electronics

MDPI

Review

Blockchain-Based E-Voting Systems: A Technology Review

Mohammad Hajian Berenjestanaki [1,*], Hamid R. Barzegar [1], Nabil El Ioini [2] and Claus Pahl [1,*]

[1] Faculty of Engineering, Free University of Bozen-Bolzano, 39100 Bolzano, Italy; hamidreza.barzegar@unibz.it

[2] School of Computer Science, University of Nottingham Malaysia, Semenyih 43500, Selangor, Malaysia; elioini.nabil@nottingham.edu.my

* Correspondence: mhajian@unibz.it (M.H.B.); claus.pahl@unibz.it (C.P.); Tel.: +39-0471-016000 (M.H.B.); +39-0471-016177 (C.P.)

Abstract: The employment of blockchain technology in electronic voting (e-voting) systems is attracting significant attention due to its ability to enhance transparency, security, and integrity in digital voting. This study presents an extensive review of the existing research on e-voting systems that rely on blockchain technology. The study investigates a range of key research concerns, including the benefits, challenges, and impacts of such systems, together with technologies and implementations, and an identification of future directions of research in this domain. We use a hybrid review approach, applying systematic literature review principles to select and categorize scientific papers and reviewing the technology used in these in terms of the above key concerns. In the 252 selected papers, aspects such as security, transparency, and decentralization are frequently emphasized as the main benefits. In contrast, although aspects like privacy, verifiability, efficiency, trustworthiness, and auditability receive significant attention, they are not the primary focus. We observed a relative lack of emphasis on aspects such as accessibility, compatibility, availability, and usability in the reviewed literature. These aspects, although acknowledged, are not as thoroughly discussed as the aforementioned key benefits in the proposed solutions for blockchain-based e-voting systems, whereas the considered studies have proposed well-structured solutions for blockchain-based e-voting systems focusing on how blockchain can strengthen security, transparency, and privacy, in particular, the crucial aspect of scalability needs attention.

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

check for updates

Citation: Hajian Berenjestanaki, M.; Barzegar, H.R.; El Ioini, N.; Pahl, C. Blockchain-Based E-Voting Systems: A Technology Review. *Electronics* **2024**, *13*, 17. https://doi.org/10.3390/electronics13010017

Academic Editor: Hamed Taherdoost

Received: 10 November 2023
Revised: 7 December 2023
Accepted: 13 December 2023
Published: 19 December 2023

1. Introduction

Blockchain technology has been recognized as a potential solution for secure and transparent e-voting systems. By leveraging the decentralization, immutability, and transparency of blockchain technology, e-voting systems can prevent fraud and manipulation, improve voter anonymity, and increase trust in the electoral process. Moreover, blockchain-based e-voting systems can reduce the cost and time associated with traditional voting systems.

Traditional voting mechanisms commonly rely on centralized entities, which can give the opportunity for vulnerabilities such as the tampering of results or electoral fraud. The decentralized and immutable features inherent in blockchain technology offer a promising solution to the vulnerabilities related to traditional and other e-voting approaches. Blockchain technology has the ability to create a tamper-proof and transparent platform for conducting e-voting. Blockchain-based e-voting systems provide secure, verifiable, and auditable voting procedures through the integration of cryptographic techniques and consensus protocols.

The growing interest in blockchain-based e-voting systems indicates the importance of a comprehensive and systematic evaluation of the current knowledge in this domain. One of the aims of this review is to identify the main benefits of e-voting systems based on blockchain technology through an in-depth review of the previous research. These benefits include heightened security, transparency, decentralization, and privacy. Additionally, we intend to identify the challenges and limitations that come with these systems, which include privacy and security concerns, scalability issues, and technical limitations.

Moreover, a comprehensive understanding of the technologies and implementations involved in blockchain-based e-voting platforms is imperative in order to evaluate their feasibility and functionality. Furthermore, this systematic review provides technical insight into common blockchain frameworks, consensus algorithms, and security and privacy-enhancing techniques used in these systems. In addition, we aim to conduct an examination of the impacts of proposed blockchain-based e-voting systems in the literature on various aspects of the voting process, including security, privacy, efficiency, and scalability.

Overall, the purpose of this review is to conduct an extensive review of the current state of the literature related to blockchain-based e-voting systems. We look into the benefits, challenges, technological aspects, impacts, and potential research and development areas in the context of e-voting systems using blockchain technology. We conduct a combined review method, employing the principles of systematic literature review to choose and classify scientific papers. Additionally, we examine the technology implemented in these with respect to the already mentioned key concerns. The evaluation follows the PRISMA guidelines [1], which guarantee a rigorous and transparent methodology for the synthesis of available research data. The PRISMA protocol (Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols) is a reporting guideline designed to aid researchers in the preparation and documentation of systematic review and meta-analysis protocols.

2. Voting System Types and Requirements

We first categorize the types of voting systems before defining relevant requirements for them.

2.1. Voting Systems

Voting systems have been combined with advancements in information technology, making them increasingly efficient and accessible. There are a number of voting system types that can be differentiated from a technical standpoint.

1. Traditional voting: the conventional method where voters either mark paper ballots manually or use mechanical lever machines. The ballots, whether marked remotely or at a polling station, are collected and counted by election officials. Within traditional voting, there are two main categories:
    - Paper-based voting: In this method, voters typically mark their choices on the ballot paper by hand next to the candidate or option they wish to vote for, and then the ballots are counted manually [2]. It can be further categorized into remote and on-site voting. Remote paper-based voting refers to the process of casting a vote by mail or other means of delivery, whereas on-site paper-based voting refers to the process of casting a vote in person at a polling station [3].
    - Mechanical lever machines: They were first used in the 1890s and are operated by the voter indicating their choice by pressing a lever next to the preferred candidate. Once the voter is finished, the voter pulls the large lever again, which causes the counters associated with their choice to be incremented by one and the machine prepared for the next voter [4].
2. E-Voting: A voting method that uses electronic devices to record, cast, or count votes. In general, e-voting systems can be divided into four subcategories, as follows:
    - Punch-card: Developed in the 1960s, utilized modified Hollerith cards where voters used a stylus to punch out chads corresponding to their candidate choices. After voting, the punched card was deposited in a ballot box. These cards were later counted using a card reader [2].
    - Direct Recording Electronic (DRE): An electronic system that presents ballots and records voter selections directly into computer memory. Voters interact

with DREs using push-buttons, touchscreens, or dials. Some DREs feature Voter Verified Paper Audit Trail (VVPAT) printers, allowing voters to confirm their choices on a paper record, which can be used for post-election audits or recounts [5].

- Optical scanning systems: Specialized computer hardware and software are used to read and interpret votes. Voters mark their choices on machine-readable ballots by filling in symbols next to their preferred candidates. Once marked, these ballots can either be scanned directly at the polling place or collected and scanned at a central location [6].
- Ballot-Marking Devices (BMDs): Presents ballots electronically, lets voters make selections, and then produces a human-readable paper ballot without storing the vote electronically. Introduced after the Help America Vote Act of 2002 to aid voters with disabilities, BMDs can either mark pre-existing ballots or print summaries, sometimes with barcodes or QR codes. From 2016 onwards, some areas expanded BMD usage to all voters, becoming more common in 2020 [7].
- I-voting: Internet voting denotes a subset of e-voting methodologies wherein ballots are transmitted and registered via the Internet [8,9]. Terms such as "remote e-voting", "mobile voting", and "online voting" are often used in the literature to describe these systems. All of the terms outlined above are, however, grouped under the broader conceptual framework of i-voting systems, which is itself an instance of an e-voting paradigm. Furthermore, Blockchain-based e-voting systems are a type of i-voting that relies on the internet by using a peer-to-peer computer network that employs blockchain technology to cast and count votes in an election [10–12].

2.2. Voting Systems Requirements

A requirement is a need or constraint on the software or system to be developed. We can distinguish the properties of these systems into functional requirements (FR) and non-functional requirements (NFR). According to [13–20], an e-voting system is required to comply with a number of requirements if considered as an alternative to traditional voting systems.

Based on the above references, we propose here a division of requirements into different categories, namely functional and non-functional non-security requirements on the one hand and security as a functional and non-functional requirement type on the other hand. Our categorization forms a structured base set of properties that we will refer to in the discussion of benefits, challenges, impacts, and future research directions later.

2.2.1. Non-Security Requirements

- Functional Requirements
  - User-Centric Voting Design: The concept that a voting system should be easy for all people to use. This means that it should have a user-friendly interface and show choices without giving any candidate an advantage.
  - Flexibility: It refers to the ability of the system to adapt to a variety of formats, languages, and voting ballots, making it compatible with different platforms and technologies. To provide a flexible and adaptable electronic voting experience, this phrase emphasizes adapting to changes, complying with deadlines, and permitting numerous ballot question types, including open-ended questions.
- Non-Functional Requirements
  - Equality: It assigns priority to equitable and consistent voter access, ensuring that regardless of the process of voting, all voters have equal voting rights and opportunities and receive the same information and opportunities.
  - Accessibility: This term highlights the importance of providing individuals with functional limitations or disabilities with the necessary access to vote, ensuring

  voters have undiscriminating access to the voting infrastructure, and enabling entities to have logical and/or physical access to the voting system.
  - Openness: For an e-voting system, the functioning of the system (hardware and software) should be transparent to citizens, and the people should be able to understand and verify how the voting system works.
  - Auditability: It refers to the necessity of being able to verify that all votes in the final election tally are precisely accounted for, along with having reliable and authentic election records with a (possibly) physical but always permanent audit trail that ensures voter secrecy.
  - Cost-effectiveness: It addresses the need for essentially affordable and reusable systems with implementation and maintenance costs that are acceptable and competitive with traditional voting methods.
  - Interoperability: In order to ensure smooth integration and compatibility with different components and technologies, it makes sure that voting system data are imported, exported, or reported in an interoperable format using widely accepted, openly available interfaces and communications protocols.

2.2.2. Security Requirements

- Functional Requirements
  - Authentication and eligibility:
    - Voter authenticity: requires voter identification based on the voter registration database and ensures that only eligible voters cast their votes.
    - Uniqueness: the voter can only submit a vote once, and the final result of that vote can never be altered.
    - Eligibility: guarantees that only legitimate voters are able to vote and that their identities are confirmed precisely.
  - Anonymity and secrecy:
    - Anonymity: the voter's identity remains unlinked to their vote, and personal information or identity should remain concealed.
    - Secrecy: ensuring that no one involved in the voting process can link a specific ballot to a particular voter, preserving voter anonymity; in addition, the content of their vote remains confidential.
  - Uncoercible ballot assurance:
    - Uncoercibility: the fundamental principle of an e-voting system is to prevent any external influence, coercion, or vote-selling, ensuring that voters cannot prove or reveal their voting decisions, thereby safeguarding the integrity of the voting process and obstructing attempts at manipulating or pressuring voters for electoral gain.
    - Non-valid voting capability: voters should be able to cast ballots that they know are invalid if they so desire without compromising the integrity of the election in any way.
- Non-functional Requirements
  - Integrity and reliability:
    - Data protection: guarantee that each vote is reliably recorded and remains tamper-proof, while also applying rigorous data protection measures to prevent unauthorized access to or manipulation of voting data.
    - System integrity: ensure resistance against security failures or vulnerabilities, the voting system needs to maintain its functionality by preventing reconfiguration during operation and using multiple levels of controls.
    - Reliability: ensure the system functions robustly without losing any votes, even in the presence of multiple failures, including those related to voting machines and network communication, and prevent malicious code or bugs,

thus providing voters with the utmost confidence in its secure and efficient operation under anticipated physical conditions.

- Detection and monitoring:
    - Testing: The principle that electoral authorities, political parties, and social organizations should have the ability to put the voting systems to the test to ensure they meet the established criteria. This testing process should be thorough and conducted by experts to evaluate and verify that the systems meet the required security standards.
    - Monitoring: record important activities through event logging mechanisms in a format suitable for automated processing while also generating, storing, and reporting error messages in real time as they occur during the voting process.
- Fairness: the importance of maintaining a fair voting environment by avoiding biased or misleading information, ensuring that the voting system does not provide evidence about any voter's intention before the end of the voting phase, and remaining neutral so that the system does not influence the eligible voter's intention during the voting process.
- Verifiability and accuracy: allowing voters and election officials, parties, and independent observers to verify that the votes are accurately recorded and counted, ensuring the system can securely record votes, enabling them to use control mechanisms accurately with direct control of ballot changes and selections, providing voters the ability to verify their intentions in the vote without alterations, and offering sound and independently verifiable evidence that each authentic vote is accurately reflected in the election results.
- Availability: the system's ability to remain consistently available to all eligible voters, protect against denial of service attacks, establish redundant communication paths, ensure continuous availability during the election, have alternative support and election sites ready in case of failures, maintain a minimum Mean Time Between Failures (MTBF), have updated backups readily available for disaster recovery, and protect sensitive information.

Integrating blockchain technology into e-voting can satisfy some of these requirements. However, we will see that multiple challenges remain to be addressed to establish a reliable and trustworthy voting system.

3. Background, Related Work, and Objectives

We introduce blockchain basics before summarizing related work on blockchain for e-voting. From this, we will identify gaps and define objectives for this review.

3.1. Blockchain Technology

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

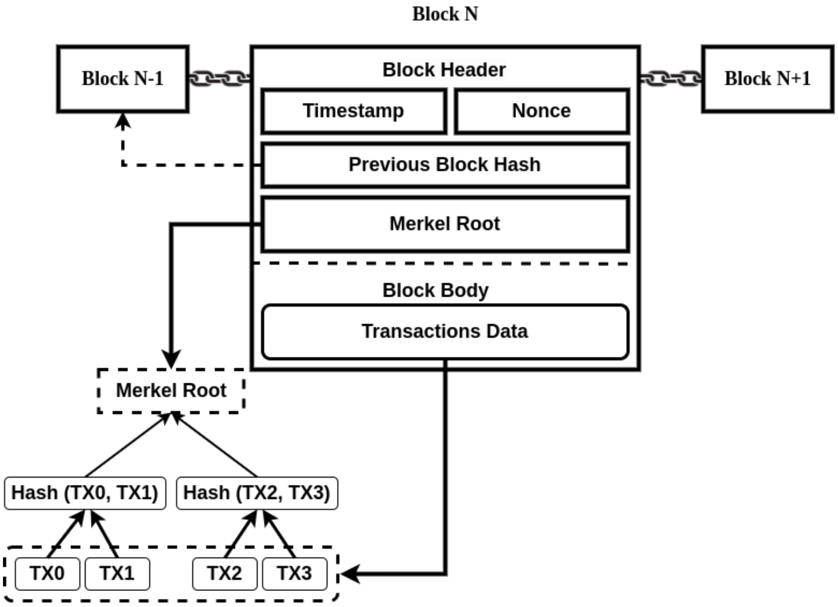

Figure 1. The blockchain structure.

3.2. *Blockchain Applications Across Domains*

Blockchain technology has emerged as a revolutionary trend across various domains, and whereas blockchain technology application in e-voting systems attracts interest in enhancing electoral integrity and transparency, it is equally valuable in other domains, each with distinct requirements and objectives. This section aims to provide a comparison and analysis of blockchain applications in different domains such as healthcare, financial services, supply chain management, cloud computing, education, and IoT (Internet of Things) [21], highlighting their parallels and contrasts with their use in e-voting systems.

- Blockchain in healthcare: In healthcare, blockchain is employed for secure data sharing, patient privacy, and interoperability among different healthcare systems [22]. Its application in healthcare shares some aspects of e-voting, such as the emphasis on data security and privacy. However, whereas blockchain in healthcare deals with continuous data flow and personal health records, in e-voting, it addresses the singular event of casting and recording votes.
- Blockchain in financial services: In financial services, blockchain technology revolutionizes transactions and trust mechanisms. Similar to e-voting, where blockchain brings transparency and verifiability to the voting process, in financial services, it introduces a new concept of trust and efficiency in transactions [23]. The key difference lies in blockchain's role in handling continuous financial transactions as opposed to the discrete event of voting.
- Blockchain in supply chain management: blockchain technology in supply chain management focuses on improving transparency, reducing fraud, and enhancing efficiency [24], whereas both supply chain management and e-voting systems benefit from blockchain's immutability and transparency, supply chain management uniquely utilizes blockchain for continuous tracking of goods and transactions, in contrast to the periodic nature of elections.

- Blockchain in cloud computing: In cloud computing, blockchain enhances security, data provenance, and creates new service models like Blockchain-as-a-Service (BaaS). The integration of blockchain in cloud computing shares similarities with e-voting in terms of improving security and reliability. However, the use cases in cloud computing are more varied and continuous, focusing on service enhancement and data integrity across diverse cloud-based applications [25].
- Blockchain in education: Blockchain technology in education mainly focuses on enhancing data security, credential verification, traceability, and record management. Through its immutable feature, blockchain technology not only ensures the integrity of educational records and certificates, consequently creating trust in academic credentials, additionally, it effectively secures and tracks the progress of academic patents, copyrights, and research innovations, significantly enhancing the management and protection of property within the educational domain [26–28]. Compared to its application in e-voting, where blockchain ensures vote integrity and transparency, in education, it serves to preserve academic achievements and automate administrative processes.
- Blockchain in IoT: Blockchain technology in IoT includes enhancing security, scalability, and trustworthiness in diverse applications like smart cities. The decentralized nature of blockchain in IoT addresses issues similar to those in e-voting, like ensuring security and scalability [29]. However, IoT applications deal with a broader range of data types and greater scalability challenges than electronic voting systems.

3.3. Related Work

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

Taş and Tanrıöver [30] reviewed in 2020 the state of blockchain-based voting research, identifying potential challenges and forecasting future directions. They presented a conceptual description of the desired blockchain-based e-voting application and conducted a review of 63 research papers. The articles that were examined were categorized into five main categories: general, integrity, coin-based, privacy, and consensus. They concluded that, whereas blockchain-based voting systems can prevent data manipulation and integrity issues, the most frequently highlighted issues are scalability, cost-effectiveness, authentication, privacy, and security in blockchain-based e-voting systems.

Jafar et al. [31] presented a conceptual description of a blockchain-based e-voting application in addition to an introduction to the blockchain's fundamental structure and characteristics in relation to e-voting. They mentioned that whereas blockchain systems could help solve some of the issues that currently affect election systems, the authors conclude that the most frequently mentioned issues in blockchain applications are scalability, user identity, transactional privacy, energy efficiency, immatureness, acceptableness, and political leaders' resistance.

In [32], Pawlak et al. indicated the remaining problems like security attacks, coercion, cost efficiency, and privacy that still need to be solved. The paper serves as a valuable resource for understanding the current trends and challenges in blockchain-based electronic voting systems.

Huang et al. [33] in 2021 provided a comprehensive review of blockchain-based voting systems, discussing their advantages, challenges, and technical innovations. They also provide a taxonomy of blockchain and identify key challenges in blockchain-based voting systems such as authentication, anonymity, coercion-freeness, and auditability.

Jafar and Ab Aziz in [34] emphasized the benefits and challenges of blockchain-based e-voting systems, providing useful details on probable future applications of this technology with regard to democratic processes. They demonstrated how blockchain technology offers security, transparency, and a reduced risk of fraud. However, they brought up issues with scalability, transactional privacy, and immaturity for these systems.

Devi and Bansal [35] provided a comprehensive review of the security requirements and potential threats in e-voting systems. They discuss various cryptographic techniques that can be used to secure these systems.

Benabdallah et al. [36] presented a comprehensive analysis of blockchain solutions for e-voting. They discussed the challenges faced by e-voting systems and how blockchain technology can address these issues. They also provide a comparison of several blockchain-based e-voting solutions, identifying their strengths and weaknesses. The paper also addressed the limitations and issues raised by this technology, such as scalability, unpredictable attacks, weakness of the identification system, new issues raised using blockchain technology, efficiency and decentralization, the digital divide, and vulnerabilities in smart contracts.

Jafar et al. in their systematic literature review [37] discussed the challenges and solutions for scalable blockchain-based electronic voting systems, in addition to anticipating future developments. To evaluate cost and time, they identified well-known proposals, their implementations, verification methods, and various cryptographic solutions in previous research. They analyzed performance parameters, the primary benefits and limitations of different systems, and the most common approaches to blockchain scalability.

In [38], Vladucu et al. provided a thorough overview of blockchain-based e-voting systems currently in use by various countries and companies, as well as those proposed for academic research. The authors discussed the challenges that blockchain e-voting systems face and identified areas for future research to improve their trustworthiness. Furthermore, they included a detailed explanation of the terminology used in blockchain-based e-voting systems, such as consensus algorithms, cryptography, and system characteristics.

Despite this number of reviews, a comprehensive and comparative analysis is still required, as we will justify below.

3.4. Implementations of Blockchain-Based E-Voting Systems

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

- Luxoft: Luxoft Holding Inc., a global IT service provider of technology solutions, is developing an e-voting infrastructure that will enable the world's first consultative vote on blockchain in Zug, Switzerland. Hyperledger Fabric was used to create an authorized blockchain that included a network, applications, and algorithms. In order to allow voters to cast their ballots, Zug's digital ID registration app based on Ethereum was authorized through uPort. Luxoft announces its intention to open source this technology and creates a Government Alliance Blockchain to encourage blockchain use in public institutions [39].
- Votem: A company specializing in election management, its main product is the CastIron platform. This platform is built on blockchain technology and offers several distinctive features, including a distributed database, immutability, permission-based access, and an audit trail. Votem has successfully handled over 13 million voters, serving both government elections and various associations in the United States and around the world. Notably, their track record boasts zero instances of fraud, compromise, attacks, or hacking, highlighting the security and reliability of their system [40].
- Voatz: A blockchain-based mobile voting tool that was launched in 2018 in West Virginia for overseas military voters participating in the 2018 midterm elections in the United States. Voatz includes biometric validation, such as fingerprints or retinal scans, so that voters validate their applicants and themselves on the application. A recent study found Voatz has major security flaws that allow attackers to monitor votes and edit or block ballots in large amounts [41].
- POLYAS: In the summer of 1996, Finland held the first POLYAS online election, with 30,000 voters participating in three languages. The company uses blockchain technology to offer an electronic voting system to the public and private sectors. Germany's

Federal Office for Information Security granted the first online election certification in 2016. The online voting system satisfies anonymity, accuracy, singularity, verifiability, and auditability. In Europe and the USA, several important companies employ POLYAS to manage their electronic voting systems [42].

- Polys: An online voting system that increases confidence in the voting process and results. Because it is based on blockchain technology, it is secure and transparent. Both the voting procedure and the results are immutable. Transparent cryptographic techniques are employed on the top of the blockchain to protect voter anonymity. Voters can check at any moment to ensure that their vote is valid and unmodified [43].
- DecentraVote: A blockchain-based solution for virtual meetings was originally developed by a team at the iteratec location in Vienna. DecentraVote uses a public Ethereum network based on Proof of Authority consensus with permissioned validator nodes. The smart contract constructed a Merkle tree of all voting rights on-chain, and the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) generated a proof for every voting right off-chain. DecentraVote does not address national political elections [44].

3.5. Research Gap and Objectives

Our systematic analysis of blockchain-based e-voting systems is guided by identified gaps in the current literature and specific objectives we aim to achieve. Despite ongoing research in this domain, existing studies often focus on the limitations of blockchain-based e-voting, lacking a comprehensive comparison with traditional and electronic voting systems in terms of benefits and challenges. The primary objectives of this systematic analysis are therefore:

1. To conduct a comprehensive comparison of blockchain-based e-voting systems against traditional and e-voting systems, focusing on understanding their relative benefits and challenges.
2. To review and analyze the concrete implementation techniques of blockchain in e-voting systems, identifying how they address existing challenges.
3. To provide the potential implications of blockchain-based e-voting systems for addressing existing challenges in the blockchain-based e-voting systems.
4. To establish an up-to-date roadmap for future research, emphasizing areas that require further investigation in the rapidly evolving landscape of blockchain-based e-voting.

This study aims to fill these gaps by offering a comprehensive and holistic review of blockchain-based e-voting systems. This involves an in-depth exploration of current challenges and potential areas for future research, thereby contributing to a more thorough understanding of blockchain technology's role in enhancing the integrity and efficiency of voting processes.

3.6. Contribution of the Review

To address the research gaps, this review conducts a comprehensive analysis of the existing literature on blockchain-based e-voting systems by, firstly, selecting papers using systematic literature review principles and, secondly, analyzing their technology aspects systematically. Specifically, the research aims to achieve the following objectives:

- Identify and analyze the benefits and challenges of blockchain-based e-voting systems in comparison to traditional voting and other e-voting systems, identifying the impact of blockchain-based e-voting systems on various aspects of the voting process.
- Explore the implementation technologies utilized in blockchain-based e-voting systems.
- Provide summarizing observations and recommendations for future research and development in this field.

In order to address the aforementioned objectives, the following research questions guide this systematic review:

- Benefits: What are the benefits of using blockchain technology in e-voting systems over other implementation approaches? The benefits are expressed in terms of requirements met by blockchain-based e-voting systems but not by other voting and e-voting types.
- Challenges: What are the challenges faced in implementing blockchain-based e-voting systems? These are expressed in terms of requirements that are already satisfied by other types of voting and e-voting systems but generally not yet met by blockchain-based e-voting systems.
- Impact: What are the impacts of proposed blockchain-based e-voting systems on different qualities? Impacts are expressed in terms of requirements that have been shown as satisfied (becoming a benefit of these) or not satisfied (becoming a challenge for blockchain-based e-voting systems).
- Technologies: what are the common technologies and implementations used in blockchain-based e-voting systems, including popular blockchain frameworks, consensus algorithms, security and privacy enhancing techniques?
- Future Research: based on the challenges identified and technologies reviewed, what future research and development directions should be explored in blockchain-based e-voting systems to enhance their functionality and quality?

Our results and observations aim to provide insights to legislators, researchers, and practitioners regarding the essential technical challenges that need to be tackled to establish widespread and secure blockchain-based e-voting systems. In addition, this study aims to provide guidance for future research by recognizing areas where research is lacking and indicating potential possibilities for future studies. Finally, this review shall provide insights into the potential solutions for implementing secure and ubiquitous blockchain-based e-voting systems, which can contribute to the practical implementation of such systems.

4. Methodology

This review follows the PRISMA protocol to ensure a transparent and rigorous review process and applies systematic literature review principles to selected papers. This systematic approach includes a structured review of the current literature on blockchain-based e-voting systems. The objective of this review is to provide a fair analysis of the available information using a systematic approach designed to minimize bias by following common selection, analysis, and validation procedures.

The hypothesis of this study is that by applying the distinct features of blockchain technology, such as decentralization, immutability, and transparency, it is possible to address the weaknesses and constraints related to traditional voting systems. This idea suggests integrating blockchain technology, and this hypothesis implies that this leads toward enhanced democratic procedures.

A search technique is used to discover relevant research, which includes utilizing precise keywords and concepts that relate to electronic voting, such as e-voting, i-voting, evoting, ivoting, electronic voting, internet voting, and election. Furthermore, the search approach encompasses blockchain-related terms such as blockchain, distributed ledger, and DLT. Boolean operators, in particular ("OR", "AND") are used to combine keywords and filter search results, ensuring that only papers that address both subjects are retrieved.

- Search query: *(evoting OR ivoting OR e-voting OR i-voting OR ((electronic OR internet) AND (voting OR vote OR election))) AND (blockchain OR "distributed ledger" OR DLT)*

The literature search was conducted using reputable databases (ACM, IEEE, Elsevier, Springer, and Scopus). The process of searching for relevant studies involves initially screening titles to identify potentially relevant ones. This is followed by a thorough review of the full text of the articles to determine whether they answer any of the research questions.

A number of exclusion and inclusion criteria can be established. Inclusion criteria are:

- Papers that are directly related to or contribute to the comprehension of blockchain-based e-voting systems are relevant to the title.
- Papers should be available in English to ensure accessibility and comprehension.

- Papers with an available full-text version, which allows for a comprehensive analysis and extraction of data.

Exclusion criteria are:

- To avoid repetition and ensure a unique set of papers, it is necessary to remove any duplicate titles.
- Exclude papers that are not written in English, as they can hamper comprehension and analysis.
- Exclude book chapters and focus on research articles and conference papers.
- To ensure the inclusion of valid and reliable research, papers that are officially retracted are excluded.
- Exclude papers if their topic does not align with the blockchain-based e-voting systems.

Figure 2 indicates the approach employed to conduct database analysis and, afterward, the inclusion and exclusion of publications for the purpose of our study.

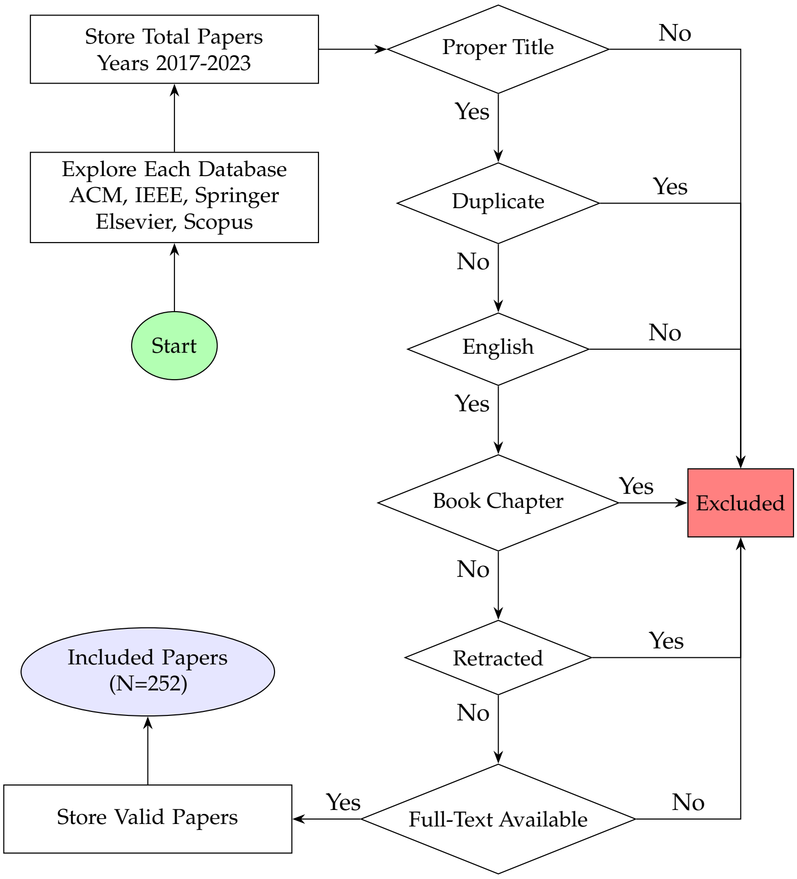

Figure 2. Procedure for database examination and paper inclusion.

The process of certainty assessment includes the evaluation of the level of certainty in the research outcomes. That confidence depends on the quality of the included studies and the cohesiveness of their results. High certainty indicates strong and reliable evidence, whereas low certainty indicates the need for further investigation or the existence of significant limitations in the currently available set of data. In order to ensure an efficient and rigorous assessment, separate reviewers are responsible for conducting an accurate assessment for each study that was randomly chosen. In cases where disagreements occur between the reviewers, these disagreements are resolved through broad consideration or, if determined essential, by requesting the perspective of an additional reviewer in order to attain a consensus.

5. Results—Benefits, Challenges, and Impacts

In this section, we present results derived from the selection process indicated earlier. Through the analysis of the data collected, our objective is to explore the research questions and construct findings from the outcomes of the systematic review. We identified the final number of publications from each database that should be included in the systematic review by applying these criteria to the corresponding databases. The results of this procedure are presented in Table 1.

Table 1. Overview of paper categories across databases.

Category	ACM	IEEE	Elsevier	Springer	Scopus	Total
Total	34	187	20	142	250	633
Inappropriate Title	18	80	0	30	2	130
Duplicate	0	1	9	42	176	228
Not English	0	2	0	0	2	4
Book Chapter	0	0	2	0	0	2
Retracted	0	0	0	0	1	1
Not Available	0	1	0	1	14	16
Included Papers	16	103	9	69	55	252

Figure 3 illustrates the publication trend of academic research literature that passed the inclusion and exclusion criteria, showing an increasing academic interest within this domain over time.

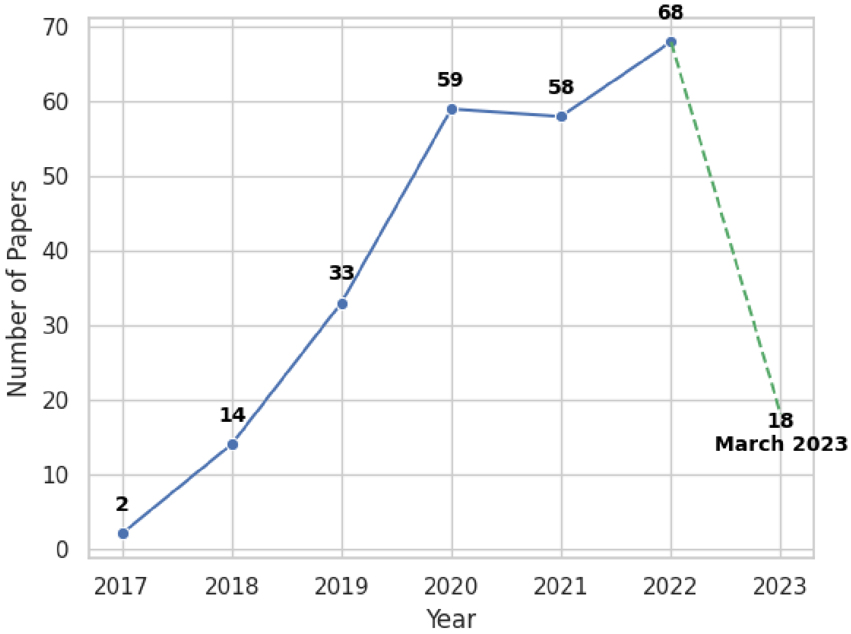

Figure 3. Publication trend in blockchain-based e-voting research.

We present the results for each of the research questions as follows:

- We address benefits, challenges, and impacts before looking at implementation technologies and summarizing future research in the following sections.
- For each, we comment on all properties mentioned in relation to the specific blockchain perspective.

- We also list the properties in the order of their frequency for the specific concern across the selected study papers, summarizing total occurrences and normalized numbers for better comparison.

5.1. Results—Benefits of Blockchain-Based E-Voting Systems

Various studies recommend blockchain-based e-voting systems due to their benefits. We compare here the benefits associated with blockchain-based e-voting systems with those of traditional (e-)voting systems, in terms of the requirements listed above for e-voting.

We categorize these benefits into major requirement categories, each further decomposed into several more detailed specific properties, if needed. In order to extract these benefit properties, we employed a hybrid strategy that includes both syntactic and semantic selection methods. We extracted the properties from relevant sections (Abstract, Introduction, and Related Work), thereby ensuring a targeted assessment of the content. These properties were identified as general benefits of blockchain technology and advantages offered by proposed blockchain-based e-voting systems, as discussed in the related work sections of the respective literature in comparison to conventional election systems.

We now list properties identified as benefits in the literature over traditional voting system types. We provide further comments on sources and explanations on each indicating how blockchains can achieve the benefits. Note that we order the benefits based on their frequency of occurrence across the selected study papers.

1. Security: a major benefit of blockchain-based e-voting systems, where subcategories highlight a unique perspective:
    - Integrity: holistic assurance of security aligned with the design [45].
    - Immutability: once a vote is recorded, it cannot be altered, ensuring the voting process's finality [46].
    - Durability: robust against data loss and ensures the permanency of stored data.
    - Stability: Resistance to disruptions or manipulations like hacking. Stability is enhanced by strong encryption systems, often inherent in blockchain technology [47].
    - Non-repudiation: a voter cannot dispute the validity of their cast vote [48].
2. Transparency: The blockchain-based e-voting system's inherent design encourages open voting, recording, management, and counting procedures. It facilitates independent audits [49] and ensures that all transactions (votes) on the blockchain are visible to all participants and can be independently verified.
3. Privacy: the ability of blockchain-based e-voting systems to protect voters' personal information and the confidentiality of their voting choices.
    - Anonymity: protecting a voter's identity [50].
    - Confidentiality (secrecy): the voters' choices are private, and outcomes are not presented ahead of time [51].
    - Untraceability: prevent the tracing of a vote back to its individual voter [50].
    - Pseudoanonymity: voters' actual identities are masked, but their voting activities are linked to unique identifiers similar to pseudonyms or addresses [52,53].
4. Verifiability: the ability to confirm that votes have been cast as intended, stored, and counted.
    - Public verifiability: the ability of all to verify the entire election process [54].
    - Individual verifiability: the ability for every voter to verify that their vote was precisely recorded and counted [54].
5. Auditability: ensure the voting process accuracy and truthfulness [55].
6. Accessibility: provide every eligible voter with an equal opportunity to participate in the voting process.
    - Availability: blockchains generally ensure that voters are able to cast their votes anytime within the stipulated period without facing any issue.
    - Broad turnout: technology allows substantial participation of eligible voters.

- Universal access: the ability of the system to be used effectively by all eligible voters.

7. Decentralization: Refers to the distribution of voting system authority, responsibility, and operations across a network compared to a central entity. This property is fundamental to blockchain technology and is essential for enhancing confidence among citizens by minimizing control of a potentially corrupt third party [36].
8. Usability: facilitate an extensive number of voters casting votes in accordance with their choices in an effective way while being satisfied with the process [56].
    - Simplicity: how simple and straightforward the system is to operate.
    - Understandability: clarity in system operation ensures that voters cast their votes as intended.
9. Efficiency: ability of an e-voting system to allow voters to cast votes in a swift and inexpensive manner.
    - Cost efficiency: The system's capacity to carry out voting operations at a cost that is affordable. This can involve a lower-cost setup and maintenance, material distribution, and human expenses.
    - Time efficiency: the system's ability to speed up voting and vote tallying.
    - Performance efficiency: the ability to handle massive amounts of data (votes), process, and count votes accurately, securely, and swiftly.
10. Trustworthiness: Secure, transparent, and fair system that ensures the accurate tracking and integrity of each vote. It is a balance of rigorous security measures, prompt results, and scalability, all of which are critical to preserving trust in the voting process [57].
    - Eligibility: only eligible voters can participate [58].
    - Fairness: election results are not exposed before the voting process finalizes [58].
    - Accountability: ability to determine whether or not the official vote record is inaccurate is facilitated by the blockchain [59].
    - Uniqueness: each eligible voter merits one and only one vote.
    - Accuracy: each vote is precisely accounted for, ensuring there is no modification, omission, or unauthorized inclusion [14].
    - Credibility: how much voters, politicians, and the general public trust and believe in the e-voting system.
    - Reliability: the system's consistency in performance through time ensures accurate, error-free function and availability [60].
11. Compatibility: ability of the e-voting system to operate in conjunction with various types of hardware, software, protocols, and legislation.
    - Adaptability: ability of an e-voting system to alter or adjust in order to accommodate various circumstances or necessities that may emerge [61,62].
    - Flexibility: ability to adapt to different frameworks, election types, voting methods, and voter interfaces.
12. Resistance to coercion: capacity of an e-voting system to shield voters from potential manipulations or coercions [36,63].

We enumerate in Table 2 the papers that mention the above properties as benefits of blockchain-based systems, ordered by the number of occurrences within the 252 selected papers. These properties are referred to as benefits either in the abstract, the introduction, or the related works sections of these papers.

Table 2. Distribution of papers mentioning the benefits of blockchain-based e-voting systems.

Benefit Category	No. of Papers	Normalized (%)
Security	224	88.89
Transparency	180	71.43
Decentralization	139	55.16
Privacy	96	38.10
Verifiability	85	33.73
Efficiency	67	26.19
Trustworthiness	63	25.00
Auditability	58	23.02
Accessibility	44	17.46
Usability	7	2.78
Compatibility	5	1.98
Resistance to Coercion	3	1.19

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Total Number of Papers}} \times 100$.

Blockchain-based e-voting systems offer first and foremost security, transparency, and decentralization, as mentioned in 224, 180, and 139 papers, respectively. Moreover, 96, 85, and 67 papers mention privacy, verifiability, and efficiency as significant benefits. Although less frequently discussed, trustworthiness, auditability, and accessibility also have significant advantages. The least frequently discussed factors are usability, compatibility, and resistance to coercion.

5.2. Results—Challenges in Blockchain-Based E-Voting Systems

Despite the properties of blockchain technology and the benefits it offers, these systems are not inherently applicable across all voting contexts due to some barriers. Our objective is an understanding of the obstacles and challenges associated with using blockchain technology for e-voting systems, specifically identifying properties that traditional e-voting systems have but blockchain-based ones do not.

As before, we arranged them into groups, ordered according to their frequency.

1. Privacy: It encompasses efforts to protect the secrecy of everyone who casts a vote, keep sensitive voter information from leaking out, and minimize the risk of tracking individual voters. However, ensuring privacy in e-voting causes challenges due to the conflicting objectives of auditability and transparency with privacy [64,65].
2. Security: It is a crucial aspect of blockchain-based e-voting systems, as it encompasses various measures to maintain the voting process's integrity, and availability. Defensive measures against cyber-attacks, Zero-Day exploits, and smart contract vulnerabilities are challenges for the blockchain security fundamental qualities. In [66], several types of attacks on blockchain such as hash-based attack, centralization attack, traffic attack, network level attack, injection attack, integrity attack, and private key leakage attack are discussed. It is necessary to mitigate such threats and prevent fraudulent use or disclosure of sensitive voter data without authorization [67,68].
3. Scalability: As the number of participants and transactions increases, it becomes crucial to maintain high performance and throughput. The inherent characteristics of blockchain, such as the need for consensus among distributed nodes and the necessity of storing every transaction on the blockchain, present scalability challenges. The decentralized nature of blockchain can lead to slow transaction processing times and increased resource requirements. In order to reach scalability in blockchain-based e-voting systems, it is necessary to address transaction throughput, network bandwidth, and data storage capacity. To ensure that blockchain-based e-voting

systems can accommodate an increasing number of participants and transactions while maintaining the security and decentralization nature of blockchain, scalability concerns need to be dealt with [36,69].

4. Technical aspects: various implementation challenges for blockchain-based e-voting systems arise, encompassing algorithm restrictions, technical complexity of consensus algorithms, hardware platform compatibility, integration with existing systems, complexity of technology, interoperability (including protocol interoperability), technical limitations, transparency in certain implementations, implementation challenges, complexity of implementation, complex design requirements, automating configuration, and limitations of authentication schemes [70–73].
5. Efficiency and feasibility: This encompasses various factors, including computation resource efficiency, energy consumption, performance efficiency, cost efficiency, and feasibility. Computation resource efficiency includes minimizing computational overhead associated with the consensus protocol and effectively allocating resources to handle the increasing workload. For minimizing the operational costs of blockchain-based e-voting systems, energy efficiency is crucial. The development of energy-efficient protocols, algorithms, and hardware can help reduce energy consumption [31,74–76].
6. Acceptability and immaturity: It refers to the level of trust and confidence stakeholders have in blockchain-based e-voting systems. To address this, it is necessary to achieve security, privacy, transparency, and reliability, thus building an environment that encourages the acceptance of blockchain-based e-voting systems. The immaturity of blockchain technology in e-voting leads to a lack of real-world experiments, extensive testing, stakeholder engagement, and comprehensive evaluation [11,34,38,77,78].
7. Usability: it is necessary to achieve a balance between a user-friendly interface and the security and integrity of the voting process [38,79].
8. Coercion freeness: it refers to challenges to protect voters from external pressures or coercive influences that could compromise their right to vote freely [33,64,80].
9. Accuracy and reliability: Ensuring accuracy is paramount to guaranteeing that each vote is recorded and counted correctly, without any errors or omissions. Blockchain technology has the potential to enhance accuracy by creating a transparent and tamper-proof record of all voting transactions. However, to achieve a reliable and credible e-voting system, it is crucial to design a protocol that is fair, prevents double-voting, and avoids reliance on a central authority [81,82]. By developing and implementing robust cryptographic techniques, secure consensus algorithms, and comprehensive auditing mechanisms, blockchain-based e-voting systems can enhance accuracy, reliability, and credibility, ensuring the integrity and fairness of the electoral process [83,84].
10. Accessibility: Access to voting opportunities is a fundamental principle. Limited internet access in certain locations presents a significant challenge to accessibility in blockchain-based e-voting systems. Providing a method such as offline voting that is consistent with the overall system is complex [85–87].
11. Regulatory and governance: Implementing blockchain-based e-voting systems requires adherence to legislation as well as adjusting to a constantly evolving legal landscape. Addressing regulatory and legal difficulties entails managing jurisdictional requirements, data privacy legislation, and electoral laws, and ensuring legal standards are challenging.

    Furthermore, ensuring interoperability and compatibility across different e-voting systems and platforms needs to establish common standards and protocols for blockchain-based e-voting, as it can provide seamless integration and collaboration among various stakeholders. Addressing regulatory and governance challenges, including the establishment of standards, is a significant challenge for blockchain-based e-voting systems [88–90].
12. Decentralization and consensus mechanisms: The distribution of authority, control, and decision-making power throughout the e-voting process, from registration to

result calculation, is referred to as decentralization at all stages. Achieving the appropriate level of decentralization is a challenge for ensuring transparency, avoiding central points of failure, and increasing system trustworthiness. Furthermore, for reaching a proper level of decentralization, selecting a suitable consensus mechanism to securely and quickly validate and confirm transactions is a related issue [91]. Consensus techniques are crucial for assuring network participant agreement and defending against fraudulent operations. Choosing the best consensus mechanism necessitates careful consideration of variables such as scalability, security, energy efficiency, and the specific needs of the e-voting system [92,93].

In Table 3, we provide a summary of papers that identify the above features as challenges of blockchain-based e-voting systems. These items are selected from various sections, primarily the Abstract, Introduction, and Related Works, applying a hybrid technique combining syntactic and semantic selection techniques. This approach signifies that these features are acknowledged either as inherent challenges to blockchain technology or as specific issues introduced by proposed blockchain-based e-voting systems.

Table 3. Distribution of papers mentioning the challenges of blockchain-based e-voting systems.

Challenge Category	No. of Papers	Normalized (%)
Privacy	108	42.86
Security	104	41.27
Scalability	87	34.52
Technical Aspects	40	15.87
Efficiency and Feasibility	36	14.29
Acceptableness and Immaturity	32	12.70
Coercion Freeness	21	8.33
Usability	18	7.14
Accuracy and Reliability	16	6.35
Accessibility	8	3.17
Regulatory and Governance	8	3.17
Decentralization and Consensus Mechanisms	3	1.19

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Total Number of Papers}} \times 100$.

Some advancements addressing the challenges in blockchain-based e-voting systems can be observed.

1. Enhanced privacy: Recent advances in cryptographic techniques, such as zero-knowledge proofs and homomorphic encryption, blind signatures, ring signatures, and mix networks, have significantly enhanced the privacy aspect of blockchain-based e-voting systems. These methods enable the verification of votes without revealing the voter's private information, simultaneously balancing privacy with the necessary transparency and auditability.
2. Enhanced security: In response to security challenges, there have been significant developments in both blockchain architecture and cryptographic defenses. In addition, enhanced consensus algorithms, like Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT), have been implemented to counteract various blockchain-specific attacks. Additionally, the integration of advanced security protocols and mechanisms could become standard methods, improving these systems against cyber threats.
3. Scalability improvement: To address scalability issues, innovative solutions such as off-chain transactions, sharding, optimized consensus protocols, and layer-2 scaling solutions like Lightning Networks have been introduced. These technologies have

proven effective in increasing transaction throughput, allowing for more scalable e-voting systems.

4. Technical improvement: to address the technical complexities, approaches for optimizing the chosen consensus algorithm for efficiency, simplifying technical complexities, ensuring hardware platform compatibility, ensuring interoperability with existing systems and protocols, implementing automation for configuration, and constantly seeking feedback for refinement are some of the steps taken or that need further research to evolve the system.
5. Energy and cost efficiency: The shift towards more energy-efficient consensus mechanisms, like Delegated Proof of Stake (DPoS), has notably reduced the operational costs and energy consumption of blockchain networks. Further, ongoing research into optimizing blockchain infrastructure and in other layers (on-chain and non-chain) can lead to the economic feasibility of blockchain-based e-voting systems.
6. Increasing acceptability: Experimental projects and real-world evaluations can play an important role in building trust and demonstrating the viability of blockchain-based e-voting systems. By developing educational resources and engaging stakeholders, this technology can be accepted and understood by a broader audience.
7. User-friendly interfaces: Significant efforts can be made to develop interfaces that are both simple for voters and secure. These interfaces often include guiding instructions and reliable verification mechanisms to ensure a seamless and secure voting experience.
8. Provide coercion-resistant: To achieve this aim in a blockchain-based e-voting system, there are several methods in the literature: implementing strong end-to-end encryption, utilizing zero-knowledge proofs, enforcing receipt-freeness, using blind signatures, employing multi-step authentication, securing physical components, maintaining a transparent blockchain, implementing auditing and monitoring, and ensuring user-friendly interfaces. Together, these strategies ensure the integrity of the voting process, prevent coercion, and enable voters to participate freely and without fear of repercussions.
9. Accuracy and reliability enhancements: By adopting robust cryptographic techniques and providing a decentralized ledger with transparent, auditable transactions, accuracy and reliability can be enhanced. By using identity verification mechanisms and smart contracts to ensure fairness, double voting can be prevented, whereas decentralized oracles and on-chain storage of critical data can reduce reliance on centralized sources. Consensus mechanisms and regular security testing are key to overall reliability. In all these cases, blockchain-based e-voting systems become more accurate and reliable.
10. Improved accessibility: Efforts to expand accessibility include developing offline voting mechanisms and protocols in mobile voting apps and establishing remote voting centers in areas with limited internet access. These centers can be equipped with the necessary technology to ensure that mobile voting applications are accessible to voters. Provide features for people with disabilities, such as screen readers, voice-guided interfaces, etc. Consider having backup plans in place in case of technical failures or disruptions in areas with limited internet access.
11. Regulatory compliance and governance: establishing legal frameworks and standards is a key focus, ensuring that these systems comply with the regulatory challenges associated with blockchain-based e-voting.
12. Decentralization and consensus mechanism optimization: customized consensus mechanisms that adjust to the unique requirements of e-voting systems can enable achieving a balance between speed, security, and decentralization.

5.3. Results—Impacts of Blockchain-Based E-Voting Systems

In this section, we discuss the identified impacts of different proposed systems. This extraction process involves retrieving the data from various sections of the studies, including evaluation and results, discussion, and conclusion. The impact categories follow those for benefits and challenges stated in the preceding sections.

Table 4 presents a quantitative description of the impacts of proposed systems across various categories.

The attributes that have the most notable relative impacts are security (41.67%), efficiency (34.52), and privacy (18.65%). These three attributes play a key role in maintaining the integrity, performance, and secrecy of the e-voting procedure.

Table 4. Impacts of proposed systems in various categories.

Impact Category	No. of Papers	Normalized (%)
Security	105	41.67
Efficiency	87	34.52
Privacy	47	18.65
Reliability	35	13.89
Scalability	27	10.71
Verifiability	22	8.73
Usability	16	6.35
Transparency	14	5.56
Accessibility	13	5.16
Resistance to Coercion	10	3.97
Auditability	8	3.17
Acceptableness	3	1.19

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Total Number of Papers}} \times 100$.

5.4. In-Depth Analysis of Results

The analysis, particularly focused on the data presented in Sections 5.1 and 5.2 and their respective tables, revealed insights. Section 5.1, as indicated by its table, shows broad agreement on blockchain's role in enhancing security and integrity, with a majority of the papers emphasizing these advantages. This trend emphasizes blockchain's potential to increase trust and participation in electoral processes. Furthermore, Section 5.2 indicates scalability and voter privacy as leading concerns, with a significant percentage of studies highlighting these issues. This suggests an urgent need for developing scalable blockchain architectures and integrating advanced privacy-preserving techniques in e-voting systems.

Section 5.3, supported by its respective table, further enriches our understanding. A notable percentage of studies in the impacts section report significant improvements in the efficiency and speed of voting processes facilitated by blockchain technology. This highlights blockchain's role not just in security, but also in optimizing and automating electoral procedures.

6. Results—Technologies and Implementation of Blockchain-Based E-Voting Systems

E-voting systems based on blockchains use a variety of concepts and technologies to enable secure and trustworthy elections. Blockchain frameworks like Ethereum and Hyperledger Fabric, consensus algorithms like Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance, and privacy-enhancing techniques like homomorphic encryption and zero-knowledge proofs are among these technologies. Furthermore, authentication mechanisms such as biometric verification and identity management systems are critical in confirming voter legitimacy and maintaining the voting system's integrity.

In this section, we present a technology summary in five broader categories:

- Blockchain platforms;
- Consensus algorithms;

- Security and privacy techniques;
- Authentication and identity verification techniques;
- Other techniques (cryptography, development, testing).

6.1. Blockchain Platforms

The blockchain frameworks and technologies domain includes a variety of platforms and tools used in the design and implementation of blockchain-based systems. Blockchain frameworks such as Ethereum, Hyperledger Fabric, Bitcoin, and Multichain provide the foundation required for developers to create decentralized apps.

Figure 4 includes a range of widely used blockchain frameworks, including the proposed blockchain e-voting systems context. In all of the frameworks mentioned, Ethereum is the most popular choice, as evidenced by the 34.91% portion of utilized frameworks. Although particular papers mentioned specific frameworks, there are further studies, and no specific blockchain framework is explicitly stated. Instead, they proposed customized systems that are based on the general concept of blockchain technology.

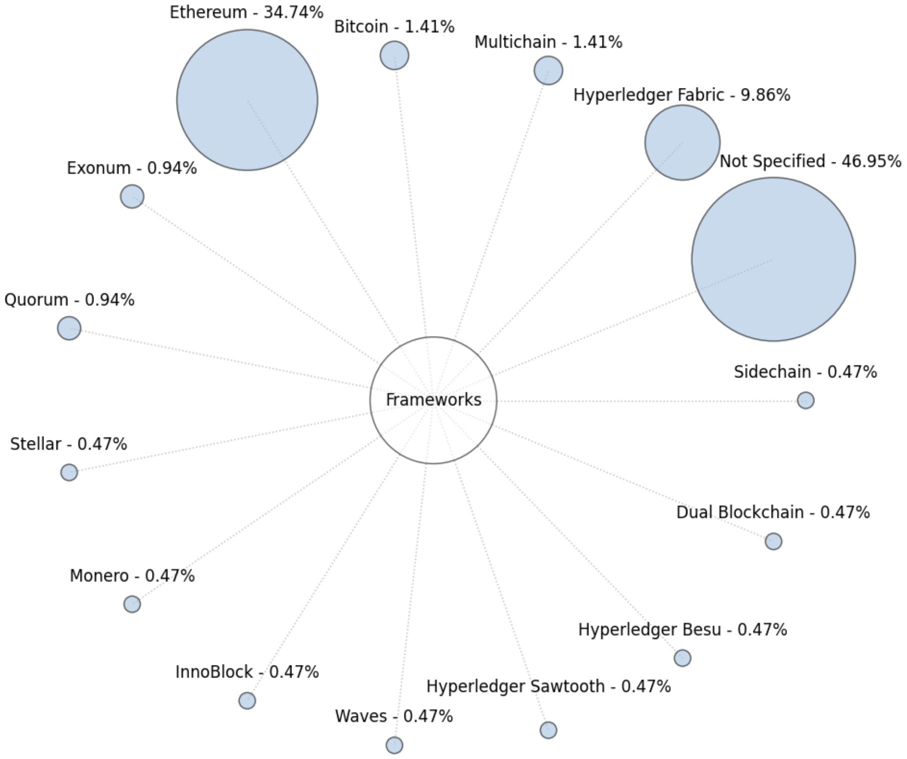

Figure 4. Blockchain frameworks distribution of proposed blockchain-based e-voting systems.

6.2. Consensus Algorithms

The consensus algorithms that were mentioned are illustrated in Table 5. Although a substantial number of papers do not explicitly mention the consensus algorithm used, it is reasonable to assume that for most proposed systems that use Ethereum as their framework, the consensus algorithm can be considered as Proof of Work (PoW). The following and most substantial protocol is referred to as "Proof of Work (PoW)", resulting in approximately 5.2% portion of used consensus algorithms. In the following, we provide a brief definition for each of these consensus algorithms:

Table 5. Adoption of consensus algorithms in blockchain-based e-voting systems (if mentioned).

Consensus Algorithm	No. of Papers	Normalized (%)
Proof of Work (PoW)	11	100
Proof of Stake (PoS)	6	54.55
Proof of Authority (PoA)	6	54.55
Byzantine Fault Tolerance (BFT)	6	54.55
Practical Byzantine Fault Tolerance (PBFT)	4	36.36
Raft consensus algorithm	3	27.27
Delegated Proof of Stake (DPoS)	2	18.18
Crash Fault Tolerant (CFT)	1	9.09
Stellar consensus protocol (SCP)	1	9.09
Hybrid (PoC combined with PoS)	1	9.09

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Max Number of Papers in any Category}} \times 100.$

1. Proof of Work (PoW): Commonly used consensus algorithm, including Bitcoin. It is a technique that requires members, known as miners, to solve computationally demanding puzzles in order to secure the network and validate transactions [94].
2. Proof of Stake (PoS): a consensus process in which block creators (validators) are selected depending on their wealth or stake in the network, and their possessions act as a guarantee, inciting honesty and network security [95].
3. Proof of Authority (PoA): A consensus approach used with authorized entities or individuals as block validators. Unlike other consensus methods, PoA is based on a predetermined set of reliable validators who proved their credibility in the network [96].
4. Byzantine Fault Tolerance (BFT): A technique that obtains agreement among participants even in the presence of malfunctioning or malicious nodes. BFT consensus algorithms are designed for dealing with Byzantine failures, in which nodes behave unexpectedly and inconsistently [97].
5. Practical Byzantine Fault Tolerance (PBFT): A specific algorithm that provides BFT in distributed systems. A leader node is selected to propose a block of transactions, which the other nodes, called replicas, validate and agree on [98].
6. Raft consensus algorithm: Developed for fault-tolerant log management to handle replicated logs. The Raft algorithm elects a leader to replicate logs across all nodes. The leader logs client requests and replicates them to cluster nodes. After a majority of nodes acknowledge log entries, the leader commits them and informs the followers [99,100].
7. Delegated Proof of Stake (DPoS): A PoS consensus algorithm variant. DPoS relies on the PoS concept by delegating block creation and validation commitments to a selected number of trusted delegates elected through vote [101].
8. Crash Fault Tolerant (CFT): A type of consensus method established for distributed systems that can endure crash failures, in which nodes in the system stop responding or crash. In it, a simple majority voting method is frequently used, in which nodes vote on the proposed state or decision. The system considers a value or decision to be acceptable if a majority of nodes agree on it [102].
9. Stellar consensus protocol (SCP): It combines the principles of federated agreement and Byzantine agreement to offer the Stellar network with a decentralized and fault-tolerant consensus mechanism. It enables nodes to agree on the state of the blockchain and keep the security and integrity of system transactions [103].
10. Hybrid (Proof of Credibility (PoC) combined with Proof of Stake (PoS): The weight of each vote in the consensus process is determined by the value of the tokens staked by

validators through the Proof of Stake (PoS) mechanism. The method brings Proof of Credibility (PoC) to address the issue of coin collapse in the PoS consensus mechanism. This combination of PoS and PoC is a safe hybrid structure that ensures full security when deployed in e-voting systems [104].

6.3. Security and Privacy Techniques

The use of blockchain-based e-voting systems needs to take security and privacy into consideration. Since it is decentralized and transparent, blockchain offers the possibility to boost the trustworthiness and credibility of e-voting systems. The use of security and privacy techniques in blockchain-based e-voting systems could assist in alleviating concerns about vote tampering, manipulation, and privacy violations.

Table 6 shows the number of studies that deploy security and privacy techniques. Data collection covers a broad spectrum of concepts and techniques. We list the number of publications and a normalized value in order to indicate the magnitude relative to other techniques.

The acronyms for each technique are explained in the listed discussion below. The zero-knowledge proofs (ZKPs) technique was referenced in a majority of studies. In addition, homomorphic encryption, blind signature, and ring signatures have been subject to a moderate degree of exploration. Several techniques, such as mix networks, time-lock encryption, machine learning, circle shuffle, and multi-signature schemes, were briefly discussed in a few publications.

Table 6. Distribution of security and privacy techniques in blockchain-based e-voting papers (if mentioned).

Technique	No. of Papers	Normalized (%)
ZKP	24	100
HE	24	100
BS	16	66.67
RS	13	54.17
SS	3	12.50
QKD	2	8.33
MN	2	8.33
TLE	2	8.33
ML	2	8.33
CS	1	4.17
RoPO	1	4.17
PMS	1	4.17
BC	1	4.17
DP	1	4.17
PB	1	4.17

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Max Number of Papers in any Category}} \times 100.$

As for the consensus protocols, we provide an overview of each of the techniques.

1. Zero-Knowledge Proofs (ZKPs): a cryptographic technique that enables one party to prove to another party the truthfulness of a statement or claim without disclosing any extra information [33,105].
2. Homomorphic Encryption (HE): a cryptographic technique that facilitates computations to be executed on encrypted data without the need for decryption [106–108].
3. Blind Signature (BS): a cryptographic method that enables a party to receive a valid signature on a message without disclosing the message's contents to the signer [109].

4. Ring Signatures: A cryptographic technique that offers anonymity and unlinkability to the signer within a group (ring) of potential signers. In the context of cryptographic protocols, a ring signature allows the signer to generate a signature on a specific message, thus convincing the verifier that the message was signed by an entity within a specific group while at the same time obscuring the true identity of the singer [110].
5. Shamir's Secret Sharing Scheme (SS): a cryptographic method that enables the division of a secret into multiple shares that are distributed among participants [92].
6. Quantum Key Distribution (QKD): a method of establishing secure cryptographic keys between two parties that makes use of the concepts of quantum physics [111,112].
7. Mix Network (MN): This technique is used to protect the privacy of voters and the secrecy of votes. Through serving as a channel between voters and the authority responsible for counting the votes [113,114].
8. Time-lock encryption (TLE): in this technique, a time-based delay is added to the encoding of encrypted data [114].
9. Machine Learning (ML): By integrating machine learning and blockchain technology, along with deep learning algorithms, significant enhancements can be achieved in biometric ID authentication. This involves utilizing machine learning methods to analyze facial features and verify the identities of users [84,115].
10. Circle Shuffle (CS): this method relies on a circular arrangement of votes, wherein each vote is assigned to a particular place in the circular structure [92].
11. Reputation-Based PayOff algorithm (RoPO): an incentive mechanism that is used in different decentralized systems to motivate players based on their reputation or performance history [116].
12. Proxy Multi-Signature Scheme (PMS): a variant of the common multi-signature method that includes the idea of a proxy or delegate to make signing on behalf of multiple individuals [117].
13. Bit Commitment (BC): a cryptographic technique in which one party (the committer) makes a commitment to another (the verifier) about a value without initially disclosing that value to the verifiers until the committer decides to reveal the committed value at a later time [118].
14. Differential Privacy (DP): It intends to maintain voters' sensitive data private while still allowing effective aggregate voting data analysis. It provides a structure for protecting voters' anonymity by adding random noise or perturbations to the data in a controlled manner [119].
15. Provenance-Based solution (PB): this solution involves tracking the origin and transformations of data (provenance) within the blockchain [120].

6.4. Authentication and Identity Verification Techniques

In blockchain-based e-voting systems, reliable authentication and identity verification is important to protect the integrity and security of the voting process. Authentication and identity verification in blockchain-based e-voting systems play an essential duty in satisfying various important objectives, such as ensuring voter eligibility, preventing fraud, and maintaining vote secrecy [121,122].

1. Biometric authentication: This method uses an individual's unique characteristics to validate their authenticity. These qualities can include fingerprints, facial recognition, iris or retina patterns, and even voice.
2. OTP (One-Time Password): a password that can only be used for one login session or transaction, often used to give a higher level of protection to sensitive transactions or systems [123,124] .
3. Aadhaar ID verification: the Unique Identification Authority of India (UIDAI) issues Indian residents a 12-digit Aadhaar number based on the resident's self-portrait, ten fingerprints, and two iris scans [125,126].

4. Multifactor authentication: this is the safety mechanism that requires multiple authentication methods from different categories to validate a user's identity for a login or other transaction.
5. Multi-step authentication: a security procedure that requires a user to provide extra evidence of identification when an additional level of assurance is required.
6. PKI-based X.509: PKI-based X.509 is a widely adopted standard that outlines how public key certificates are structured [127,128].
7. Unique IDs based on hash values: this method entails creating a unique identifier by applying a hash function to the biometric data, name, and date of birth of the voters [129].

Table 7 summarizes the distribution of authentication approaches utilized in different research papers. According to the results, the biometric authentication approach is frequently addressed across different studies.

Table 7. Distribution of authentication and identity verification techniques in blockchain-based e-voting papers (if mentioned).

Technique	No. of Papers	Normalized (%)
Biometric Authentication	27	100
Aadhaar ID Verification	7	25.93
OTP (One-Time Password)	6	22.22
Multifactor Authentication	3	11.11
Multi-Step Authentication	3	11.11
PKI-based X.509	2	7.41
Unique Hash IDs	1	3.70

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Max Number of Papers in any Category}} \times 100$.

6.5. Other Concepts

We identified several key concepts that deserve further consideration during the development and implementation of blockchain-based e-voting systems. These concepts address areas such as

- Cryptography techniques;
- Choice of development environments for smart contracts;
- Utilization of testing and benchmarking tools.

Table 8 categorizes them and provides relevant tools, environments, and techniques. This table serves as guidance for future research and facilitates exploration in the advancement of blockchain-based e-voting systems.

Table 8. Key concepts in blockchain-based e-voting systems.

Category	Tool	Description
Smart Contract Development and Execution	Solidity	Programming language for writing smart contracts on various blockchain platforms.
	Remix	A popular web-based development environment and IDE (Integrated Development Environment) specifically designed for writing, testing, and deploying smart contracts on the Ethereum blockchain.
	RIDE language	A specific language used for developing decentralized applications (DApps) on the Waves blockchain.

Table 8. *Cont.*

Category	Tool	Description
Smart Contract Development and Execution	Chaincode	Smart contract code written in Hyperledger Fabric for executing transactions.
	Truffle	Development framework for Ethereum smart contracts, providing testing and deployment.
	Hyperledger Composer	Framework for building blockchain applications and smart contracts on Hyperledger.
Blockchain Development and Testing Tools	Ganache	Personal Ethereum blockchain for local development and testing of smart contracts.
	Hyperledger Caliper	Benchmarking tool for measuring the performance of blockchain systems.
Performance Testing	Gatling Performance tool	A load testing tool used to simulate and measure the performance of systems, including blockchain-based applications.
Monitoring and Visualization	Grafana Monitoring tool	A tool used for monitoring and visualizing various metrics and data from systems, including blockchain networks.
Blockchain Interaction	Metamask	A browser extension that allows users to interact with the Ethereum blockchain, manage wallets, and execute transactions.
Cryptography	SHA	A family of cryptographic hash functions used for data integrity verification and password hashing.
	Chameleon hash	A type of hash function that allows for the creation of “trapdoor” information, enabling efficient collision generation.
	Advanced Encryption Standard (AES)	A widely-used symmetric encryption algorithm. It operates on fixed-size blocks of data and supports key lengths of 128, 192, and 256 bits.
	ElGamal cryptosystem	An asymmetric encryption algorithm based on the discrete logarithm problem.
	Paillier cryptosystem	An asymmetric encryption algorithm that allows for homomorphic operations, such as encrypted data manipulation.
	Cryptography over an elliptic curve	Encryption schemes based on elliptic curve mathematics, offering efficient and secure asymmetric encryption.
	RSA-based Public Key	A reference to the RSA encryption algorithm and key generation, which involves the use of a public key and a private key pair.
	RSA digital signature	A signature algorithm that utilizes the RSA encryption scheme for signing and verifying digital signatures.
	ECDSA (Elliptic Curve Digital Signature Algorithm)	A widely-used digital signature algorithm based on elliptic curve cryptography.

Table 8. *Cont.*

Category	Tool	Description
Cryptography	Schnorr signature	A digital signature algorithm known for its simplicity and security, offering efficient signature generation and verification.
	Lattice	A mathematical structure used in lattice-based cryptography, which relies on the hardness of certain lattice problems for security.
	SM2	The Chinese national standard introduced the SM2 algorithm, which utilizes a specific 256-bit elliptic curve for Elliptic Curve Diffie–Hellman key agreement and signature. This version incorporates functionalities for both signature generation and verification [130].
	SM9	It was issued by the Chinese State Cryptographic Authority and utilized for identity-based cryptography. It includes three components: a digital signature algorithm, an identity encryption algorithm, and a key agreement protocol [131].

6.6. Analysis of Results

This study reviewed a variety of blockchain platforms in Section 6.1, including Ethereum, Hyperledger Fabric, Bitcoin, and Multichain, each offering unique capabilities crucial for e-voting systems. Platforms like Ethereum are notable due to their smart contract functionality, which allows the creation of complex voting protocols, thus enhancing security and transparency. The choice of platform plays a critical role in determining the scalability, security, and flexibility of the e-voting system [132].

In Section 6.2, we analyzed the consensus mechanisms employed in the blockchain platforms, which are fundamental to the integrity and reliability of e-voting systems. Algorithms such as Proof of Work and Proof of Stake each bring different strengths and trade-offs in terms of security, energy efficiency, and processing speed. For e-voting systems, particularly on a national scale, selecting an appropriate consensus algorithm is critical, as it directly influences the system's ability to handle plenty of votes securely and efficiently while also preserving voter privacy.

The findings in Section 6.3 indicated the importance of incorporating advanced security and privacy techniques in e-voting systems. Techniques like homomorphic encryption and zero-knowledge proofs play a major role in ensuring that a voter's anonymity is maintained without compromising the transparency and verifiability of their vote. Implementing these techniques is essential for improving public trust in the electoral process. Furthermore, in Section 6.4, this study indicated the significance of methods such as biometric verification and identity management systems in maintaining the integrity of the voting process. These methods are crucial for preventing unauthorized access to the voting system, ensuring that each vote cast is legitimate, and preserving the principle of only one vote for one eligible person.

Lastly, in Section 6.5, the role of additional concepts like cryptographic development and thorough testing methods and tools cannot be neglected. As blockchain technology and cybersecurity threats continue to develop, continuously advancing cryptographic techniques and meticulous monitoring and testing tools are essential for ensuring the security and reliability of e-voting systems.

7. Discussion and Outlook

Many papers provide a discussion of current limitations and suggestions for future research. We summarize both non-functional and functional properties directly extracted from the selected studies, but we also take into account the technology concerns from the previous section.

In the second part of this section, we provide some observations on the different aspects—benefits, challenges, impact, and also identified future research—that we gained by comparing the answers across those aspects, checking them for consistency, and emerging patterns and trends.

7.1. Results—Suggested Roadmap for Blockchain-based E-Voting Systems

Table 9 provides an overview of the importance of suggested study areas for future exploration. Each category is accompanied by the number of research papers related to it as well as the normalized frequency associated with it. We summarize the areas in terms of two categories. The first refers to the properties (P) that e-voting systems need to maintain. The second focuses on the features or functions (F) that such systems should offer.

Properties singled out for further investigation are the following, again in order of frequency:

1. Scalability and Performance Improvements (Scal&Perf): Future work in this matter concentrates on developing more efficient consensus algorithms and investigating how to integrate blockchain technology into large-scale e-voting systems. The primary goal is to improve transaction processing rates, block generation rates, and block sizes while maintaining privacy, security, and energy efficiency [32,133–135].
2. Security and Privacy (Sec&Priv): This requires the development and implementation of advanced cryptographic techniques, such as zero-knowledge proofs, secure multiparty computation, blind signatures, ring signatures, and homomorphic encryption, to safeguard the identities and voting preferences of voters. To ensure a robust, anonymous, and trustworthy e-voting system, research concentrates on enhancing transparency and mitigating various types of attacks, like scalability attacks and transaction malleability [136–138].
3. Implementation, Evaluation, and Testing (Impl&Eval): This involves implementing, evaluating, and testing blockchain-based e-voting systems on a larger scale to measure their performance, scalability, and usability in real-world scenarios. Additionally, efforts will be made to address security evaluations, incorporate privacy-by-design features, explore different blockchain protocols, and conduct user acceptance testing with real voters to validate the system's effectiveness and feasibility for large-scale elections [113,133,139–141].
4. Authentication and Identity Verification (Auth&ID): Future work involves creating a comprehensive and secure authentication system for applications in e-voting using biometric measures and blockchain technology. This should focus on enhancing biometric algorithm accuracy and efficiency, investigating decentralized identifiers, incorporating several biometric recognition technologies, and addressing issues related to user eligibility and trust assumptions throughout the voting process. These schemes intend to improve the overall security and convenience of user authentication and verification in blockchain-based e-voting systems [125,142–144].
5. Coercion-Resistance (Coerc-Res): Future research should examine techniques that allow voters to make choices without the influence of coercers. This can be achieved by enabling voters to modify their votes multiple times, incorporating randomized tokens, leveraging face expression analysis, and employing facial tracking to enhance coercion detection. Additionally, ensuring receipt-free voting can be accomplished using various techniques, including ring signatures, while safeguarding voter privacy and security. The focus should remain on the proper design and execution of these tools to protect the integrity and privacy of the voting process [104,145–147].
6. Accessibility (Access): This involves deploying a voting module on mobile devices that supports offline voting and provides accessibility options for disabled voters. Proper mobility, enhanced design, and increased system availability seek to provide all eligible voters with a user-friendly, accessible, and effective voting experience, with potential solutions proposed for locations where remote voting is not feasible [115,148,149].

7. Legal and Governance Aspects (Leg&Gov): Future work refers to the establishment of regulations and standards for the deployment of blockchain technology, particularly in the context of electoral integrity. It comprises researching the influence of blockchain-based systems on election processes, developing a privacy-compliant framework, and exploring the sociological and psychological variables influencing online voter behavior in order to make blockchain technology more adaptable and suitable in more countries [89,150].

Features or functions that should be developed better in order of frequency:

1. Integration and Interoperability (Int&Inter): The creation and testing of blockchain-based e-voting systems that effectively interact with current voting infrastructures while maintaining compatibility with various legacy systems. The aim is to investigate the growth of blockchain-based voting solutions beyond elections, including agent-based methods and smart city services, as well as support adjusting in other industries like healthcare and auctions [151–153].
2. Consensus Algorithms and Smart Contracts (Cons&SC): Future work for e-voting systems aims to develop self-administering blockchain systems that do not require central authorities while improving scalability and privacy using new consensus algorithms and privacy-preserving approaches such as homomorphic encryption and zero-knowledge proofs. The investigation looks at the use of various consensus techniques, such as PBFT, BFT, and PoW, as well as smart contracts, to automate electoral processes, integrate complex voting rules, and increase security in e-voting systems. Furthermore, improving consensus techniques can also contribute to scalability and energy efficiency [154–157].
3. Usability and User Interface (Usab&UI): future work includes User Interface Enhancement, integrating it with a mobile app [156,158].
4. Machine Learning (ML): future work in Machine Learning for e-voting systems consists of detecting fraudulent behavior and fake voters, predicting voting patterns and identifying anomalies for enhanced security and transparency, and investigating the use of deep learning mechanisms to optimize sidechain parameters [84,159,160].
5. Acceptance (Accept): it involves conducting User Acceptance Testing (UAT) with a diverse group of stakeholders in order to improve system quality, reduce failures, and promise voter satisfaction [161–163].
6. General Concept (Gen): future research includes studying a variety of electoral systems employing blockchain technology.
7. Hybrid Systems (HS): future work should address the integration of paper ballots with electronic or blockchain-based voting mechanisms, studying the possibility of combining online and offline voting methods in different scenarios such as quadratic voting [125,164].
8. Blockchain and IoT (BC&IoT): The future should involve integrating blockchain and IoT technologies in e-voting systems to improve voting process security, transparency, and verifiability. The focus of the research is on developing IoT-based applications to ensure easy data exchange between devices and the blockchain network, checking user authentication through biometrics and other secure methods, and examining the integration of blockchain to revolutionize different industries [38,70,165].

Future work indications were extracted from the evaluation and results, discussion, future work, and conclusion sections of the papers, where 88 of the studies analyzed lacked clear statements regarding future work.

Table 9. Prominence of topics for future research (if mentioned).

Category	Type	No. of Papers	Normalized (%)
Scal&Perf	P	74	100.00
Sec&Priv	P	70	94.59
Impl&Eval	P	59	79.73
Int&Inter	F	34	45.95
Cons&SC	F	24	32.43
Auth&ID	P	23	31.08
Coerc-Res	P	15	20.27
Usab&UI	F	13	17.57
Accept	F	10	13.51
ML	F	7	9.46
Gen	F	7	9.46
Leg&Gov	P	6	8.11
Access	P	5	6.76
HS	F	4	5.41
BC-IoT	F	4	5.41

Normalized Percentage = $\frac{\textbf{Number of Papers in a Category}}{\textbf{Max Number of Papers in any Category}} \times 100.$

The "Scalability and Performance" research field emerged as the most prominent, showing its crucial importance. Furthermore, the areas "Security and Privacy", "Implementation, Evaluation, and Testing" and "Interaction and Interoperability" received attention. Figure 5 highlights these critical directions for future study.

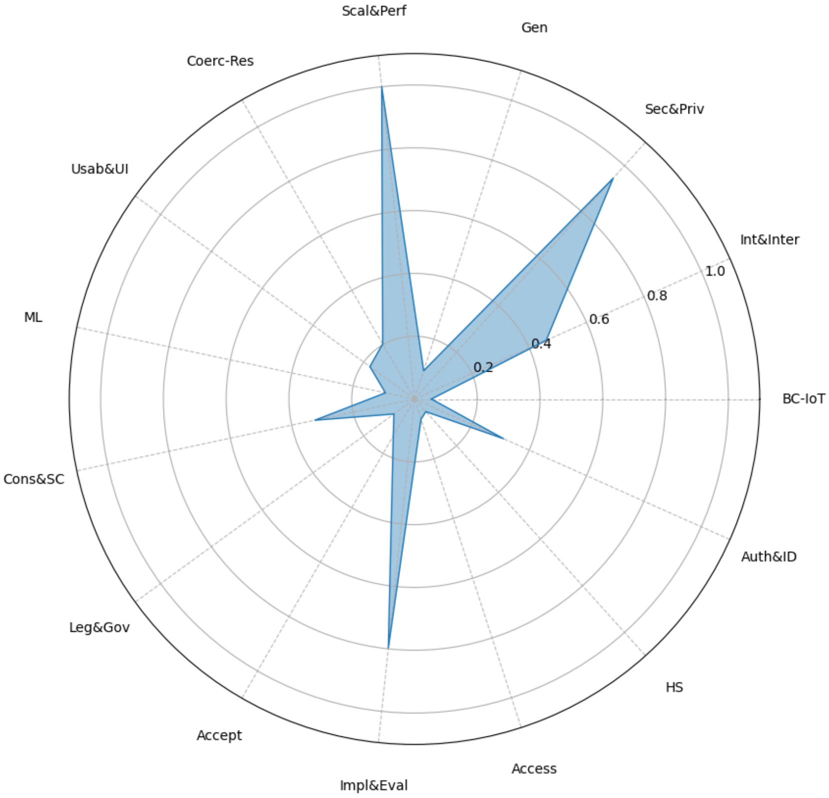

Figure 5. Prospective of research topics for future investigation

7.2. Final Observations

We have defined a number of research questions covering benefits, challenges, impacts, and future research as four perspectives based on system properties related to a list of requirements. A further technology review has helped to make the demonstrated solutions described in the studies, as well as concrete implementation gaps, more clear.

Based on the definitions of the different perspectives, we would expect that the suggested benefits have been demonstrated and shown to positively impact the field and that the challenges have been reiterated as areas for future work.

In order to detect inconsistencies and clarify possible conflicts between, for instance, assumed and demonstrated benefits, we note some observations on these concerns. For this, we mainly refer to the frequency position of a respective property in the frequency lists of the tables above.

- Security: This is the most frequently named property in relation to e-voting systems in general and blockchain-based systems in particular. An initial discrepancy emerges in that security appears at rank 1 or 2 in all lists, showing it as a demonstrated benefit as well as an open challenge. A closer investigation, however, shows that some principle blockchain properties such as integrity, immutability, and durability are acknowledged, but specific concerns relating to attacks on keys or smart contracts still exist, and possible remediation techniques such as zero-knowledge proofs, signature schemes, and homomorphic encryption are proposed.
- Privacy: As a property specifically relevant to the voter and their votes, this is separated from security. Here the picture is consistent by being ranked higher on challenges and future research (ranks 1 and 2, compared to 3 and 4 for benefits and impact), thus clearly showing this as a concern to be better addressed.
- Scalability: not even listed in the benefits, with positions 3 and 1 in challenges and future work, it is clearly seen as a serious open problem of blockchain solutions on a par with security and privacy.
- Usability: Although not a core property associated with blockchain platforms, it is mentioned in the context of a wider e-voting system with front end being integrated. As for privacy, it is consistently discussed across the factors. The ranks (between 8 and 10) are slightly lower, probably showing this as important but not being a core concern of blockchains but of a wider e-voting system.
- Coercion-freeness: this is similar to usability consistently ranked, with ranks 10 and 12 for benefits and impacts and 7 and 10 for impact and future also seen as a property still to be demonstrated, though with potential to improve via blockchains as a transparent and secure ledger mechanism.
- Technical concerns: these appear in the challenges and future work at a relatively high rank (between positions 3 and 4), referring to general implementation and evaluation methods, but also more specifically to interoperability and integration with other platforms and concrete blockchain-specific research needed on consensus protocols and smart contracts.
- Transparency and auditability: these are the only ones that are undisputed as demonstrated benefits of blockchain-based e-voting systems, with no concerns or open problems noted.
- Other properties: properties such as verifiability, accessibility, accuracy/reliability, and acceptability are also consistently referred to as properties of relevance, but not as critical ones.

7.3. Insights and Implications from the Observations

Through this study, convincing evidence for supporting the benefits of blockchain in enhancing security, transparency, decentralization, and privacy suggests that election organizations and governments should consider adopting blockchain technology in their voting systems. The improvement of the mentioned features of blockchain-based systems can increase voter confidence in the voting process and by clearly demonstrating these features to the public, electoral authorities can achieve a more trusting relationship with voters.

Observations of this research indicates the applicability of blockchain technology in e-voting systems. However, it is important to address the challenges highlighted in Section 5.2. These challenges indicate critical areas requiring further investigation and development.

Future research should focus on the challenge areas to enhance the understanding and application of blockchain in e-voting. In addition, the benefits of blockchain, as evidenced in e-voting, can inspire its application in other areas requiring similar levels of security, efficiency, and privacy, including but not limited to digital identity management, healthcare, financial service, supply chain, and education. As well, the success of blockchain in e-voting systems should encourage collaborative efforts between researchers to explore innovative applications of blockchain in public service.

8. Conclusions

We presented a systematic review of the state of research into blockchain-based e-voting systems. This study is motivated by the need to comparatively assess benefits, challenges, and impacts and open future research in comparison to other types of voting systems. Furthermore, a discussion of technology aspects to address the required properties was lacking.

The evolution of blockchain-based e-voting systems from 2017 to 2023 has been marked by significant advancements, as evidenced by research papers from this period. Significant studies emerged, proposing a novel approach to utilizing blockchain technology for recording votes for different voting scenarios. These systems aimed to address common limitations in existing voting systems and involved a critical evaluation of popular blockchain frameworks suitable for e-voting applications. During the years, the primary research emphasis shifted towards enhancing security and developing robust frameworks for blockchain-based e-voting systems. In recent years, the other aspects of e-voting systems, scalability and cost efficiency, have received more attention. Moreover, the importance of privacy-preserving protocols grew significantly, prompting the development of coercion-resistant and privacy-preserving e-voting protocols.

This study followed the PRISMA protocol, resulting in a selection of 252 papers. Five research questions centered on benefits, challenges, impacts, and open future research, as well as technology aspects, guided this study. To provide context, we supplemented this study of the literature with a comprehensive definition of voting system types as a framework, but also technology definitions, also extracted from the literature, in order to make the concerns better understood from an implementation perspective.

The results show that blockchain technology has the potential to successfully implement e-voting systems. Transparency and auditability are seen as undisputed benefits. Security and privacy are, as would be expected for voting processes, the central properties. Here, the potential is seen in blockchain technology over other platform technologies, but whereas some specific aspects are acknowledged, both remain serious open problems, which their top rankings in the frequency lists for challenges and future directions show.

An undisputed limitation of blockchains is their lack of scalability, which is the most serious non-security concern. Beyond core platform concerns, usability, verifiability, accessibility, reliability, and acceptability are properties of concern that in the wider voting systems implementation require more attention. Where evident from the studies considered, we supplemented these observations with concrete solution techniques.

Therefore, this study effectively clarifies both the potential and the limitations of blockchain-based e-voting systems. It achieves this by jointly integrating an analysis of fundamental properties with practical technological implementations and exploring a future roadmap, concluding in a comprehensive discussion that offers a holistic view of the topic.

Author Contributions: All authors have contributed substantially to the work presented. Conceptualization and methodology, M.H.B., H.R.B., N.E.I., and C.P.; data (study) curation, M.H.B.; data (study) analysis, M.H.B.; validation, M.H.B., H.R.B., N.E.I., and C.P.; writing—original draft preparation, M.H.B. and C.P.; writing—review and editing, H.R.B. and N.E.I.; supervision: C.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Südtiroler Informatik AG (SIAG) through the PhD bursary for the years 2021–2025.

Data Availability Statement: Relevant data for the survey has been included in the manuscript. Further data sharing is not applicable to this article.

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

References

1. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Int. J. Surg.* **2021**, *88*, 105906. [CrossRef] [PubMed]
2. Voting Technology. Available online: https://electionlab.mit.edu/research/voting-technology (accessed on 22 April 2023).
3. Krimmer, R.; Volkamer, M. Bits or Paper? Comparing Remote Electronic Voting to Postal Voting. In Proceedings of the EGOV (Workshops and Posters), Copenhagen, Denmark, 22–26 August 2005; Citeseer: State College, PA, USA, 2005; pp. 225–232.
4. Jones, D.W. The evaluation of voting technology. In *Secure Electronic Voting*; Springer: New York, NY, USA, 2003; pp. 3–16.
5. Fischer, E.A.; Coleman, K.J. *The Direct Recording Electronic Voting Machine (DRE) Controversy: FAQs and Misperceptions*; Congressional Research Service, Library of Congress: Washington, DC, USA, 2007.
6. Electoral Technology. Available online: https://aceproject.org/ace-en/topics/et/eta/default (accessed on 19 March 2023).
7. Verified Voting–The Verifier. Available online: https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024 (accessed on 19 March 2023).
8. Oostveen, A.-M.; van den Besselaar, P. E-voting and media effects, an exploratory study. In Proceedings of the Conference on New Media, Technology and Everyday Life in Europe, Amsterdam, The Netherlands, 18–19 September 2003.
9. Buchstein, H. Online democracy, is it viable? Is it desirable? Internet voting and normative democratic theory. In *Electronic Voting and Democracy: A Comparative Analysis*; Palgrave Macmillan UK: London, UK, 2004; pp. 39–58.
10. Akbari, E.; Wu, Q.; Zhao, W.; Arabnia, H.R.; Yang, M.Q. From blockchain to internet-based voting. In Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 218–221.
11. Kshetri, N.; Voas, J. Blockchain-enabled e-voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
12. Tanwar, S.; Gupta, N.; Kumar, P.; Hu, Y.-C. Implementation of blockchain-based e-voting system. *Multimed. Tools Appl.* **2023**, 1–32. [CrossRef]
13. Gritzalis, D.A. Principles and requirements for a secure e-voting system. *Comput. Secur.* **2002**, *21*, 539–556. [CrossRef]
14. Anane, R.; Freeland, R.; Theodoropoulos, G. E-voting requirements and implementation. In Proceedings of the the 9th IEEE International Conference on E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), Tokyo, Japan, 23–26 July 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 382–392.
15. Volkamer, M. *Evaluation of Electronic Voting: Requirements and Evaluation Procedures to Support Responsible Election Authorities*, 1st ed.; Springer Science & Business Media: Berlin, Germany, 2009; Volume 30.
16. Wolf, P.; Nackerdien, R.; Tuccinardi, D. *Introducing Electronic Voting: Essential Considerations*, 1st ed.; International Institute for Democracy and Electoral Assistance (International IDEA): Stockholm, Sweden, 2011.
17. Neumann, S. Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements. Ph.D. Thesis, Technische Universität Darmstadt, Darmstadt, Germany, 2016.
18. De Faveri, C.; Moreira, A.; Araújo, J.; Amaral, V. Towards security modeling of e-voting systems. In Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW), Beijing, China, 12–13 September 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 145–154.
19. Recommendation CM/Rec (2017) 5 of the Committee of Ministers to Member States on Standards for E-Voting. Available online: https://rm.coe.int/0900001680726f6f (accessed on 20 March 2023).
20. Election Assistance Commission. *Voluntary Voting System Guidelines VVSG 2.0.(2021)*; Election Assistance Commission: Washington, DC, USA, 2023.
21. Kong, X.; Wu, Y.; Wang, H.; Xia, F. Edge Computing for Internet of Everything: A Survey. *IEEE Internet Things J.* **2022**, *9*, 23472–23485. [CrossRef]
22. Arbabi, M.S.; Lal, C.; Veeraragavan, N.R.; Marijan, D.; Nygård, J.F.; Vitenberg, R. A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 386–424. [CrossRef]
23. Ali, O.; Ally, M.; Dwivedi, Y. The state of play of blockchain technology in the financial services sector: A systematic literature review. *Int. J. Inf. Manag.* **2020**, *54*, 102199. [CrossRef]

24. Du, M.; Chen, Q.; Xiao, J.; Yang, H.; Ma, X. Supply Chain Finance Innovation Using Blockchain. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1045–1058. [CrossRef]
25. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain Meets Cloud Computing: A Survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2009–2030. [CrossRef]
26. Steiu, M. Blockchain in education: Opportunities, applications, and challenges. *First Monday* **2020**, *25*. . [CrossRef]
27. Hu, J.; Zhu, P.; Qi, Y.; Zhu, Q.; Li, X. A patent registration and trading system based on blockchain. *Expert Syst. Appl.* **2022**, *201*, 117094. [CrossRef]
28. Zhu, P.; Hu, J.; Li, X.; Zhu, Q. Using blockchain technology to enhance the traceability of original achievements. *IEEE Trans. Eng. Manag.* **2023**, *70*, 1693–1707. [CrossRef]
29. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions. *Electronics* **2022**, *11*, 630. [CrossRef]
30. Taş, R.; Tanrıöver, Ö.Ö. A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry* **2020**, *12*, 1328. [CrossRef]
31. Jafar, U.; Ab Aziz, M.J.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors* **2021**, *21*, 5874. [CrossRef] [PubMed]
32. Pawlak, M.; Poniszewska-Marańda, A. Trends in blockchain-based electronic voting systems. *Inf. Process. Manag.* **2021**, *58*, 102595. [CrossRef]
33. Huang, J.; He, D.; Obaidat, M.S.; Vijayakumar, P.; Luo, M.; Choo, K.-K.R. The application of the blockchain technology in voting systems: A review. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–28. [CrossRef]
34. Jafar, U.; Ab Aziz, M.J. A state of the art survey and research directions on blockchain based electronic voting system. In Proceedings of the Second International Conference, ACeS 2020, Penang, Malaysia, 8–9 December 2020; Revised Selected Papers 2; Springer: Singapore, 2021.
35. Devi, U.; Bansal, S. Secure e-Voting System—A Review. In Proceedings of the Hybrid Intelligent Systems, Olten, Switzerland; Porto, Portugal; Vilnius, Lithuania; Kochi, India, 12–14 December 2023; Springer Nature: Cham, Switzerland, 2023; pp. 1209–1224.
36. Benabdallah, A.; Audras, A.; Coudert, L.; El Madhoun, N.; Badra, M. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access* **2022**, *10*, 70746–70759. [CrossRef]
37. Jafar, U.; Ab Aziz, M.J.; Shukur, Z.; Hussain, H.A. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors* **2022**, *22*, 7585. [CrossRef]
38. Vladucu, M.-V.; Dong, Z.; Medina, J.; Rojas-Cessa; R.Vladucu, M.-V.; Dong, Z.; Medina, J.; Rojas-Cessa, R. E-Voting Meets Blockchain: A Survey. *IEEE Access* **2023**, *11*, 23293–23308. [CrossRef]
39. Luxoft. Available online: https://www.luxoft.com/ (accessed on 18 November 2023).
40. Votem. Available online: https://votem.com/ (accessed on 20 November 2023).
41. Voatz. Available online: https://voatz.com/ (accessed on 20 November 2023).
42. Polyas. Available online: https://www.polyas.com/ (accessed on 21 November 2023).
43. Kaspersky Box. Available online: https://box.kaspersky.com/f/e68a161d8e7241909ea3/ (accessed on 21 November 2023).
44. Decentra.Vote. Available online: https://decentra.vote/ (accessed on 25 November 2023).
45. Harley, K.; Cooper, R. Information Integrity: Are We There Yet? *ACM Comput. Surv.* **2021**, *54*, 1–35. [CrossRef]
46. Çabuk, U.C.; Adiguzel, E.; Karaarslan, E. A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems. *arXiv* **2020**, arXiv:2002.07175.
47. Kugusheva, A.; Yanovich, Y. Ring Signature-Based Voting on Blockchain. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 9–11 December 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 70–75.
48. Haiyan, X.; Lifang, W.; Yuechuan, W. A New Fair Electronic Contract Signing Protocol. In Proceedings of the Advances in Intelligent Networking and Collaborative Systems (INCoS-2019), Oita, Japan, 5–7 September 2019; Springer International Publishing: Cham, Switzerland, 2020; pp. 289–295.
49. Hjálmarsson, F.Þ.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjálmtýsson, G. Blockchain-Based E-Voting System. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 983–986.
50. Kumar, M.; Katti, C.P.; Saxena, P.C. A secure anonymous e-voting system using identity-based blind signature scheme. In Proceedings of the 13th International Conference, ICISS 2017, Mumbai, India, 16–20 December 2017; Springer International Publishing: Cham, Switzerland, 2017.
51. Russo, A.; Anta, A.F.; Vasco, M.I.G.; Romano, S.P. Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 417–424.
52. Ikundi, O.; Nwosu, K.C.; Abdulgader, M. LegitVote: A Blockchain-Based System to Facilitate E-Voting Process. In Proceedings of the 2022 International Conference on Computer and Applications (ICCA), Cairo, Egypt, 20–22 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.

53. Fusco, F.; Lunesu, M.; Pani, F.; Pinna, A. Crypto-voting, a Blockchain based e-Voting System. In Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2018)—Volume 3: KMIS, Seville, Spain, 18–20 September 2018; pp. 223–227.
54. Vivek, S.K.; Yashank, R.S.; Prashanth, Y.; Yashas, N.; Namratha, M. E-Voting Systems using Blockchain: An Exploratory Literature Survey. In Proceedings of the 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 15–17 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 890–895.
55. Mello-Stark, S.; Lamagna, E.A. The Need for Audit-Capable E-Voting Systems. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 535–540.
56. Hsu, J.; Bronson, G. E-Voting Technologies Usability: A Critical Element for Enabling Successful Elections. In *Emerging Challenges in Business, Optimization, Technology, and Industry: Proceedings of the Third International Conference on Business Management and Technology, Vancouver, BC, Canada, 13–17 March 2017*; Springer International Publishing: Cham, Switzerland, 2018.
57. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
58. Sheer Hardwick, F.; Gioulis, A.; Naeem Akram, R.; Markantonakis, K. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1561–1567.
59. Küsters, R.; Müller, J. Cryptographic security analysis of e-voting systems: Achievements, misconceptions, and limitations. In Proceedings of the Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, 24–27 October 2017, Springer International Publishing: Cham, Switzerland, 2017.
60. Conti, V.; Taş, R.; Tanrıöver, Ö.Ö. A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Secur. Commun. Networks* **2021**, *2021*, 6673691.
61. Borras, J. *Overview of the Work on E-Voting Technical Standards*; Cabinet Office, UK Government: London, UK, 2002.
62. Prajapati, P.; Dave, K.; Shah, P. A review of recent blockchain applications. *Int. J. Sci. Technol. Res.* **2020**, *9*, 897–903.
63. Kho, Y.-X.; Heng, S.-H.; Chin, J.-J. A Review of Cryptographic Electronic Voting. *Symmetry* **2022**, *14*, 858. [CrossRef]
64. buidris, Y.; Kumar, R.; Wenyong, W. A Survey of Blockchain Based on E-Voting Systems. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, Xi'an, China, 25–30 June 2019; Association for Computing Machinery: New York, NY, USA, 2020; pp. 99–104.
65. Nguyen, T.; Thai, M.T. zVote: A Blockchain-based Privacy-preserving Platform for Remote E-voting. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 4745–4750.
66. Anita, N.; Vijayalakshmi, M. Blockchain Security Attack: A Brief Survey. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
67. Alamleh, H.; AlQahtani, A.A.S. Analysis of the Design Requirements for Remote Internet-Based E-Voting Systems. In Proceedings of the 2021 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 10–13 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 386–390.
68. Chaeikar, S.S.; Jolfaei, A.; Mohammad, N.; Ostovari, P. Security Principles and Challenges in Electronic Voting. In Proceedings of the 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Gold Coast, Australia, 25–29 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 38–45.
69. Hajian Berenjestanaki, M.; Barzegar, H.R.; El Ioini, N.; Pahl, C. An Investigation of Scalability for Blockchain-Based E-Voting Applications. In Proceedings of the Blockchain and Applications, 5th International Congress, Guimarães, Portugal, 12–14 July 2023; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 134–143.
70. Geng, T.; Njilla, L.; Huang, C.T. A Survey of Blockchain-Based Electronic Voting Mechanisms in Sensor Networks. In Proceedings of the 20th ACM Conference on Embedded Networked Sensor Systems, Boston, MA, USA, 6–9 November 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1222–1228.
71. Hapsara, M.; Imran, A.; Turner, T. E-Voting in Developing Countries. In Proceedings of the Electronic Voting, Bregenz, Austria, 24–26 October 2017; Springer International Publishing: Cham, Switzerland, 2017; pp. 36–55.
72. Goel, A.K.; Rai, A.; Narain, A.; Richard, A.; Kumar, K. Trusted Vote: Reorienting eVoting using Blockchain. In Proceedings of the 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Coimbatore, India, 15–17 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 129–138.
73. Majumder, S.; Ray, S. Usage of Blockchain Technology in e-Voting System Using Private Blockchain. In *Intelligent Data Engineering and Analytics*; Springer Nature: Singapore, 2022; pp. 51–61.
74. Pawlak, M.; Poniszewska-Marańda, A.; Kryvinska, N. Towards the Intelligent Agents for Blockchain E-Voting System. *Procedia Comput. Sci.* **2018**, *141*, 239–246. [CrossRef]
75. Gong, B.; Lu, X.; Fat, L.W.; Au, M.H. Blockchain-Based Threshold Electronic Voting System. In *Security and Privacy in Social Networks and Big Data, Proceedings of the 5th International Symposium, SocialSec 2019, Copenhagen, Denmark, 14–17 July 2019; Revised Selected Papers 5*; Springer: Singapore, 2019.

76. Tirodkar, V.; Patil, S. Proposed Infrastructure for Census Enumeration and Internet Voting Application in Digital India with Multichain Blockchain. In *Advanced Computing Technologies and Applications, Proceedings of the 2nd International Conference on Advanced Computing Technologies and Applications—ICACTA 2020, Mumbai, India, 28–29 Feburary 2020*; Springer: Singapore, 2020.
77. Yang, Z.; Hu, H.; Ou, J.; Qian, B.; Luo, Y.; He, P.; Zhou, M.; Chen, Z. A Practical Anonymous Voting Scheme Based on Blockchain for Internet of Energy. *Secur. Commun. Netw.* **2022**, *2022*, 4436824.
78. Daramola, O.; Thebus, D. Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections. *Informatics* **2020**, *7*, 16. [CrossRef]
79. Wang, Z.; Luo, X.; Li, M.; Sun, W.; Xue, K. WeVoting: Blockchain-based Weighted E-Voting with Voter Anonymity and Usability. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 2585–2590.
80. Spadafora, C.; Longo, R.; Sala, M. *A Coercion-Resistant Blockchain-Based E-Voting Protocol with Receipts*; Department of Mathematics, University Of Trento: Trento, Italy, 2020. Available online: https://eprint.iacr.org/2020/674 (accessed on 18 March 2023).
81. Isirova, K.; Potii, O. Development Principles for Electronic Voting System Using Distributed Ledger Technology. In Proceedings of the 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 14–18 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 446–450.
82. Lijuan, Z.; Dunyue, L.; Rui, Z.; Yongbin, Z.; Rouxin, F.; Ziyang, C. Electronic Voting Scheme Based on Blockchain and SM2 Cryptographic Algorithm Zero-Knowledge Proof. In Proceedings of the 2022 IEEE International Conference on Web Services (ICWS 2022), Barcelona, Spain, 11–15 July 2022; Springer Nature: Cham, Switzerland, 2022; pp. 88–103.
83. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function. *IEEE Access* **2019**, *7*, 115304–115316. [CrossRef]
84. Cheema, M.A.; Ashraf, N.; Aftab, A.; Qureshi, H.K.; Kazim, M.; Azar, A.T. Machine Learning with Blockchain for Secure E-voting System. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020; IEEE: Piscataway, NJ, USA, 2020. pp. 177–182.
85. Denis González, C.; Frias Mena, D.; Massó Muñoz, A.; Rojas, O.; Sosa-Gómez, G. Electronic Voting System Using an Enterprise Blockchain. *Appl. Sci.* **2022**, *12*, 531. [CrossRef]
86. Churi, M.; Bajaj, A.; Pannu, G.; Patil, M. Blockchain Based E-Voting System. In *Intelligent Computing and Networking: Proceedings of IC-ICN 2022*; Springer Nature: Singapore, 2023; pp. 123–142.
87. Oprea, S.-V.; Bâra, A.; Andreescu, A.-I.; Cristescu, M.P. Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level. *IEEE Access* **2023**, *11*, 18461–18474. [CrossRef]
88. Pawlak, M.; Poniszewska-Marańda, A. Blockchain E-Voting System with the Use of Intelligent Agent Approach. In Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia (MoMM2019), Munich, Germany, 2–4 December 2019; Association for Computing Machinery: New York, NY, USA, 2020; pp. 145–154.
89. Ohammah, K.L.; Thomas, S.; Obadiah, A.; Mohammed, S.; Lolo, Y.S. A Survey on Electronic Voting On Blockchain. In Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, 17–19 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–4.
90. Neziri, V.; Dervishi, R.; Rexha, B. Survey on Using Blockchain Technologies in Electronic Voting Systems. In Proceedings of the 2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC), Crete Island, Greece, 19–22 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 61–65.
91. Werth, J.; Hajian Berenjestanaki, M.; Barzegar, H.; El Ioini, N.; Pahl, C. A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma. In Proceedings of the 25th International Conference on Enterprise Information Systems (ICEIS 2023), Prague, Czech Republic, 24–26 April 2023; Volume 1, pp. 146–155.
92. Bartolucci, S.; Bernat, P.; Joseph, D. SHARVOT: Secret SHARe-Based VOTing on the Blockchain. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB '18), Gothenburg, Sweden, 27 May 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 30–34.
93. 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 2022 International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022; IEEE: Piscataway, NJ, USA, 2022.
94. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 14 May 2023).
95. King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012. Available online: https://peercoin.net/assets/paper/peercoin-paper.pdf (accessed on 19 August 2012).
96. Kovan—Stable Ethereum Public Testnet. Available online: https://github.com/kovan-testnet/proposal/blob/master/README.md (accessed on 14 May 2023).
97. Buchman, E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. Ph.D. Thesis, University of Guelph, Guelph, ON, Canada, 2016.
98. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI 99), New Orleans, LA, USA, 22–25 February 1999.
99. Ongaro, D.; Ousterhout, J. In Search of an Understandable Consensus Algorithm (Extended Version). In Proceedings of the USENIX Annual Technical Conference, USENIX ATC, Philadelphia, PA, USA, 19–20 June 2014; pp. 19–20.

100. Chaisawat, S.; Vorakulpipat, C. Towards Achieving Personal Privacy Protection and Data Security on Integrated E-Voting Model of Blockchain and Message Queue. *Secur. Commun. Netw.* **2021**, *2021*, 1–14. [CrossRef]
101. Delegated Proof of Stake (DPOS). Available online: https://how.bitshares.works/en/master/technology/dpos.html (accessed on 15 May 2023).
102. Li, W.; Meese, C.; Nejad, M.; Li, W.; Meese, C.; Nejad, M.; Guo, H. P-CFT: A Privacy-preserving and Crash Fault Tolerant Consensus Algorithm for Permissioned Blockchains. In Proceedings of the 2021 4th International Conference on Hot Information-Centric Networking (HotICN), Nanjing, China, 25–27 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 26–31.
103. Stellar Consensus Protocol (SCP). Stellar Documentation. Available online: https://developers.stellar.org/docs/fundamentals-and-concepts/stellar-consensus-protocol (accessed on 1 September 2023).
104. Abuidris, Y.; Kumar, R.; Yang, T.; Onginjo, J. Secure Large-Scale E-Voting System Based on Blockchain Contract Using a Hybrid Consensus Model Combined with Sharding. *ETRI J.* **2021**, *43*, 357–370. [CrossRef]
105. Fatrah, A.; El Kafhali, S.; Haqiq, A.; Salah, K. Proof of Concept Blockchain-Based Voting System. In Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT '19), Rabat, Morocco, 23–24 October 2019; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–5.
106. Zhang, S.; Wang, L.; Xiong, H. Chaintegrity: Blockchain-Enabled Large-Scale E-Voting System with Robustness and Universal Verifiability. *Int. J. Inf. Secur.* **2020**, *19*, 323–341. [CrossRef]
107. Gupta, S.P.; Tripathi, A.M. E-Voting using Blockchain. *J. Physics Conf. Ser.* **2021**, *1911*, 1–14. [CrossRef]
108. Qu, W.; Wu, L.; Wang, W.; Liu, Z.; Wang, H. A Electronic Voting Protocol Based on Blockchain and Homomorphic Signcryption. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e5817. [CrossRef]
109. Carcia, J.C.P.; Benslimane, A.; Boutalbi, S. Blockchain-based system for e-voting using Blind Signature Protocol. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 01–06.
110. Kurbatov, O.; Kravchenko, P.; Poluyanenko, N.; Shapoval, O.; Kuznetsova, T. Using Ring Signatures For An Anonymous E-Voting System. In Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 18–20 December 2019; IEEE: Piscataway, NJ, USA, 2022; pp. 187–190.
111. Verma, G. A Secure Framework for E-Voting Using Blockchain. In Proceedings of the 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 8 September 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
112. Gupta, S.; Gupta, A.; Pandya, I.Y.; Bhatt, A.; Mehta, K. End to End Secure E-Voting Using Blockchain & Quantum Key Distribution. *Mater. Today Proc.* **2023**, *80*, 3363–3370.
113. Chaieb, M.; Yousfi, S. LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol. In Proceedings of the Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, 25–26 November 2020; Springer International Publishing: Cham, Switzerland, 2020.
114. Golnarian, D.; Saedi, K.; Bahrak, B. A decentralized and trustless e-voting system based on blockchain technology. In Proceedings of the 2022 27th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Islamic Republic of Iran, 23–24 February 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
115. Parmar, A.; Gada, S.; Loke, T.; Jain, Y.; Pathak, S.; Patil, S. Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
116. Li, M.; Luo, X.; Sun, W.; Li, J.; Xue, K. AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 4751–4756.
117. Luo, T. An Efficient Blockchain Based Electronic Voting System Using Proxy Multi-signature. In Proceedings of the 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 10–12 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 513–516.
118. Doost, M.; Kavousi, A.; Mohajeri, J.; Salmasizadeh, M. Analysis and Improvement of an E-voting System Based on Blockchain. In Proceedings of the 2020 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran, 4–6 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–4.
119. Xu, Z.; Cao, S. Efficient Privacy-Preserving Electronic Voting Scheme Based on Blockchain. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 190–196.
120. Khan, K.M.; Arshad, J.; Khan, M.M. Empirical Analysis of Transaction Malleability within Blockchain-Based E-Voting. *Comput. Secur.* **2021**, *100*, 102081. [CrossRef]
121. Panja, S.; Roy, B. A Secure End-to-End Verifiable E-Voting System Using Blockchain and Cloud Server. *J. Inf. Secur. Appl.* **2021**, *59*, 102815. [CrossRef]
122. Ch, R.; Kumari D, J.; Gadekallu, T.R.; Iwendi, C. Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis. *Electronics* **2022**, *11*, 3308. [CrossRef]

123. Abegunde, J.; Spring, J.; Xiao, H. SEVA: A Smart Electronic Voting Application Using Blockchain Technology. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 353–360.
124. Kumar, R.; Badwal, L.; Avasthi, S.; Prakash, A. A Secure Decentralized E-Voting with Blockchain & Smart Contracts. In Proceedings of the 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 19–20 January 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 419–424.
125. Jain, A.K.; Kalra, S.; Kapoor, K.; Jangra, V. Blockchain-Based Secure E-Voting System Using Aadhaar Authentication. In *Predictive Data Security Using AI: Insights and Issues of Blockchain, IoT, and DevOps*; Springer Nature: Singapore, 2022; pp. 89–103.
126. Sudha, N.; Reddy, A.B. E-Voting System Using U-Net Architecture with Blockchain Technology. In *Intelligent Computing and Applications: Proceedings of ICDIC 2020*; Springer Nature: Singapore, 2022; pp. 69–79.
127. Díaz-Santiso, J.; Fraga-Lamas, P. E-Voting System Using Hyperledger Fabric Blockchain and Smart Contracts. *Eng. Proc.* **2021**, *7*, 11.
128. Saeed, S.H.; Hadi, S.M.; Hamad, A.H. Iraqi Paradigm E-Voting System Based on Hyperledger Fabric Blockchain Platform. *Ing. Syst. Inf.* **2022**, *27*, 737–745. [CrossRef]
129. Awalu, I.L.; Kook, P.H.; Lim, J.S. Development of a Distributed Blockchain EVoting System. In Proceedings of the 2019 10th International Conference on E-Business, Management and Economics (ICEME), Beijing, China, 15–17 July 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 207–216.
130. OpenSSL Foundation, Inc. OpenSSL. Available online: https://www.openssl.org/docs/man1.1.1/man7/SM2.html (accessed on 24 May 2023).
131. Cheng, Z. The SM9 Cryptographic Schemes. Cryptology ePrint Archive, Paper 2017/117. 2017. Available online: https://eprint.iacr.org/2017/117 (accessed on 6 March 2023).
132. Werth, J.; El Ioini, N.; Hajian Berenjestanaki, M.; Barzegar, H.R.; Pahl, C. A Platform Selection Framework for Blockchain-Based Software Systems Based on the Blockchain Trilemma. In Proceedings of the ENASE, Prague, Czech Republic, 24–25 April 2023; pp. 362–371.
133. Mustafa, M.K.; Waheed, S. An E-Voting Framework with Enterprise Blockchain. In *Advances in Distributed Computing and Machine Learning: Proceedings of ICADCML 2020*; Springer: Singapore, 2021.
134. Anwar ul Hassan, C.; Hammad, M.; Iqbal, J.; Hussain, S.; Ullah, S.S.; AlSalman, H.; Mosleh, M.A.A.; Arif, M. A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. *Sci. Program.* **2022**, *2022*, 1–10. [CrossRef]
135. Olaniyi, O.M.; Dogo, E.M.; Nuhu, B.K.; Treiblmaier, H.; Abdulsalam, Y.S.; Folawiyo, Z. A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies. In *Blockchain Applications in the Smart Era*; Springer International Publishing: Cham, Switzerland, 2022; pp. 41–63.
136. Madhani, N.; Gajria, V.; Kanani, P. Distributed and Anonymous E-Voting Using Blockchain and Ring Signatures. In *Communication and Intelligent Systems: Proceedings of ICCIS 2020*; Springer: Singapore, 2021.
137. Subah, Z.; Rozario, S.; Islam, N.; Amir, S.A.B. Blockchain Technology Integrated Electronic Vote Casting System. In Proceedings of the 2nd International Conference on Computing Advancements, Dhaka, Bangladesh, 10–12 March 2022; ACM: New York, NY, USA, 2022; pp. 133–137.
138. Neziri, V.; Shabani, I.; Dervishi, R.; Rexha, B. Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain. *Appl. Sci.* **2022**, *12*, 5477. [CrossRef]
139. Verwer, M.B.; Dionysiou, I.; Gjermundrød, H. TrustedEVoting (TeV) a Secure, Anonymous and Verifiable Blockchain-Based e-Voting Framework. In Proceedings of the E-Democracy—Safeguarding Democracy and Human Rights in the Digital Age, Athens, Greece, 12–13 December 2019; Springer International Publishing: Cham, Switzerland, 2020; pp. 129–143.
140. Khan, K.M.; Arshad, J.; Khan, M.M. Simulation of Transaction Malleability Attack for Blockchain-Based E-Voting. *Comput. Electr. Eng.* **2020**, *83*, 106583. [CrossRef]
141. Indrason, N.; Khongbuh, W.; Saha, G. Blockchain-Based Boothless E-Voting System. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2020*; Springer: Singapore, 2021; Volume 1, p. 1.
142. Pooja, S.; Raju, L.K.; Chhapekar, U. Face Detection Using Deep Learning to Ensure a Coercion Resistant Blockchain-Based Electronic Voting. *Eng. Sci.* **2021**, *16*, 341–353.
143. Tandon, S.; Singh, N.; Porwal, S.; Satiram; Maurya, A.K. E-Matdaan: A Blockchain based Decentralized E-Voting System. In Proceedings of the 2022 IEEE Students Conference on Engineering and Systems (SCES), Prayagraj, India, 1–3 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
144. S. A, S.; Kumar, K.T.G. E-voting System using Public Blockchain. In Proceedings of the 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 16–17 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
145. Adiputra, C.K.; Hjort, R.; Sato, H. A Proposal of Blockchain-Based Electronic Voting System. In Proceedings of the 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 30–31 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 22–27.
146. Killer, C.; Rodrigues, B.; Matile, R.; Scheid, E.; Stiller, B. Design and Implementation of Cast-as-Intended Verifiability for a Blockchain-Based Voting System. In Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC 2020), Brno, Czech Republic, 30 March–3 April 2020; pp. 286–293.

147. Kyazhin, S.; Popov, V. Yet Another E-Voting Scheme Implemented Using Hyperledger Fabric Blockchain. In Proceedings of the Computational Science and Its Applications—ICCSA 2020, Cagliari, Italy, 1–4 July 2020; Springer International Publishing: Cham, Switzerland, 2020; pp. 37–47.
148. Ouyang, J.; Deng, Y.; Tang, H. Blockchain Electronic Voting System for Preventing One Vote and Multiple Investment. In Proceedings of the Blockchain and Trustworthy Systems: First International Conference, BlockSys 2019, Guangzhou, China, 7–8 December 2019; Springer: Singapore, 2020; Volume 1.
149. APEH, J.; Ayo, C.K.; Adebiyi, A. Implementing a Secured Offline Blockchain Based Electronic Voting System. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 18.
150. Malhotra, M.; Kumar, A.; Kumar, S.; Yadav, V. Untangling E-Voting Platform for Secure and Enhanced Voting Using Blockchain Technology. In *Transforming Management with AI, Big-Data, and IoT*; Springer International Publishing: Cham, Switzerland, 2022; pp. 51–72.
151. Tyagi, A.K.; Fernandez, T.F.; Aswathy, S.U. Blockchain and Aadhaar based Electronic Voting System. In Proceedings of the 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 5–7 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 498–504.
152. Kumar, A.V.; Sarvani, G.V.; Satya, D. Blockchain Based Public Cloud Security for E-Voting System on IoT Environment. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Warangal, India, 9–10 October 2020; IOP Publishing: Bristol, UK, 2020; p. 042013.
153. Barański, S.; Szymański, J.; Sobecki, A.; Gil, D.; Mora, H. Practical I-voting on stellar blockchain. *Appl. Sci.* **2020**, *10*, 7606. [CrossRef]
154. Pandey, A.; Bhasi, M.; Chandrasekaran, K. VoteChain: A Blockchain Based E-Voting System. In Proceedings of the 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 18–20 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–4.
155. Kumar, M. Securing the E-voting system through blockchain using the concept of proof of work. In Proceedings of the 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 10–12 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 423–427.
156. Echchaoui, H.; Roumaissa, B.; Boudour, R. A Proposal of Blockchain and NFC-Based Electronic Voting System. In Proceedings of the Advanced Computational Techniques for Renewable Energy Systems, Tamanghasset, Algeria, 20–22 November 2021; Springer International Publishing: Cham, Switzerland, 2023; pp. 66–75.
157. Kumar, D.; Dwivedi, R.K. Designing a Secure E Voting System Using Blockchain with Efficient Smart Contract and Consensus Mechanism. In Proceedings of the International Conference on Advanced Network Technologies and Intelligent Computing, Varanasi, India, 22–24 December 2022; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 452–469.
158. Rosasooria, Y.; Mahamad, A.K.; Saon, S.; Isa, M.A.M.; Yamaguchi, S.; Ahmadon, M.A. E-Voting on Blockchain using Solidity Language. In Proceedings of the 2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE), Surabaya, Indonesia, 3–4 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
159. VasanthaKumar, C.; Kabilan, V.; Kathiravan, M.; Ragashanmugam, R.G. A Study on Decentralized Electronic-Voting Using Blockchain. In Proceedings of the 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 16–17 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
160. Kohad, H.; Kumar, S.; Ambhaikar, A. Scalability of Blockchain based E-voting system using Multiobjective Genetic Algorithm with Sharding. In Proceedings of the 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 11–13 February 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–4.
161. Baudier, P.; Kondrateva, G.; Ammi, C.; Seulliet, E. Peace engineering: The contribution of blockchain systems to the e-voting process. *Technol. Forecast. Soc. Chang.* **2021**, *162*, 120397. [CrossRef]
162. Khudoykulov, Z.; Tojiakbarova, U.; Bozorov, S.; Ourbonalieva, D. Blockchain based e-voting system: Open issues and challenges. In Proceedings of the 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 3–5 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
163. Wahab, Y.; Ghazi, A.; Al-Dawoodi, A.; Alisawi, M.; Abdullah, S.; Hammood, L.; Nawaf, A. A Framework for Blockchain Based E-Voting System for Iraq. *Int. J. Interact. Mob. Technol.* **2022**, *16*, 210–222. [CrossRef]
164. Sudharsan, B.; Tharun, V.R.; Nidhish, K.M.P.; Raj, J.B.; Surya, A.M.; Alagappan, M. Secured Electronic Voting System Using the Concepts of Blockchain. In Proceedings of the 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, Canada, 17–19 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 675–681.
165. Dhulavvagol, P.M.; Bhajantri, V.H.; Totad, S.G. Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application. *Procedia Comput. Sci.* **2020**, *167*, 2506–2515. [CrossRef]

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.