1–6 (2017). https://doi.org/10.14445/22492593/ijcot-v45p301
34. Villafiorita, A., Weldemariam, K., Tiella, R.: Development, formal verification, and evaluation of an e-voting system with VVPAT. IEEE Trans. Inf. Forensics Secur. **4**(4), 651–661 (2009). https://doi.org/10.1109/tifs.2009.2034903
35. Abdelkader, R., Youssef, M.: UVote: a ubiquitous e-voting system. IEEE (2012). https://doi.org/10.1109/music.2012.20
36. Daramola, O., Thebus, D.: Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections. Informatics (2020). https://doi.org/10.3390/informatics7020016
37. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain technology overview. Technical report, National Institute of Standards and Technology (NIST) (2019). https://doi.org/10.6028/NIST.IR.8202
38. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. IEEE Commun. Surv. Tutor. **21**(3), 1653–1676 (2017). https://doi.org/10.1109/SURV.2017.1700202
39. Xu, L., Chen, L., Gao, Y., Chang, V., Li, Z., Islam, M.K.A., Mhamdi, L., Xu, K., Wang, J.: Blockchain-enabled internet of things (IoT): architecture, emerging technologies, and open issues. IEEE Internet Things J. **6**(5), 8076–8094 (2019). https://doi.org/10.1109/JIOT.2019.2931232

40. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. In: 2018 Annual National Seminar, pp. 1–11 (2008)
41. Zhang, T., Huang, Z.: Blockchain and central bank digital currency. Ict Express **8**(2), 264–270 (2022). https://doi.org/10.1016/j.icte.2021.09.014
42. Zhang, T., Wu, Q., Wang, Q., Han, T., Li, B., Zhu, Y.: Covert communication via blockchain: hiding patterns and communication patterns. Comput. Stand. Interfaces **90**, 103851 (2024). https://doi.org/10.1016/j.csi.2024.103851
43. Zhang, T.: Privacy evaluation of blockchain based privacy cryptocurrencies: a comparative analysis of dash, monero, verge, zcash and grin. IEEE Trans. Sustain. Comput. (2023). https://doi.org/10.1109/tsusc.2023.3303180
44. Yang, J., Yang, K., Xiao, Z., Jiang, H., Xu, S., Dustdar, S.: Improving commute experience for private car users via blockchain-enabled multitask learning. IEEE Internet Things J. **10**(24), 21656–21669 (2023). https://doi.org/10.1109/JIOT.2023.3317639
45. Sun, G., Li, Y., Liao, D., Chang, V.: Service function chain orchestration across multiple domains: a full mesh aggregation approach. IEEE Trans. Netw. Serv. Manag. **15**(3), 1175–1191 (2018). https://doi.org/10.1109/TNSM.2018.2861717
46. Sun, G., Xu, Z., Yu, H., Chang, V.: Dynamic network function provisioning to enable network in box for industrial applications. IEEE Trans. Ind. Inf. **17**(10), 7155–7164 (2021). https://doi.org/10.1109/TII.2020.3042872
47. Carnley, R., Bagui, S.: A public infrastructure for a trusted wireless world. Future Internet (2022). https://doi.org/10.3390/fi14070200
48. Diaconita, V., Belciu, A., Stoica, M.G.: Trustful blockchain-based framework for privacy enabling voting in a university. J. Theor. Appl. Electron. Commer. Res. **18**(1), 150–169 (2023). https://doi.org/10.3390/jtaer18010008
49. Bastiaan, M.: Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. In: 22nd Twente Student Conference on IT, Netherlands, pp. 1–10 (2015)
50. Raj, A., George, G.T., Konnully, P., Nair, S.R.: Vote blocks: a block chain based e-voting system. Int. J. Comput. Sci. Trends Technol. **7**(3), 49–54 (2019)
51. Zhang, W., Anand, T.: blockchain implementations overview: bitcoin, ethereum, and hyperledger. Apress (2022). https://doi.org/10.1007/978-1-4842-8164-2_5
52. Suralkar, S., Udasi, S., Gagnani, S., Tekwani, M., Bhatia, M.: E-voting using blockchain with biometric authentication. Int. J. Res. Anal. Rev. **6**(1), 72–81 (2019)
53. Al-Madani, A.M., Gaikwad, A.T., Mahale, V., Ahmed, Z.A.: Decentralized e-voting system based on smart contract by using blockchain technology. In: 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), pp. 176–180. IEEE (2020). https://doi.org/10.1109/icsidempc49020.2020.9299581
54. Kondo, M., Oliva, G.A., Jiang, Z.M., Hassan, A.E., Mizuno, O.: Code cloning in smart contracts: a case study on verified contracts from the ethereum blockchain platform. Empir. Softw. Eng. **25**, 4617–4675 (2020). https://doi.org/10.1007/s10664-020-09852-5
55. Mursi, M.F., Assassa, G.M., Abdelhafez, A., Samra, K.M.A.: On the development of electronic voting: a survey. Int. J. Comput. Appl. (2013). https://doi.org/10.5120/10009-4872
56. Akbari, E., Wu, Q., Zhao, W., Arabnia, H.R., Yang, M.Q.: From blockchain to internet-based voting. In: 2017 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 218–221. IEEE (2017). https://doi.org/10.1109/csci.2017.34
57. Baudier, P., Kondrateva, G., Ammi, C., Seulliet, E.: Peace engineering: the contribution of blockchain systems to the e-voting process. Technol. Forecast. Soc. Change **162**, 120397 (2021). https://doi.org/10.1016/j.techfore.2020.120397
58. 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. **80**, 3363–3370 (2023). https://doi.org/10.1016/j.matpr.2021.07.254
59. Al-Farsi, S., Rathore, M.M., Bakiras, S.: Security of blockchain-based supply chain management systems: challenges and opportunities. Appl. Sci. **11**(12), 5585 (2021). https://doi.org/10.3390/app11125585
60. Khan, F.A., Asif, M., Ahmad, A., Alharbi, M., Aljuaid, H.: Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustain. Cities Soc. **55**, 102018 (2020). https://doi.org/10.1016/j.scs.2020.102018
61. Jafar, U., Aziz, M.J.A., Shukur, Z.: Blockchain for electronic voting system-review and open research challenges. Sensors **21**(17), 5874 (2021). https://doi.org/10.3390/s21175874
62. Khoury, D., Kfoury, E.F., Kassem, A., Harb, H.: Decentralized voting platform based on ethereum blockchain. In: 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1–6. IEEE (2018). https://doi.org/10.1109/imcet.2018.8603050
63. Kiran, A., Puri, M., Srinivasa, S.: Privacy preserving model using homomorphic encryption. Int. J. Comput. Appl. **182**(38), 12–18 (2019). https://doi.org/10.5120/ijca2019918390
64. Kharchineh, B., Ettelaee, M.: A new electronic voting protocol using a new blind signature scheme. IEEE (2010). https://doi.org/10.1109/icfn.2010.40
65. Panja, S., Roy, B.: A Secure End-to-End Verifiable E-Voting System Using Zero-Knowledge Proof and Blockchain. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-6991-7_6
66. Squarepants, S.: Bitcoin: a peer-to-peer electronic cash system. SSRN Electron. J. (2008). https://doi.org/10.2139/ssrn.3977007
67. Faruk, M.J.H., Alam, F., Islam, M., Rahman, A.: Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. Clust. Comput. (2024). https://doi.org/10.1007/s10586-023-04261-x
68. Tanwar, S., Gupta, N., Kumar, P., Hu, Y.-C.: Implementation of blockchain-based e-voting system. Multimed. Tools Appl. **83**(1), 1449–1480 (2024). https://doi.org/10.1007/s11042-023-15401-1
69. Agate, V., Paola, A.D., Ferraro, P., Re, G.L., Morana, M.: SecureBallot: a secure open source e-voting system. J. Netw. Comput. Appl. **191**, 103165 (2021). https://doi.org/10.1016/j.jnca.2021.103165
70. Khan, S., Arshad, A., Mushtaq, G., Khalique, A., Husein, T.: Implementation of decentralized blockchain e-voting. EAI Endorsed Trans. Smart Cities **4**(10), 164859 (2020). https://doi.org/10.4108/eai.13-7-2018.164859
71. Comuzzi, M., Grefen, P., Meroni, G.: Private Blockchain. Routledge, London (2023). https://doi.org/10.4324/9781003321187-9
72. Ibáñez, J.W., Moccia, S.: Designing the architecture of a blockchain platform. Int. J. Enterp. Inf. Syst. **16**(3), 34–48 (2020). https://doi.org/10.4018/ijeis.2020070103
73. Ajayi, O., Igbe, O., Saadawi, T.: Consortium blockchain-based architecture for cyber-attack signatures and features distribution. IEEE (2019). https://doi.org/10.1109/uemcon47517.2019.8993036
74. Ni, L., Zhang, S., Li, G., Han, K., Sun, H.: A design of extensible architecture based on consortium blockchain. IEEE (2022). https://doi.org/10.1109/icait56197.2022.9862749
75. Han, Y., Wang, X., Zhang, Y., Yang, G., Tan, X.: A UAV swarm communication network architecture based on

consortium blockchain. J. Phys.: Conf. Ser. **2352**(1), 012008 (2022). https://doi.org/10.1088/1742-6596/2352/1/012008
76. Desai, H., Kantarcioglu, M., Kagal, L.: A hybrid blockchain architecture for privacy-enabled and accountable auctions. In: 2019 IEEE International Conference on Blockchain (Blockchain). IEEE (2019). https://doi.org/10.1109/blockchain.2019.00014
77. Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., Han, W.: An overview on cross-chain: mechanism, platforms, challenges and advances. Comput. Netw. **218**, 109378 (2022)
78. Lohachab, A., Garg, S., Kang, B., Amin, M.B., Lee, J., Chen, S., Xu, X.: Towards interconnected blockchains: a comprehensive review of the role of interoperability among disparate blockchains. ACM Comput. Surv. (CSUR) **54**(7), 1–39 (2021)
79. Nikhare, R.V., Chandavarkar, B.R.: A comparative analysis of traditional versus blockchain-based voting systems. In: 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE (2023). https://doi.org/10.1109/icccnt56998.2023.10307550
80. Pawlak, M., Poniszewska-Marańda, A.: Trends in blockchain-based electronic voting systems. Inf. Process. Manag. **58**(4), 102595 (2021). https://doi.org/10.1016/j.ipm.2021.102595
81. 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 **22**(19), 7585 (2022). https://doi.org/10.3390/s22197585
82. Hjalmarsson, F., Hreidharsson, G.K., Hamdaqa, M., Hjalmtysson, G.: Blockchain-based e-voting system. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983–986. IEEE (2018). https://doi.org/10.1109/cloud.2018.00151
83. Çabuk, U.C., Adiguzel, E., Karaarslan, E.: A survey on feasibility and suitability of blockchain techniques for the e-voting systems. arXiv preprint arXiv:2002.07175 (2020)
84. Naik, A.C., Prajapati, A.M., Pandey, S.N., Mishra, A.C.: Blockchain based e-voting system. In: 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 316–320. IEEE (2023). https://doi.org/10.1109/icoei56765.2023.10125883
85. Kaudare, A., Hazra, M., Shelar, A., Sabnis, M.: Implementing electronic voting system with blockchain technology. In: 2020 International Conference for Emerging Technology (INCET), pp. 1–9. IEEE (2020). https://doi.org/10.1109/incet49848.2020.9154116
86. Abuidris, Y., Kumar, R., Wenyong, W.: A survey of blockchain based on e-voting systems. In: Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, pp. 99–104 (2019). https://doi.org/10.1145/3376044.3376060
87. McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom voting with maximum voter privacy. In: Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers 21, pp. 357–375. Springer (2017). https://doi.org/10.1007/978-3-319-70972-7_20
88. Szabo, N.: Formalizing and securing relationships on public networks. First Monday (1997). https://doi.org/10.5210/fm.v2i9.548
89. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy, pp. 104–121. IEEE (2015). https://doi.org/10.1109/sp.2015.14
90. Xu, J., Wang, C., Jia, X.: A survey of blockchain consensus protocols. ACM Comput. Surv. (2023). https://doi.org/10.1145/3579845
91. Buterin, V., et al.: A next-generation smart contract and decentralized application platform. White Paper **3**(37), 2–1 (2014)
92. Zohar, A.: Bitcoin: under the hood. Commun. ACM **58**(9), 104–113 (2015). https://doi.org/10.1145/2701411
93. Kowalik, O., Górny, M.: Distributed, decentralized registries and digital state. are we moving toward a blockchain democracy? In: Digital Communication and Populism in Times of Covid-19: Cases, Strategies, Examples, pp. 163–177. Springer (2023). https://doi.org/10.1007/978-3-031-33716-1_12
94. Sanjaya, M.: A blockchain based approach for secure e-voting system. BA Thesis, University of California, Santa Cruz, 1156 High St, Santa Cruz, CA 95064, United States (2021)
95. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat. Inform. **36**, 55–81 (2019). https://doi.org/10.1016/j.tele.2018.11.006
96. Luan, L., Wang, Z., Liu, S.: Progress of Grover quantum search algorithm. Energy Procedia **16**, 1701–1706 (2012). https://doi.org/10.1016/j.egypro.2012.01.263
97. Xu, F., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W.: Quantum cryptography with realistic devices. arXiv preprint arXiv:1903.09051 (2019)
98. Grasselli, F.: Introducing Quantum Key Distribution, pp. 35–54. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-64360-7_3
99. Liu, Z., et al.: Improving the security and reliability of application systems with blockchain technology. Master's Thesis, Hong Kong Polytechnic University (2023)
100. Dogo, E., Nwulu, N., Olaniyi, O.M., Aigbavboa, C., Nkonyana, T.: Blockchain 3.0: towards a secure ballotcoin democracy through a digitized public ledger in developing countries (2018)
101. Bulut, R., Kantarcı, A., Keskin, S., Bahtiyar, Ş.: Blockchain-based electronic voting system for elections in turkey. In: 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 183–188. IEEE (2019). https://doi.org/10.1109/ubmk.2019.8907102
102. Zambrano, R., Young, A., Verhulst, S.: Seeking ways to prevent electoral fraud using blockchain in Sierra Leone. The GovLab **1**(1), 1–11 (2018)
103. Specter, M.A., Koppel, J., Weitzner, D.: The ballot is busted before the blockchain: a security analysis of Voatz, the first internet voting application used in {US}. federal elections. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 1535–1553 (2020)
104. Kshetri, N., Voas, J.: Blockchain-enabled e-voting. IEEE Softw. **35**(4), 95–99 (2018). https://doi.org/10.1109/ms.2018.2801546
105. Al Barghuthi, N.B., Hamdan, I., Al Suwaidi, S., Lootah, A., Al Amoudi, B., Al Shamsi, O., Al Aryani, S.: An analytical view on political voting system using blockchain technology-UAE case study. In: 2019 Sixth HCT Information Technology Trends (ITT), pp. 132–137. IEEE (2019). https://doi.org/10.1109/itt48889.2019.9075074
106. Stan, I.-M., Barac, I.-C., Rosner, D.: Architecting a scalable e-election system using blockchain technologies. In: 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), pp. 1–6. IEEE (2021). https://doi.org/10.1109/roedunet54112.2021.9638303
107. Chafiq, T., Azmi, R., Mohammed, O.: Blockchain-based electronic voting systems: a case study in Morocco. Int. J. Intell. Netw. (2024). https://doi.org/10.1016/j.ijin.2024.01.004
108. Khudnev, E.: Blockchain: foundational technology to change the world. Master's Thesis, Lapland University of Applied Sciences (2017)
109. Al-Shammari, A.F.N., Villafiorita, A., Weldemariam, K.: Understanding the development trends of electronic voting

systems. In: 2012 Seventh International Conference on Availability, Reliability and Security, pp. 186–195. IEEE (2012). https://doi.org/10.1109/ares.2012.76
110. Negka, L.D., Spathoulas, G.P.: Blockchain state channels: a state of the art. IEEE Access **9**, 160277–160298 (2021)
111. Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: SoK: layer-two blockchain protocols. In: Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24, pp. 201–226. Springer (2020)
112. Dang, H., Dinh, T.T.A., Loghin, D., Chang, E.-C., Lin, Q., Ooi, B.C.: Towards scaling blockchain systems via sharding. In: Proceedings of the 2019 International Conference on Management of Data, pp. 123–140 (2019)
113. Singh, A., Parizi, R.M., Han, M., Dehghantanha, A., Karimipour, H., Choo, K.-K.R.: Public blockchains scalability: an examination of sharding and segregated witness. In: Blockchain Cybersecurity, Trust and Privacy, pp. 203–232 (2020)
114. Wang, H., Cen, Y., Li, X.: Blockchain router: a cross-chain communication protocol. In: Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, pp. 94–97 (2017)
115. Pillai, B., Biswas, K., Muthukkumarasamy, V.: Cross-chain interoperability among blockchain-based systems using transactions. Knowl. Eng. Rev. **35**, 23 (2020)
116. Qasse, I.A., Abu Talib, M., Nasir, Q.: Inter blockchain communication: a survey. In: Proceedings of the ArabWIC 6th Annual International Conference Research Track, pp. 1–6 (2019)
117. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on {Bitcoin's}{peer-to-peer} network. In: 24th USENIX Security Symposium (USENIX Security 15), pp. 129–144 (2015)
118. Lin, I.-C., Liao, T.-C.: A survey of blockchain security issues and challenges. Int. J. Netw. Secur. **19**(5), 653–659 (2017)
119. Luo, T.: An efficient blockchain based electronic voting system using proxy multi-signature. In: 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), pp. 513–516. IEEE (2021)
120. Emami, A., Yajam, H., Akhaee, M.A., Asghari, R.: A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations. J. Inf. Secur. Appl. **79**, 103645 (2023)
121. Tso, R., Liu, Z.-Y., Hsiao, J.-H.: Distributed e-voting and e-bidding systems based on smart contract. Electronics **8**(4), 422 (2019)
122. Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., Chen, R.: NutBaaS: a blockchain-as-a-service platform. IEEE Access **7**, 134422–134433 (2019)
123. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2018)
124. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology?—a systematic review. PLoS ONE **11**(10), 0163477 (2016)
125. Xu, X., Weber, I., Staples, M.: Architecture for Blockchain Applications. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-03035-3
126. Alharby, M., Moorsel, A.: Blockchain-based smart contracts: a systematic mapping study. In: Proceedings of the International Conference on Computer Science and Information Technology, pp. 125–136 (2017). https://doi.org/10.1109/CSIT.2017.42
127. Manpearl, E.: Securing us election systems: designating us election systems as critical infrastructure and instituting election security reforms. BUJ Sci. Technol. Law **24**, 168 (2018)
128. Suwito, M.H., Dutta, S.: Verifiable e-voting with resistance against physical forced abstention attack. In: 2019 International Workshop on Big Data and Information Security (IWBIS), pp. 85–90. IEEE (2019). https://doi.org/10.1109/iwbis.2019.8935763
129. Ahmad, M., Rehman, A.U., Ayub, N., Alshehri, M.D., Khan, M.A., Hameed, A., Yetgin, H.: Security, usability, and biometric authentication scheme for electronic voting using multiple keys. Int. J. Distrib. Sens. Netw. **16**(7), 1550147720944025 (2020). https://doi.org/10.1177/1550147720944025
130. Adekunle, S.E., et al.: A review of electronic voting systems: strategy for a novel. Int. J. Inf. Eng. Electron. Bus. (2020). https://doi.org/10.5815/ijieeb.2020.01.03
131. Alam, M., Yusuf, M.O., Sani, N.A.: Blockchain technology for electoral process in Africa: a short review. Int. J. Inf. Technol. **12**(3), 861–867 (2020). https://doi.org/10.1007/s41870-020-00440-w
132. Mitrou, L., Gritzalis, D., Katsikas, S., Quirchmayr, G.: Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications, pp. 43–60. Springer US (2003). https://doi.org/10.1007/978-1-4615-0239-5_4
133. Abed, H., Al-Zoubi, O., Alayan, H., Alshboul, M.: Towards maintaining confidentiality and anonymity in secure blockchain-based e-voting. Clust. Comput. **27**(4), 4635–4657 (2024). https://doi.org/10.1007/s10586-023-04194-5
134. Robinson, D.G., Halderman, J.A.: Ethical Issues in E-Voting Security Analysis, pp. 119–130. Springer, Berlin/Heidelberg (2012). https://doi.org/10.1007/978-3-642-29889-9_10
135. Cong, K., Ren, Z., Pouwelse, J.: A blockchain consensus protocol with horizontal scalability. In: 2018 IFIP Networking Conference (IFIP Networking) and Workshops, pp. 1–9. IEEE (2018). https://doi.org/10.23919/ifipnetworking.2018.8696555
136. Chauhan, A., Malviya, O.P., Verma, M., Mor, T.S.: Blockchain and scalability. In: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 122–128. IEEE (2018). https://doi.org/10.1109/qrs-c.2018.00034
137. Lombrozo, E., Lau, J., Wuille, P.: Segregated witness (consensus layer). Bitcoin Core Development Team, Technical Report BIP **141** (2015)
138. Khan, D., Jung, L.T., Hashmani, M.A.: Systematic literature review of challenges in blockchain scalability. Appl. Sci. **11**(20), 9372 (2021). https://doi.org/10.3390/app11209372
139. Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.: Blockchain with internet of things: benefits, challenges, and future directions. Int. J. Intell. Syst. Appl. **10**(6), 40–48 (2018). https://doi.org/10.5815/ijisa.2018.06.05
140. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 17–30 (2016). https://doi.org/10.1145/2976749.2978389
141. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., Ford, B.: Omniledger: a secure, scale-out, decentralized ledger via sharding. In: 2018 IEEE Symposium on Security and Privacy (SP), pp. 583–598. IEEE (2018). https://doi.org/10.1109/sp.2018.000-5
142. Porkodi, S., Kesavaraja, D.: Integration of blockchain and internet of things. In: Handbook of Research on Blockchain Technology, pp. 61–94. Elsevier (2020). https://doi.org/10.1016/b978-0-12-819816-2.00003-4
143. Singh, S., Hosen, A.S., Yoon, B.: Blockchain security attacks, challenges, and solutions for the future distributed IoT network. IEEE Access **9**, 13938–13959 (2021)

144. Priya, S., Srivastava, G., Kumar, S.: Secured electronic voting transactions integrated with blockchain. Int. J. Res. Anal. Rev. **8**(2), 408–414 (2021)
145. Ajao, L.A., Umar, B.U., Olajide, D.O., Misra, S.: Application of crypto-blockchain technology for securing electronic voting systems. In: Blockchain Applications in the Smart Era, pp. 85–105. Springer (2022). https://doi.org/10.1007/978-3-030-89546-4_5
146. Jagdale, K., Shelke, C., Achary, R., Wankhede, D., Bhandare, T.: Artificial intelligence and its subsets: machine learning and its algorithms, deep learning, and their future trends. Int. J. Emerg. Technol. Innov. Res. **9**(5), (2022)
147. Grimaldi, D., Cely, J.D., Arboleda, H.: Inferring the votes in a new political landscape: the case of the 2019 Spanish presidential elections. J. Big Data **7**(1), 58 (2020). https://doi.org/10.1186/s40537-020-00334-5
148. Safiullah, M., Parveen, N.: Big data, artificial intelligence and machine learning: a paradigm shift in election campaigns. In: The New Advanced Society: Artificial Intelligence and Industrial Internet of Things Paradigm, pp. 247–261 (2022) https://doi.org/10.1002/9781119884392.ch11
149. Zhang, M., Alvarez, R.M., Levin, I.: Election forensics: using machine learning and synthetic data for possible election anomaly detection. PLoS ONE **14**(10), 0223950 (2019). https://doi.org/10.1371/journal.pone.0223950
150. Ajao, L.A., Apeh, S.T.: Blockchain integration with machine learning for securing fog computing vulnerability in smart city sustainability. In: 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), pp. 1–6. IEEE (2023). https://doi.org/10.1109/icaisc56366.2023.10085192
151. Gupta, C., Johri, I., Srinivasan, K., Hu, Y.-C., Qaisar, S.M., Huang, K.-Y.: A systematic review on machine learning and deep learning models for electronic information security in mobile networks. Sensors **22**(5), 2017 (2022). https://doi.org/10.3390/s22052017
152. Praet, S., Van Aelst, P., Erkel, P., Veeken, S., Martens, D.: Predictive modeling to study lifestyle politics with Facebook likes. EPJ Data Sci. **10**(1), 50 (2021). https://doi.org/10.1140/epjds/s13688-021-00305-7
153. Di Franco, G., Santurro, M.: Machine learning, artificial neural networks and social research. Qual. Quant. **55**(3), 1007–1025 (2021)
154. M, K., V, G.P., Ramar, K., Hariharan, S.: Secure e-voting system using deep learning techniques. In: 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT). IEEE (2022). https://doi.org/10.1109/cisct55310.2022.10046486
155. Mahanayak, S.P., Nikhita, B., Bilgaiyan, S.: Enhancing e-voting security with quantum-resistant encryption: a blockchain-based approach utilizing elliptic curve diffie-hellman and decentralized storage. SN Comput. Sci. (2023). https://doi.org/10.1007/s42979-023-02041-3
156. Aidynov, T., Goranin, N., Satybaldina, D., Nurusheva, A.: A systematic literature review of current trends in electronic voting system protection using modern cryptography. Appl. Sci. **14**(7), 2742 (2024). https://doi.org/10.3390/app14072742
157. Ngabo, D., Wang, D., Iwendi, C., Anajemba, J.H., Ajao, L.A., Biamba, C.: Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics **10**(17), 2110 (2021). https://doi.org/10.3390/electronics10172110
158. Attaran, M., Gunasekaran, A.: Applications of Blockchain Technology in Business: Challenges and Opportunities. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-27798-7
159. Komatineni, S., Lingala, G.: Secured e-voting system using two-factor biometric authentication. In: 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 245–248. IEEE (2020). https://doi.org/10.1109/iccmc48092.2020.iccmc-00046
160. Othman, A.A., Muhammed, E.A., Mujahid, H.K., Muhammed, H.A., Mosleh, M.A.: Online voting system based on IoT and ethereum blockchain. In: 2021 International Conference of Technology, Science and Administration (ICTSA), pp. 1–6. IEEE (2021). https://doi.org/10.1109/ictsa52017.2021.9406528
161. Rathee, G., Iqbal, R., Waqar, O., Bashir, A.K.: On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities. IEEE Access **9**, 34165–34176 (2021). https://doi.org/10.1109/access.2021.3061411
162. El Fezzazi, A., Adadi, A., Berrada, M.: Towards a blockchain based intelligent and secure voting. In: 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), pp. 1–8. IEEE (2021). https://doi.org/10.1109/icds53782.2021.9626751
163. Peiris, K., Gunathilake, G., Attanayaka, J., Ilankoon, I., Chandrasiri, S., Wijendra, D.R.: Digital democracy: a secure platform for voting. In: 2021 2nd International Informatics and Software Engineering Conference (IISEC), pp. 1–4. IEEE (2021). https://doi.org/10.1109/iisec54230.2021.9672367
164. Tyagi, A.K., Aswathy, S., Abraham, A.: Integrating blockchain technology and artificial intelligence: synergies perspectives challenges and research directions. J. Inf. Assur. Secur. **15**(5), 1554 (2020)
165. Wang, J.: Exploring digital timestamping using smart contract on the Solana blockchain. In: Yuan, X. (ed.) Second International Conference on Green Communication, Network, and Internet of Things (CNIoT 2022). SPIE (2023). https://doi.org/10.1117/12.2667788
166. Yakovenko, A.: Solana: a new architecture for a high performance blockchain v0. 8.13. Whitepaper (2018)

Henry O. Ohize is an Associate Professor of Electrical and Electronics Engineering at the Federal University of Technology Minna. Having obtained a Doctorate Degree from the University of Cape Town in 2017, Ohize possesses a strong academic background in the field. With a rich passion for teaching and research, Ohize has accumulated over fifteen years of valuable experience in the domain. In the capacity of a postgraduate supervisor, Ohize has successfully guided and graduated several Master's students, demonstrating adeptness in academic mentorship. In the realm of research, Ohize's interests lie in the full realization and

implementation of 6G technology. These encompass various aspects such as Cognitive Radio, Wireless Sensor Networks, MIMO, mmWave, and 6G application areas. Notably, the focus extends to the application of 6G technology in fields like e-Health, Telemedicine, and IoT, reflecting a commitment to cutting-edge technological advancements. Furthermore, Ohize has actively participated in prominent conferences, including the 2017 IEEE Wireless Communications and Networking Conference (WCNC) in the USA and the 2016 Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) in Valencia, Spain. Notably, Ohize's contributions have been featured in several publications in Scopus indexed journals, highlighting a significant research footprint in the academic community. Notably, Ohize has received recognition for scholarly contributions, including the SA NRF awards in South Africa and the TETFUND NRF award from the Nigerian government. These accolades signify the impactful contributions made by Ohize in the realm of academia and research.

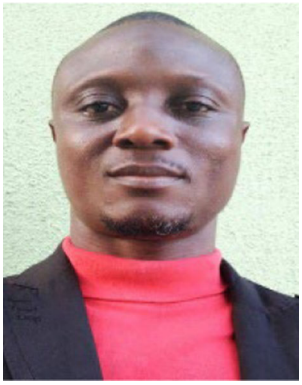
Adeiza James Onumanyi obtained his PhD in Communication Engineering from the Federal University of Technology, Minna, Nigeria, in 2014. He currently serves as a senior researcher at the Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa. His research contributions are published in various peer-reviewed journals as well as in different IEEE flagship conferences. His research interests span a broad spectrum, including studies in cognitive radio, wireless sensor networks, smart transactive microgrids, DC nanogrids, radar systems, image processing, cyber-physical systems, and low-powered wireless area networks.

Buhari U. Umar is a Lecturer/researcher at the Department of Computer Engineering, Federal University of Technology, Minna. His research areas focus on Artificial Intelligence, Image Processing, Blockchain, e-voting, and embedded systems. He holds a Ph.D. in Computer Engineering from the Federal University of Technology, Minna., Nigeria. Engr. Dr. Buhari Ugbede Umar has authored more than 50 research papers in refereed journals, Book Chapters, and International Conferences. He is a Professional member of the Nigeria Computer Society (NCS) and a Certified Register Engineer with the Council for Regulation of Engineering in Nigeria.

Lukman A. Ajao is a Senior Research Fellow, currently working in the Department of Computer Engineering, Federal University of Technology, Minna, Nigeria. He obtained his post graduate diploma degree in Computer Science at the University of Ilorin (2014), and a Master of Engineering Degree (M. Eng) in Computer Engineering from the Federal University of Technology, Minna, Nigeria (2018). He is currently a Ph. D research associate in the department of Computer Engineering, Ahamadu Bello University Zaria, Nigeria. He is a corporate member of Nigerian Association of Technologist in Engineering (NATE), Registered Engineer (R. COREN), Member IEEE, IAENG, IACSIT and IRED. His research interests are Real-Time Embedded System, Internet of Things, Wireless Sensor Network, Computer Security, FPGA, Machine Learning, Artificial Intelligence (AI) and Computational Intelligence (CI).

Rabiu O. Isah received his B.Eng. degree in Electrical and Computer Engineering from the Federal University of Technology, Minna, Nigeria in 2008. He later proceeded to the prestigious Ahmadu Bello University, Zaria, where he obtained his MSc. and Ph.D. both in Computer Engineering in 2017 and 2024 respectively. He has a lot of national and international publications from reputable journals and conferences to his credit. His current research interests include intelligent and embedded systems, telemedicine and biomedical imaging.

Eustace M. Dogo holds a BSc and MEng in Electrical and Electronic Engineering from Peter the Great Saint Petersburg Polytechnic University, Russia and a PhD in Electrical and Electronic Engineering from the University of Johannesburg, South Africa, with specialization in Artificial Intelligence and Machine Learning. He currently lectures and Heads the Department of Computer Engineering, Federal University of Technology Minna, Nigeria. He has extensive knowledge in industry, research, training and teaching. He is an active undergraduate and postgraduate supervisor and have authored and co-authored in reputable journals, conferences and several scholarly research book chapters in his areas of interest. His broad research interest includes Artificial Intelligence, Theoretical and Applied Machine Learning, Deep Learning, Intelligent Systems, Cloud Computing and Emerging Technologies.



Bello K. Nuhu is a Lecturer in the Department of Computer Engineering at the Federal University of Technology, Minna, Niger State, Nigeria, with over twelve years of experience in teaching and research. He obtained his B.Eng. in Electrical/Computer Engineering from Federal University of Technology, Minna, and M.Tech. In Computer Science from the Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He obtained his PhD in Computer Engineering from Ahmadu Bello University, Zaria, Nigeria. He has published in reputable journals and learned conferences. His areas of research include Computer and information security, intelligent/embedded systems, Wireless and computer networks, Internet of things and precision agriculture. Among other administrative and academic responsibilities in the University, Dr. Nuhu is the current final year undergraduate project coordinator, deputy coordinator Student Work Experience Program (SWEP), Faculty of Engineering, Federal University of Technology (FUT) Minna, commercialization officer representing Engineering at Intellectual Property and Technology Transfer Office (IPTTO), FUT Minna. With over 50 publications in reputable Journals and conferences. He has extensive knowledge in research, training, and teaching with over eleven years of experience. His broad research interest includes theoretical and applied Machine Learning, Deep Learning, Intelligent Systems, Cloud Computing and Emerging Technologies.

Olayemi M. Olaniyi is currently a Full Professor in the Department of Computer Science at the Faculty of Computing, National Open University of Nigeria, Abuja, Nigeria. He holds a Ph.D. in Computer Science and Engineering (Computer Security) from Ladoke Akintola University of Technology, Nigeria. Prof. Olaniyi is the author of more than 150 research papers in refereed journals, Book Chapters, and International Conferences. His research interests are in Computer Security, Intelligent Systems, Embedded Systems, Telemedicine, and Applied medical informatics. He is an Associate Editor of Computing, Information Systems, Development Informatics and Allied Research: A Multidisciplinary Journal; Editorial Board member of several national and international journals and an evaluator expert for national and international projects. He has served as Session Chair of several International Workshop and Conferences held in Nigeria. He participated in many international conferences as an Organizer, Session Chair, and member of the International Program Committee. He is a member of ACM and a Professional Member of IEEE, a Professional member of Nigeria Computer Society (NCS) – The Institute of Research Engineers and Doctors (IRED), a Professional member of the Cyber Security Expert Association of Nigeria (CSEAN), and a Certified Register Engineer with Council for Regulation of Engineering in Nigeria. Prof Olayemi Mikail Olaniyi is a progressive academic professional demonstrating consistent success in research, professional impact, national and global recognition as well as community development. He was the coach of the Bronze, Silver and Gold Medallist of the National International Collegiate Programming Contest/American Computer Machinery (ICPC/ACM) for the years 2009, 2010, and 2011 respectively.

James G. Ambafi, Obtained BEng in Electrical and Electronics Engineering from the Federal University of Technology Yola, Nigeria, an MEng degree in Electrical Power and Machines from the Federal University of Technology Minna, Nigeria, and a Ph.D. degree in Electrical Engineering at Bayero University, Kano, Nigeria. He is currently a Senior Lecturer in the Department of Electrical & Electronics Engineering at the Federal University of Technology, Minna. Nigeria. His research interests include; power system stability and control, hybrid renewable energy systems, computational intelligence. He can be contacted at email: ambafi@futminna.edu.ng.

Vincent B. Sheidu is a graduate of Electrical and Electronics Engineering at the Federal University of Technology, Minna. He has a keen interest in technology and innovation, and is dedicated to using his skills and knowledge to make a positive impact on the world. His research interest includes computational intelligence, Cognitive Radio, Wireless Sensor Networks, MIMO, mmWave, and 6G application areas.

Muhammad M. Ibrahim is a graduate of Electrical Engineering from the Federal University of Technology, Minna and a writer known for his work in Electronic voting system on blockchain technology. Born and raised in Bida. His research interest includes computational intelligence, Cognitive Radio, Wireless Sensor Networks, MIMO, mmWave, and 6G application areas.

Authors and Affiliations

Henry O. Ohize[1,2] · Adeiza James Onumanyi[3] · Buhari U. Umar[4] · Lukman A. Ajao[4] · Rabiu O. Isah[4] · Eustace M. Dogo[4] · Bello K. Nuhu[4] · Olayemi M. Olaniyi[5] · James G. Ambafi[1] · Vincent B. Sheidu[1] · Muhammad M. Ibrahim[1]

✉ Adeiza James Onumanyi
aonumanyi@csir.co.za

Henry O. Ohize
henryohize@futminna.edu.ng; ohizeho@custech.edu.ng

Buhari U. Umar
buhariumar@futminna.edu.ng

Lukman A. Ajao
ajao.wale@futminna.edu.ng

Rabiu O. Isah
isah.rabiu@futminna.edu.ng

Eustace M. Dogo
eustace.dogo@futminna.edu.ng

Bello K. Nuhu
nuhubk@futminna.edu.ng

Olayemi M. Olaniyi
omolaniyi@noun.edu.ng

James G. Ambafi
ambafi@futminna.edu.ng

Vincent B. Sheidu
vincentsheidu@gmail.com

Muhammad M. Ibrahim
mktmakantamkt@gmail.com

[1] Department of Electrical and Electronics Engineering, Federal University of Technology, Gidan Kwano, PMB 65, Minna, Niger, Nigeria

[2] Department of Electrical and Electronics Engineering, Confluence University of Science and Technology, PMB 1040, Osara, Kogi, Nigeria

[3] Next Generation Enterprises and Institutions, Council for Scientific and Industrial Research (CSIR), Meiring Naude, Pretoria 0001, Gauteng, South Africa

[4] Department of Computer Engineering, Federal University of Technology, Gidan Kwano, PMB 65, Minna, Niger, Nigeria

[5] Department of Computer Science, National Open University of Nigeria, 900108 Abuja, Nigeria