



Digital Forensic-Ready Voting Model

Edmore Muyambo¹, Stacey Baror², Sheunesu Makura³

edmore.muyambo@tuks.co.za¹, stacey.baror@tuks.co.za², makura.sm@up.ac.za³

^{1,2,3}Department of Computer Science, University of Pretoria

Article Information

Received : 6 Nov 2025

Revised : 19 Dec 2025

Accepted : 23 Dec 2025

Keywords

Digital forensics,
E-voting, Blockchain,
Forensic Readiness,
Cyber Forensics,
Electoral Integrity

Abstract

The increasing digitalization of elections through internet-based voting (e-voting) systems introduces both opportunities for enhanced accessibility and threats to electoral integrity. Existing electronic voting systems often lack built-in forensic capabilities necessary to detect, preserve, and prove incidents of vote rigging or cyber manipulation. This paper proposes a Digital Forensic-Ready Voting Model (DFRVM) that integrates forensic-by-design principles, blockchain technology, and legal admissibility frameworks to ensure accountability, transparency, and verifiability in the electoral process. The model emphasizes proactive evidence collection, real-time monitoring, and tamper-evident audit trails to strengthen post-election dispute resolution.

A. Introduction

The rapid expansion of digital democracy and the emergence of e-voting systems have reshaped how elections are conducted globally. While technology promises greater accessibility, efficiency, and faster tallying of results, it also introduces new vulnerabilities such as hacking, malware, denial-of-service attacks, and insider threats [1], [2].

Traditional paper-based elections, though tangible, suffer from manipulation risks such as ballot stuffing and human counting errors [3]. The digitalization of electoral systems thus necessitates not only security but also forensic readiness; the proactive capability to collect, preserve, and present digital evidence that can withstand judicial scrutiny [4].

Recent studies emphasize the importance of integrating forensic-by-design concepts into e-voting systems [5]. However, existing systems often focus on cryptographic protections while neglecting forensic traceability [6]. The Digital Forensic-Ready Voting Model (DFRVM) proposed in this paper bridges that gap by embedding digital forensics into every phase of the election process, from voter registration to result publication.

B. Research Method

This systematic review focused exclusively on scholarly publications that were peer-reviewed and disseminated by accredited academic publishers. The primary objective was to explore existing research on digital forensics within internet-based voting systems, particularly those integrating blockchain technology as a means to enhance electoral transparency, security, and accountability. To ensure thematic relevance, publications were required to contain at least three of the following primary keywords: *digital forensic*, *internet voting*, and *blockchain*. Studies employing synonymous terminology, such as *online voting* or *electronic voting* in place of *internet voting*, were also considered eligible for inclusion, provided they satisfied the three-keyword criterion.

To preserve methodological rigor and ensure contemporary relevance, the review excluded studies published more than five years prior to the research period. Only works published between 1 January 2020 and 31 March 2025 were included. The review primarily targeted studies addressing ballot paper-based voting systems, electronic or internet-based voting mechanisms, and blockchain-enabled electoral architectures. Further inclusion criteria were established based on language, credibility, and authenticity. Only studies published in English, subjected to peer review, and appearing in internationally accredited journals or conference proceedings were retained.

Furthermore, to uphold academic integrity and ensure verifiability, only publications indexed in recognized academic databases and digital libraries were reviewed. Grey literature including unverified reports, preprints, or non-peer-reviewed articles was deliberately excluded or referenced sparingly where necessary to contextualize specific findings. The primary stakeholders discussed across the reviewed literature include voters, electoral candidates, election observers and election management bodies. The overarching aim emerging from these studies underscores the necessity of a secure, transparent, and digitally forensically ready vote administration system capable of safeguarding voter intent,

ensuring data immutability, and providing admissible digital evidence in case of electoral disputes.

B.1 Information Sources

Data for this review were sourced from a total of thirteen internationally recognized academic databases. These repositories were selected for their comprehensive coverage of interdisciplinary research in digital forensics, information security, and e-voting technologies.

Searches were confined to peer-reviewed journal articles, conference proceedings, and technical reports published within the defined review period (2020–2025). Each database query was constructed using Boolean operators to combine key terms such as “*digital forensic*”, “*internet voting*”, “*blockchain*”, and their permutations. The compiled data sources and their respective query dates are summarized in **Table 1** below.

Table 1. Consulted Databases

Database	Date Searched
ACM	1 March 2025
Academic Search Complete	1 March 2025
IEE	1 March 2025
Web of Science	4 March 2025
Science Direct	4 March 2025
Access Science	7 March 2025
Proquest	7 March 2025
Oxford Academy	9 March 2025
Ingenta	9 March 2025
Open Global Trusted	9 March 2025
Clarivate	9 March 2025
Cambridge Core	11 March 2025
Brill	11 March 2025

B.2 Search Technique

To ensure the retrieval of high-quality and thematically relevant literature, a systematic keyword-based search strategy was employed. The process involved constructing targeted search queries across multiple academic databases to identify publications that explicitly addressed the intersection of digital forensics, internet voting, and blockchain technology.

Only publications containing the specified core keywords were considered eligible for review. The primary search terms included: *digital forensics*, *internet voting*, *blockchain*, *online voting*, and *e-voting*. To increase specificity and precision, a combinatorial keyword strategy was applied to refine search results and exclude irrelevant studies. The following keyword combinations were systematically used in the search console:

1. *Digital forensic*
2. *Digital forensic + internet voting*
3. *Digital forensic + internet voting + blockchain*
4. *Digital forensic + internet voting + blockchain + online voting*

5. *Digital forensic + internet voting + blockchain + online voting + e-voting*
6. *Digital forensic + internet voting + blockchain + online voting + e-voting + published date between 2020/01/01 and 2025/03/31*

The initial search using the standalone term “*Digital forensic*” generated several thousand results. While this provided a broad overview of the research field, it was too extensive for detailed review. Consequently, more specific combinations of the core keywords were applied iteratively to narrow the scope and isolate publications most relevant to the research focus.

After refining the search queries, a date filter was then introduced to limit results to publications produced between January 2020 and March 2025. The decision to exclude older literature was based on the recognition that earlier studies may rely on outdated or obsolete technologies, thereby introducing potential bias and reducing the relevance of findings.

Following the application of the date restriction, the dataset was substantially reduced, yielding a more manageable and focused body of literature. Each publication was then subjected to manual screening, where titles, abstracts, and where necessary, introductions were reviewed to assess thematic alignment and methodological soundness. This step ensured that only studies offering substantive contributions to the discourse on digital forensic readiness in blockchain-based e-voting systems were retained for full analysis.

The overall search and screening process are visually represented in **Figure 1**, which outlines the logical flow of the literature identification, filtering, and inclusion stages on one of the databases used.

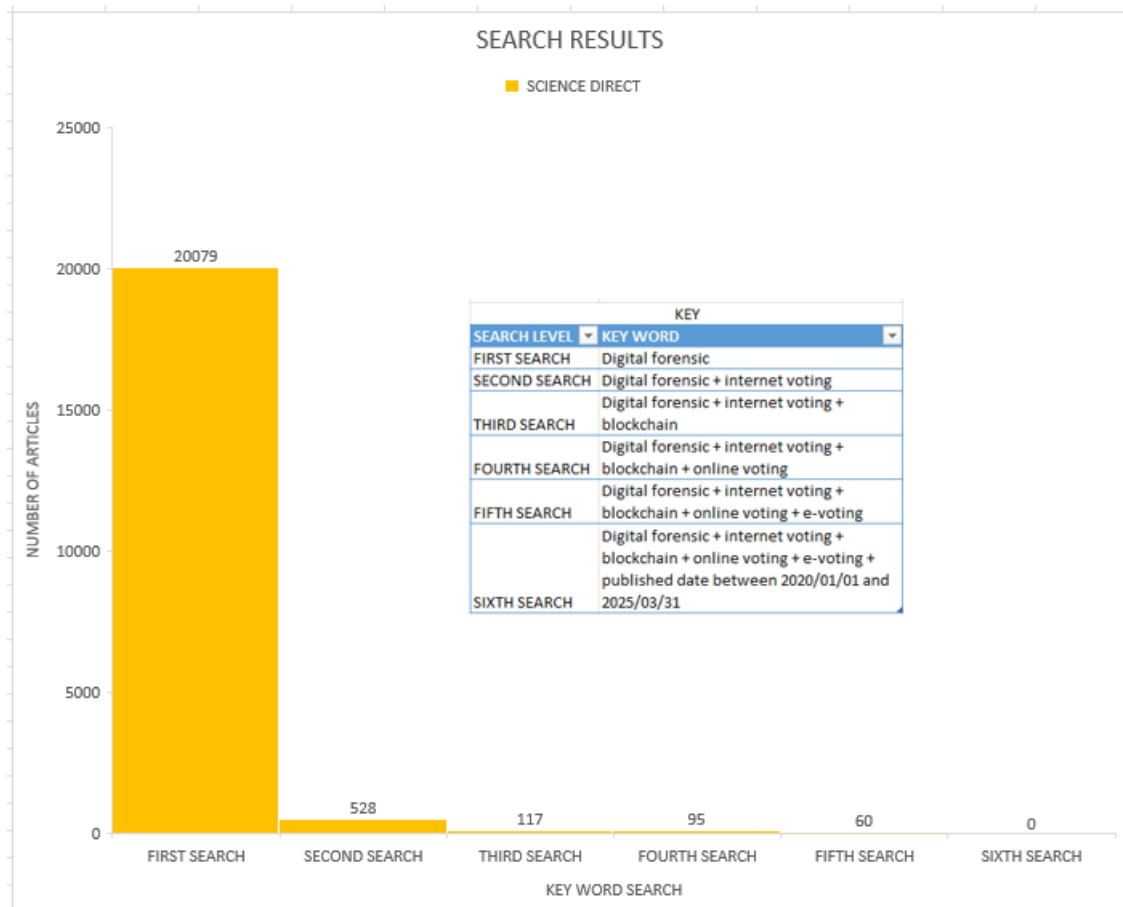


Figure 1. Search criteria against results

Figure 2 Below shows a wholistic view across all the thirteem database consulted when the key word “Digital Forensic” was used on the first search criteria.

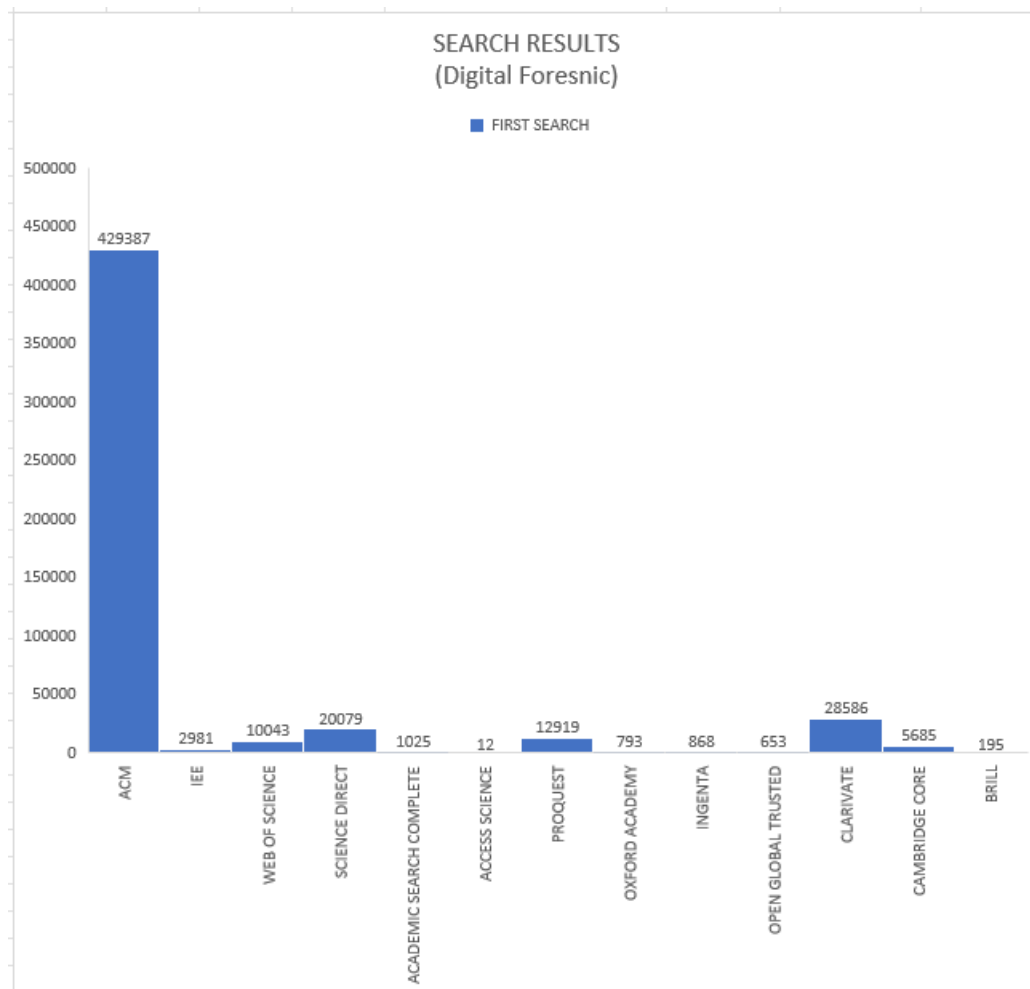


Figure 2. Number of records per database after the initial search criteria

Detailed results for selection criteria per database are shown in **Figure 3**. This depicts the actual number of records retrieved per database and a combined screening thereafter.

B.3 Screening and Inclusion Criteria

Following the initial keyword-based search, a two-stage screening process was implemented to ensure that only high-quality and relevant publications were included in the systematic review. The screening process was designed to uphold methodological rigor, minimize selection bias, and ensure that reviewed studies directly addressed the research focus on digital forensic readiness in blockchain-integrated internet voting systems.

B.3.1 Preliminary Screening

In the preliminary screening stage, publications identified through the database search were first evaluated based on titles, abstracts, and keywords. The objective of this phase was to eliminate duplicates and exclude studies that were clearly unrelated to the scope of the research. Publications that did not explicitly engage with digital forensics, e-voting, or blockchain-based systems were immediately removed.

Only studies published in English, between 1 January 2020 and 31 March 2025, and appearing in peer-reviewed academic journals or conference proceedings were retained. This temporal limitation was adopted to ensure the inclusion of recent and technologically relevant research. Additionally, publications originating from accredited academic publishers or indexed in recognized databases such as IEEE Web of Science, Science Direct, Access Science, Proquest, Clarivate, and ACM Digital Library were prioritized.

B.3.2 Secondary Screening

The secondary screening involved a comprehensive review of the full text of publications that had passed the preliminary phase. During this stage, the methodology, scope, and contextual relevance of each study were examined in detail. Publications that lacked methodological transparency, scientific depth, or linguistic clarity were excluded. Similarly, papers that were conceptually aligned but failed to provide empirical or analytical insights into forensic mechanisms, blockchain integration, or e-voting security frameworks were omitted.

The review also excluded grey literature, including non-peer-reviewed reports, opinion pieces, and non-academic blogs, except where such documents provided substantial technical or legal insights that were otherwise unavailable in peer-reviewed sources. This approach strengthened the credibility, replicability, and academic robustness of the final corpus of reviewed works.

B.3.3 Inclusion Criteria Summary

Publications were deemed eligible for inclusion if they met the following criteria:

- Addressed at least three core research concepts, namely: *digital forensics*, *internet or online voting*, and *blockchain technology*;
- Were peer-reviewed and published by accredited academic publishers;
- Were written in English and accessible through reputable databases;
- Were published between January 2020 and March 2025;
- Offered empirical, technical, or conceptual contributions relevant to forensic readiness in e-voting systems; and
- Maintained academic integrity, with proper referencing and verifiable sources.

This multi-layered screening framework ensured that the final body of literature accurately represented the current state of academic and technical knowledge concerning the integration of digital forensics and blockchain technology in online voting environments. The resulting dataset formed the empirical foundation for the subsequent analysis and synthesis of research findings presented in this study.

B.4 Data Items

Data were extracted manually by a single reviewer using a standardized template designed for this study. The template captured bibliographic metadata (author, year, title, publisher, and DOI where available), methodological attributes (research design, data type, and analytical approach), and substantive content (key findings, implications, and limitations). Extracted information was categorized into five main analytical dimensions:

1. **Security and Integrity of Voting Systems** – including studies discussing cryptographic mechanisms, tamper-proof architectures, and integrity verification methods;
2. **Digital Forensic Readiness** – identifying proactive measures, evidence collection frameworks, and admissibility protocols applicable to online elections;
3. **Blockchain Integration and Trust Models** – evaluating how blockchain enhances transparency, immutability, and traceability in voting systems;
4. **Comparative Analysis of Voting Models** – contrasting traditional ballot-based systems with digital and blockchain-enhanced e-voting systems; and
5. **Legal and Ethical Implications** – reviewing literature addressing evidence admissibility, privacy protection, and regulatory frameworks.

This framework ensured a consistent and replicable extraction of key research elements while maintaining academic rigor and methodological transparency.

B.5 Effect Measures

From a total of 131 reviewed publications, 116 studies (88.5%) explicitly identified the vulnerability of ballot paper-based voting systems to vote rigging and fraud. The consensus across these studies underscored that the traditional paper ballot process is susceptible to undetectable tampering, untraceable manipulation, and procedural inconsistencies.

Of these 116 studies, 111 (95.6%) emphasized the significance of blockchain technology as a mitigating solution to these vulnerabilities, noting its capability to ensure data integrity, transparency, and non-repudiation in online voting systems. However, only 27 publications (23%) explicitly discussed the integration of digital forensics within blockchain-based e-voting systems, highlighting a substantial research gap in this area.

Notably, just 2% of the reviewed literature focused primarily on digital forensics in online voting, suggesting that this domain remains significantly underexplored. While blockchain technology has been extensively studied for its security properties, its synergy with digital forensic readiness, especially in the context of electoral integrity has not yet been fully developed in the scholarly discourse.

B.6 Synthesis Methods

To guide the synthesis and analysis of the reviewed literature, a set of thematic codes was applied to categorize publications. These included:

- Online or Internet voting processes;
- Ballot paper-based voting mechanisms;

- Blockchain technology applications;
- Digital forensics and evidence management; and
- Vote rigging and electoral manipulation techniques.

These coding dimensions were used to extract information relevant to both traditional and electronic voting systems. The comparative approach provided insights into the operational strengths and weaknesses of each voting paradigm. Given the widespread allegations of electoral manipulation in conventional systems, this review particularly emphasized studies exploring how blockchain and digital forensic mechanisms can fortify online voting processes against tampering and fraud.

Blockchain technology was consistently identified as a reliable means of ensuring data integrity, immutability, and transactional privacy. However, while blockchain provides a technical layer of security, it does not inherently enable forensic traceability or admissibility of digital evidence. Therefore, this study recognized that digital forensic readiness must operate as a complementary layer; transforming the blockchain infrastructure into a verifiable, evidence-preserving ecosystem.

Graphical analyses (e.g., histograms) were used to visualize search results across databases and keyword combinations, illustrating the frequency and distribution of relevant studies within the review scope (see Figure 1 and 2).

B.7 Bias Assessment

Given the interdisciplinary and emerging nature of digital forensic research in internet voting, a comprehensive bias assessment was necessary to ensure the reliability, validity, and reproducibility of this systematic review. This section critically examines potential sources of bias that may have influenced the selection, interpretation, and synthesis of literature, as well as the inherent methodological limitations of the review process.

B.7.1 Risk of Selection Bias

The primary source of potential bias also stemmed from the selection criteria used during the screening phase. Since inclusion was restricted to peer-reviewed, English-language publications indexed between *January 2020 and March 2025*, relevant research published in other languages or prior to this timeframe may have been excluded. Although this decision was made to maintain recency and linguistic consistency, it may have inadvertently omitted earlier foundational works or non-English research that could contribute to a broader understanding of the subject.

Additionally, the single-reviewer approach adopted during study selection introduced the possibility of subjective judgment in determining inclusion eligibility. While the reviewer employed structured screening templates and inclusion criteria to maintain consistency, the absence of multiple independent reviewers or inter-rater reliability checks presents a moderate risk of selection bias.

B.7.2 Publication Bias

A further consideration is publication bias, which arises when only studies with significant or positive findings are more likely to be published in academic databases. Given that this review emphasized peer-reviewed literature, studies presenting null or inconclusive results, particularly in experimental blockchain or forensic implementations may not have been represented. This limitation could lead to an overrepresentation of studies reporting successful blockchain E-Voting integrations or effective forensic mechanisms, thus overstating the maturity of the field.

Moreover, the scarcity of literature explicitly integrating *blockchain* and *digital forensics* in the context of *internet voting* heightened this risk. While efforts were made to supplement formal databases with referral searches through Google Scholar and institutional repositories, the imbalance between exploratory and empirical studies remains an inherent limitation of the available research corpus. This discrepancy underscores a gap in the existing literature and highlights the need for greater academic focus on digital forensic mechanisms within blockchain-secured electoral frameworks.

B.7.3 Methodological and Reporting Bias

Several methodological inconsistencies were also noted within the reviewed studies themselves. A significant proportion of publications lacked quantitative validation, relying instead on conceptual or prototype-based demonstrations of blockchain-enabled forensic processes. In such cases, the absence of statistical evidence or real-world testing made it challenging to assess the external validity of the reported findings.

Additionally, reporting bias was observed where authors omitted essential implementation details such as encryption parameters, forensic chain-of-custody procedures, or system performance metrics, thus limiting reproducibility. Some studies presented generalized claims about blockchain's immutability or forensic value without empirically substantiating these assertions. This poses a risk of interpretive bias when synthesizing evidence across studies with heterogeneous methodological quality.

B.7.4 Geographic Bias

Geographically, the majority of reviewed publications originated from Europe, Asia, and North America, with limited representation from Africa and South America. This imbalance reflects disparities in global research output rather than topic relevance. As a result, findings may be less generalizable to developing nations where infrastructural, legal, and socio-political contexts differ significantly.

B.7.5 Mitigation Strategies

To reduce the impact of the above biases, several mitigation measures were integrated into the review process:

- Clear definition of inclusion and exclusion criteria before data collection;
- Use of multiple databases and referral searches to enhance coverage;
- Application of date and keyword filters to refine relevance;
- Manual verification of abstracts and introductions to ensure topic alignment; and

- Consistent reference tracking to avoid duplication or omission.
- A second independent reviewer was used on the selection of the final study list.

While complete elimination of bias is impractical in qualitative systematic reviews, the methodological rigor employed ensures that the findings of this study remain credible, reproducible, and representative of the current academic discourse on *digital forensic-ready e-voting systems*.

B.8 Certainty Assessment

To establish confidence in the findings, a certainty assessment was conducted based on the consistency and reliability of the retrieved data. Publications were examined for convergence in their results and theoretical arguments. Studies presenting consistent findings across diverse contexts were considered high-confidence sources, while isolated or contradictory studies were subjected to further scrutiny.

The analysis indicated a high degree of consistency among studies asserting that blockchain technology enhances data integrity, auditability, and transparency in electronic voting. However, there remains a lack of empirical studies that rigorously evaluate the performance of blockchain-based voting systems under forensic investigation scenarios.

Overall, this review demonstrates moderate-to-high certainty regarding the advantages of blockchain-enabled voting systems over traditional ballot paper methods. However, it also identifies a low certainty and limited evidence base concerning the integration of digital forensic readiness within such systems; a gap that this research aims to address through the proposed Digital Forensic-Ready Voting Model (DFRVM).

C. Result and Discussion

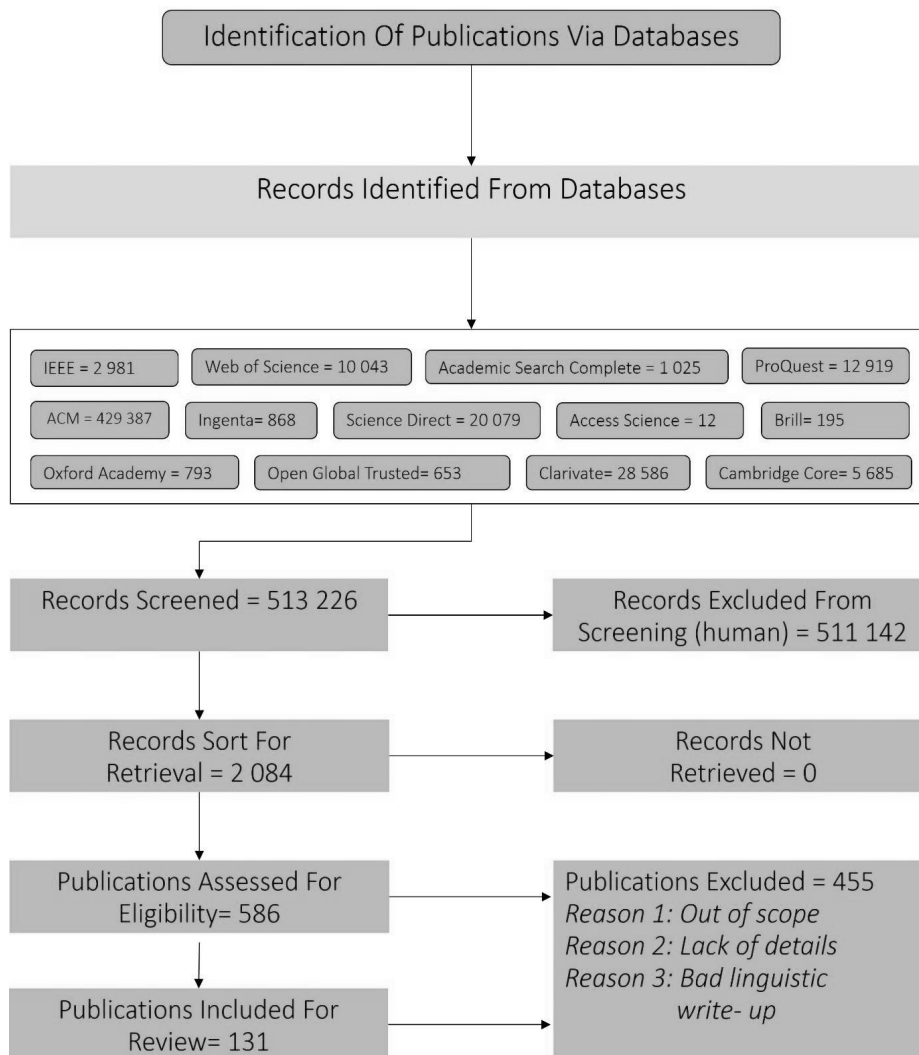


Figure 3. Number of Articles Per Selection Criteria

As illustrated in **Figure 3** above, the initial search yielded a total of 513,226 records from multiple academic databases and online repositories. These records underwent an initial screening process based on the inclusion and exclusion criteria established for this review. During this phase, broad search results were refined through the application of keyword filters, publication date restrictions, and subject relevance parameters.

Following the first round of screening, 511,142 records were excluded for failing to meet one or more of the eligibility criteria. The remaining 2,084 publications were subjected to a more targeted evaluation, focusing on relevance to digital forensics, internet voting, and blockchain technology.

In the subsequent screening phase, a total of 586 studies progressed to manual assessment. Each publication was individually examined by carefully reading the titles, abstracts, and introductions to determine its suitability for

inclusion. This manual evaluation process aimed to ensure that only publications that demonstrated methodological soundness, conceptual relevance, and academic rigor were retained.

Following this detailed review, 131 studies were shortlisted for final consideration. From this pool, 17 studies were later excluded after an in-depth quality and content assessment. The reasons for exclusion included technical irrelevance to the review focus, insufficient scientific depth, and non-compliance with standard academic writing conventions as highlighted for some in **Table 2** below. Moreover, several of these excluded studies exhibited poor grammatical structure or lack of conceptual clarity, rendering them unsuitable for inclusion in a high-rigor academic synthesis.

To maintain focus and prevent the paper from exceeding standard publication length, only five of the seventeen excluded studies are presented as examples in **Table 2** below. These exemplify the types of publications omitted at this stage due to their methodological weaknesses, lack of analytical depth, or limited contribution to the central discourse on digital forensics in blockchain-based e-voting systems.

Table 2. Exclusion List

Author	Year	Title	Exclusion Reason
Neloy, Mohammad Nabiluzzaman; Wahab, Md. Abdul; Wasif, Sheikh; All Noman, Abdulla	2023	A remote and cost- optimized voting system using blockchain and smart Contract[7]	Does not cover digital forensic scope
Chaabane, Faten; Ktari, Jalel; Frikha, Tarek; Hamam, Habib	2022	Low Power Blockchained E- Vote Platform for University Environment[8]	Limited scope
Vatsa, Avimanyou	2021	BCT-Voting : A Blockchain Technology Based Voting System BCT-Voting : A Blockchain Technology Based Voting System[9]	Does not cover digital forensic scope
Dimitri, Nicola	2022	Quadratic Voting in Blockchain Governance[10]	Too technical and lacks clear linguistic literature
Desai, Shreya; Desai, Shreya; Desai, Shreya; Li, Zhigang; He, Jing; Xu, Xiaohua	2020	Untampered electronic voting in entertainment industry: A blockchain- based implementation[11]	Outside the required scope

Subsequently, **Table 3** below details out the inclusion list for this reserach. Likewise, in order to maintain focus and prevent the paper from exceeding standard publication length, only ten of the included studies are presented as examples.

Table 3. Included Study List

Author	Year	Title	Study Area
Li, Meng; Lal, Chhagan; Conti, Mauro; Conti, Mauro	2021	LEChain: A blockchain- based lawful evidence management scheme for digital forensics[12]	Blockchain and Digital Forensic
Englbrecht, Ludwig	2020	A privacy-aware digital forensics investigation in enterprises[13]	Digital Forensics
McCorry, Patrick; Mehrnezhad, Maryam; Toreini, Ehsan; Shahandashti, Siamak F; Hao, Feng	2021	On Secure E-Voting over Blockchain[14]	E-voting and Blockchain
Huang, Jun; He, Debiao; Obaidat, Mohammad S.; Vijayakumar, Pandi; Luo, Min; Choo, Kim Kwang Raymond	2021	The Application of the Blockchain Technology in Voting Systems[15]	Blockchain and Voting
Rabia, Fatih; Sara, Arezki; Sara, Arezki	2021	A survey on e-voting based on blockchain[16]	Blockchain and E-Voting
Vladucu, Maria Victoria; Dong, Ziqian; Medina, Jorge; Rojas-Cessa, Roberto	2023	E-voting Meets Blockchain: A Survey[17]	Blockchain and E- Voting
Shah, Akhil; Sodhia, Nishita; Saha, Shruti; Banerjee, Soumi; Chavan, Madhuri	2020	Blockchain Enabled Online-Voting System[18]	Blockchain and Online Voting
Anitha, V; Marquez Caro, Orlando Juan; Sudharsan, R.; Yoganandan, S.; Vimal, M.	2023	Transparent voting system using blockchain[19]	Blockchain
K., Edison; B., Venansius	2022	Blockchain Based Electronic Voting Protocol[20]	Blockchain
Holmes, C	2022	How Blockchain Technology could support Democracy and E-Voting[21]	Blockchain and E- Voting

C.1 Summary of Findings and Conceptual Integration

The systematic review conducted in this study synthesized evidence from interdisciplinary sources spanning digital forensics, blockchain technologies, and electronic voting systems. The findings collectively underscore the critical need for a secure, transparent, and forensically verifiable voting architecture capable of mitigating the enduring vulnerabilities of traditional ballot-based elections. This section summarizes the main findings across the reviewed domains and explains how these insights informed the conceptualization of the Digital Forensic-Ready Voting Model (DFRVM).

C.1.1 Overview of Key Findings

The review identified five overarching themes that define the current state of research in blockchain-assisted digital forensics within online voting systems:

1. **Persistent Vulnerabilities in Traditional Voting Systems**

The evidence consistently indicates that ballot paper-based voting systems remain highly susceptible to manipulation, including ballot stuffing, vote destruction, and unauthorized tampering during counting and transportation stages. The lack of an immutable audit trail severely undermines the ability of election management bodies (EMBs) and judicial entities to provide verifiable, scientific proof in electoral dispute resolution. Studies such as those by Kshetri and Vosa [22] reaffirmed that these weaknesses have direct implications for public trust and political stability.

2. **Emergence of Blockchain as a Trust Enabler:**

Blockchain has emerged as a foundational technology for ensuring data immutability, traceability, and tamper detection. Through distributed consensus and cryptographic hashing, blockchain can record each vote transaction as an immutable ledger entry. Research by Li et al. [12] and McCorry et al. [14] demonstrated that blockchain architectures particularly permissioned ledgers can provide verifiable evidence trails suitable for forensic auditing. However, scalability and data privacy remain active challenges, especially in high-turnout national elections.

3. **Digital Forensics as a Mechanism for Evidentiary Integrity**

The integration of digital forensics into e-voting processes offers a structured mechanism for the preservation, extraction, and authentication of electronic evidence. Forensic readiness defined as the proactive capability of a system to generate admissible digital evidence, was identified as a critical success factor for legal credibility. Studies such as Ryu et al. [23] and Englbrecht [13] emphasized the necessity of automated evidence generation through system logs, cryptographic timestamps, and verifiable metadata to support post-election investigations.

4. **Need for Interoperable and Transparent Frameworks**

Despite notable advancements, the review found limited cross-domain frameworks that combine blockchain, forensic evidence management, and electoral governance. Existing systems tend to operate in silos blockchain mechanisms ensuring transaction integrity, and forensic tools ensuring evidence analysis. The absence of an integrated architecture results in gaps between vote casting, data storage, and evidence validation, which the proposed DFRVM seeks to address.

5. **Ethical, Legal, and Socio-Technical Challenges**

The integration of forensic technologies into electoral systems raises new legal and ethical questions regarding data privacy, voter anonymity, and chain-of-custody governance. Jurisdictions differ significantly in their

treatment of digital evidence and the admissibility of blockchain-generated logs in judicial contexts. As a result, the review identified a growing need for harmonized international standards and digital evidence policies that align with emerging forensic-ready architectures.

C.2 Proposed Model

The synthesis of these findings directly informed the development of the Digital Forensic-Ready Voting Model (DFRVM), a conceptual architecture designed to enhance transparency, evidentiary admissibility, and systemic accountability in online voting. The model comprises four interconnected layers, namely: the Vote Casting Layer, the Data Store Layer, the Data Reconciliation Layer, and the Reporting Layer (see **Figure 4**), each addressing a specific challenge identified in the literature:

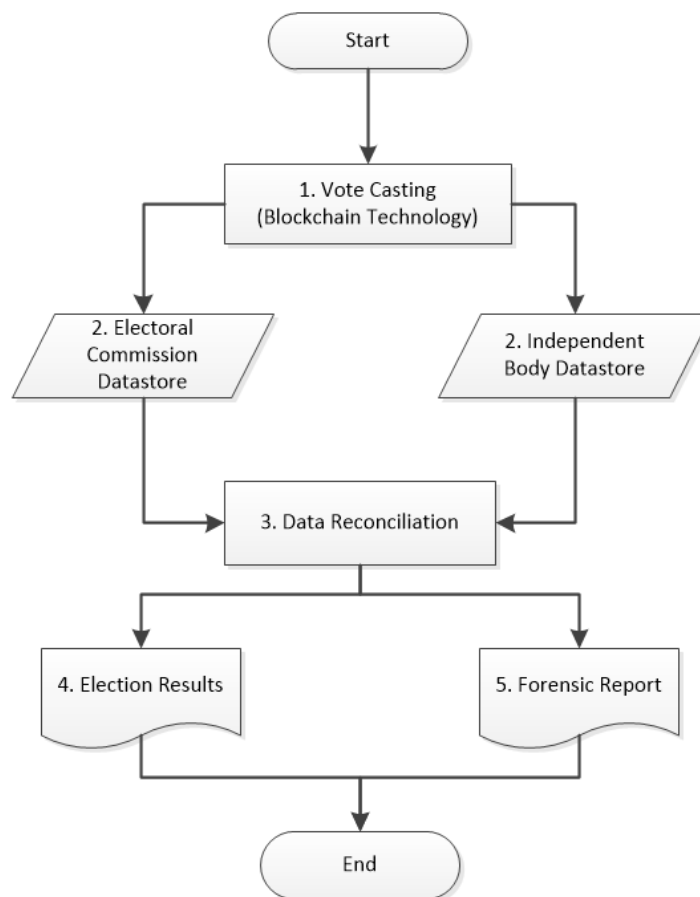


Figure 4. High level view of the proposed model.

At the point of vote casting, each ballot is processed through blockchain encryption technology, which ensures that the vote remains secure, immutable, and traceable.

Following encryption, the vote is concurrently stored in two distinct and independently managed repositories: one maintained by the Electoral Commission and another by an Independent Oversight Body. These data stores are architected with embedded digital forensic mechanisms that facilitate tamper detection, data

validation, and chain-of-custody integrity. As the electoral data flows through the system, it undergoes continuous verification via cryptographic and forensic validation checks, thus enabling proactive detection of anomalies.

At the reconciliation stage, datasets from both storage points are systematically compared to identify discrepancies, alterations, or unauthorized interventions. This data reconciliation process serves as a critical point for validating the integrity of the election data. The final output includes not only the official election results but also a comprehensive Digital Forensic Election Audit Report. This report provides an evidentiary trail detailing the provenance of each vote and flags any instances of data tampering or procedural irregularities, thereby strengthening the evidential credibility and legal defensibility of the electoral outcome. Below is a contextual layout for each of the layers identified.

C.2.1 Integration of Blockchain and Forensic Readiness Principles

The DFRVM's architecture is grounded in the convergence of blockchain immutability and forensic readiness design principles. By embedding forensic logging mechanisms within the blockchain infrastructure, the model ensures that every vote-related transaction is provable, non-repudiable, and reconstructible. Each block in the ledger contains a hash of the previous block, encrypted payloads, and validation metadata forming a continuous, tamper-evident chain of custody. Moreover, the system enforces dual evidence storage, ensuring that forensic and administrative data remain synchronized yet segregated. This dual architecture not only enhances system reliability but also satisfies the evidentiary requirements for legal admissibility under digital forensics frameworks, as defined by international standards such as ISO/IEC 27037 [24] and the Association of Chief Police Officers (ACPO) digital evidence guidelines.

C.2.2 System Implementation and Forensic Integration

C.2.2.1 Evidence Collection and Chain of Custody

DFROVM's forensic subsystem ensures all events (vote casting, transmission, tallying) generate metadata such as timestamps, IP addresses, and session identifiers. These logs are hashed and stored on blockchain nodes to preserve integrity [18].

C.2.2.2 Tamper Detection and Anomaly Analysis

The reconciliation module correlates blockchain entries with server logs, identifying discrepancies that may indicate tampering [19]. Suspicious transactions trigger automated forensic alerts for human analysis.

C.2.2.3 Legal Admissibility of Digital Evidence

The model follows the Daubert Standard [25] and ISO/IEC 27037 [24] protocols for evidence handling, ensuring that forensic data can be presented in court without question of authenticity.

D. Conclusion

In conclusion, the Digital Forensic-Ready Voting Model (DFRVM) represents a critical step toward building trustworthy, transparent, and legally defensible

digital democracies. By embedding forensic readiness within blockchain-powered voting infrastructures, the model not only secures the act of voting but also safeguards the evidence of truth underpinning democratic legitimacy.

In an era where electoral integrity is constantly challenged by both technological and human threats, the fusion of digital forensics and blockchain technology stands as a promising paradigm, one that transforms elections into auditable, accountable, and scientifically verifiable processes. The DFRVM, therefore, offers not merely a technological innovation but a democratic safeguard, reinforcing citizens' confidence in the fairness and accuracy of electoral outcomes across the digital frontier.

E. References

- [1] D. Chaum, R. L. Rivest, and P. Y. A. Ryan, "E-voting: From cryptography to practical implementation," *Proc. 8th Workshop on Trustworthy Elections (WOTE)*, Leuven, Belgium, 2009.
- [2] J. Clark and V. Essex, "End-to-end verifiable elections," *IEEE Security Privacy*, vol. 10, no. 5, pp. 46–53, 2012.
- [3] P. Norris, *Why Elections Fail*. Cambridge, U.K.: Cambridge University Press, 2015.
- [4] M. Ruan, A. Baggili, and J. Mislán, "Forensic readiness: A comprehensive approach," *Digital Investigation*, vol. 8, no. 3–4, pp. 155–164, 2011.
- [5] S. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. London, U.K.: Academic Press, 2011.
- [6] R. Mercuri, "Electronic vote tabulation: Checks and balances," Ph.D. dissertation, Univ. Pennsylvania, USA, 2001.
- [7] Nelay, M.N., Wahab, M.A., Wasif, S., All Noman, A., Rahaman, M., Pranto, T.H., Haque, A.B. and Rahman, R.M., 2023. A remote and cost-optimized voting system using blockchain and smart contract. *IET Blockchain*, 3(1), pp.1-17.
- [8] Chaabane, F., Ktari, J., Frikha, T. and Hamam, H., 2022. Low power blockchained e-vote platform for university environment. *Future Internet*, 14(9), p.269.
- [9] Raikar, D. and Vatsa, A., 2021. BCT-Voting: A Blockchain Technology Based Voting System. In *The 27th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21)*, July (pp. 26-29).
- [10] Dimitri, N., 2022. Quadratic voting in blockchain governance. *Information*, 13(6), p.305.
- [11] Desai, S., Han, M., Li, L., Li, Z., He, J. and Xu, X., 2019, September. Untampered Electronic Voting in Entertainment Industry: A Blockchain-based Implementation. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (pp. 166-166).
- [12] Li, M., Lal, C., Conti, M. and Hu, D., 2021. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, 115, pp.406-420.
- [13] Englbrecht, L. and Pernul, G., 2020, August. A privacy-aware digital forensics investigation in enterprises. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

- [14] McCorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S.F. and Hao, F., 2021. On secure e-voting over blockchain. *Digital Threats: Research and Practice (DTRAP)*, 2(4), pp.1-13.
- [15] Huang, J., He, D., Obaidat, M.S., Vijayakumar, P., Luo, M. and Choo, K.K.R., 2021. The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR)*, 54(3), pp.1- 28.
- [16] F. Rabia and A. Sara, "A survey on e-voting based on blockchain," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 6, pp. 528–536, 2021.
- [17] M. V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. 11, pp. 7653–7678, 2023
- [18] Shah, A., Sodhia, N., Saha, S., Banerjee, S. and Chavan, M., 2020. Blockchain enabled online-voting system. In *ITM Web of Conferences* (Vol. 32, p. 03018). EDP Sciences.
- [19] Anitha, V., Caro, O.J.M., Sudharsan, R., Yoganandan, S. and Vimal, M., 2023. Transparent voting system using blockchain. *Measurement: Sensors*, 25, p.100620. [20] K. Edison and B. Venansius, "Blockchain based electronic voting protocol," *Int. J. Comput. Applic.*, vol. 183, no. 28, pp. 1–7, 2022.
- [21] Holmes, C., 2022. How Blockchain Technology could support Democracy and E-Voting. *The Journal of The British Blockchain Association*.
- [22] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul.–Aug. 2018.
- [23] J. H. Ryu, P. K. Sharma, and J. H. Jo, "A blockchain-based decentralized efficient investigation framework for IoT digital forensics," *Electronics*, vol. 8, no. 7, p. 828, 2019.
- [24] ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*, Geneva: ISO, 2012.
- [25] U.S. Supreme Court, *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 1993.