

Democratic Innovation: Systematic Evaluation of Blockchain-Based Electronic Voting (2022–2025)

Oscar Revelo Sánchez , Alexander Barón Salazar and Manuel Bolaños González 

Galeras.NET Research Group, Universidad de Nariño, San Juan de Pasto 52001, Colombia;
abaron_98@udenar.edu.co (A.B.S.); mbolanos@udenar.edu.co (M.B.G.)

* Correspondence: orevelo@udenar.edu.co

Abstract

This systematic review examines recent advances in blockchain-based electronic voting systems, motivated by the need for more transparent, secure, and verifiable electoral processes. The rapid growth of research between 2022 and 2025 highlights blockchain as a promising foundation for addressing long-standing challenges of integrity, anonymity, and trust in digital elections, particularly in academic contexts where pilot deployments are more feasible. The review followed PRISMA 2020 guidelines and applied the evidence-based methodology proposed by Kitchenham & Charters. Searches were conducted in six major databases, yielding 861 records; after removing duplicates and applying eligibility criteria, 338 studies were retained. Data were extracted using a structured template and synthesised qualitatively due to the conceptual and methodological heterogeneity of the evidence. The included studies reveal significant progress in blockchain architectures, smart contracts, and advanced cryptographic mechanisms—such as blind signatures, zero-knowledge proofs, and homomorphic encryption. Multiple authentication and verification strategies were identified; however, real-world validations remain limited and largely confined to small-scale academic pilots. Overall, blockchain-based voting systems demonstrate conceptual advantages over traditional and conventional electronic models, especially regarding transparency and auditability. Nevertheless, the field requires stronger empirical evaluation, greater scalability, and clearer regulatory alignment to support broader institutional adoption.

Keywords: blockchain; electronic voting; systematic literature review



Academic Editors: Arash Habibi Lashkari, Aref Meddeb and Bacem Mbarek

Received: 22 November 2025

Revised: 19 December 2025

Accepted: 22 December 2025

Published: 2 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

In recent decades, technological advances have driven significant changes in electoral processes, particularly through the adoption of electronic voting systems. These systems seek to improve the efficiency, speed, and accessibility of voting and vote counting, offering a modern alternative to traditional methods based on physical ballots. However, their implementation presents crucial challenges in terms of security, transparency, privacy, and trust, aspects that are fundamental to legitimacy and social acceptance of election results [1,2].

In this context, blockchain technology emerges as a promising solution to address these issues, thanks to its inherent properties of decentralisation, immutability, and public traceability. Blockchain enables the construction of robust electoral systems in which votes can be recorded, stored, and audited transparently and securely, thereby mitigating historical risks such as manipulation, double voting, and fraud [3,4]. The use of smart contracts and advanced cryptographic techniques also enhances automation and confidentiality, balancing voter authenticity with the preservation of necessary anonymity [5,6].

Although the technical benefits of blockchain-based voting have been widely discussed, a significant gap remains between technological development and its effective application in real-world scenarios, particularly in organisations and contexts with complex regulatory and social requirements [7]. Furthermore, the consolidation of this technology depends not only on advances in security and scalability, but also on institutional and public trust, which implies transparency not only in terms of technology but also in terms of communication and education [8,9].

This study presents a systematic review of recent scientific literature from 2022 to 2025, focusing on blockchain-based electronic voting systems with a special emphasis on applications in academic contexts. Different technical approaches, authentication methods, audit mechanisms, and empirical validation experiences are analysed to identify current trends, persistent challenges, and opportunities for future research. The review is based on a rigorous methodological protocol that ensures comprehensiveness, reproducibility, and critical integrative analysis [10,11], reported in accordance with the PRISMA Statement [12]. Against this background, this review is guided by the central question of how far blockchain-based electronic voting systems have progressed from conceptual and technical proposals toward empirically validated and institutionally viable solutions. This work contributes to clarifying the contemporary landscape of blockchain solutions for electronic voting systems, supporting informed decisions in the design of more reliable, transparent, and democratic electoral systems in the digital age.

The paper is organised as follows: Section 2 presents a brief foundation for blockchain-based electronic voting systems; Section 3 describes the related work; Section 4 presents the review method; Section 5 describes the results of the review, answering the research questions; Section 6 discusses the implications of the results for research and practice, and the limitations of this review; finally, Section 7 presents the conclusions and some ideas for future work.

2. Theoretical Foundations

This section establishes the fundamental concepts and definitions necessary to understand the scope and characteristics of blockchain-based electronic voting systems, with the aim of providing a solid conceptual framework for the critical analysis and synthesis of the reviewed literature.

2.1. Electronic Voting and Voting Systems

Electronic voting refers to the use of digital technologies for casting, recording and counting votes in electoral processes. Electronic voting systems seek to improve the efficiency, speed, and accessibility of election management, but they have historically faced critical challenges in terms of security, transparency, privacy, and reliability of the process [2]. Traditional systems, based on manual voting with physical ballots, have vulnerabilities such as direct manipulation, human error, and lack of verifiable traceability.

Conventional electronic systems, which use proprietary software and centralised databases, can offer improvements in speed and automation, although they are exposed to risks related to data integrity, centralisation of control, and difficulties in ensuring anonymity and public auditing [1].

2.2. Blockchain and DLT Technology

Blockchain is a DLT that allows data to be stored in a decentralised, immutable and transparent manner [3]. Each block contains a set of transactions or records, cryptographically linked by hashes to previous blocks, creating a secure structure that is resistant to unauthorised modifications.

The essential properties of blockchain include:

- **Decentralisation:** Information is replicated and validated by a network of distributed nodes, eliminating single points of failure or centralised control.
- **Immutability:** Stored records cannot be modified without cryptographic evidence and joint consensus from the network.
- **Transparency:** Transactions are recorded publicly or semi-publicly, allowing participants to audit the entire history.

These characteristics position blockchain as an ideal platform for solving traditional challenges in voting systems, where manipulation, opacity, and lack of trust are recurring concerns [4].

2.3. Blockchain-Based Voting Systems

Blockchain-based voting systems integrate the properties described above to offer enhanced guarantees of security, transparency, and verifiability in electoral processes. They generally use:

- **Smart contracts:** Automatic programmes deployed on the chain that regulate the issuance, counting, and validation of votes without human intervention, increasing reliability and reducing errors or fraud [13].
- **Advanced cryptographic mechanisms:** These include digital signatures, blind signatures, ZKPs, and homomorphic encryption to protect voter identity and vote confidentiality, ensuring anonymity and auditability simultaneously [5,6].
- **Types of blockchain networks:** These can be public (open to any participant, such as Ethereum or Solana), private (controlled by an entity, such as Hyperledger Fabric), or consortium (shared among a limited group of organisations). The selection impacts the scalability, governance and level of transparency of the electoral system [14].

2.4. Transparency, Security, and Trust in Voting Systems

Blockchain-based systems increase transparency by allowing public auditing and independent scrutiny of each recorded vote, mitigating the need to trust central authorities [8]. In terms of security, they resist manipulation through cryptographic techniques and decentralised consensus that protects the integrity of the vote and prevents attacks and fraud [15].

Voter confidence is strengthened by mechanisms that ensure end-to-end immutability and verifiability: from authentication and issuance to final counting and publication of results [16]. However, the literature indicates that technical transparency must be accompanied by literacy and communication efforts to achieve effective social acceptance [9].

A crucial aspect in the design of electronic voting systems is the balance between robust verification of voter identity and preservation of voting anonymity [17]. The use of biometrics, decentralised digital identities (DIDs), and cryptographic techniques ensures that only authorised users can vote, without their vote being traceable back to their identity [18].

2.5. Verification and Auditing

Blockchain-based systems employ methods to facilitate verification and auditing, such as smart contracts for automatic validation, accessible immutable records, and cryptographic proofs that allow voters and external observers to verify the integrity of the process without compromising individual privacy [1,19].

3. Related Work

Recent literature on blockchain-based electronic voting systems shows that, during the period from 2022 to May 2025 and in the bibliographic databases consulted, only two formal systematic reviews dedicated to the topic have been identified. Both present valuable contributions, although with methodological and scope limitations that justify the need for complementary and more exhaustive studies.

The first, ‘Blockchain Electoral Vote Counting: Comparative Analysis of Methods, Constraints, and Approaches’ [4], focuses on evaluating existing solutions for blockchain-based vote counting. Its main objective is to comparatively analyse the methodologies used, the technical and operational constraints present, and the different approaches implemented from 2015 to 2022. The methodology adopted is systematic, following protocols like PRISMA to ensure rigour in the search, selection, and evaluation of studies, assessing their quality using quantified criteria and limiting the review to studies with acceptable scores. Although it provides a solid overview of current strengths and limitations, the review is restricted to a time frame prior to the current explosion in research and lacks comprehensive coverage of aspects such as validation in real-world scenarios and detailed technical integration. Furthermore, the inclusion of articles beyond 2022 could limit the perspective on recent advances.

The second corresponds to ‘Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges’ [7], which comprehensively analyses the architectures adopted, emerging technological trends, technical and regulatory challenges, and proposed solutions in the field of secure electronic voting using blockchain. Its scope covers a broader and more up-to-date set of research and highlights the importance of advanced cryptographic protocols, privacy, and scalability, as well as the incorporation of complementary technologies such as IoT and AI. It uses a systematic methodology with consolidated academic databases and rigorous review protocol monitoring. However, although detailed and recent, the review is partial in terms of practical verification and field demonstration of many systems, and some regulatory or socio-technical aspects are not explored in the same depth, leaving room for a more comprehensive analysis.

Both contributions differ from the present study in that they do not comprehensively cover the most recent academic period (2022–2025), nor do they implement a review protocol that combines thoroughness, in-depth critical evaluation, and transparent methodological traceability. Furthermore, they lack a systematic integration of technical, practical, legal, and social aspects into a single analysis. There is little attention to empirical validation in real environments, analysis of implementation in specific contexts such as academic ones, and the combination of advanced authentication and verification techniques in blockchain.

On the other hand, there is also a growing body of survey-type or exploratory studies in the literature which, although useful for presenting general overviews of blockchain and electronic voting, do not meet the methodological standards of a rigorous systematic review. Some of these studies focus on aspects such as specific blockchain platforms (Ethereum, Hyperledger), cryptographic mechanisms, mobile voting and remote access, auditing and traceability, or integration with IoT and AI technologies. However, they often have recurring limitations in terms of the absence of an explicit search protocol, lack of detailed inclusion and exclusion criteria, lack of evaluation of the quality of the studies included, and no or limited methodological transparency.

In this context, the review proposed here provides original and necessary value by comprehensively covering the most recent academic period (until May 2025), articulating a clear and reproducible protocol, emphasising critical and systematic evaluation of the quality of studies, and integrating technical, institutional, legal and social perspectives. This innovative approach aims to consolidate the state of the art in blockchain-based electronic voting systems, identifying gaps, trends and future lines of research, while strengthening the comparison between solutions and real-world application contexts.

Although there are previous systematic reviews and a variety of exploratory studies on blockchain and electronic voting, this study is positioned as a methodologically sound, comprehensive, and up-to-date contribution that responds to the urgent need to map and critically evaluate this area of research to promote its safe and responsible adoption.

4. Method

To develop this systematic literature review, an adaptation of the evidence-based research approach from the field of software engineering was used [10]. This approach has been widely used by the scientific community because it allows knowledge to be created from evidence published in primary studies. The stages of the method defined for this review are described below and outlined in Figure 1.

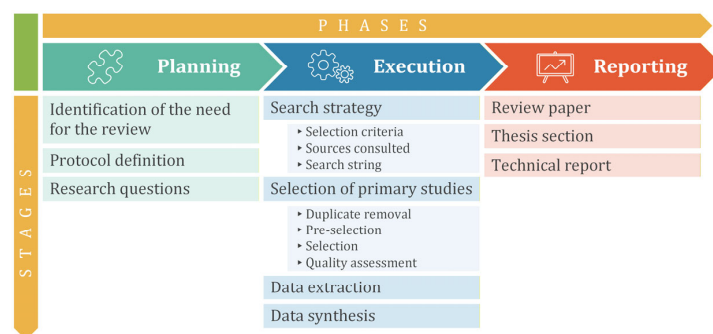


Figure 1. Diagram of the review method used. Adapted from Kitchenham & Charters [10].

4.1. Research Questions

The objective of this literature review was to analyse and systematise the existing evidence on the proposals, technical characteristics, authentication mechanisms, validation and implementation experiences of blockchain-based electronic voting systems, with an emphasis on their application in academic contexts, and to compare them with traditional and electronic solutions in terms of transparency, security and trust. In searching for related primary studies, the following research questions were defined under the PICO framework to guide data extraction, analysis, synthesis, and presentation of results (see Table 1):

Table 1. Research questions.

RQ1: How do blockchain-based electronic voting systems compare to traditional and electronic systems in terms of transparency, security, and trust?			
P: Electoral processes	I: Blockchain-based voting systems	C: Traditional and electronic systems	O: Transparency, security, trust
Introduce the topic by evaluating the benefits and weaknesses of blockchain compared to other technologies in key aspects of trust.			
RQ2: What proposals for blockchain-based electronic voting systems have been developed and applied in academic or university contexts, and which ones have shown the best results?			
P: Educational institutions	I: Blockchain systems applied to academic voting	C: Not applicable	O: Results obtained, acceptance, feasibility
Focus on real experiences in academic environments, exploring impact and results.			
RQ3: What implementation techniques and types of blockchain networks have been used in electronic voting system proposals, and how do they address the main challenges of security, anonymity, and verification?			
P: Electronic voting systems	I: Types of blockchain networks and techniques implemented (Ethereum, Hyperledger, smart contracts, etc.)	C: Not applicable	O: Solutions to technical challenges
Explores both technological decisions (network type) and methods implemented to address critical aspects of security, privacy, and verifiability.			
RQ4: What voter authentication methods have been used in blockchain-based electronic voting solutions, and how do they balance identity and anonymity?			
P: Voters in blockchain systems	I: Authentication methods (biometrics, DID, tokens)	C: Classic authentication or no anonymity	O: Balance between identity and privacy
Examine identification technologies and how anonymity is preserved without losing legitimacy.			
RQ5: What verification and audit methods have been applied to ensure the integrity and reliability of blockchain-based electronic voting systems?			
P: Blockchain voting solutions	I: Verification and auditing (ZKP, cryptographic proofs)	C: Not applicable	O: Verifiable integrity and trust
Review transparency mechanisms to ensure that votes can be reliably audited.			
RQ6: How effective have real-world scenario tests been in validating scalable blockchain-based electronic voting systems?			
P: Actual proposals for blockchain voting systems	I: Testing in real contexts	C: Simulations or controlled environments	O: Level of validation and applicability
Conclude the analysis by observing the degree of maturity and effectiveness of solutions tested in real conditions.			

4.2. Selection Criteria

The following inclusion (I) and exclusion (E) criteria were defined for adding or removing studies from the analysis, some of which were applied directly as filters in the corresponding databases:

- I1: Studies published between 2022 and 2025.
- I2: Studies published in journals, book chapters, or conference proceedings.
- I3: Studies that are directly related to or contribute to the understanding of blockchain-based electronic voting systems.
- E1: Studies in languages other than English or Spanish.
- E2: Studies presenting literature reviews related to blockchain-based electronic voting systems.
- E3: Studies without access to the full text.
- E4: Studies presented as proposals, without results, or incomplete studies.

4.3. Sources Consulted

To ensure comprehensiveness, validity, and replicability in a systematic literature review in the field of computer science, it is essential to use recognised and specialised bibliographic databases. Databases such as IEEE Xplore, ACM Digital Library, Scopus, and Web of Science are considered key pillars due to their comprehensive coverage of scientific literature in this field. These sources offer rigorous indexing criteria, allow the use of advanced Boolean operators, and facilitate the traceability of citations, which are essential aspects for reducing bias and ensuring the methodological quality of the study [10,11].

Additionally, incorporating open access sources such as Google Scholar and DOAJ is essential to accommodate scientific literature published in emerging journals, theses, technical reports, and conferences that, while not always indexed in traditional databases, can provide relevant and innovative perspectives. Google Scholar, due to its integrative nature and cross-cutting coverage, allows for the retrieval of grey literature and content from academic institutions that complement the research landscape [20]. DOAJ offers curated and free access to peer-reviewed scientific journals, ensuring editorial quality within the open access ecosystem [21]. The inclusion of these types of sources contributes to a more inclusive and transparent review that is aligned with the principles of open science.

4.4. Search String

A search string composed of keywords was defined to locate potentially relevant documents using the search functions available in the selected sources. This string was refined by including synonyms, alternative spellings of terms, and other keywords identified in the bibliographic records (see Table 2). The search string was constructed from prototype expressions and Boolean operators that were initially tested in Scopus, as it is the database with the widest coverage and the best search capabilities. These actions were performed iteratively, resulting in the string shown in Table 2.

Table 2. Key terms, related terms, and search string.

Key Terms	Related Terms
e-voting	i-voting electronic voting internet voting online voting digital voting
Blockchain	distributed ledger DLT

Table 2. Cont.

Key Terms	Related Terms
voting system	voting protocol secure voting election system blockchain voting
("e-voting" OR "i-voting" OR "electronic voting" OR "internet voting" OR "online voting" OR "digital voting") AND (blockchain OR "distributed ledger" OR DLT) AND ("voting system" OR "voting protocol" OR "secure voting" OR "election system" OR "blockchain voting").	

The search engines for each database use different mechanisms and standards. They were configured according to each of these particularities, as shown in Table 3, to search titles, abstracts, and keywords, thus obtaining an initial set of primary studies. The different specific filters applied in one of them are also shown.

Table 3. Database search configuration.

Database	Search String	Applied Filters
ACM	("e-voting" OR "i-voting" OR "electronic voting" OR "internet voting" OR "online voting" OR "digital voting") AND (blockchain OR "distributed ledger" OR DLT) AND ("voting system" OR "voting protocol" OR "secure voting" OR "election system" OR "blockchain voting")	• Publication Date: [2022–2025] • Content Type: Research Article
DOAJ	Articles: ('e-voting' OR 'i-voting' OR 'electronic voting' OR 'internet voting' OR 'online voting' OR 'digital voting') AND (blockchain OR 'distributed ledger' OR DLT) AND ('voting system' OR 'voting protocol' OR 'secure voting' OR 'election system' OR 'blockchain voting')	
IEEE	("e-voting" OR "i-voting" OR "electronic voting" OR "internet voting" OR "online voting" OR "digital voting") AND (blockchain OR "distributed ledger" OR DLT) AND ("voting system" OR "voting protocol" OR "secure voting" OR "election system" OR "blockchain voting")	Year: [2022–2025]
Google Scholar	TITLE_ABS_KEY(("e-voting" OR "i-voting" OR "electronic voting" OR "internet voting" OR "online voting" OR "digital voting") AND (blockchain OR "distributed ledger" OR DLT) AND ("voting system" OR "voting protocol" OR "secure voting" OR "election system" OR "blockchain voting"))	Custom range: [2022–2025]
Scopus	Article title, Abstract, Keywords: ("e-voting" OR "i-voting" OR "electronic voting" OR "internet voting" OR "online voting" OR "digital voting") AND (blockchain OR "distributed ledger" OR DLT) AND ("voting system" OR "voting protocol" OR "secure voting" OR "election system" OR "blockchain voting")	• Year: [2022–2025] • Document type: Conference Paper, Article, Book Chapter • Language: English, Spanish
WOS	Topic: ("e-voting" OR "i-voting" OR "electronic voting" OR "internet voting" OR "online voting" OR "digital voting") AND (blockchain OR "distributed ledger" OR DLT) AND ("voting system" OR "voting protocol" OR "secure voting" OR "election system" OR "blockchain voting")	• Publication Years: [2022–2025] • Document Types: Article, Early Access • Languages: English

4.5. Selection of Studies

The selection of relevant documents was carried out in three steps: elimination of duplicates, preselection, and selection, as established in the guidelines for systematic reviews by Kitchenham and Charters [10]. To eliminate duplicates, the preliminary results of the search procedure were sorted by number of documents in each source, looking for duplicate records from the sources with the fewest documents to those with the most. In the preselection step, the documents resulting from the previous step were analysed by reviewing the title and abstract, excluding documents that were clearly not relevant to the research questions. The guidelines recommend that preselection should be cautious, i.e., if the researcher has doubts about a study, it should be included. This recommendation was

followed in this step to avoid discarding potentially relevant documents. In the selection step, the set of documents resulting from the preselection step was read in full, applying the quality criteria described in Section 4.6, to obtain the final set of documents. Both in the preselection and selection steps, the inclusion and exclusion criteria described in Section 4.2 were applied. Figure 2 summarises this process.

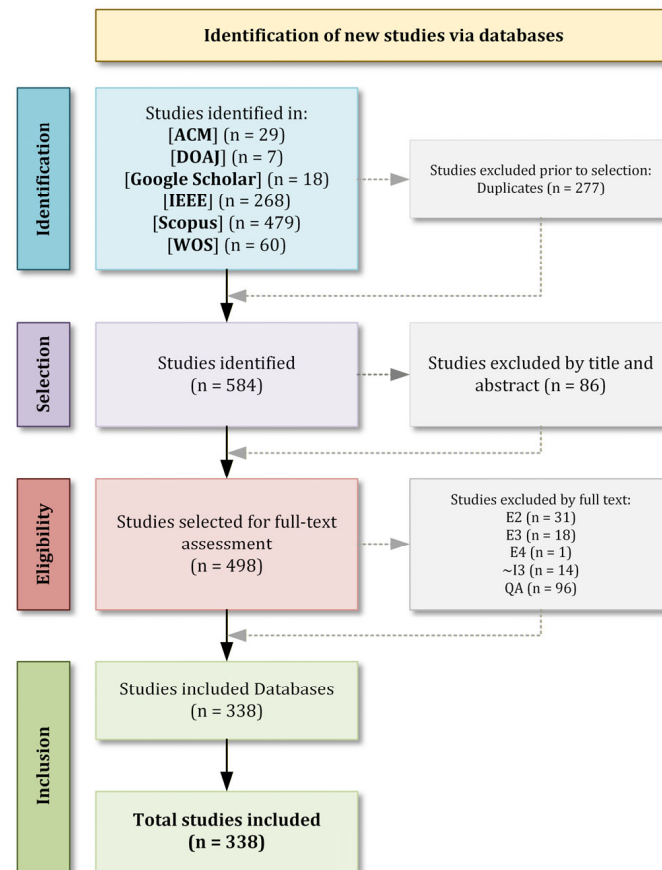


Figure 2. PRISMA flow of the document search and selection process.

4.6. Quality Assessment

To assess the methodological quality of studies related to technological developments, especially those that propose, design, or evaluate systems, such as blockchain-based electronic voting systems in this case, this review used an adapted version of the checklist by Kitchenham and Charters [10], combined with quality criteria for empirical software engineering studies proposed by Dyba et al. [22]. These have been used extensively in systematic technology reviews. Table 4 presents the corresponding rubric.

The ten quality assessment criteria were selected to reflect the technological and methodological diversity of blockchain-based electronic voting studies. Given that the included works range from conceptual models and architectural proposals to prototype implementations and pilot evaluations, the criteria prioritise aspects such as clarity of objectives, methodological transparency, technical consistency, validation strategy, and reproducibility. These dimensions allow for a consistent assessment across studies that lack standardised experimental designs or comparable quantitative outcomes. Other quality assessment frameworks were considered; however, many include criteria specific to clinical, statistical, or intervention-based studies, which are not applicable to the majority of the evidence analysed in this review.

Table 4. Quality assessment rubric used.

No.	Criterion	Question	Type of Response	Score
1	Clear Objectives	Are the objectives or purposes of the study clearly defined?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
2	Study Context	Does it clearly describe the context or environment of the proposed or evaluated system?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
3	Method Justification	Does it justify why the specific architecture, technology, or technique was chosen?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
4	Detailed Technical Design	Does it present a clear and reproducible description of the proposed system (architecture, algorithms, tools)?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
5	Implementation	Has the system been implemented, or is it only a theoretical proposal?	Implemented/Partial/Theoretical only	Implemented = 2 Partial = 1 Only theoretical = 0
6	Empirical Evaluation	Does the study include tests, experiments, or simulations with clear metrics?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
7	Analysis of Results	Is the performance of the system presented and analysed quantitatively?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
8	External Validity	Does the study mention the possibility of applying the system in real contexts or different environments?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
9	Limitations	Does it clearly report on the limitations of the approach or study?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0
10	Contribution	Does the study contribute anything new to the state of the art in blockchain/e-voting technology?	Yes/Partially/No	Yes = 2 Partially = 1 No = 0

4.7. Data Extraction

Table 5 shows the data extracted from all selected documents. The process was supported by an extraction form implemented in Microsoft Excel™. Appendix A (Table A1) presents a sample extraction form for one paper.

Table 5. Data extracted from the studies.

Data	Description
Source	Bibliographic source of the document
Title	Title of the document
Year	Year of publication of the document
Type of publication	Paper, conference paper or book chapter
Authors	Names of all authors
Country *	Country of affiliation of the authors
RQ1-RQ6	How the document addresses each of the RQs

* For the country, an additional extraction form is used for each of the sources consulted (see Table 6).

Table 6. Data extracted from studies by source consulted (countries).

Data	Description
Title	Title of the document
Country	Country of affiliation of the authors
Contribution	Proportion of authors' contribution, Serenko et al. [23]

4.8. Data Synthesis

Data synthesis was carried out using a mixed approach, combining quantitative and qualitative techniques to ensure a comprehensive and in-depth characterisation of the evidence extracted.

The procedure began by consolidating all relevant information from the selected primary studies using a structured data extraction form implemented in Microsoft Excel™ (see Section 4.7). This instrument gathered key variables such as the bibliographic source, title, year of publication, authors, country of affiliation of the authors, and the explicit relationship of each document to the research questions (RQ1–RQ6). The use of Excel allowed for tabular organisation and systematic management of the data, as well as flexible exporting of the data to other formats for analysis.

For coding and categorisation, previously defined explicit criteria were used: studies were grouped by year and country of institutional affiliation, type of blockchain network used (public, private, consortium), authentication method (biometric, cryptographic, multi-factor, etc.), validation modality (simulation, laboratory, pilot in real environment) and other relevant technical aspects. Likewise, the texts extracted related to each research question were coded thematically, ensuring explicit alignment with the study objectives. The coding was reviewed iteratively to ensure completeness and avoid ambiguities and validated through triangulation among the researchers responsible for the analysis.

To facilitate the interpretation and comparison of patterns, bar charts, radial charts, and temporal and geographical distribution diagrams were used. These visualisations made it possible to identify trends, dispersion, and significant clusters, as well as facilitating comparative discussion between different technological approaches and application contexts. Extraction matrices facilitated the traceability of each piece of data with respect to the source study and its association with the research questions, reinforcing the validity of the analysis.

During the synthesis process, detailed records were kept linking each coded piece of data to the corresponding research question, ensuring analytical consistency and the possibility of auditing each inference made. The successive stages of grouping and synthesis were guided by both theoretical frameworks and pragmatic criteria of comparability between studies, ensuring that the analysis was aligned with the objectives of the review and methodological reproducibility.

5. Results

This section presents the results of the review study along with the answers to the research questions. Information mappings are also provided to link the answers to the individual research questions. These results are divided into two groups. The results presented in Section 5.1 address the descriptive nature of the individual studies, while the results related to the research questions (RQ1–RQ6), Section 5.2, address the conceptual aspects of the studies and the interactions between them. All data processing can be consulted in the file http://www.galeras.net/ors/data_processing_2.xlsx (accessed on 21 October 2025).

5.1. Descriptive Information on Primary Studies

This section summarises descriptive information on the primary studies examined in this systematic literature review. Appendix B presents the complete references for the final set of 338 studies.

5.1.1. Results of the Search and Selection Process

The result obtained using the search string in the six selected databases was a set of 861 bibliographic records of potentially relevant scientific documents published between 2022 and 2025 (May) in journals, book chapters or conference proceedings, in English or Spanish, and related to blockchain-based electronic voting systems.

In each of the databases consulted, the metadata from the records was exported to comma-separated value (CSV) text files. The aim was to consolidate the results from each of the sources in a Microsoft Excel™ workbook and facilitate their processing in the different stages of the implementation phase. In the case of ACM, DOAJ, and Google Scholar, which do not offer this option, it was necessary to use the Zotero bibliographic manager as a bridge to obtain the corresponding text files through BIB files.

The 861 bibliographic records were refined by eliminating duplicates, resulting in 584 records, retaining the record in the source with the highest number of results, in this case Scopus. In the pre-selection stage, applying the inclusion and exclusion criteria, 498 records were obtained. The selection stage involved reading the full text of the 498 documents and applying the inclusion and exclusion criteria, as well as assessing the quality criteria defined in Section 4.6. At this stage, a final set of 338 documents was selected to serve as the primary data sources for the systematic literature review. Figure 2 presents the PRISMA flow of the document search and selection process.

5.1.2. Temporal Distribution of Primary Studies

The temporal distribution of primary studies (see Figure 3) related to blockchain-based electronic voting systems reveals a significant evolution in research interest during the period between 2022 and 2025. In 2022, 80 papers were identified, marking the beginning of a rapidly growing emerging line of research. This interest intensified considerably in 2023, reaching a peak of 123 papers, reflecting a boom in innovative proposals, concept validations and technological developments linked to secure and transparent electronic voting.

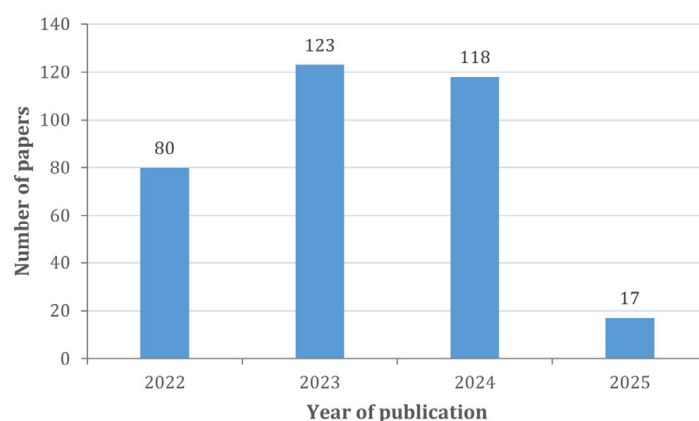


Figure 3. Temporal distribution of primary studies.

In 2024, academic output remained high with 118 papers showing relative stability and thematic maturity. However, the data recorded at the time of this study (May 2025) show a sharp decline, with only 17 papers. Nevertheless, when projecting this trend for the full year, an approximate total of 41 papers is estimated, which still represents a significant decrease of 66% from the peak in 2023.

The 2022–2025 time window is a critical period for understanding the development and maturation of blockchain research for e-voting, making it highly relevant for a systematic review focused on identifying advances, persistent challenges, and future projections in this domain.

Detailed analysis of the temporal distribution of primary studies reveals a significant evolution in how blockchain-based electronic voting systems have been implemented. Throughout the period from 2022 to 2025, there has been a gradual shift from theoretical proposals to technical validations, albeit with low adoption in real-world scenarios (see Figure 4).

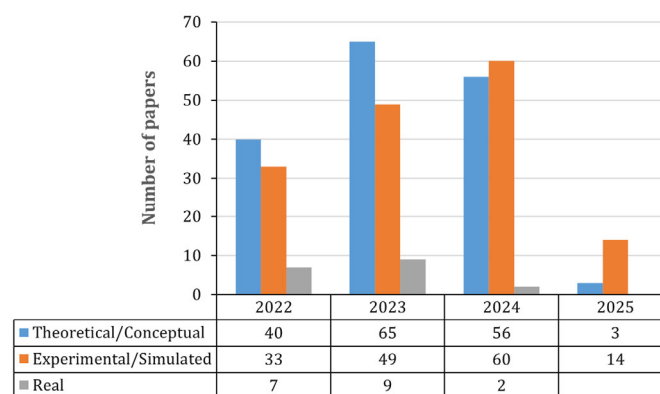


Figure 4. Temporal distribution of implementation types.

During 2022, the landscape was characterised by a relative balance between theoretical (40) and experimental (33) approaches, with seven studies applied in real contexts, demonstrating an initial interest in both conceptualising and technically exploring these solutions.

In 2023, there was the greatest surge in conceptual proposals (65), but also a notable increase in experimental validations (49). However, only nine studies were implemented in real-world settings, suggesting a growing gap between design and practical application.

2024 marked a turning point, with the experimental/simulated approach surpassing the theoretical approach for the first time (60 vs. 56), indicating a shift in the field towards practical evaluation. However, actual application declined sharply to only two studies, highlighting the persistent difficulties in transferring developments to real-world settings.

So far in 2025, the trend points to a consolidation of experimental studies (14) compared to a low number of theoretical proposals (3). However, no actual implementations have been reported to date, reaffirming the need to overcome structural, regulatory and adoption barriers so that these technologies can be tested in specific scenarios.

Although the field has experienced methodological maturity with a steady increase in experimental validations, adoption in real-world settings remains marginal. This poses a key challenge: transcending the laboratory to the real world, strengthening the trust, infrastructure, and institutional support necessary for blockchain-based electronic voting systems to effectively impact democratic processes.

5.1.3. Geographical Distribution of Publications

Another descriptive aspect identified was the geographical location of the authors of the studies reviewed, to establish the percentage of documents by country of origin. The percentage of production for each country was calculated based on the affiliation of the authors, following the equivalent credit approach to authorship used by Serenko et al. [23]. Figure 5 shows documents originating mainly from seven different countries.

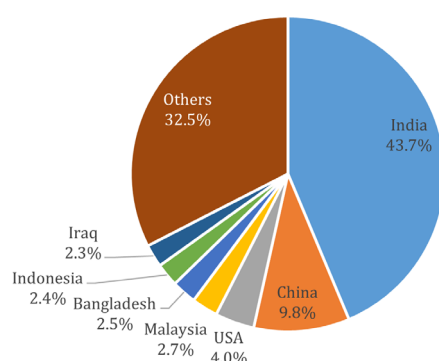


Figure 5. Geographical distribution of publications.

With 43.7% of all studies, India largely dominates academic production in this field. This pre-eminence suggests a high institutional and academic priority towards exploring blockchain-based electoral systems, possibly motivated by the need to strengthen electoral processes in a country with a large population and democracy.

China (9.8%) and the United States (4.0%) rank second and third, respectively. Both countries are recognised for their technological innovation, but in this specific domain, they show significantly lower participation than India. This could be due to alternative approaches to electoral cybersecurity or priorities focused on other emerging technologies.

Countries such as Malaysia (2.7%), Bangladesh (2.5%), Indonesia (2.4%) and Iraq (2.3%) are showing growing interest in using blockchain to solve structural problems in their electoral systems. Although their participation is lower, it reflects an emerging trend in regions undergoing democratic digitalisation.

The fact that one-third of the studies come from countries with less than 2% individual participation indicates that interest in this technology is widespread globally, although it is still not very representative or intensively produced in many regions. This suggests opportunities for more geographically balanced future research.

This distribution reveals considerable geographical asymmetry in the academic development of blockchain-based voting technologies. Although India's leadership is driving the field forward, the underrepresentation of countries with a long tradition of digital voting (such as some European countries) and the incipient presence of Latin America and Africa highlights the need to promote more contextualised and collaborative research at a global level.

An additional aspect that warrants discussion is the strong geographical concentration of research outputs, with a significant proportion of studies originating from a limited number of countries, notably India. While this reflects active research ecosystems and pressing local interest in electronic voting technologies, it may also constrain the generalisability of proposed solutions. Blockchain-based voting systems are inherently shaped by national electoral laws, governance models, digital infrastructure, and socio-cultural attitudes toward technology and trust. Consequently, solutions validated within specific regional or institutional contexts may not be directly transferable to other jurisdictions without substantial adaptation, particularly in countries with different legal frameworks, administrative capacities, or levels of digital literacy.

5.1.4. Distribution of Studies by Type of Publication

Figure 6 shows the distribution of primary studies according to academic source (ACM, IEEE, Scopus, and WOS) and type of publication (paper, conference paper, and book chapter). This analysis reveals important patterns regarding editorial preferences and the most common dissemination channel for this area of research.

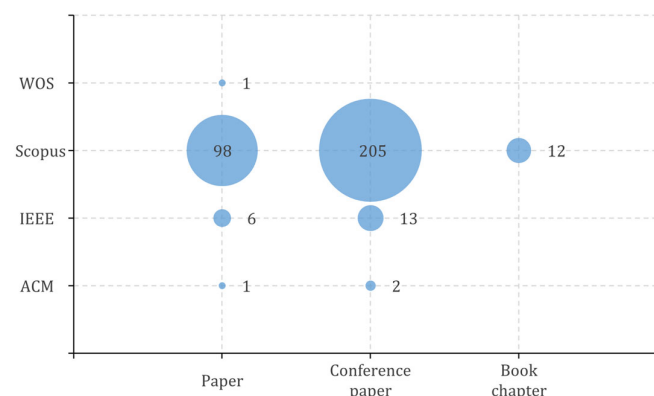


Figure 6. Distribution of studies by type of publication.

The highest concentration is found in conference papers indexed in Scopus, with 205 publications representing the largest core of literature in this field. This shows that much of the knowledge about electronic voting with blockchain is being generated and disseminated at technical or applied scientific events, where developments are more agile and emerging technologies are discussed. Scopus also leads in journal papers (98), consolidating its position as the most representative and diverse source of information for this type of research, covering journals, conferences and book chapters.

IEEE shows modest but significant participation with 6 journal papers and 13 conference papers, which is consistent with its specialised focus on information technology, networking, and cryptography. IEEE may represent a more technical and rigorous source, although less voluminous than Scopus.

WOS and ACM have a minimal presence: only one paper in WOS, and in ACM, one paper and two conferences. This could be due to less indexing of work on electoral blockchain on these platforms, stricter editorial selection criteria, and different approaches to the publication of applied developments.

Twelve book chapters are identified in Scopus, indicating that there are also efforts at theoretical systematisation or thematic compilations that address the topic from a more structured perspective, possibly in educational or regulatory contexts.

The distribution observed shows that scientific output on blockchain-based electronic voting is predominantly technical and rapidly circulating, with conference papers taking precedence over peer-reviewed journal articles. Scopus has established itself as the most diverse and robust source, while IEEE plays a specialised technical role. This overview suggests that researchers should prioritise Scopus as the central source for a comprehensive review, but also consider the technical specificity offered by IEEE or ACM for more advanced developments.

5.2. Answers to the Research Questions

The answers to the research questions were obtained by extracting, synthesising, and combining data from the 338 studies.

RQ1: How do blockchain-based electronic voting systems compare to traditional and electronic systems in terms of transparency, security, and trust?

The studies reviewed agree that blockchain-based electronic voting systems represent a significant advance over traditional and conventional electronic systems, especially in terms of transparency, security, and trust. Most proposals exploit the inherent properties of blockchain technology, such as immutability, node distribution and verifiable public record, to mitigate historical risks associated with vote manipulation, centralisation of power and lack of traceability.

One of the most recurrent contributions is the guarantee of electoral transparency without compromising the secrecy of the vote. For example, the study by Hamidey and Heng [8] states that their decentralised proposal allows any voter to verify the recording of their vote without revealing its content, thus eliminating the need to trust central authorities. Along the same lines, Spadafora et al. [16] introduce coercion-resistant mechanisms that improve voter confidence, even in contexts of external pressure.

In terms of security, multiple systems integrate advanced cryptographic techniques (e.g., blind signatures and zero-knowledge proofs) to protect the integrity and confidentiality of votes. The study by Chen et al. [5] highlights the use of homomorphic cryptography and computationally verifiable anonymity mechanisms, which allow votes to be counted securely without compromising the identity of voters.

The explicit comparison with traditional or previous electronic systems is addressed in greater depth in studies such as that by Huang et al. [1], which argues that combining

blockchain with self-tallying mechanisms eliminates potential fraudulent intermediaries while improving the efficiency and credibility of the electoral process.

However, some studies acknowledge that these theoretical improvements still require more robust empirical validation, especially in real-world contexts with high participation and sophisticated threats [24–26].

To compare the capabilities of traditional voting systems, conventional electronic systems, and blockchain-based systems, a radar chart has been constructed (see Figure 7) that summarises their relative performance in five fundamental criteria: transparency, security, trust, anonymity, and verifiability. This representation is derived from a critical synthesis of primary studies and allows us to intuitively highlight the advantages offered by blockchain technology over previous models. The values assigned to each system in each criterion reflect the most recurrent and robust findings identified in the reviewed literature.

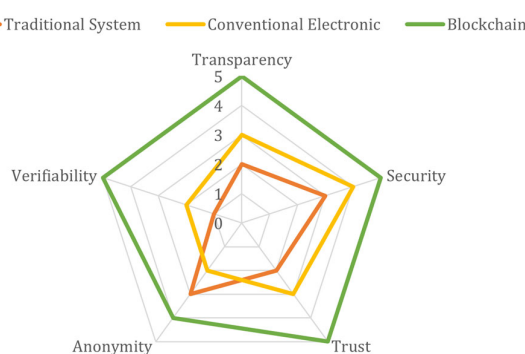


Figure 7. Comparison of voting systems according to key criteria.

Table 7 below references some studies for each of the criteria analysed:

Table 7. Studies relevant to the key criteria.

Criterion	Studios	Justification
Transparency	[2,27,28]	Highlights include the public record of votes, decentralisation as a mechanism for transparency, and verifiable self-counting.
Security	[15,29,30]	They integrate advanced cryptography such as Zk-SNARKs, secure data structures, and validation mechanisms that are resilient to attacks.
Trust	[31–33]	They analyse how decentralisation, Byzantine fault tolerance, and redundant backup mechanisms strengthen voter confidence.
Anonymity	[5,34,35]	They present distributed anonymity techniques, separation of identity and vote, and concealment cryptography to ensure voter privacy.
Verifiability	[19,36,37]	They promote self-verification schemes, cryptographic threshold tests, and efficiency in the mass verification of election results.

Blockchain-based electronic voting systems are emerging as a solid alternative to the limitations of previous models, thanks to their cryptographic guarantees and distributed structure. However, their widespread adoption still depends on contextual validations and improvements in usability and scalability.

RQ2: What proposals for blockchain-based electronic voting systems have been developed and implemented in academic or university contexts, and which ones have shown the best results?

Findings on the application of blockchain-based electronic voting systems in academic or university settings reveal an emerging, diverse landscape that still faces practical implementation challenges. Although literature is largely dominated by theoretical works and simulations

focused on general or national contexts, concrete progress has been made in recent years, with some studies reporting applied experiences or pilot projects in academic settings.

A small number of studies report pilot applications in academic institutions, although generally without detailed reports on impact or systematic results. A significant example is the study by Pereira et al. [38], which describes the implementation of a decentralised system with real-time results validation and auditing, successfully used in academic elections, highlighting as a contribution the robustness of privacy through advanced cryptography and verifiable end-to-end mechanisms. Similarly, Bhamare et al. [35] emphasise the applicability and acceptance of Ethereum platforms with smart contracts in real university electoral processes, reporting improvements in transparency, speed of counting, and participant confidence.

In terms of technological frameworks, both public blockchains (Ethereum, NEAR Protocol) and permissioned blockchains (Hyperledger Fabric) predominate, adjusted according to institutional requirements for anonymity, traceability, and access control. The work of Marouan et al. [14] reports on its effective application in a Moroccan university, achieving optimal results in terms of efficiency and security compared to traditional manual systems, relying on digital signatures, PoW and PoS consensus, and smart contracts to eliminate manual counting and ensure integrity. Similarly, Torre et al. [39] present a positive validation in student elections, highlighting that the use of OTP and unique cryptographic keys allowed anonymity and auditability to be preserved without storing real identities.

Among the achievements observed, the reduction of manipulation risks, automatic vote auditing, improved processing times, and the possibility of public scrutiny stand out. However, it remains clear that many of the studies with more innovative approaches, for example, the use of zero-knowledge proofs or hybrid mechanisms with biometrics and multi-factor authentication, remain in the conceptual testing phase, without direct empirical evidence on campuses or in real elections [40,41].

It should be noted that there are significant differences: while studies such as those by Adeniyi et al. [17] and Zhang et al. [41] report only limited experimental evidence without real institutional validation, other proposals have reached pilot stages, allowing for the measurement of impact in areas such as usability, acceptance, and fraud reduction, as is the case with the studies by Bhamare et al. [35] and Duran et al. [42].

Table 8 lists some of the most relevant studies developed and applied in real academic contexts.

Table 8. Relevant studies conducted in real academic contexts.

Study	Type of Publication	Authors
Blockchain for the electronic voting system: Case study: Student representative vote in Tunisian institute	Conference paper	[43]
Blockchain-Based Electronic Voting: A Secure and Transparent Solution	Paper	[38]
Blockchain-Based Electronic Voting: Case of Student Council Polls	Conference paper	[44]
Blockchain-based e-voting system in a university	Paper	[14]
EASY E-VOTE: An Ethereum-based Voting System using IPFS and MetaMask for Student Government Election	Conference paper	[42]
PUPVOTE: Blockchain-Based Voting System Using NEAR Protocol	Conference paper	[39]
Revolutionizing College Elections with a Secure Blockchain Voting Solution	Conference paper	[35]

Although the field shows robust technical development, implementation in educational contexts remains more of a promise than a reality. The experiences reported are isolated and lack systematic validation. Future research should focus on real-world de-

ploysments, integrating organisational, regulatory, and cultural factors that condition the adoption of these technologies in academia.

RQ3: What implementation techniques and types of blockchain networks have been used in electronic voting system proposals, and how do they address the main challenges of security, anonymity, and verification?

Recent literature on blockchain-based electronic voting systems reveals a rapidly evolving ecosystem characterised by a diversity of technical approaches to addressing classic challenges: security, anonymity, and verification. The primary studies analysed agree on the use of public blockchains (such as Ethereum and Solana), private blockchains (Hyperledger Fabric), or consortium blockchains, selected based on the application context, scale, and governance requirements [3,13,14].

In terms of implementation techniques, the use of smart contracts is practically universal, enabling the automation of processes such as voter registration, ballot casting and counting, and result validation. Ethereum stands out for its flexibility and broad ecosystem of development tools, although the cost of “gas” and scalability limitations are recurring concerns [25,45]. The integration of advanced cryptographic technologies is central to privacy and integrity. Ring signatures, blind signatures, and zero-knowledge proofs are being adopted, allowing voter anonymity to be balanced with end-to-end verifiability [46,47].

Security is addressed through homomorphic encryption, the use of public/private keys, and the explicit separation between authentication and voting processes, preventing the voter’s identity from being linked to their individual vote. Some systems explore the integration of biometrics (fingerprints, facial recognition) as a strong authentication mechanism, although generally combined with robust encryption to prevent direct correlation between identity and vote [9,48].

In terms of verification, many designs adopt public auditing mechanisms: votes are recorded immutably and transparently on the blockchain, allowing voters and external observers to independently validate results [3,38]. The trend toward self-verification and decentralised counting (self-tallying) is also notable, favoured by the possibilities of smart contracts and advanced cryptography.

Table 9 summarises the key technical and functional aspects that determine the design of these systems and allows for a comparison of how different combinations of components address historical problems with electronic voting (especially the dilemmas of security, anonymity, and verifiability). The modular structure facilitates the selection of the most appropriate architectures and techniques according to the regulatory context, the level of confidence required, and the scale of implementation.

The studies reviewed show conceptual and technical maturation in the field: the combination of blockchain with advanced cryptographic techniques makes it possible to increasingly respond to the challenges of security, anonymity, and verifiability, although challenges remain in scalability, efficiency, and validation in real-world scenarios.

RQ4: What voter authentication methods have been used in blockchain-based electronic voting solutions, and how do they balance identity and anonymity?

The integration of authentication methods into blockchain-based electronic voting systems reveals clear trends aimed at balancing robust identity verification with the preservation of voter anonymity. The recurring approaches identified in the studies reviewed fall mainly into three broad categories: biometrics, advanced cryptographic techniques, and national identity systems.

On the one hand, biometric authentication (fingerprints, facial recognition) is positioned as an effective mechanism for strengthening security and minimising identity fraud, without automatically compromising anonymity. This is achieved using public keys derived from biometrics or asymmetric techniques, which authenticate participation but

protect identity during the registration and voting phases, as exemplified by studies such as those by Adeniyi et al. [17] and D. Kumar & Kumar Dwivedi [49].

Table 9. Technical and functional aspects in the design of e-voting systems.

Aspects	Components/Examples	Relevance and Applications in e-Voting
Types of blockchain networks	- Public (Ethereum, Solana) - Private (Hyperledger Fabric) - Consortium (Ethereum in universities)	They determine governance, transparency, scalability, and external trust. Public networks emphasise openness; private and consortium networks prioritise control and efficiency.
Implementation techniques	- Smart contracts (Solidity, Go) - Cryptographic mechanisms: homomorphic encryption (ElGamal, Paillier), ring signatures, blind signatures, ZKPs/zk-SNARKs - Biometric authentication (facial, fingerprint) - Multi-factor (OTP, public/private keys) - Sharding and sidechains for scalability	They automate electoral processes (registration, voting, counting). They reinforce privacy and auditability. Biometric and multi-factor integration strengthens authentication without sacrificing anonymity. Sharding and sidechains resolve bottlenecks.
Mechanisms for security, anonymity, and verification	- Anonymisation techniques: ring signatures, blind signatures, ZKPs - Decentralised verification: public audit, self-tallying - Immutability and traceability via blockchain, hash, node validation	They guarantee integrity, robust privacy, and end-to-end verifiability. They promote third-party auditing and transparency, reducing the risks of manipulation or voter-vote correlation.

A second relevant group consists of cryptography-based authentication solutions, notably ring signature schemes, blind signatures, ZKPs, and distributed thresholds. These methods make it possible to verify voter eligibility and uniqueness without linking individual identity to the vote cast. For example, in the works of Chen et al. [5] and Sangraula & Adhikari [6], cryptographic authentication is used to ensure that the verification process always remains unlinked to the content of the vote, preserving anonymity and avoiding direct traceability.

Thirdly, the integration of national identities (such as Aadhaar, social security numbers (SSN), or unique tokens generated from government databases) constitutes a robust authentication alternative, especially in models that seek high interoperability and eligibility control. Studies such as that by Jain et al. [50] demonstrate how an acceptable balance can be achieved by associating pseudonymised or encrypted credentials—sometimes combined with one-time passwords (OTPs)—with the authentication process, preventing the tracking of votes or real identities during the counting phase.

Other emerging approaches include multifactorial schemes (biometrics combined with OTP, facial recognition powered by machine learning) and authentication anchored in mobile devices or IoT sensors, which reinforces the robustness of the process without compromising privacy [18,49,51].

Figure 8 visually summarises the frequency with which the different approaches appear in the included primary studies, based on the following main categories of authentication:

- Biometric (fingerprints, facial recognition, finger vein, iris).
- Cryptographic (ring signatures, blind signatures, zero-knowledge proofs, hashes).
- National identity-based (Aadhaar, SSN, government ID cards).
- Multifactorial (combinations of OTP with biometrics, two- or more-step authentication).
- Device/IoT (validations by mobile devices, IoT sensors, QR codes).
- Other/Miscellaneous (methods not covered by the above).

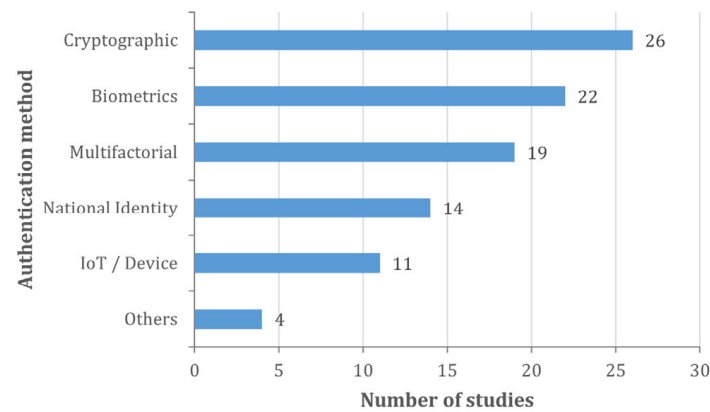


Figure 8. Authentication methods in literature.

It should be noted that not all the 338 studies included in the review explicitly reported authentication mechanisms. Therefore, the analysis presented in Figure 8 considers only the 96 studies that provided sufficient and explicit information regarding user authentication methods, which explains the reduced sample size in this specific result.

The figure shows a clear and hierarchical distribution of the authentication methods used in blockchain-based electronic voting systems, revealing a marked preference for cryptographic techniques (26 studies), followed by biometric (22) and multi-factor (19) approaches. This distribution suggests a trend toward solutions that seek to balance technical security and practical usability. Only 96 studies are included instead of the 338 resulting from the review, as some did not provide sufficient or relevant information for this research question and were excluded from this summary. Furthermore, the subset reflected is a representative sample that illustrates predominant patterns and trends, facilitating interpretation without the noise produced by marginal or incomplete data.

Cryptographic methods lead the way due to their ability to guarantee integrity, anonymity, and non-repudiation in voting processes. The use of blind signatures, zero-knowledge proofs, and hashes has established itself as a robust basis for verifying and protecting identities without compromising voter privacy. This predominance demonstrates the research community's alignment with advanced cybersecurity standards.

Secondly, biometric mechanisms, such as facial recognition or fingerprinting, stand out for their ability to offer non-transferable, highly reliable authentication, especially in contexts with limited access to electronic identity documents. However, their implementation poses ethical and technical challenges associated with the protection of sensitive personal data.

Multifactor schemes—combining OTP, biometrics, and passwords—are emerging as an adaptable response to contexts where a balance between robustness and accessibility is required. The variety of combinations suggests an attempt to strengthen security without compromising the user experience.

For its part, the use of national identity (14 studies) is limited to countries where there are centralised interoperable registries, such as Aadhaar in India. Although they promote inclusion, these systems can raise concerns about surveillance and state dependency.

Device- and IoT-based methods (11) show an emerging exploration of mobile technologies and sensors, suitable for urban contexts and remote voting. However, their reliability depends on the available technological infrastructure.

Finally, the category Others (4 studies) groups together experimental or hybrid proposals that do not yet fit into dominant classifications, reflecting the exploratory nature of some recent approaches.

Overall, the picture reveals an evolving ecosystem, where methodological diversity reflects the search for secure, inclusive solutions adapted to different socio-technical realities. Future adoption will depend on the ability to integrate these technologies while respecting democratic principles, privacy, and transparency.

Although studies are advancing with increasingly integrated solutions—where cryptographic methods allow for the separation of authentication and voting—practical and conceptual challenges remain about total verification without identity leakage. However, the combination of biometrics, advanced cryptography, and national identity management represents the core of current technological progress. The field shows technical maturity and a diversity of alternatives, although the perfect balance between reliable authentication and absolute anonymity remains the great challenge and driver of innovation in blockchain e-voting research.

RQ5: What verification and auditing methods have been applied to ensure the integrity and reliability of blockchain-based electronic voting systems?

Verification and auditing of blockchain-based electronic voting systems is essential to ensuring their integrity and reliability. Critical and combined analysis of the primary studies extracted reveals a remarkable diversity of approaches, although all converge on the need for robust verification mechanisms to counter threats such as vote manipulation and guarantee transparency for participants.

Among the recurring methods, the use of smart contracts as automated tools for auditing and verifying the electoral process stands out. Several proposals use smart contracts on platforms such as Ethereum to independently validate the integrity and immutable record of each vote, ensuring transparency and allowing it to be audited by any node in the network [25,52]. Automation significantly reduces the risk of human intervention and associated errors.

Another relevant avenue is advanced cryptographic mechanisms. For example, the use of ZKPs and homomorphic encryption allows votes to be counted and verified without compromising voter privacy [8,53]. Systems that implement ring signatures and blind signatures also provide public verifiability and resistance to linking votes to identities, thus balancing transparency and anonymity [5].

Universal and individual verifiability is another cross-cutting issue. Several studies enable mechanisms for both voters and third parties to audit the correct inclusion of votes, whether through public hashes, blockchain explorers, or the disclosure of records without revealing sensitive information [42,43]. Similarly, some systems allow for the receipt of cryptographic receipts, which provide voters with certainty that their votes have been recorded without alteration [16].

On the other hand, studies applied in university contexts demonstrate the validity of experimental audits and hybrid systems that combine public and private blockchains, highlighting end-to-end traceability and the value of simulation in strengthening trust before large-scale adoption [3,14].

However, methodological challenges remain, especially regarding the scalability of verification in large-scale elections and robust protection against possible attempts at coercion or vote buying; some studies address these limitations through self-scrutiny protocols [1].

Figure 9 visually summarises the frequency with which the different verification and audit mechanisms or methods appear in the included primary studies, grouped into the following main categories:

- Use of blockchain to ensure integrity and immutability (immutable records).
- Auditing through smart contracts or code.
- Automated public or universal verification (individual or results).

- Use of digital signatures, ZKPs, blind signatures, ring signatures, or similar for authenticity and anonymity.
- Use of verifiable receipt mechanisms or transparency with public traceability.
- External auditing or observer roles to validate integrity.
- Use of combined mechanisms (blockchain + biometrics, OTP, multiple factors).
- Verification and validation using advanced cryptographic techniques (such as homomorphic encryption, zk-SNARKs, etc.).

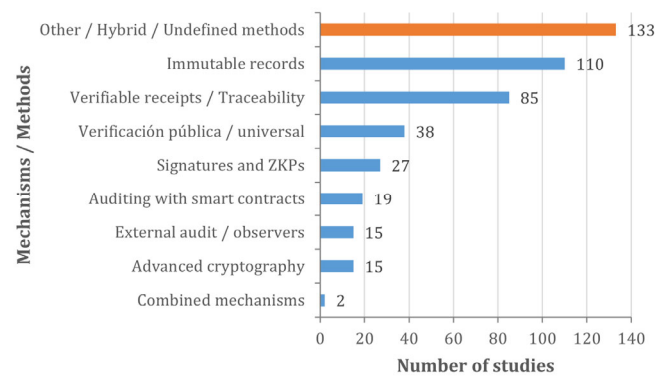


Figure 9. Verification and audit mechanisms/methods in the literature.

The total number of studies in the graph (444) is the sum of mentions by category, not the number of unique studies (338). In other words, some studies appear in more than one category because they report on several verification and audit mechanisms/methods.

The graph provides a structured overview of the verification and auditing mechanisms and methods used in blockchain-based electronic voting systems, highlighting a clear preference for approaches focused on immutability, traceability, and public transparency as fundamental pillars for ensuring trust in electoral processes.

The most frequently represented mechanism is the use of “Other mechanisms” (133 studies), a category that includes specific non-standardised approaches, emerging techniques, or hybrid strategies still in the exploratory phase. Its high frequency indicates the evolving dynamics of the field, in which researchers are testing new forms of verification beyond conventional frameworks. The “Other” category also includes studies in which the mechanism/method is not directly related to the main categories but addresses alternative, insufficiently specified, or secondary techniques (e.g., administrative verifications, internal organisational methods); or, when a study does not mention any explicit mechanism/method.

This is followed by immutable records (110 studies), a native attribute of blockchain technologies, which ensures that recorded votes cannot be modified or deleted without leaving a trace. This technical principle has become the pillar of legitimacy for many proposals, providing a transparent and tamper-proof record.

Verifiable receipts and public traceability systems appear in 85 studies and allow voters to confirm that their vote was counted correctly without compromising anonymity. These mechanisms reinforce public confidence by allowing independent verification without relying on a central authority.

Public or universal verification (38 studies)—automated and accessible—further strengthens transparency by facilitating individual and collective audits of election results, making it a key feature in open democratic environments.

Cryptographic and technical signatures such as ZKPs (Zero-Knowledge Proofs), used in 27 studies, guarantee voter anonymity and authenticity, addressing two essential principles: privacy and security. These tools allow a transaction (vote) to be validated without

revealing sensitive information, consolidating the value of blockchain in contexts of enhanced privacy.

Auditing through smart contracts (19 studies) is a significant innovation, as it enables automatic control and validation processes, reducing dependence on third parties. This automation provides efficiency and avoids potential human bias in electoral monitoring.

To a lesser extent, advanced cryptography mechanisms (15 studies) such as homomorphic encryption or zk-SNARKs are emerging, promising high levels of security but still facing technical challenges in scalability and implementation complexity. The same is true for external auditing or observers (15 studies), which, while providing institutional legitimacy, has been less addressed from a technical perspective.

Finally, combined mechanisms (only 2 studies) reflect limited attempts to integrate multiple approaches (such as blockchain + biometrics + OTP), possibly due to their technical complexity or high infrastructure requirements.

The current body of research reveals a consensus on the capacity of blockchain technology, supported by cryptographic techniques and decentralised verification mechanisms, to strengthen the integrity and auditing of electronic voting systems. However, research highlights the need for sustained empirical validation and solutions that ensure verifiability on a large scale and in real-world scenarios to consolidate social and institutional trust.

RQ6: How effective have real-world scenario tests been in validating scalable blockchain-based electronic voting systems?

The validation of scalable blockchain-based electronic voting systems in real-world scenarios is one of the most critical challenges and issues in recent literature. A synthesis of the primary studies that passed the quality assessment reveals that, although there is consensus on the disruptive potential of blockchain to ensure transparency, immutability, and verifiability of voting, systematic testing of its effectiveness in real environments remains limited and heterogeneous.

Predominantly, studies refer to testing in simulated contexts, pilot tests, or controlled deployments, while applications in large-scale real-world voting scenarios are scarce. For example, some studies did achieve implementations in university or institutional settings, where the systems were subjected to realistic functional conditions, obtaining promising results in terms of integrity and cost reduction compared to traditional processes [35,38]. However, in most proposals, experiments were confined to laboratories or proof-of-concept tests, without facing challenges inherent to complex environments, such as resistance to sustained attacks, population scalability, or large-scale anonymisation management.

A recurring pattern is the emphasis on auditability and automatic verification through smart contracts and immutable records, an aspect validated both in simulations and in small-scale real-world applications [3,54]. In scenarios where actual voting took place, improvements in participant confidence and transparency were observed, albeit with limitations in terms of anonymity and interoperability with conventional electoral processes.

There are notable differences in the scope and robustness of the tests. Some studies, such as those by Al-Maaitah et al. [55] and Pereira et al. [38], report empirical validation using real cases (university or national), showing that the technology is capable of withstanding public scrutiny and independent audits. In contrast, other studies, such as Marouan et al. [14], even when applied in academic settings, are limited to simulations or semi-real tests, recognising that scalability and adaptation to massive national contexts still raise technical and political concerns. A significant contribution lies in those experiences that documented the process of gradual integration of the blockchain system before applying it to real contexts, emphasising the importance of institutional acceptance and digital literacy of participants [42].

The behaviour described in the preceding paragraphs is presented in detail in Section 5.1.2 in Figure 4.

Although progress has been made in validating blockchain-based electronic voting systems in controlled settings and academic contexts, empirical evidence from large-scale real-world testing remains scarce. The field requires coordinated efforts that go beyond simulation and allow for rigorous assessment of the effectiveness, resilience, and social legitimacy of these systems under complex and diverse electoral conditions.

6. Discussion

The discussion of the results obtained in this systematic review provides a critical perspective on the quantitative and qualitative findings on blockchain-based electronic voting systems, highlighting both methodological and technological advances and persistent challenges in recent literature.

The results show a clear evolution from predominantly theoretical approaches during 2022 to a sustained increase in experimental testing and simulations in subsequent years, reflecting a natural process of maturation in the field. However, actual implementation in mass contexts remains marginal, as evidenced by the few studies reporting cases applied in universities or real institutional processes, for example, the works of Pereira et al. [38], Bhamare et al. [35], and Marouan et al. [47]. This phenomenon corresponds to the vast conceptual literature, where most proposals have been validated only in laboratory settings or controlled pilot tests, reiterating the gap between proposal and effective adoption.

Therefore, although experimental progress is remarkable and the literature shows a growing sophistication curve in terms of the integration of cryptographic mechanisms, smart contracts, and biometric technologies, the transition to real-world scenarios is limited by structural and regulatory factors. It is telling that even studies reporting successful empirical validations in university contexts emphasise the need for greater institutional robustness and interoperability to scale these systems safely.

A distinctive feature of the state of the art is the plurality of techniques and architectures employed. The predominance of public blockchains, especially Ethereum, is justified by their openness, robustness, and development ecosystem, although operating costs and scalability constraints represent recurring obstacles. Alternatively, the use of permissioned blockchains such as Hyperledger Fabric is emerging as a viable option for institutions that require greater control and privacy, as is the case in some academic and sectoral experiences [3,38].

The intensive use of smart contracts to automate the electoral process and innovations in auditing and verification mechanisms (smart contracts, cryptographic hashes, self-tallying) demonstrate an effective response to historical limitations in traceability and transparency. Likewise, the introduction of cryptographic techniques such as ring signatures, blind signatures, and zero-knowledge proofs allows for balancing two traditionally antagonistic axes: robust authentication and voter anonymity, thus overcoming one of the historical criticisms of traditional electronic voting solutions [5,6].

At the methodological level, the literature's ability to combine biometric methods (fingerprint, facial), multi-factor authentication, and validation using national tokens (e.g., Aadhaar) is noteworthy, designing solutions that can be adapted to heterogeneous socio-technical environments. However, ethical and technical challenges remain with regard to the protection of personal data and possible state surveillance [9,50].

The analysis reveals that the transparency–verifiability–trust triad continues to be the main conceptual foundation that legitimises the relevance of blockchain for e-voting. The systems reviewed surpass their traditional and electronic predecessors in enabling universal auditability, immutable recording, and automatic traceability of votes, reducing

the scope for manipulation and fraud [8,16]. The use of zero-knowledge proofs and self-tallying techniques strengthens both individual and collective trust in electoral processes, one of the most notable shortcomings in the previous state of the art.

However, studies warn that technical transparency does not always translate into perceived transparency. Cryptographic complexity can create barriers to understanding and social acceptance, particularly among voters unfamiliar with technology. In this regard, future research should complement technical safeguards with digital literacy strategies and transparent explanations of the underlying mechanisms.

Despite progress, gaps and challenges remain before widespread adoption. First, large-scale validation under real electoral conditions is still rare; the risks of sustained attacks, coercion, and scalability issues require more consistent empirical analysis [47,55]. Second, the management of national or institutional identities raises questions about cross-border interoperability, privacy, and government control of processes.

Beyond scalability, the transition from academic pilot projects to national-level electoral deployment faces several translational barriers. These include regulatory and legal constraints, as most electoral systems operate under strict constitutional and statutory requirements; institutional trust and legitimacy concerns involving electoral authorities, political actors, and citizens; interoperability with existing electoral infrastructure; cybersecurity governance and accountability mechanisms; and socio-political acceptance, particularly in environments with high polarisation or low trust in digital systems. Addressing these barriers requires not only technical maturity but also multidisciplinary collaboration among technologists, policymakers, electoral bodies, and civil society.

The review also demonstrates the inadequacy of standardised comparative metrics that allow for weighing performance, robustness, and acceptance among different proposals. The field still favours specific innovation over comparative systematisation, which makes it difficult to extract clearly transferable best practices.

Finally, it highlights the geographical concentration of scientific production, especially in India, and the poor representation of regions with high levels of digital voting development, which suggests the need to promote a collaborative and contextualised agenda to broaden the spectrum of realities and validate the applicability of the proposed solutions.

The patterns identified suggest that the future of secure electronic voting lies in the consolidation of hybrid systems: capable of combining advanced cryptographic guarantees, architectural flexibility, and adaptability to diverse legal and cultural frameworks.

The literature on blockchain-based e-voting shows remarkable technical maturity and consensus on its potential advantages, although effective adoption and large-scale validation remain pending. Progress toward functional and socially acceptable models will depend on the ability of systems to overcome regulatory barriers, bridge usability gaps, and demonstrate, with robust empirical evidence, their superiority in real electoral conditions.

7. Conclusions and Future Work

This systematic review has examined in depth the development, implementation, and evaluation of blockchain-based electronic voting systems between 2022 and 2025, providing a critical and up-to-date overview of the advances, challenges, and prospects in this field. The results obtained allow us to affirm that blockchain technology represents a solid alternative to traditional and electronic systems, thanks to its properties of immutability, decentralisation, verifiability, and ability to increase transparency, security, and trust in electoral processes. The integration of advanced cryptographic mechanisms and smart contracts has made it possible to overcome historical limitations associated with fraud, manipulation, and centralisation, while strengthening the auditability and individual and collective verification of suffrage.

At the implementation level, although significant progress has been made in the variety of techniques applied—including public and permissioned blockchains, biometrics, multifactor authentication, and cryptographic testing—actual adoption in large-scale scenarios and highly regulated contexts remains limited. Most effective deployments are confined to academic environments or controlled pilot tests, highlighting a gap between conceptual innovation and practical adoption. Furthermore, although scientific output is extensive and diverse, there remains a geographical asymmetry and a shortage of standardised empirical comparisons, which hinders the transfer and integration of best practices between different jurisdictions and realities.

The main contributions of this study lie in the critical synthesis of technological trends, the identification of key technical and methodological axes, and the identification of factors that influence the effective adoption of these solutions. It highlights the ability of blockchain systems to balance anonymity and authentication, as well as to support new models of democratic participation tailored to contemporary challenges in governance and cybersecurity. However, the technical maturity achieved has not yet been fully translated into robust institutional adoption or validation under complex electoral conditions.

Among the main limitations identified are the lack of large-scale empirical evidence, interoperability challenges, regulatory restrictions, and socio-technical barriers to achieving public trust and acceptance. Although there are integrative proposals capable of combining high-security authentication with effective anonymity, their viability in national electoral processes remains a pending challenge.

This review makes three main contributions to the field of blockchain-based electronic voting. It consolidates recent evidence into a coherent knowledge base, maps emerging trends in authentication and verification mechanisms, and clarifies the current state of empirical validation by highlighting the gap between technical maturity and real-world deployment.

Based on the above, it is proposed that future research address the validation of these solutions in real and diverse scenarios, prioritising large-scale testing, longitudinal comparative studies, and integration with regional and international regulatory frameworks. It will be essential to advance the development of objective metrics for performance, robustness, and acceptance, as well as inclusive digital literacy strategies that accompany the necessary explanation and social legitimisation of these technologies. The success of blockchain-based electronic voting will depend not only on its technical refinement, but also on a comprehensive understanding of the regulatory, cultural, and organisational factors that condition its effective adoption.

Supplementary Materials: The following supporting information can be downloaded at: http://www.galeras.net/ors/data_processing_2.xlsx (accessed on 21 October 2025), data processing.

Author Contributions: Conceptualisation, O.R.S., A.B.S. and M.B.G.; methodology, O.R.S., A.B.S. and M.B.G.; validation, O.R.S., A.B.S. and M.B.G.; formal analysis, O.R.S., A.B.S. and M.B.G.; investigation, O.R.S., A.B.S. and M.B.G.; resources, O.R.S., A.B.S. and M.B.G.; data curation, O.R.S., A.B.S. and M.B.G.; writing—original draft preparation, O.R.S.; writing—review and editing, O.R.S., A.B.S. and M.B.G.; supervision, O.R.S.; project administration, O.R.S.; funding acquisition, O.R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Vice-Rectorate for Research and Social Interaction of the University of Nariño (San Juan de Pasto, Colombia), Teaching Research Project Number 3191 “Blockchain and democratic culture”. The APC was funded by the Vice-Rectorate for Research and Social Interaction of the University of Nariño (San Juan de Pasto, Colombia), Teaching Research Project Number 3191 “Blockchain and democratic culture”.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article/Supplementary Materials. Further inquiries can be directed to the corresponding author.

Acknowledgments: The authors express their thanks to Galeras.NET Group, Universidad de Nariño, for allowing and supporting the development of this work. During the preparation of this study, the authors used ChatGPT 5.0 to generate some texts and to adjust the writing. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ACM	Association for Computing Machinery
DID	Decentralised Identifier
DLT	Distributed Ledger Technology
DOAJ	Directory of Open Access Journals
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
OTP	One-Time Password
PoS	Proof of Stake
PoW	Proof of Work
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RQ	Research Question
WOS	Web of Science
ZKP	Zero-Knowledge Proof

Appendix A

Table A1. Example of the extraction form.

Data	Description
Source	Scopus
Title	A Block-Chain Based Decentralized Mechanism to Ensure the Security of Electronic Voting System Using Solidity Language
Year	2024
Type of publication	Conference paper
Authors	P. Savaridassan, Swapnil Lohani, Harshal Gupta
Country	(see table below)
RQ1	Provides integrity, transparency, and immutability through smart contracts and decentralised consensus; an improvement over traditional methods.
RQ2	Cites pilot applications in Telangana (India), Zug (Switzerland), and Seoul (South Korea); with limited success but positive results.
RQ3	Uses Ethereum, Solidity, smart contracts, and Proof-of-Stake consensus mechanism; addresses security, privacy, and data manipulation.
RQ4	Includes authentication and identity management mechanisms through smart contracts; mention of authentication but without clear technical specifications.
RQ5	Automated auditing and verification through smart contracts; provides traceability and integrity of votes.
RQ6	Yes, pilot tests were conducted in real-world contexts such as municipal elections and citizen participation.
Country	India
Participation	1 *

* The paper has three authors, all of whom belong to the same institution in India.

Appendix B

Appendix B presents the complete references for the final set of 338 studies, which can be consulted at <http://www.galeras.net/ors/appendix.pdf> (accessed on 21 November 2025).

References

- Huang, J.; He, D.; Chen, Y.; Khan, M.K.; Luo, M. A Blockchain-Based Self-Tallying Voting Protocol With Maximum Voter Privacy. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 3808–3820. [\[CrossRef\]](#)
- Suganthi, N.; Gokul, S.; Shravanth, E.; Veena, K. E—Voting Using Blockchain. In *Proceedings of the 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA 2023), Coimbatore, India, 16–17 June 2023*; IEEE: Coimbatore, India, 2023; pp. 1–4.
- Enzo, L.P.; Rodrigo, G.M.; Juan, F.M. Boxting: A Blockchain Based Voting System. In *Proceedings of the IEEE Engineering International Research Conference (EIRCON 2022), Lima, Peru, 26–28 October 2022*; IEEE: Lima, Peru, 2022; pp. 1–4.
- Mwansa, P.; Kabaso, B. Blockchain Electoral Vote Counting Solutions: A Comparative Analysis of Methods, Constraints, and Approaches. In *Proceedings of the International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD 2023), Durban, South Africa, 3–4 August 2023*; IEEE: Durban, South Africa, 2023; pp. 1–10.
- Chen, M.; Chen, B.; Lin, Z.; Ye, L.; Zhang, S.; Zhang, S. A Blockchain-Based Distributed Anonymous Weighted Voting System. In *Blockchain Technology and Application*; Zhu, J., Wu, Q., Ding, Y., Song, X., Lu, Z., Eds.; Springer Nature: Singapore, 2024; Volume 2098, pp. 185–197, ISBN 978-981-97-3202-9.
- Sangraula, P.; Adhikari, N.B. Zero Knowledge Proof on Top of Blockchain for Anonymous and Verifiable E-Voting System. *J. Inst. Eng. Ser. B* **2025**, *106*, 1861–1872. [\[CrossRef\]](#)
- Ohize, H.O.; Onumanyi, A.J.; Umar, B.U.; Ajao, L.A.; Isah, R.O.; Dogo, E.M.; Nuhu, B.K.; Olaniyi, O.M.; Ambafi, J.G.; Sheidu, V.B.; et al. Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges. *Clust. Comput.* **2025**, *28*, 132. [\[CrossRef\]](#)
- Hamidey, M.H.B.; Heng, S.-H. A Blockchain-Based E-Voting System. In *Proceedings of the 9th International Conference on Computational Science and Technology (ICCST 2022), Johor Bahru, Malaysia, 27–28 August 2022*; Kang, D.-K., Alfred, R., Ismail, Z.I.B.A., Baharum, A., Thiruchelvam, V., Eds.; Springer Nature Singapore: Singapore, 2022; Volume 983, pp. 553–567.
- Olaniyi, O.M.; Dogo, E.M.; Nuhu, B.K.; Treiblmaier, H.; Abdulsalam, Y.S.; Folawiyi, Z. A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies. In *Blockchain Applications in the Smart Era*; Misra, S., Kumar Tyagi, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 41–63, ISBN 978-3-030-89545-7.
- Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering—Version 2.3*; Keele University & University of Durham: Keele, Staffs, UK, 2007; p. 65.
- Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [\[CrossRef\]](#)
- Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. PRISMA 2020 Explanation and Elaboration: Updated Guidance and Exemplars for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n160. [\[CrossRef\]](#)
- Priscilla, R.; Kathrine, G.J.W.; Rubavathi, M.; Sruthi Krithika, T. Blockchain-Based Decentralized E-Voting System Using Smart Contract. In *Disruptive Technologies for Big Data and Cloud Applications*; Peter, J.D., Fernandes, S.L., Alavi, A.H., Eds.; Springer Nature: Singapore, 2022; Volume 905, pp. 481–491, ISBN 978-981-19-2176-6.
- Marouan, A.; Badrani, M.; Kannouf, N.; Zannou, A.; Chetouani, A. Blockchain-Based e-Voting System in a University. *Indones. J. Electr. Eng. Comput. Sci.* **2024**, *34*, 1915. [\[CrossRef\]](#)
- Banerjee, A. A Fully Anonymous E-Voting Protocol Employing Universal Zk-SNARKs and Smart Contracts. In *Blockchain and Applications*; Prieto, J., Partida, A., Leitão, P., Pinto, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; Volume 320, pp. 349–354, ISBN 978-3-030-86161-2.
- Spadafora, C.; Longo, R.; Sala, M. A Coercion-Resistant Blockchain-Based E-Voting Protocol with Receipts. *Adv. Math. Commun.* **2023**, *17*, 500–521. [\[CrossRef\]](#)
- Adeniyi, J.K.; Ajagbe, S.A.; Adeniyi, E.A.; Mudali, P.; Adigun, M.O.; Adeniyi, T.T.; Ajibola, O. A Biometrics-Generated Private/Public Key Cryptography for a Blockchain-Based e-Voting System. *Egypt. Inform. J.* **2024**, *25*, 100447. [\[CrossRef\]](#)
- Kaladevi, P.; N., S.R.; S.A., S.H.; K., M.A. Secured Electronic Voting System with Appropriate Authentication Using Blockchain. In *Proceedings of the 5th International Conference on Inventive Research in Computing Applications (ICIRCA 2023), Coimbatore, India, 3–5 August 2023*; IEEE: Coimbatore, India, 2023; pp. 1303–1309.
- Jafar, U.; Aziz, M.J.A.; Shukur, Z.; Hussain, H.A. Empowering Secure and Cost-Efficient Blockchain Electronic Voting by Optimized ZK-SNARK Algorithm. In *Proceedings of the International Conference on Electrical Engineering and Informatics (ICEEI 2023), Bandung, Indonesia, 10–11 October 2023*; IEEE: Bandung, Indonesia, 2023; pp. 1–6.
- Haddaway, N.R.; Collins, A.M.; Coughlin, D.; Kirk, S. The Role of Google Scholar in Evidence Reviews and Its Applicability to Grey Literature Searching. *PLoS ONE* **2015**, *10*, e0138237. [\[CrossRef\]](#)
- Björk, B.-C.; Welling, P.; Laakso, M.; Majlender, P.; Hedlund, T.; Guðnason, G. Open Access to the Scientific Journal Literature: Situation 2009. *PLoS ONE* **2010**, *5*, e11273. [\[CrossRef\]](#)

22. Dybå, T.; Dingsøy, T.; Hanssen, G.K. Applying Systematic Reviews to Diverse Study Types: An Experience Report. In *Proceedings of the First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007), Madrid, Spain, 20–21 September 2007*; IEEE: Madrid, Spain, 2007; pp. 225–234.
23. Serenko, A.; Bontis, N.; Booker, L.; Sadeddin, K.; Hardie, T. A Scientometric Analysis of Knowledge Management and Intellectual Capital Academic Literature (1994–2008). *J. Knowl. Manag.* **2010**, *14*, 3–23. [\[CrossRef\]](#)
24. Jafar, U.; Aziz, M.J.A.; Shukur, Z.; Hussain, H.A. A Cost-Efficient and Scalable Framework for E-Voting System Based on Ethereum Blockchain. In *Proceedings of the International Conference on Cyber Resilience (ICCR 2022), Dubai, United Arab Emirates, 6–7 October 2022*; IEEE: Dubai, United Arab Emirates, 2022; pp. 1–6.
25. Kumar, A.; Menaria, S.; Sagar, K.; Choudhary, A.; Bajaj, P.K. A Blockchain-Based Voting System for Elections. In *Communication and Intelligent Systems*; Sharma, H., Shrivastava, V., Tripathi, A.K., Wang, L., Eds.; Springer Nature: Singapore, 2024; Volume 969, pp. 365–379, ISBN 978-981-97-2081-1.
26. Saim, M.; Mamoon, M.; Shah, I.; Samad, A. E-Voting via Upgradable Smart Contracts on Blockchain. In *Proceedings of the International Conference on Futuristic Technologies (INCOFT 2022), Belgaum, India, 25–27 November 2022*; IEEE: Belgaum, India, 2022; pp. 1–6.
27. Enuga, K.; Batthula, P.; Aleti, S.S.; Kolluru, N.; Sakthidharan, G.R. A Secure and Decentralized Method of E-Voting Using Blockchain and Smart Contracts. In *Proceedings of the 7th International Conference on Intelligent Computing and Control Systems (ICICCS 2023), Madurai, India, 17–19 May 2023*; IEEE: Madurai, India, 2023; pp. 1448–1453.
28. Wang, L.; Li, H.; Li, Y.; Yu, Y.; Du, X. Self-Tallying Voting with Blockchain in Wireless Network Environment. *IEEE Wirel. Commun.* **2024**, *31*, 142–147. [\[CrossRef\]](#)
29. Su, P.-C.; Su, T.-C. Secure Blockchain-Based Electronic Voting Mechanism. *Int. Arab J. Inf. Technol.* **2023**, *20*, 253–261. [\[CrossRef\]](#)
30. Misiakoulis, G.; Niavis, H.; Kundig, S.; Loupos, K. Enhancing Security and Scalability in Electronic Voting Through Privacy-Preserving Cryptography and Efficient Data Structures. In *Proceedings of the International Conference on Blockchain (Blockchain 2024), Copenhagen, Denmark, 19–22 August 2024*; IEEE: Copenhagen, Denmark, 2024; pp. 631–636.
31. Somasekhar, G.; Jinka, S.; Kanekal, C.K.; Marimuthu, A. Digital Voting with Blockchain Using Interplanetary File System and Practical Byzantine Fault Tolerance. *Eng. Technol. Appl. Sci. Res.* **2024**, *14*, 19009–19015. [\[CrossRef\]](#)
32. Savitha, R.; Ashwini, K.B.; Prashanth, K. Blockchain-Based Online Voting System. *ECS Trans.* **2022**, *107*, 13195–13203. [\[CrossRef\]](#)
33. Joni, S.A.; Rahat, R.; Tasnin, N.; Ghose, P.; Gaur, L. HAC-Bchain: A Secure and Scalable Blockchain-Shard Based E-Voting System. In *Proceedings of the Technology & Engineering Management Conference—Asia Pacific (TEMSCON-ASPAC 2023), Bengaluru, India, 14–16 December 2023*; IEEE: Bengaluru, India, 2023; pp. 1–6.
34. Rajendra Prasad, P.; Ahmed, R.Z. Secured E-Voting System Implementation Using Block-Chain Network. In *Proceedings of the International Conference on Electronics, Computing and Communication Technologies (CONECCT 2023), Bangalore, India, 14–16 July 2023*; IEEE: Bangalore, India, 2023; pp. 1–6.
35. Bhamare, M.; Kulkarni, P.; Mhetre, A.; Shipra, K.; Wani, S.; Pai, V. Revolutionizing College Elections with a Secure Blockchain Voting Solution. In *Proceedings of the 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA 2023), Hamburg, Germany, 7–8 October 2023*; IEEE: Hamburg, Germany, 2023; pp. 121–125.
36. Onur, C.; Yurdakul, A. ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol. *arXiv* **2022**. [\[CrossRef\]](#)
37. Zhao, W.; Xu, J.; Yang, S. A Secure Electronic Voting Protocol Base on Threshold Proof. In *Proceedings of the 7th International Conference on Electronic Information Technology and Computer Engineering (EITCE 2023), New York, NY, USA, 20–22 October 2023*; ACM: Xiamen China, 2023; pp. 704–708.
38. Pereira, B.M.B.; Torres, J.M.; Sobral, P.M.; Moreira, R.S.; Soares, C.P.D.A.; Pereira, I. Blockchain-Based Electronic Voting: A Secure and Transparent Solution. *Cryptography* **2023**, *7*, 27. [\[CrossRef\]](#)
39. Torre, L.M.J.D.; Mengoy, R.V.M.; Quindoza, R.E.E.; Tamondong, N.J.S.; Tubola, O.D. PUPVOTE: Blockchain-Based Voting System Using NEAR Protocol. In *Proceedings of the 13th International Conference on Information and Communication Technology Convergence (ICTC 2022), Jeju Island, Republic of Korea, 19–21 October 2022*; IEEE: Jeju Island, Republic of Korea, 2022; pp. 1127–1132.
40. Li, F.; Wang, X.; Chen, T.; Li, L.; Huang, H. ASEV: Anonymous and Scored-Based E-Voting Protocol on Blockchain. In *Frontiers in Cyber Security*; Yang, H., Lu, R., Eds.; Springer Nature: Singapore, 2024; Volume 1992, pp. 309–322, ISBN 978-981-99-9330-7.
41. Zhang, J.; Wu, C.; Simon Sherratt, R.; Wang, J. An Improved Secure and Efficient E-Voting Scheme Based on Blockchain Systems. *IEEE Internet Things J.* **2025**, *12*, 8626–8637. [\[CrossRef\]](#)
42. Duran, R.S.; Balbon, C.B.; Balmes, J.Z.E.; Castro, P.B.G.; Lopez, U.G.; Talosig, K.A.; Noriega, M.E.A.; Tubola, O.D. EASY E-VOTE: An Ethereum-Based Voting System Using IPFS and MetaMask for Student Government Election. In *Proceedings of the International Conference on Information Technology (ICIT 2023), Amman, Jordan, 9–10 August 2023*; IEEE: Amman, Jordan, 2023; pp. 815–820.
43. Ezzeddini, L.; Ktari, J.; Zouaoui, I.; Talha, A.; Jarray, N.; Frikha, T. Blockchain for the Electronic Voting System: Case Study: Student Representative Vote in Tunisian Institute. In *Proceedings of the 15th International Conference on Security of Information and Networks (SIN 2022), Sousse, Tunisia, 11–13 November 2022*; IEEE: Sousse, Tunisia, 2022; pp. 1–7.

44. Ndlovu, S.; Sitsha, S.M.G.; Nleya, S.M.; Dube, S.S.; Zengeya, T.; Marabada, N.; Mutengeni, J.; Mapenduka, W. Blockchain-Based Electronic Voting: Case of Student Council Polls. In *Proceedings of the 2nd Zimbabwe Conference of Information and Communication Technologies (ZCICT 2023)*, Gweru, Zimbabwe, 2–3 November 2023; IEEE: Gweru, Zimbabwe, 2023; pp. 1–5.
45. Singathala, H.; Narayansetty, S.; Kata, H. Blockchain Based E-Voting System. In *Proceedings of the Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE 2024)*, Vellore, India, 22–23 February 2024; IEEE: Vellore, India, 2024; pp. 1–6.
46. Li, M.; Xue, K.; Luo, X.; Sun, W.; Wei, D.S.L.; Sun, Q.; Lu, J. S3Voting: A Blockchain Sharding Based E-Voting Approach With Security and Scalability. *IEEE Trans. Dependable Secur. Comput.* **2025**, *22*, 1596–1611. [\[CrossRef\]](#)
47. Marouan, A.; Badrani, M.; Zannou, A.; Kannouf, N.; Chetouani, A. E-Voting System Based on Blockchain for Enhanced University Elections. *SN Comput. Sci.* **2025**, *6*, 204. [\[CrossRef\]](#)
48. Faruk, M.J.H.; Islam, M.; Alam, F.; Shahriar, H.; Rahman, A. Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework. In *Proceedings of the Fourth International Conference on Blockchain Computing and Applications (BCCA 2022)*, San Antonio, TX, USA, 5–7 September 2022; IEEE: San Antonio, TX, USA, 2022; pp. 253–258.
49. Kumar, D.; Kumar Dwivedi, R. Blockchain and Internet of Things (IoT) Enabled Smart E-Voting System. In *Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2023)*, Bengaluru, India, 5–7 January 2023; IEEE: Bengaluru, India, 2023; pp. 28–34.
50. Jain, A.K.; Kalra, S.; Kapoor, K.; Jangra, V. Blockchain-Based Secure E-Voting System Using Aadhaar Authentication. In *Predictive Data Security Using AI*; Thakkar, H.K., Swarnkar, M., Bhadoria, R.S., Eds.; Springer Nature: Singapore, 2023; Volume 1065, pp. 89–103, ISBN 978-981-19-6289-9.
51. Upadhyay, K.; Bansal, A.; Gupta, A.; Kansal, V.; Jain, U.; Bhatla, S. Authentication of Voter Using Convolutional Neural Network and Blockchain. In *Proceedings of the 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS 2023)*, Tashkent, Uzbekistan, 1–3 November 2023; IEEE: Tashkent, Uzbekistan, 2023; pp. 122–127.
52. Savaridassan, P.; Lohani, S.; Gupta, H. A Block-Chain Based Decentralized Mechanism to Ensure the Security of Electronic Voting System Using Solidity Language. In *Deep Sciences for Computing and Communications*; R, A.U., Kottursamy, K., Raja, G., Bashir, A.K., Kose, U., Appavoo, R., Madhivanan, V., Eds.; Springer Nature: Cham, Switzerland, 2024; Volume 2176, pp. 44–51, ISBN 978-3-031-68904-8.
53. Homoliak, I.; Li, Z.; Szalachowski, P. BBB-Voting: Self-Tallying End-to-End Verifiable 1-out-of-k Blockchain-Based Boardroom Voting. In *Proceedings of the IEEE International Conference on Blockchain (Blockchain 2023)*, Ocean Flower Island, China, 17–21 December 2023; IEEE: Danzhou, China, 2023; pp. 297–306.
54. Chafiq, T.; Azmi, R.; Mohammed, O. Blockchain-Based Electronic Voting Systems: A Case Study in Morocco. *Int. J. Intell. Netw.* **2024**, *5*, 38–48. [\[CrossRef\]](#)
55. Al-Maaitah, S.; Quzmar, A.; Qatawneh, M. Blockchain-Based E-Voting System For Elections In Jordan. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 1584–1593.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.