symmetry

MDPI

Review

A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting

Ruhi Taş [1,2,*] and Ömer Özgür Tanrıöver [1]

[1] Computer Engineering, Ankara University, 06830 Ankara, Turkey; ozgur.tanriover@ankara.edu.tr
[2] Turkish Radio Television Corporation, IT Department, 06550 Ankara, Turkey
* Correspondence: ruhi.tas@trt.net.tr; Tel.: +90-53-3423-3351

Received: 18 July 2020; Accepted: 7 August 2020; Published: 9 August 2020

Abstract: A blockchain is a distributed, digitized and consensus-based secure information storage mechanism. The present article provides an overview of blockchain based e-voting systems. The primary purpose of this review is to study the up-to-date state of blockchain-based voting research along with associated possible challenges while aiming to forecast future directions. The methodology applied in the review is a systematic review approach. Following an introduction to the basic structure and features of the blockchain in relation to e-voting, we provide a conceptual description of the desired blockchain-based e-voting application. Symmetrical and asymmetrical cryptography improvements play a key role in developing blockchain systems. We have extracted and reviewed 63 research papers from scientific databases that have advised the adoption of the blockchain framework to voting systems. These articles indicate that blockchain-supported voting systems may provide different solutions than traditional e-voting. We classified the main prevailing issues into the five following categories: general, integrity, coin-based, privacy and consensus. As a result of this research, it was determined that blockchain systems can provide solutions to certain problems that prevail in current election systems. On the other hand, privacy protection and transaction speed are most frequently emphasized problems in blockchain applications. Security of remote participation and scalability should be improved for sustainable blockchain based e-voting. It was concluded that frameworks needed enhancements in order to be used in voting systems due to these reservations.

Keywords: blockchain; voting; consensus; bitcoin; ethereum; ballot

1. Introduction

Electoral integrity is not only imperative for countries that are ruled by democracy, but it is also influential in enhancing public voters' confidence and accountability. In this regard, political voting systems are critical. From the point of government, electronic voting systems may increase both voter turnout and voter confidence and renew interest in the voting system. Amplified research demonstrates that implementing e-voting systems can enhance security. While adopting an electronic voting system, one must ask: Why is the electronic voting system considered a better option than a traditional ballot voting paper? It not only improves the effectiveness and efficiency of democracy, [1], but it is expected to be a solution for some problematic situations, such as improving accessibility to the election, the elderly and the disabled ability to vote, increase in election turnout, as well as being easy to operate and getting a quick result. However, it is a well-known fact that operating e-voting systems under strict security procedures are crucial, especially when relying on the utilization of advanced encryption techniques.

Initially, e-voting was proposed to be a solution to the challenges of paper-based voting to ensure accurate and bias-free elections [2]. Security issues with respect to e-voting systems have been among the topics that extensively studied in the literature [3]. The studies show that the utilization of electronic

voting may entail the following challenges: data integrity, reliability, transparency, the secrecy of the ballot, consequences of breakdown, uneducated voters, specialized IT skills, storage of equipment, security, consequences of fraud and cost [4].

Blockchain recently has emerged as a solution to enhance the thrust of systems used in different domains. The initial and primary use of blockchain technology was for monitoring cryptocurrency transactions. However, other usage and applications have emerged in the last few years. Recently, the blockchain-based e-voting system has increasingly become an important option in order to overcome certain challenges that may be associated with e-voting. Blockchain-enabled voting systems were proposed as the next generation of modern electronic voting systems because the immutable feature of the blockchain has made it a decentralized distributed ballot box [5]. Blockchain technology encourages governments to adopt smart sustainable voting systems and integrate sustainability information into voting systems. It ensures that all participants have reliable information for sustainable assets. It is important to underline that although blockchain is increasingly being applied to the electronic voting system in order to enhance its security, several issues still prevail.

In this respect, determining which issues are to be addressed in the design of a blockchain-based voting system is crucial. For this purpose, we have used a systematic mapping process to review the literature and clarify such problems. The paper makes the following contributions: identifying a set of current e-voting system gaps; potentials of the blockchain concept to improve e-voting systems through a classification of the main prevailing issues into five categories: general, integrity, coin-based, privacy and consensus; assessing current solutions for blockchain-based e-voting and identifying potential research directions for the Blockchain-based e-voting system. This study showed although blockchain based voting systems can prevent data manipulation and integrity problems, privacy protection and transaction speed are most frequently emphasized issues. These should be improved in a sustainable e-voting system.

The rest of the paper is organized as follows. We first start by presenting general information on the blockchain concept and the scope of the current blockchain applications. Then, we present the research methodology and literature review on electronic voting based on the research questions. Finally, threats to validity are assessed.

2. Information on the Blockchain Concept

This section provides an overview of the blockchain concept. The blockchain concept was initially proposed by Haber and Stornetta in 1991. The main purpose of designing a timestamp for digital documents that would avoid tampering [6]. The first system based on blockchain is believed to be developed by Satoshi Nakamoto in 2008 [7]. It is also evident that the first extensive use of blockchain technology was with Bitcoin [8]. The blockchain concept can be seen analogous to an open and secure data book distributed worldwide. Therefore, the concept can be used not only in cryptocurrency and financial sectors but also in many different fields where transactions are involved. Therefore, the concept is mostly seen as an essential component of industry 5.0 applications for upcoming years. Although blockchain is well known in the field of cryptocurrencies, it would not be wrong to argue that its potential could extend far beyond digital money. Private corporations and government organizations have also begun experimenting with blockchain.

Blockchain can be defined as a chain of blocks, which are time stamped and linked cryptographic hashes. The chain is constantly growing by adding new blocks so that each new block keeps the hash of the previous block information. In essence, blockchain helps to protect both private and public information from alteration and manipulation. The blockchain is essentially a distributed ledger of all transactions that are carried out directly between consumers and providers on the system. A distributed network of nodes that preserve a joint source of transactions. These transactions are validated by the nodes. Therefore the blockchain allows the creation of trust without the need for a central authority [7]. Blockchain systems rely on asymmetric cryptography which is slower than symmetric cryptography.

2.1. Consensus Protocols

To include a block of transactions in the peer to peer distributed ledger, a consensus mechanism is initiated among the nodes. The consensus algorithm on the blockchain ensures that all transactions are valid and authentic besides all nodes on the network have an identical copy of the ledger. There are many different consensus algorithms. Proof-of-Work (PoW) and Proof-of-Stake (PoS) models have frequently been preferred as consensus mechanisms in blockchain infrastructures [9]. POW is a method that allows the transactions to be verified as unique and trustworthy. The transactors can exchange a transaction fee that could be sent to the users so they can verify it successfully and the fee is optional. For example, in the case of Bitcoin, it could be mandatory in some other application setting. In addition to a transaction fee, the network will reward verifiers with a certain number of coins after a block of transactions has successfully been verified. This process is called "mining", which is basically a problem-solving transaction when there is an initiation by a user. The results of this process are easy to verify but very difficult to reproduce. Nevertheless, the downside of POW is a costly and time-consuming process. Another negative aspect is too much energy consumption [10].

On the other hand, PoS is a protocol that uses mining to validate and validate new blocks, PoS chains generate and validate new blocks through staking. PoS validators are chosen based on the number of coins they want to stake, rather than competing for the next block with intense computation [11,12]. The cryptocurrencies included in this network are pre-created and there is no mining process as in the case of PoW. In this way, energy costs are low since there is no need for a complex problem-solving transaction and it processes much faster than PoW [12]. There are also other used other popular consensus protocols relying on other concepts such as proof of importance, capacity and weight [13].

2.2. Blockchain Network Types

From a privacy perspective, the blockchain can be designed in three different ways. Depending on the requirements, it may be designed as a public, private or consortium blockchain. In Table 1, the categorization of these types is provided based on management, type of participants, centralization, consensus and transaction duration to be considered in system design. In private blockchain also known as permission-based, only the designated peers with specific rights can contribute to blocking information and the consensus mechanism. In a private blockchain, the network is not open to everyone where write permissions are reserved centralized in one group.

Table 1. Blockchain network types.

Property	Public	Private	Consortium
Management	No Centralized Management	Single organization	Multiple organization
Participants	Permissionless	Permissioned	Permissioned
Centralized	no	Yes	partial
Efficiency	Low	High	High
Consensus Determination	All miners	Organization participating	Selected miners
Transaction duration	Long	Short	Short

However, in the public blockchain, the network is open to all peers, who can contribute to the recording of all information and consensus where everyone in the network can read the transactions [10]. The private blockchain fits well with traditional business and governance models [14]. Finally, consortium blockchain refers to the inclusion of predetermined specific nodes as well as reliable

individuals. Therefore, it contains more security features according to the public blockchain where the consensus procedure is controlled by pre-selected nodes.

3. Blockchain Current Applications

Several industries have begun to integrate blockchain applications into their businesses. In this way, enterprises aim to make their processes and management more transparent. As an enabler, blockchain is thought to help to address various security concerns, including issues related to identity and fraud management. Blockchain-based systems allow financial institutions to examine their clients and tackle fraudulent activities. Although most banking and payment systems are potential candidates for blockchain application areas, the distributed ledger applications are not limited to the financial services.

The second highly applicable area of blockchain is in the sustainable operations of logistics management and B2B commerce. Blockchain plays a rising role in sustainability by promoting collaboration between consumers and manufacturers, helping people adopt more sustainable existences and helping companies improve their resource and reutilizing process. Blockchain can have profound effects on supply chain management by alleviating complications through ensuring security, transparency and traceability [15]. In supply chain management, each transaction is performed on a standard blockchain and without the need for the approval of a reliable center. The payments are automatically done after the delivery phase is completed. Since the transactions are monitored by the parties, the blockchain may help to improve the end to end tracking and safety of products to a great extent. Thus, the consumer can be given accurate information about transitions in the processes before purchasing the product [16]. Major benefits are process improved visibility, integrity, faster transaction and disintermediation.

Besides the potential benefits in financial industries and supply chain management, blockchain can be utilized in other types of smart services and internet-based applications. Blockchain technology is also used in the energy sector has also made use of blockchain technology. Local energy trading and electrical car efficient charging schedule planning projects are proposed [17]. It is possible for the machines to sell and buy energy in line with the predefined Internet of Things (IoT) devices [18]. When using IoT devices to collect data in real time, this data can be saved in the blockchain chain. It starts to be used in real-time big data analysis [19,20].

The insurance industry is an additional example that utilizes the blockchain. The insurance sector nowadays is based on a trust relationship and it is ascertained that occasional error or delay could be resolved by blockchain in the future. [21]. The healthcare industry is another sector that has the opportunity to use blockchain technology; in this sector, the blockchain acts as a useful tool in enabling key stakeholders such as healthcare providers, clinical research, pharmacists and patients to gain secure, faster and reliable access to electronic medical records [13,21].

In the foreseeable future, it is possible that any sector requiring stringent security, reliability and transparency requirements such as cloud storage [22], transportation systems [23], cybersecurity and identity management in general [24], real-estate and agriculture traceability [25] may benefit from blockchain integration. E-voting systems, among other areas, also stand out as a promising but challenging area that could advantage from the integration of blockchain [26].

4. Information on Electronic Voting Systems

In this section, some a priori information on e-voting systems is given. Electronic voting is a voting method that uses electronic devices to record or count votes. Electronic voting traditionally refers to voting that utilizes some electronic hardware and/or software to support the voting process. Such systems may be capable of supporting/implementing many tasks ranging from the election initialization phase to the storing of votes. System types range from kiosks located in election offices to computers or nowadays to even mobile devices. The e-voting system should at least include registration, authentication, voting and tallying phases (Figure 1).

The following processes were involved in the e-voting system: The first process is to register voters (registration). Then, authorities check voters' credentials on election day (verification and authentication). Next phase eligible people can vote (casting collation). The vote should be encrypted and verifiable. The confidentiality, anonymity and accuracy of the votes must be guaranteed and cannot be changed or deleted in any way. Finally, electronic voting systems counting is done by adding all the votes according to the design (counting presentation of results) [27]. Central authority control is dominant in general e-voting applications. There are several drawbacks and perceived risks to such systems. Such as lack of e-voting system standards, risk related to security and reliability, vulnerability to hacking, susceptibility to fraud, malicious software programming and high expenses of machines and secure storage of transactions.

The first use of the electronic voting system was in the year 2000 in the U.S.A. This was followed by France (2001), UK (2002), Spain (2003), Ireland (2004), Estonia (2005), Portugal (2005), Netherlands (2004, 2006, 2007), Paraguay (2008), Finland (2008), Austria (2009), Germany (2009) and Norway (2011). Estonia was the first country to allow remote electronic voting in the 2007 national parliamentary elections, following the use of the system during a small-scale election in 2005 [4].

There are many different voting systems that are used for different purposes. Among these, the most used voting systems are identified as Punch Card, Direct-Recording Electronic (DRE), Public network DRE, Central count, Kiosk voting or Precinct count [28].

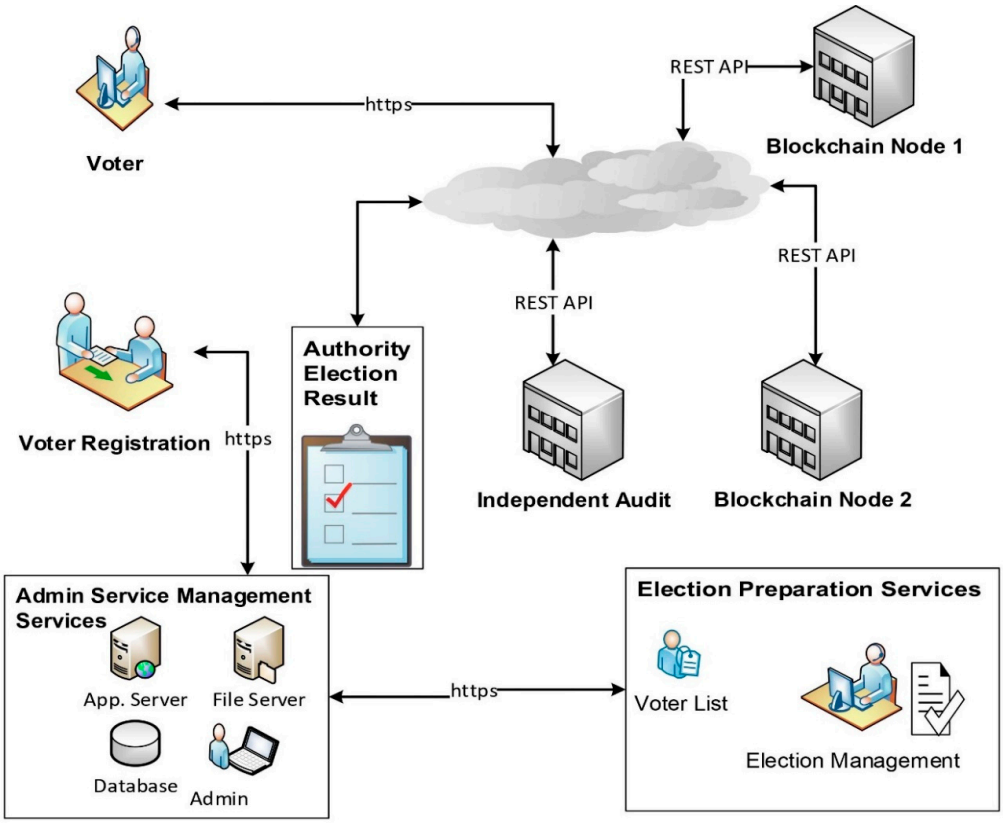

Figure 1. A Blockchain voting systems architectural overview [29,30].

It is stated that the following features should be included in e-voting systems. These are:

1. Receipt-Freeness should not produce any receipt to prove the voter's choice for a particular candidate [1].
2. Fairness, Preliminary results affecting the decisions of other voters could not reach [31,32].
3. Data Integrity ensures that each vote is recorded as intended and cannot be tampered with in any manner, once logged [33].

4. Privacy/Voter Anonymity, The identity of voters and whom they vote for should not reveal [31]. Eligibility only registered voters should be permitted to vote [34].
5. Reliability/Robustness, election systems must operate safely without loss of votes. Software and methods should be developed in such a way without any malicious code nor errors [35].
6. Uniqueness, don't allow voters to vote more than once [36,37].
7. Verifiability, voters should be able to confirm that their ballots are counted correctly [38].

Blockchain based voting systems have recently been proposed [39]. A blockchain-based e-voting system is illustrated in Figure 1. The electoral process requires very critical tasks before and during the election. As presented in figure election preparation services must prepare the current voter list, candidates, ballot design before the election as with all voting systems. Unlike other systems after the voter registration, a voting token can be used for casting vote transactions for candidates. In the design of a real voting system, the use of the permissioned blockchain structure and the inclusion of the independent control node can be used to create a safer environment. These nodes are interconnected with each other.

Nodes designed according to the permission and distributed network of selected neutral third-party organizations that provide consensus mechanisms and processing transactions on the blockchain framework. These nodes' purpose is to mine transactions according to consensus algorithm and add blocks to the voting ledger. The data is cryptographically stored in the ledger. Independent nodes will audit voting results.

Election preparation service involves voter lists, candidates, election duration. Voter registration deals with the validation of people eligible to vote. Voters are responsible for registering before the election. A voter casts their vote to blockchain node. After the end of the election, authority counts the votes and announces the results. The administrator prepares the election date, the duration, the type of election and the candidates. One of the essential tasks of the administrator is to prepare the list of voters and registered voters. Voters and registered voter classes describe who is allowed to vote. The registration process can be done either at offices or via the internet. After the registration is completed, a voting account can be sent through SMS, email or an envelope.

For the process to be efficient, the voter must have an identification number, some personal information or secret key to be able to access and authenticate the system. During the registration, the system should require voters to create secret codes to allow them to vote with them. Eligible citizens for voting should be able to vote in the elections easily by using these codes. Besides keeping log records of all operations performed by the administrator, it is also crucial to store election results safely. At this stage, blockchain systems can be rather helpful as it enables the votes to be saved on blockchain systems as a new transaction. Moreover, the nodes that are included in the system are synchronized through the necessary controls in the smart contracts according to the system design. The selection result class is responsible for counting and preparing the result.

From a development perspective, one of the fundamental advantages of e-voting systems is that it provides various controls that may be embedded both for development and in operations. To exemplify, voter anonymity can be accomplished using cryptographic techniques by taking advantage of tamper-proof structures when using blockchain. These control points could have a positive impact on increasing citizens' trust in the system. It is important to provide information to the citizens in the following fields: how to correct voter identification, how multiple voting is prevented and how citizen's votes have remained secret and are correctly counted. Additionally, it can be foreseen that during the development process, the use of independent verification and validation systems can provide extra assurances.

5. Research Methodology

In this study, we followed the proposed systematic mapping method presented in Petersen et al. [40]. Figure 2 shows the mapping method workflow and all the process steps that have been implemented. The process initially includes the definition of research questions. Secondly, an extensive search

of publications has been carried out followed by the identification of relevant sources according to criteria. Finally, the studies have been analyzed and classified while synthesizing and summarizing the information extracted.

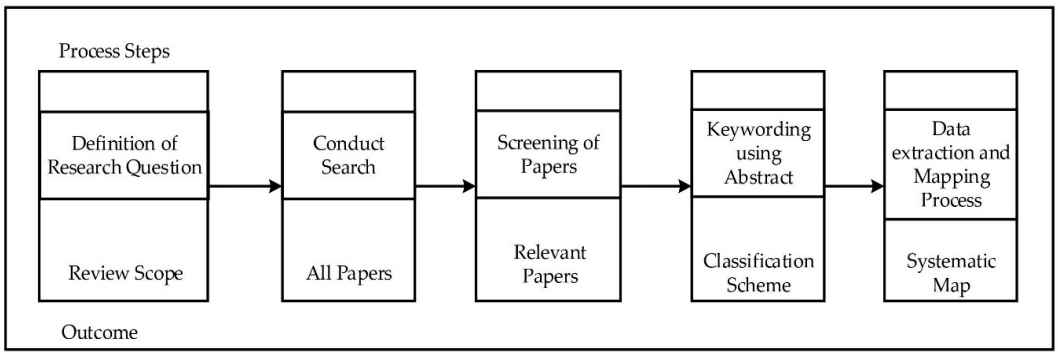

Figure 2. The Systematic Mapping Process [40].

There are several threats that may arise when conducting a systematic mapping study. We discuss validity threats in Section 7.

5.1. Research Questions

In the first stage of the systematic mapping process, we identified questions that were appropriate for our research. We have identified the following research questions on blockchain-based e-voting. The answers are evaluated in the discussion section:

1. RQ1: What are the current e-voting system gaps?
2. RQ2: Can the blockchain concept improve e-voting systems?
3. RQ3: What are the research topics and proposed solutions that have been published in blockchain-based e-voting?
4. RQ4: Which blockchain platforms/consensus models are used?
5. RQ5: What are the future research directions for the blockchain-based e-voting system?

5.2. Data Sources and Search Process

As with most systematic literature review studies, different search strings should be used depending on the synonyms and nomenclature of the interested domain. For this reason, we repeated the search with semantically related queries (Figure 3). The search included all publications in the relevant databases from 2010 until December 2019. We used four different search terms. These were "Blockchain," "e-voting," "blockchain ballot" and "blockchain voting" (Table 2). With the search string, we identified articles according to the appropriate criteria from the flowing online databases: IEEE Xplore, Arxiv, Iacr, ScienceDirect, Web of Science, Scitepress and Springer.

Table 2. The number of Search Results.

Databases	Blockchain	E-Voting	Blockchain Ballot
sciencedirect.com (Future Gen. Comp. Sys, Comp. & Sec., Journal of Network and Comp. App. Procedia Comp. Science)	317	462	80
arxiv.org	1178	56	7
ieeexplore.ieee.org (conferences and journals)	3149	290	24
scitepress.org	57	100	5
webofscience.com	4299	740	26
springer.com (journal)	510	2123	2126

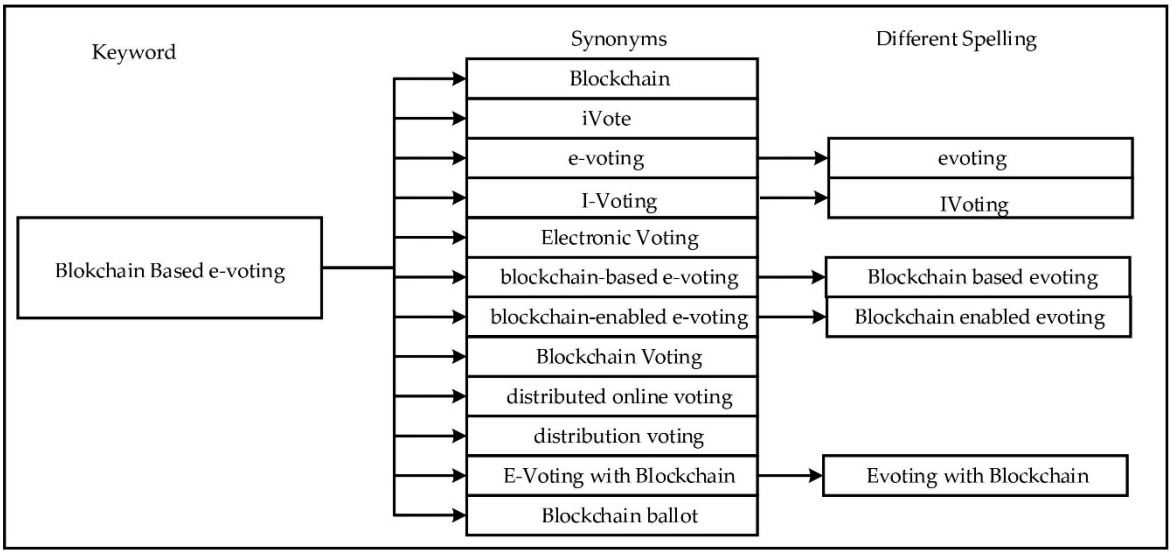

Figure 3. Terms that form the search string.

5.3. Selection of Results

Inclusion and exclusion criteria are assumed to help the researchers make a more independent decision on which article should be included in the review. In this review, articles were eligible for inclusion if they were published in English, in a peer-reviewed journal and their focus was blockchain-based e-voting systems. Conference proceedings on blockchain-based e-voting were also examined. The article selection process diagram is given in Figure 4. Since the Web of Science, Scitepress and Springer databases use different search algorithms, the number of articles was higher then we expected. Nonetheless, it did not adversely affect the desired search results. Table 3 and Figure 5 show the publication year distribution of the selected articles. Interestingly, all the selected articles were published after the year 2014. These results indicate that e-voting with blockchain as a research area is a new one.

When the articles were analyzed according to publication year, we found 7 papers (11.11%) in 2017, 25 papers (39.69%) in 2018 and 29 papers (47.62%) in 2019. This result shows that blockchain voting research has increased rapidly every year.

Table 3. Research Articles by Year.

Year	Blockchain
2015	[26]
2016	
2017	[14,38,41–45]
2018	[11,34,46–68]
2019	[30,37,69–96]

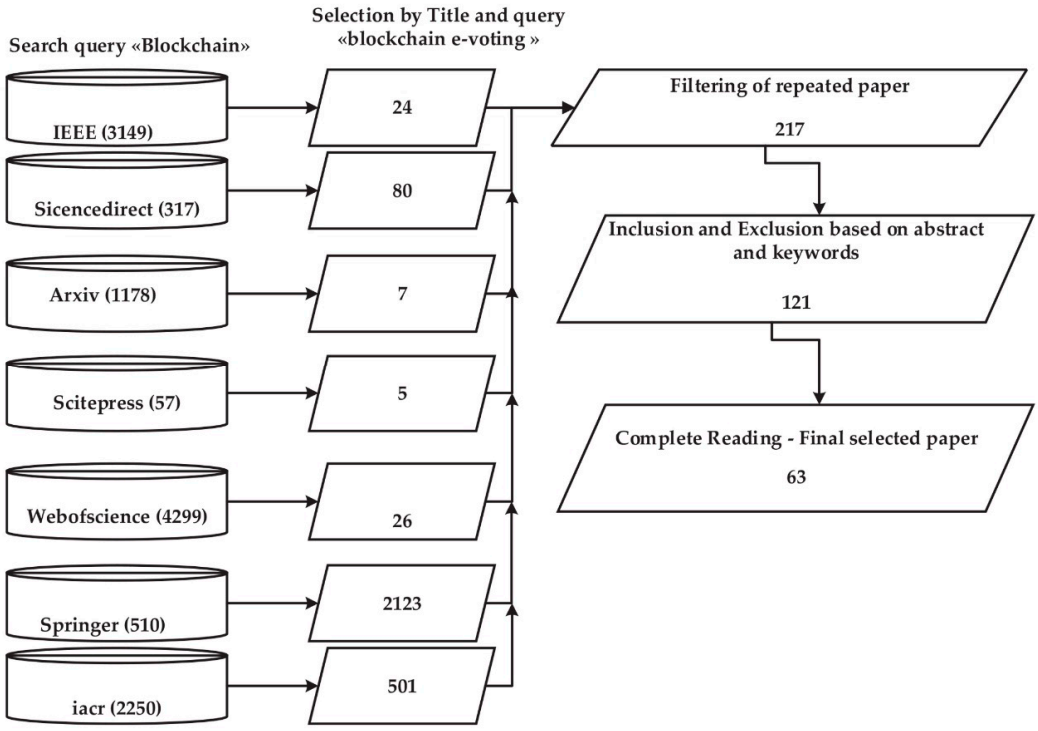

Figure 4. Article selection process diagram.

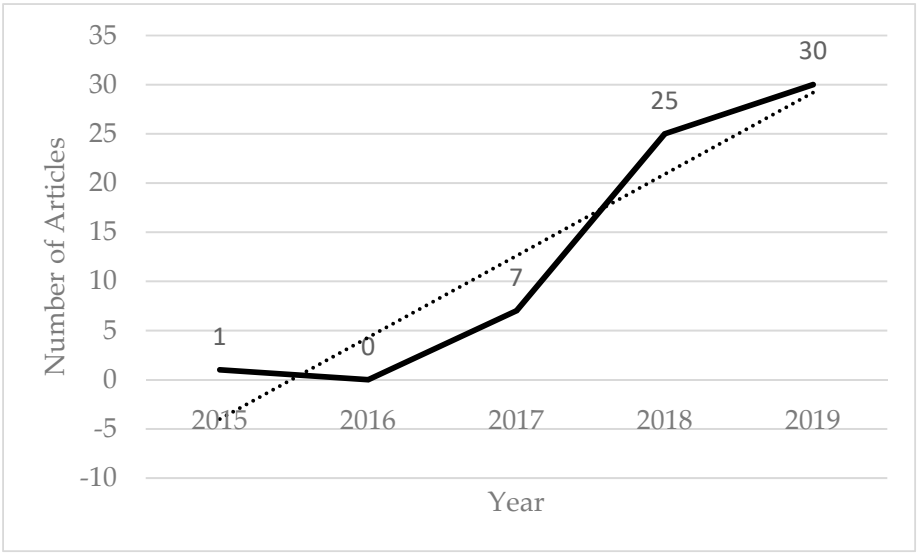

Figure 5. Research Publication Trend.

6. Research Questions and Findings

6.1. RQ1: What Are the Current E-Voting Systems Gaps?

E-voting has many advantages over traditional voting systems especially due to operational cost, less human error and faster results. Moreover, online voting advances are particularly increasing voter participation [97] due to the accessibility of the elderly, disabled and reluctant youth. In addition, voters living abroad or overseas are allowed to participate more easily in the voting. It reduces costs such as printing and counting of ballot papers [36].

However, as potential disadvantages, e-voting systems introduce software, hardware and communications infrastructure vulnerabilities [98,99]. Reviled specific security problems are identity theft, malware on the voter's computer or device trojan horses, spyware, viruses, worms), server penetration attacks, spoofing, fake web pages, DNS (Domain Name Server) attack and DDoS (Distributed Denial of Service) attack. Furthermore, insider attacks are potential problems in almost all of the election systems.

Especially, electronic voting systems designed on a centralized structure are open to different cyber-attack types such as DDoS (Distributed Denial of Service) attack can stop the server. System usability, privacy or authentication issues may occur [36]. Although to store data on remote servers is assumed to be safe, this does not provide security against hackers' attacks, this may cause data loss or damage in the event of poor system security administration. Furthermore, traditional databases are sustained by a single group, and that group has comprehensive control of the database, including the capability to manipulate with the stored records. Due to this bias, online voting is vulnerable to manipulations, both in terms of the vote count and electoral fraud.

Furthermore, unpredictable attacks (TLS attack and/or man in the middle attack [100]) can occur due to undetected vulnerabilities of software and hardware. Untrusted client devices (phones, PCs and laptops) can be infected. Any online ballot cast is open to malware attacks that could be used to manipulate vote choices. Online voting introduces the possibility that attackers can somehow obtain voters' authentication credentials. An online voting system could also be attacked over via penetration of the election server or network. It is difficult to check the accuracy of the votes recorded in the e-election results. Because the ballots are transmitted electronically, there is no way to know that the manipulated message that arrives is identical to the one sent by a voter. Therefore, the security and the risk of changing votes are the most deprecatory obstacles in an electronic voting system. It is impossible to determine the dangers on all devices in advance, especially when there are different voting methods involved. Computer viruses and hardware failures can also interrupt these processes [101]. Currently, there are examples of various programs or groups that have been attacked. These attacks can easily disrupt an online voting network, especially during the operation [11,28]. Furthermore, voting processes are generally not transparent [36]. Voting software used in applications is not accessible to the public. This leads the voter to question the trustability of the software, with the main doubt that it can be manipulated by the people in control of it. Another problem is that, if someone tries to force a voter to vote for a particular candidate, it's difficult to establish a mechanism to avoid it.

Apart from the above, it is not trivial to establish a mechanism to cross-check the counting and results by independent units. For this purpose, risk limiting audits are proposed to check the accuracy of the election results. Considering the errors found in the results calculated by statistic methods, it is stated that strong evidence is obtained for the incorrect result [102]. Unsuccessful existing practices cause a loss of motivation [103]. Due to these results, trust in electronic voting systems can generally be categorized as weak [104].

Two major e-voting applications, developed in recent years, have also identified major security risks. After the election in 2015, the Virginia Information Technologies Agency (VITA) applied security tests to several parts of their e-voting system. Physical, network, operating system, data and vote tally process were tested. VITA determined that unsafe security protocols and weak passwords were used in the system. Besides, they identified that the attacker would endanger the confidentiality and integrity of the voting data. Because of these problems, it is advised discontinuing the use of the Advanced Voting System [105]. Secondly, the Swiss government has worked for many years on the implementation of the e-voting system in the country. Swiss Post also worked on this issue and eventually opened its applications to everyone for safety tests in 2019, as they believed in the transparency of the applications. International IT experts found a critical error [106], voting manipulation that could not be detected in the shuffle method applied in the Swiss Post application source code [107]. It allows hackers to replace valid votes with fraudulent votes [108,109]. IT Experts noted that codes are not standard. The result of these critical issues the Swiss Government canceled the use of the system until the new appointment.

6.2. RQ2: Can the Blockchain Concept Improve E-Voting Systems?

There have been multiple criticisms of blockchain-based e-voting over the past few years. Some researchers stated that the blockchain system cannot solve e-voting problems and may create new vulnerabilities, such as keeping malware out of voters' phones and computers. As examples, MIT (Massachusetts Institute of Technology) experts have identified the vulnerability that has occurred in a mobile voting application used during the 2018 mid-term elections in West Virginia [110]. This vulnerability allows hackers to alter votes [98]. It even stated that blockchain can bring other additional vulnerabilities that non-blockchain systems would not suffer from [111,112]. These include security vulnerabilities in smart contracts or 51% attack is a well-known theoretically potential threat for such systems. Furthermore, malicious miners may control transactions in which items are added. Blockchain systems require software infrastructure like other e-voting systems, which are used to add or view voters' votes in the blockchain. Similar problems arise in these systems as a result of software errors [113–115]. This can be cryptographic and configuration errors, infrastructure problems, web or mobile application vulnerabilities [116]. Blockchain can contribute, especially to ensuring confidentiality and following data integrity can be specified as contributions of blockchain systems.

(i) DDOS attacks are one of the most critical challenges that are faced by the leading experts in cyber-attacks today. If some of the nodes on blockchain networks become offline as a result of the DDoS attack, the system then will continue to operate without any interruption due to its distributed nature. Whenever the nodes are brought back, everything is synced back to ensure consistency, practically making protocol and irrepressible and there would be no risk of data loss. The general architecture of blockchain is designed to avoid single points of failure. Blockchain nodes run independently and simultaneously. Therefore, blockchain provides high availability [44,51,117].

(ii) Blockchain is considered an immutable ledger for recording transactions and all participants can access the distributed ledger and its immutable records. This immutable transaction will be recorded only once and it is verifiable [14]. Therefore, none of the system participants can either modify or delete these recorded transactions leading to increase integrity and trust.

(iii) Blockchain-based e-voting provides both transparency and privacy. The participants or independent external observers can approve the voting results that are stored in the blockchain; thus, it can ensure election integrity [51].

(iv) Blockchain systems promise a cheaper cost in the long run. Installing and operating a secure data storage system in distributed architecture involves high cost and security risks. Blockchain is claimed to be safer and cheaper than standard database applications.

(v) It provides instant results. In some e-voting methods, votes should be reviewed in various voting areas and then collected in central units. While these processes consume a considerable amount of time, the announcement of the election results may also take longer. By employing e-voting with blockchain, the election results can be safely disclosed in minutes rather than hours [52].

(vi) After the first voting process, with increased confidence, more voters can participate in elections [52].

6.3. RQ3: What Are the Current Research Trends/Proposed Solutions in Blockchain-Based E-Voting System?

As the first part of the study, we tried to identify the research ideas related to how blockchain concept/technology could be a tool to implement a secure electronic voting system. In the field of blockchain-based e-voting, many e-voting schemes are proposed. The articles that we examined during the process can be categorized into five main groups (Table 4):

Table 4. Research Article Summary Matrix.

	General	Coin-Based	Privacy	Integrity	Consensus
General	[41,52,63,64,68, 72,75,81,85,86,94]	[37,83,90,93]	[47,58,73,77]	[44,49,59,79,91]	[54]
Coin-Based	[37,83,90,93]	[42,50,62,65,71, 74,76]	[26,34,46,48,51]	[22,53,57,60,61, 66,80,82,89]	[70,118]
Privacy	[47,58,73,77]	[26,34,46,48,51]		[38,46,56,61,84, 87,119]	[12]
Integrity	[44,49,59,79,91]	[22,53,57,60,61, 66,80,82,89]	[38,46,56,61,84, 87,119]	[14,30,67]	[92,95]
Consensus	[54]	[70,118]	[12]	[92,95]	[11,22]

(a) General: Many researchers published their conclusive research and pointed out that utilizing smart contracts on a blockchain platform will make a significant contribution to e-voting as it enables cost-efficiency and offers new possibilities to overcome limitations in the scalability of electronic voting systems. After reviewing both existing online voting systems and distributed systems, we have concluded that blockchain technology can be a solution that governments could adopt in order to obtain public voters' confidence and accountability [41,64,72]. From a practical point of view, in terms of development and exploitation, there are several distinct advantages and disadvantages of using blockchain-based smart contracts on electronic voting systems [79]. Blockchain can be considered as an appropriate solution in supporting complex applications with stringent security, reliability and transparency requirements pertaining in recent research [54,58,71,81]. In the proposed structure of Kshetri et al., firstly, the people authorized to vote are paid money. Then, it is stated that voting can be done by only allowing them to spend once [52]. The difference of the system proposed by Hardwick et al. from other systems proposed is a decentralized plan, allowing voters to change and update their votes during the voting period [47]. It does not offer privacy, consistency and auditability.

In addition to the general advantages of blockchain, some researchers emphasized the importance and benefits of implementing smart contracts [83] on the blockchain-based secure e-voting model [73,91]. They claimed that smart contracts simplify the use of blockchain features with 3rd party solutions and state that coercion is prevented. Na et al. proposed a web-based blockchain-based chat function and a voting system [68]. While chatting, they ensured anonymity and were able to vote at the same time. Furthermore, in some recent studies, the blockchain-based e-voting has been designed in the cloud environment with the increase of cloud-based services [85,86]. It is stated that cloud solutions provide easy access to services, superior service performance and cost advantages.

There are also studies focusing on potential technical or user-related problems due to blockchain integration. As an example, Khan et al. [93] concluded that delayed transactions on the blockchain could occur, if there is an increasing workload on the main node when transactions are simultaneously executed. On the other hand, Johnson [94] pointed out important potential risks of blockchain-based e-voting that are lack of voters' digital literacy, technical knowledge of voters and scalability of the system.

(b) Currency- and Non-Currency-Based Solutions: After the emergence and persistent use of cryptocurrencies by governments and corporations, people began to realize that one of the underlying innovations of cryptocurrencies could be used for other purposes [26]. Within this context, there are arguments that a bitcoin-based e-voting system [26,48] may allow the voting for candidates while maintaining the privacy of the individual vote. Zhao and Chan's solution used a zero-knowledge proof cryptography method [26]. In the literature, several Ethereum-based e-voting platforms are widely utilized in the electronic voting systems. Ethereum is the largest and an open-ended platform which runs on the blockchain concept [65,71]. Ether helps to enable smart contracts and distributed applications that need to be built and executed on both private and public networks [57,62,74].

Bartolucci et al. added a circle shuffle technique. However, this technique requires a central control authority. If the trusted authority becomes malicious, the entire voting protocol is destroyed. Deployment of this protocol confirms the de-linking of the electorates and their ballots [61].

Thuy et al. designed the Votereum blockchain voting system. This system is appropriate to be used in a political election because the characteristic of the implementation of voting transactions would ensure voters' privacy and security. Their system was established to support basic requirements such as robustness, privacy, verifiability and verifiability. However, this system is not capable of confirming receipt-freeness and resisting coercion [90]. Hjalmarsson et al. and Teja et al. concluded that all transactions to the voters and the government can be ensured to be safe, cost-effective and transparent [51,83]. Yavuz et al. developed the Ethereum voting app using a smart contract for the android platform. However, the main disadvantages are that it does not support the robustness and receipt of freeness features [62].

Another blockchain platform that has been adopted within the context of e-voting is Hyperledger [60,76]. Hyperledger is a private and permission-based network. It does not use any cryptocurrency or smart contracts. According to design requirements, a chaincode can be used for both the business processes and tokens. The chaincode is a program slightly different from a smart contract as it handles business logic agreed to by members of networks. It is claimed that more control over the smart contract programming language (chaincode) and restricted access usage may help to improve performance, scalability and privacy in the developed system.

Authors Zhang et al. proposed the voting system that uses the Hyperledger platform to protect end-to-end privacy. Their systems provide detectability and correctability [34]. However, it does not provide verifiability, consistency, fairness and coercion resistance.

Zcash is another public crypto-currency based solution. It distributes transaction data publicly. Zcash ensures data and privacy, unlike Bitcoin. Tarasov and Tewari proposed this solution on the blockchain. It ensures that the election is secure and transparent while providing anonymity in transactions. The underlying protocol has not been modified in any way; the voting protocol merely offers an alternative use case [85]. It should be noted that it is not coercion-resistant [42].

Sun at al. [37] on the other hand put forward Quantum blockchain as an alternative to other systems. They concluded that Quantum Blockchain simplifies electronic voting processes. Because of Quantum binding property of bid commitment and secure communication, voters cannot change submitted ballots and therefore fairness and anonymity are achieved. The main drawback of it is that it does not offer auditability consistency.

Srivastava et al. [54,55] in their article tackled scalability and security problems inherent in the election voting systems using blockchain. Instead of using the standard blockchain protocol, they decided to adopt the phantom protocol, which uses a greedy algorithm and supports large scale transactions. They stated that this method while providing solutions to scalability and security problems, it also provides a fast voting process.

On the other hand, Lai and Wu [57] designed a decentralized and anonymous blockchain-based e-voting system to maximize voters' confidence in authority or government. They designed the system so that all messages on the Ethereum blockchain and results can be viewed. In this manner, they provided transparency for the electronic voting system.

(c) Privacy: There are arguments proposing that adaptation of the new cryptographic procedures and protocol-based solutions can improve privacy and attain receipt freeness. Two recent studies presented an adaptation of solutions relying on the Chinese Remainder Theorem [96], linkable ring signature and threshold encryption system [82].

There are also other encryption-based solutions such as additively-homomorphic encryption [53,77], ring signature [38,57,119], blind signature [38,92], non-interactive zero-knowledge proofs [84,89], multi-level multi-secret sharing [95] and elliptic curve cryptography [96] to attain privacy and receipt-freeness [78]. Liu and Wang present a blockchain voting scheme without trusted third parties. It provides transparency, verifiability, consistency, auditability and anonymity, but coercion resistance

is not provided. The robustness and fairness are the limits [38]. As an example, in 2017, Wang et al. offered a large-scale voting system using the free receipt features, a one-time ring signature and a homomorphic encryption method. They analyzed the security of blockchain-based voting systems by applying smart contract-based Ethereum structure in their systems. They designed to use the homomorphic ElGamal encryption method and ring signature for protecting anonymity. However, their system does not support coercion resistance robustness [46]. Later, Shahzad and Crowcroft [91] proposed a similar framework for building and sealing blocks by using a more effective hybrid technique to secure data. The transaction pair inside the block is sealed with a hash function, while the extra use of hash function increases mathematical complexity.

Finally, Shamir's method tackles the traceability problem. Shamir's method is generally a well-accepted approach because it helps to improve traceability and control methods, specifically for voting procedures [56,61]. Such distributed data encryption techniques have been proposed for blockchain systems to increase storage efficiency.

Murtaza et al. offered a blockchain-based e-voting system that guaranteed the anonymity of voters by using Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARKs). The system used digital signatures to provide authentication, but not based on any interaction with participants [84].

Chaieb et al. aimed a secure online e-voting protocol based blockchain named Verify-Your- Vote. Their protocol promises eligibility, verifiability, fairness, vote privacy and receipt-freeness. However, this protocol does not support anonymity [92].

(d) The integrity of Data: Integrity is one of the most important criteria to consider. This involves elements such as securing the transfer of data, securing data storage and determining that the voters are the right person. A Distributed Database Management System (DDBMS) has potential advantages over traditional centralized database systems. Unfortunately, there are also disadvantages; classical DDBMS includes additional points of failures on a network between sites. Data replication adds an extra level of complexity to the distributed DBMS. Furthermore, integrity control and security of data are more difficult and database design is more complex. The use of blockchain in the distribution of databases in e-voting systems has shown that it can assist in solving the problem of database manipulation. In some voting systems, researchers proposed authentication based on various information such as national ID cards (ID number [65,109], ID card [59]) or mobile phone [66] in the registration process, along with a password. Unlike these, in others, biometric features of the voter, such as fingerprint, iris and facial characteristics, were suggested to be used for authentication [44,67]. In ID and biometric systems, the voter uses the government's identity ID Number and biometric information for verification. Therefore, fraudulent voting, problems with uncertain credentials and the same person with a false identity are eliminated. Venkatapur et al. proposed a blockchain based voting system based on Aadhar Verification. This approach ensures transparency and provides a more accurate, transparent and fair election system [59,120,121]. In a recent study, Goa et al. [87] proposed a scheme in order to prevent possible quantum computer attacks. They adapted a code-based public-key cryptographic algorithm. As a result, they concluded that this proposal provides transparency, but it is largely appropriate for small-scale elections.

(e) Consensus: Consensus algorithm is the mechanism that ensures the agreement on data and correct processing of transactions in distributed systems. Luo et al. [11] proposed the DPoS consensus algorithm in the blockchain, which improves the security and efficiency of elections. Ensuring decentralization and justice of the whole process, the election algorithm uses a ring-based consensus algorithm. For example, in 2017, McCorry et al. proposed a self-tallying Internet Voting Protocol based on blockchain. However, this system was planned to support small-scale elections and was experienced in an election that involved 40 applicants, which is an insignificant scale compared to a national election [118]. Voters send encrypted votes to the smart contract using Zero Knowledge Proof to hide their votes and to prove the validity of the vote. The protocol was based on a decentralized two-round protocol, which is called "an open vote network." It was designed for supporting a

small-scale boardroom voting. Additionally, in 2018, Hjálmarsson et al. [51] also proposed a new voting scheme based on blockchain. Their approach is based on private Ethereum blockchain and uses district-based voting. Their schemes use a smart contract to tally the results. The voters can obtain the voting information during the voting as each voter has access to the blockchain. However, the design seems quite appropriate for small-scale countries.

Li et al. [22] presented a new consensus protocol, Proof of Vote (POV), which is mainly used for blockchain. In comparison to Proof of Work (POW), the POV has a low transaction delay time to achieve controllable safety, convergence reliability and process accuracy.

Furthermore, Leonardos et al. [70] improved the PoS consensus mechanism by adding a multiplicative weight algorithm. The addition of a profiling scheme to a distributed network has posed new risks associated with the manipulation of information, such as computational overhead, valid-invalid block and updating scheme.

When selected documents are classified, they are generally determined to protect the privacy of elections. In addition to the different coin-based solutions, different signing methods were also proposed. As a result of the studies, it has been observed that the opportunities provided by blockchain systems in the field of security are prominent in 12 of 63 articles. The number of articles published per country suggests that China and India have reached the highest level in blockchain-based voting (Figure 6). The blockchain-based voting efforts of the world's most populous countries are remarkable.

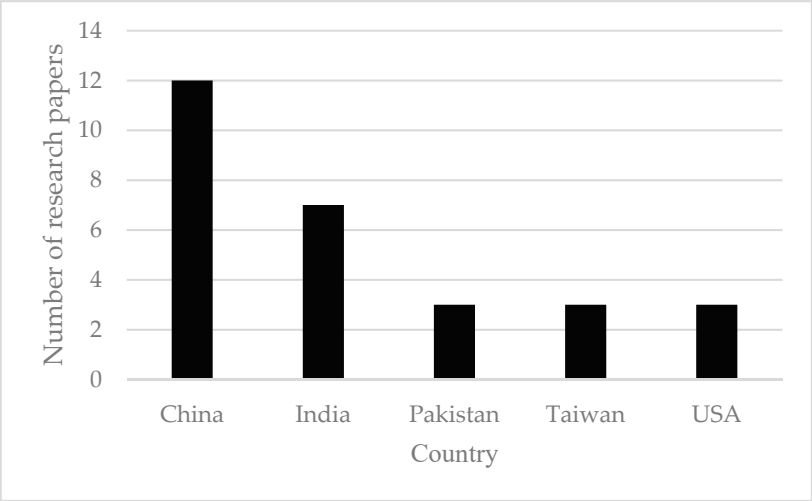

Figure 6. Journal article and proceedings papers on the blockchain voting system in the top 5 countries.

6.4. RQ4: Which Blockchain Platforms/Consensus Models Are Used?

Blockchain systems allow the development of blockchain-based applications. Bitcoin, Ethereum, Hyperledger and R3 Corda are the most renowned blockchain frameworks. We tried to find out which systems are mostly preferred for analyzing the details of the selected papers. However, we found that most of the papers containing general definitions and there were insufficient information on the technical implementation details. Many of the studies tackle the overall idea of blockchain-based e-voting and general issues affiliated with it. There seems to be a general consensus on the idea that blockchain can be applied in e-voting systems. However, technical details and implementation proposals are not explicitly stated. Nevertheless, based on the studies considered in the review, the blockchain platform usage distribution can be seen in Figure 7.

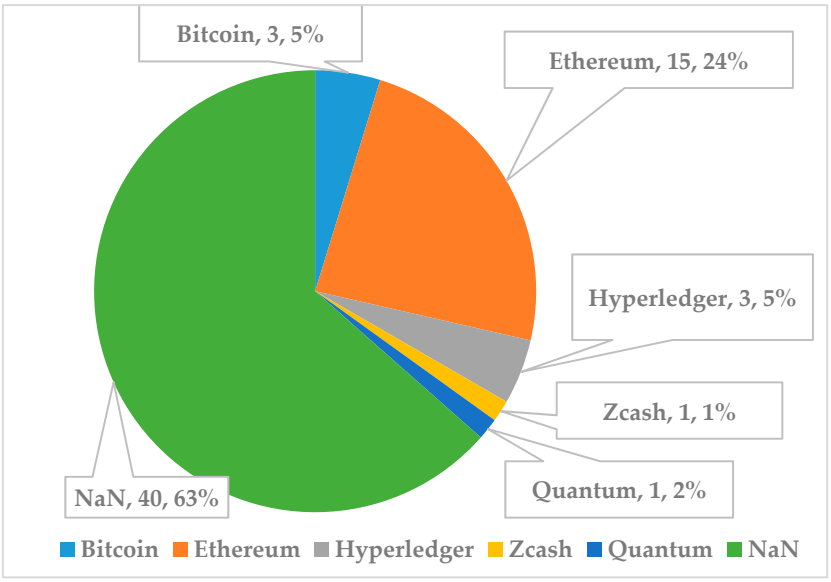

Figure 7. Blockchain framework usage rate diagram.

The most preferred blockchain platform is Ethereum (24%), with smart contracts. Secondly, Ethereum being an open-source blockchain platform permits a wide range of developers to create and deploy decentralized applications. Ethereum also uses smart contract applications and integration and flexibility qualities, which has been preferred by many developers. Although Bitcoin is only designed to validate money transactions, the Ethereum network offers a wider range of uses with smart contracts. Ethereum can trigger transactions with the criteria included in a smart contract. It performs these transactions at high speed compared to Bitcoin. While examining the blockchain platforms that were used in the previous studies, we also tried to determine which consensus algorithms have been used. However, in most of the proposals, a consensus algorithm was not clearly stated. Only three researchers indicated that the DPoS consensus model was appropriate for e-voting systems [11,22,70] unlike PoW, which consumes a lot of energy and resources [12].

6.5. RQ5: What Are the Future Research Directions for E-Voting with the Blockchain Platforms?

In general, the advantages of blockchain-based e-voting will depend on the implementation of the system. One of the main issues that need to be resolved is the doubt that possible violations of election rules specified in smart contracts or in election results can occur. Anyone who employs either a complete Bitcoin or Ethereum node by a public blockchain, by definition, can access all published data there. A possible solution may be to use a private blockchain. However, in that case, how transparency will be integrated and assured remains to be a problem requiring a solution.

Secondly, it is known that minimal intervention of the central authority is a desirable feature. However, disclosure of the intermittent voting results during the voting process may be regarded as undesirable [58]. To assure no possible intervention is carried out depending on the results, the election results must remain closed until the election process is over. Therefore, time-dependent disclosure mechanisms to guarantee results should be further investigated.

Furthermore, issues due to the blockchain itself remain to be of concern. The most important one is the issue with scalability. For instance, the performance of the system tends to decrease when there is a high rate of execution. This points to the need to further improve the system. As in the case of the transaction problem, in the 2018 elections in Turkey, the election authority [122] declared 59,369,960 voters. At least, it is necessary to have an ability to use ((59.5369.960/8 h)/60 m)/60 s = 2061.46 votes (transaction) per second, with a very rough calculation. Some researchers have proposed the use of the DPoS consensus algorithm by reducing the puzzle-solving difficulties of miners [11,46]. None of

the reviewed articles has performed a performance analysis of consensus algorithms. Consensus algorithms that can be used in real applications should be examined in detail, especially the security weaknesses in application and processes should also be examined in detail. In recent years, studies showed that some smart contracts contain vulnerabilities and are facing attacks [123], such as structure attacks (forks [124]), DDoS attacks [125] and double spending [126]. As a result of attacks, it is known that there are monetary losses [125]. As a result of compromising encryption keys, attackers can abuse the entire system. Therefore, the encryption algorithms used in such systems should be very robust.

From the above observations, it can be seen that blockchain operations need to be enriched in terms of scalability, latency, throughput, cost-effectiveness, authentication, privacy and security.

7. Threats to Validity

There are several threats that may arise when conducting a systematic mapping study. For example, not all relevant studies or sources of information may be identified [127]. In order to eliminate this threat, we have identified different search criteria and researched various databases on the topic. We have increased coverage by applying different criteria and logical operators. Using various combinations of keywords, we aimed to find all relevant documents. Although the subject is completely new, most of the research obtained after the exclusion criteria were published in 2018–2019. For this reason, we believe that the missing article review on the subject is too small to affect the findings of our study. A threat in our context is related to unpublished works or associated works that are not available in our selected scientific database. Because the selected databases are well known, the excluded publications do not affect the internal validity. Although we covered the articles according to our selection criteria, it may be argued that a margin of error may still exist because of initial sampling. Therefore, the method for calculating the MOE (margin of error) in systematic literature review studies [128] is used to check for MOE and it is calculated as 7.204%.

External validity refers to the extent the results of the study can be generalized for other situations, people and times [129]. In our systematic review, the data obtained as a result of research questions are thought to reflect general results in terms of current blockchain research and trends. Because the articles contain the results of the most recent 2010–2019 and different research from thirty countries. In addition to these articles, it was examined in articles with opposing views and in different papers obtained by snowballing.

8. Conclusions

This study aims to review and assess the recent literature on blockchain-based voting systems. The paper presents a systematic mapping study that summarizes the current research in e-voting, with blockchain technology. First, information on current e-voting systems, the blockchain concept and its applications are introduced. Then a set of gaps of current e-voting systems, potentials of the blockchain concept to improve e-voting, current solutions for blockchain-based e-voting and potential research directions on blockchain-based e-voting system are identified and discussed.

Many researchers agree that blockchain can be a suitable mechanism for a decentralized e-voting system. In addition, the voting records held in these proposed systems are transparent for all voters and independent viewers. On the other hand, we realized that most papers identified and dealt with similar topics on the blockchain-based e-voting. We grouped these issues into five categories: general, integrity, coin-based, privacy and consensus.

A number of research gaps in e-voting have presented that need to be taken into account for future studies. Scalability attacks, less transparency, use of untrusted systems and coercion resistance may have additional disadvantages and should be resolved. Since the blockchain-based e-voting systems are still required further testing, we are not fully aware of all the risks that are associated with the security and scalability of such systems. Implementing blockchain voting practices can bring unknown security risks and vulnerabilities. Blockchain systems require a more complex design in software and management skills. These critical issues should be discussed in more detail in real voting

practices using the previous experience. For this reason, e-voting systems should be applied to small pilot regions first and then its scope should be extended. The internet and voting devices still have many security weaknesses. Performing electronic voting through secure and reliable internet will require significant security advances. Although it may seem like a perfect solution, it was concluded that the blockchain system could not fully solve the problems in the voting system due to weaknesses. This study showed that blockchain systems brought issues that needed more attention and there are still many technical problems. That is why it is important to know that blockchain-based technology is still at an early stage in an e-voting solution.

Author Contributions: Conceptualization, R.T. and Ö.Ö.T.; methodology, R.T. and Ö.Ö.T.; validation, R.T. and Ö.Ö.T.; formal analysis, R.T. and Ö.Ö.T.; investigation, R.T. and Ö.Ö.T.; writing—original draft preparation, R.T. and Ö.Ö.T.; writing—review and editing, R.T. and Ö.Ö.T.; supervision, R.T. and Ö.Ö.T.; project administration, R.T. and Ö.Ö.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Ali, S.T.; Murray, J. An Overview of End-to-End Verifiable Voting Systems. *arXiv* **2016**, arXiv:160508554.
2. Daramola, O.; Thebus, D. Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections. *Informatics* **2020**, *7*, 16. [CrossRef]
3. Ryan, P.Y.A.; Schneider, S.; Teague, V. End-to-End Verifiability in Voting Systems, from Theory to Practice. *IEEE Secur. Priv.* **2015**, *13*, 59–62. [CrossRef]
4. Esteve, J.B.; Goldsmith, B.; Turner, J. International Experience with E-Voting. Available online: https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf (accessed on 15 July 2020).
5. 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]
6. Haber, S.; Stornetta, W.S. How to time-stamp a digital document. *J. Cryptol.* **1991**, *3*, 99–111. [CrossRef]
7. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 27 August 2019).
8. Bitcoin Homepage. Available online: https://bitcoin.org/ (accessed on 17 August 2019).
9. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
10. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.* **2017**, *19*. [CrossRef]
11. Luo, Y.; Chen, Y.; Chen, Q.; Liang, Q. A New Election Algorithm for DPos Consensus Mechanism in Blockchain. In Proceedings of the 2018 7th International Conference on Digital Home (ICDH), Guilin, China, 30 November–1 December 2018; pp. 116–120.
12. Solat, S. RDV: An Alternative to Proof-of-Work and a Real Decentralized Consensus for Blockchain. *arXiv* **2019**, arXiv:170705091.
13. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
14. Hanifatunnisa, R.; Rahardjo, B. Blockchain based e-voting recording system design. In Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, Indonesia, 26–27 October 2017; pp. 1–6.
15. Moura, T.; Gomes, A. Blockchain Voting and its effects on Election Transparency and Voter Confidence. In Proceedings of the 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, 7–9 June 2017; pp. 574–575.
16. Tan, B.Q.; Wang, F.; Liu, J.; Kang, K.; Costa, F. A Blockchain-Based Framework for Green Logistics in Supply Chains. *Sustainability* **2020**, *12*, 4656. [CrossRef]

17. Yahaya, A.S.; Javaid, N.; Alzahrani, F.A.; Rehman, A.; Ullah, I.; Shahid, A.; Shafiq, M. Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism. *Sustainability* **2020**, *12*, 3385. [CrossRef]
18. Gupta, Y.; Shorey, R.; Kulkarni, D.; Tew, J. The applicability of blockchain in the Internet of Things. In Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 561–564.
19. Javed, M.U.; Javaid, N.; Aldegheishem, A.; Alrajeh, N.; Tahir, M.; Ramzan, M. Scheduling Charging of Electric Vehicles in a Secured Manner by Emphasizing Cost Minimization Using Blockchain Technology and IPFS. *Sustainability* **2020**, *12*, 5151. [CrossRef]
20. Villegas-Ch, W.; Palacios-Pacheco, X.; Román-Cañizares, M. Integration of IoT and Blockchain to in the Processes of a University Campus. *Sustainability* **2020**, *12*, 4970. [CrossRef]
21. Raikwar, M.; Mazumdar, S.; Ruj, S.; Sen Gupta, S.; Chattopadhyay, A.; Lam, K.-Y. A Blockchain Framework for Insurance Processes. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–4.
22. Li, J.; Liu, Z.; Chen, L.; Chen, P.; Wu, J. Blockchain-Based Security Architecture for Distributed Cloud Storage. In Proceedings of the 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), Guangzhou, China, 12–15 December 2017; pp. 408–411.
23. Yuan, Y.; Wang, F.-Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
24. DeCusatis, C.; Zimmermann, M.; Sager, A. Identity-based network security for commercial blockchain services. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 474–477.
25. Demestichas, K.; Peppes, N.; Alexakis, T.; Adamopoulou, E. Blockchain in Agriculture Traceability Systems: A Review. *Appl. Sci.* **2020**, *10*, 4113. [CrossRef]
26. Zhao, Z.; Chan, T.-H.H. How to Vote Privately Using Bitcoin. In *Information and Communications Security*; Qing, S., Okamoto, E., Kim, K., Liu, D., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2016; Volume 9543, pp. 82–96, ISBN 978-3-319-29813-9.
27. Jardí-Cedó, R.; Pujol-Ahulló, J.; Castellà-Roca, J.; Viejo, A. Study on poll-site voting and verification systems. *Comput. Secur.* **2012**, *31*, 989–1010. [CrossRef]
28. Oo, H.N.; Aung, A.M. A Survey of Different Electronic Voting Systems. *Int. J. Sci. Eng. Technol. Res. IJSETR* **2014**, *3*, 3460–3464.
29. 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, Tangier-Tetuan, Morocco, 23–24 October 2019; pp. 1–5.
30. Yi, H. Securing e-voting based on blockchain in P2P network. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 137. [CrossRef]
31. Anane, R.; Freeland, R.; Theodoropoulos, G. e-Voting Requirements and Implementation. In Proceedings of 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; pp. 382–392.
32. Fujioka, A.; Okamoto, T.; Ohta, K. A practical secret voting scheme for large scale elections. In *Advances in Cryptology—AUSCRYPT'92*; Seberry, J., Zheng, Y., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 718, pp. 244–251, ISBN 978-3-540-57220-6.
33. Keshk, A.E.; Abdul-Kader, H.M. Development of remotely secure e-voting system. In Proceedings of the 2007 ITI 5th International Conference on Information and Communications Technology, Cairo, Egypt, 16–18 December 2007; pp. 235–243.
34. Zhang, W.; Yuan, Y.; Hu, Y.; Huang, S.; Cao, S.; Chopra, A.; Huang, S. A Privacy-Preserving Voting Protocol on Blockchain. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 401–408.
35. Ryan, P.Y.A.; Bismark, D.; Heather, J.; Schneider, S.; Xia, Z. PrÊt À Voter: A Voter-Verifiable Voting System. *IEEE Trans. Inf. Forensics Secur.* **2009**, *4*, 662–673. [CrossRef]

36. Bokslag, W.; de Vries, M. Evaluating e-voting: Theory and practice. *arXiv* **2016**, arXiv:160202509.
37. Sun, X.; Wang, Q.; Kulicki, P. A Simple Voting Protocol on Quantum Blockchain. *Int. J. Theor. Phys.* **2019**, *58*, 275–281. [CrossRef]
38. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. International Association for Cryptologic Research. 2017. Available online: https://eprint.iacr.org/2017/1043.pdf (accessed on 28 August 2019).
39. Osgood, R. The Future of Democracy: Blockchain Voting. Available online: http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgood.pdf (accessed on 26 June 2020).
40. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic mapping studies in software engineering. In Proceeding of the 12 International Conference on Evaluation and Assessment in Software Engineering, Swindon, UK, 26–27 June 2008; pp. 68–77.
41. Riemann, R.; Grumbach, S. Distributed Protocols at the Rescue for Trustworthy Online Voting. *arXiv* **2017**, arXiv:170504480.
42. Tarasov, P.; Tewari, H. Internet Voting Using Zcash. International Association for Cryptologic Research 2017. Available online: https://eprint.iacr.org/2017/585.pdf (accessed on 18 August 2019).
43. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain. In Proceedings of the 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Bangkok, Thailand, 18–20 December 2017; pp. 466–473.
44. 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; pp. 218–221.
45. Shaheen, S.H.; Yousaf, M.; Jalil, M. Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain. In Proceedings of the 2017 13th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 27–28 December 2017; pp. 1–6.
46. Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale Election Based On Blockchain. *Procedia Comput. Sci.* **2018**, *129*, 234–237. [CrossRef]
47. Hardwick, F.S.; Gioulis, A.; Akram, R.N.; Markantonakis, K. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *arXiv* **2018**, arXiv:180510258.
48. Bao, Z.; Wang, B.; Shi, W. A Privacy-Preserving, Decentralized and Functional Bitcoin E-Voting Protocol. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 252–256.
49. Panja, S.; Roy, B.K. A Secure End-to-End Verifiable E-Voting System Using Zero Knowledge Based Blockchain. International Association for Cryptologic Research 2018. Available online: https://eprint.iacr.org/2018/466.pdf (accessed on 18 August 2019).
50. Wu, W.-J.L. An efficient and effective Decentralized Anonymous Voting System. *arXiv* **2018**, arXiv:180406674.
51. Hjálmarsson, F.P.; Hreioarsson, G.K.; Hamdaqa, M.; Hjalmtysson, 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; pp. 983–986.
52. Kshetri, N.; Voas, J. Blockchain-Enabled E-Voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
53. Dagher, G.G.; Marella, P.B.; Milojkovic, M.; Mohler, J. BroncoVote: Secure Voting System using Ethereum's Blockchain. In Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Madeira, Portugal, 22–24 January 2018; pp. 96–107.
54. Srivastava, G.; Dhar Dwivedi, A.; Singh, R. Crypto-democracy: A Decentralized Voting Scheme using Blockchain Technology. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, Porto, Portugal, 26–28 July 2018; pp. 674–679.
55. Srivastava, G.; Dwivedi, A.D.; Singh, R. Phantom Protocol as the New Crypto-Democracy. In *Computer Information Systems and Industrial Management*; Saeed, K., Homenda, W., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018; Volume 11127, pp. 499–509, ISBN 978-3-319-99953-1.

56. Fusco, F.; Lunesu, M.I.; Pani, F.E.; 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, Seville, Spain, 18–20 September 2018; pp. 223–227.
57. Lai, W.-J.; Hsieh, Y.; Hsueh, C.-W.; Wu, J.-L. DATE: A Decentralized, Anonymous, and Transparent E-voting System. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 24–29.
58. Heiberg, S.; Kubjas, I.; Siim, J.; Willemson, J. On Trade-offs of Applying Blockchains for Electronic Voting Bulletin Boards. International Association for Cryptologic Research 2018. Available online: https://eprint.iacr.org/2018/685.pdf (accessed on 18 August 2019).
59. Venkatapur, R.B.; Prabhu, B.; Navya, A.; Roopini, R.; Niranjan, S.A. Electronic Voting Machine Based on Blockchain Technology and Aadhar Verification. *Int. J. Innov. Eng. Sci.* **2018**, *3*, 12–15.
60. Yu, B.; Liu, J.; Amin, S.; Nepal, S.; Steinfeld, R.; Rimba, P.; Au, M.H. Platform-Independent Secure Blockchain-Based Voting System. International Association for Cryptologic Research 2018. Available online: https://eprint.iacr.org/2018/657.pdf (accessed on 18 August 2019).
61. 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–3 June 2018; pp. 30–34.
62. Yavuz, E.; Koc, A.K.; Cabuk, U.C.; Dalkilic, G. Towards secure e-voting using ethereum blockchain. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–7.
63. Pawlak, M.; Poniszewska-Marańda, A.; Kryvinska, N. Towards the intelligent agents for blockchain e-voting system. *Procedia Comput. Sci.* **2018**, *141*, 239–246. [CrossRef]
64. Dricot, L.; Pereira, O. SoK: Uncentralisable Ledgers and their Impact on Voting Systems. *arXiv* **2018**, arXiv:180108064.
65. Shukla, S.; Thasmiya, A.N.; Shashank, D.O.; Mamatha, H.R. Online Voting Application Using Ethereum Blockchain. In Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 19–22 September 2018; pp. 873–880.
66. Khoury, D.; Kfoury, E.F.; Kassem, A.; Harb, H. Decentralized Voting Platform Based on Ethereum Blockchain. In Proceedings of the 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), Beirut, Lebanon, 14–16 November 2018; pp. 1–6.
67. 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; pp. 22–27.
68. Na, S.; Park, Y.B. Web-based Nominal Group Technique Decision Making Tool Using Blockchain. In Proceedings of the 2018 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 29–31 January 2018; pp. 1–6.
69. Li, Y.; Susilo, W.; Yang, G.; Yu, Y.; Liu, D.; Guizani, M. A Blockchain-based Self-tallying Voting Scheme in Decentralized IoT. *arXiv* **2019**, arXiv:190203710.
70. Leonardos, S.; Reijsbergen, D.; Piliouras, G. Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 376–384.
71. Zhang, Q.; Xu, B.; Jing, H.; Zheng, Z. Ques-Chain: An Ethereum Based E-Voting System. *arXiv* **2019**, arXiv:190505041.
72. Schiedermeier, M.; Hasan, O.; Mayer, T.; Brunie, L.; Kosch, H. A transparent referendum protocol with immutable proceedings and verifiable outcome for trustless networks. *arXiv* **2019**, arXiv:190906462.
73. Sadia, K.; Masuduzzaman, M.; Paul, R.K.; Islam, A. Blockchain Based Secured E-voting by Using the Assistance of Smart Contract. *arXiv* **2019**, arXiv:191013635.
74. Fan, X.; Li, P.; Zeng, Y.; Zhou, X. Implement Liquid Democracy on Ethereum: A Fast Algorithm for Realtime Self-tally Voting System. *arXiv* **2020**, arXiv:191108774.
75. Bulut, R.; Kantarci, A.; Keskin, S.; Bahtiyar, S. Blockchain-Based Electronic Voting System for Elections in Turkey. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 183–188.

76. Gajek, S.; Lewandowsky, M. Trustless, Censorship-Resilient and Scalable Votings in the Permission-based Blockchain Model. *Int. Assoc. Cryptologic Res.* **2019**.
77. Lee, J.; Choi, J.; Kim, J.; Oh, H. SAVER: SNARK-friendly, Additively-homomorphic, and Verifiable Encryption and decryption with Rerandomization. *Int. Assoc. Cryptologic Res.* **2019**.
78. Dimitriou, T. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting. International Association for Cryptologic Research 2019. Available online: https://eprint.iacr.org/2019/617.pdf (accessed on 11 November 2019).
79. Sudharsan, B.; Tharun, R.V.; Krishna, N.M.P.; Raj, B.J.; Arvindh, S.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, BC, Canada, 17–19 October 2019; pp. 0675–0681.
80. Vijayalakshmi, V.; Vimal, S. A Novel P2P based System with Blockchain for Secured Voting Scheme. In Proceedings of the 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 14–15 March 2019; pp. 153–156.
81. Bosri, R.; Uzzal, A.R.; Omar, A.A.; Hasan, A.S.M.T.; Bhuiyan, M.Z.A. Towards a Privacy-Preserving Voting System Through Blockchain Technologies. In Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019; pp. 602–608.
82. Lyu, J.; Jiang, Z.L.; Wang, X.; Nong, Z.; Au, M.H.; Fang, J. A Secure Decentralized Trustless E-Voting System Based on Smart Contract. In Proceedings of the 2019 18th IEEE International Conference on Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5–8 August 2019; pp. 570–577.
83. Teja, K.; Shravani, M.; Simha, C.Y.; Kounte, M.R. Secured voting through Blockchain technology. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1416–1419.
84. Murtaza, M.H.; Alizai, Z.A.; Iqbal, Z. Blockchain Based Anonymous Voting System Using zkSNARKs. In Proceedings of the 2019 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 27–29 August 2019; pp. 209–214.
85. Sathya, V.; Sarkar, A.; Paul, A.; Mishra, S. Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting. In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 1075–1079.
86. Bellini, E.; Ceravolo, P.; Damiani, E. Blockchain-Based E-Vote-as-a-Service. In Proceedings of the 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), Milan, Italy, 8–13 July 2019; pp. 484–486.
87. 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]
88. Vangulick, D.; Cornelusse, B.; Ernst, D. Blockchain: A Novel Approach for the Consensus Algorithm Using Condorcet Voting Procedure. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019; pp. 1–10.
89. Matile, R.; Rodrigues, B.; Scheid, E.; Stiller, B. CaIV: Cast-as-Intended Verifiability in Blockchain-based Voting. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 24–28.
90. Thuy, L.V.-C.; Cao-Minh, K.; Dang-Le-Bao, C.; Nguyen, T.A. Votereum: An Ethereum-Based E-Voting System. In Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), Danang, Vietnam, 20–22 March 2019; pp. 1–6.
91. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* **2019**, *7*, 24477–24488. [CrossRef]
92. Chaieb, M.; Koscina, M.; Yousfi, S.; Lafourcade, P.; Robbana, R. DABSTERS: Distributed Authorities using Blind Signature to Effect Robust Security in e-Voting. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, Prague, Czech Republic, 26–28 July 2019; pp. 228–235.
93. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Future Gener. Comput. Syst.* **2020**, *105*, 13–26. [CrossRef]

94. Johnson, D. Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values? *Eur. J. Risk Regul.* **2019**, *10*, 330–358. [CrossRef]
95. Li, J.; Wang, X.; Huang, Z.; Wang, L.; Xiang, Y. Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. *J. Parallel Distrib. Comput.* **2019**, *130*, 91–97. [CrossRef]
96. Tso, R.; Liu, Z.-Y.; Hsiao, J.-H. Distributed E-Voting and E-Bidding Systems Based on Smart Contract. *Electronics* **2019**, *8*, 422. [CrossRef]
97. Nevo, S.; Kim, H. How to compare and analyse risks of internet voting versus other modes of voting. *Electron. Gov. Int. J.* **2006**, *3*, 105. [CrossRef]
98. Abazorius, A. MIT Researchers Identify Security Vulnerabilities in Voting App. Available online: http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213 (accessed on 3 April 2020).
99. Lauer, T.W. The risk of e-voting. *Electron. J. E-Gov.* **2004**, *2*, 177–186.
100. Cardillo, A.; Essex, A. The Threat of SSL/TLS Stripping to Online Voting. In *E-Vote-ID 2018: Electronic Voting*; Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schürmann, C., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018; Volume 11143, pp. 35–50, ISBN 978-3-030-00419-4.
101. Susskind, J. Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System. *San Diego Law Rev.* **2017**, *54*, 785–821.
102. Bernhard, M.; Benaloh, J.; Alex Halderman, J.; Rivest, R.L.; Ryan, P.Y.A.; Stark, P.B.; Teague, V.; Vora, P.L.; Wallach, D.S. Public Evidence from Secret Ballots. In *Electronic Voting*; Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schürmann, C., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10615, pp. 84–109, ISBN 978-3-319-68686-8.
103. Palas Nogueira, J.; de Sá-Soares, F. Trust in E-Voting Systems: A Case Study. In *Knowledge and Technologies in Innovative Information Systems*; Lecture Notes in Business Information Processing; Rahman, H., Mesquita, A., Ramos, I., Pernici, B., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 129, pp. 51–66, ISBN 978-3-642-33243-2.
104. Achieng, M.; Ruhode, E. The adoption and challenges of electronic voting technologies within the South African context. *arXiv* **2013**, arXiv:13122406. [CrossRef]
105. Security Assessment of Winvote Voting Equipment for Department of Elections. Available online: https://www.wired.com/wp-content/uploads/2015/08/WINVote-final.pdf (accessed on 3 April 2020).
106. Zetter, K. Experts Find Serious Problems with Switzerland's Online Voting System Before Public Penetration Test Even Begins. Available online: https://www.vice.com/en_us/article/vbwz94/experts-find-serious-problems-with-switzerlands-online-voting-system-before-public-penetration-test-even-begins (accessed on 8 January 2020).
107. Kuenzi, R. These are the Arguments that Sank E-Voting in Switzerland. Available online: https://www.swissinfo.ch/eng/e-voting_these-are-the-arguments-that-sank-e-voting-in-switzerl;/45136608 (accessed on 8 January 2020).
108. Lewis, S.J.; Pereira, O.; Teague, V. The Use of Trapdoor Commitments in Bayer-Groth Proofs and the Implications for the Verifiabilty of the Scytl-SwissPost Internet Voting System. Available online: https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf (accessed on 3 April 2020).
109. Stone, J. Backdoor Discovered in Swiss Voting System Would Have Allowed Hackers to Alter Votes. Available online: https://www.cyberscoop.com/swiss-voting-system-flaw-encryption/ (accessed on 3 April 2020).
110. Specter, M.A.; Koppel, J.; Weitzner, D. The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Available online: https://www.usenix.org/system/files/sec20-specter.pdf (accessed on 3 June 2020).
111. Bollinger, L.C.; McRobbie, M.A. Ensuring the Integrity of Elections. In *Securing the Vote: Protecting American Democracy*; National Academies of Sciences: Washington, DC, USA, 2018; pp. 103–105, ISBN 978-0-309-47647-8.
112. Abuidris, Y.; Hassan, A.; Hadabi, A.; Elfadul, I. Risks and Opportunities of Blockchain Based on E-Voting Systems. In Proceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 14–15 December 2019; pp. 365–368.
113. Juels, A.; Eyal, I.; Naor, O. Blockchains won't Fix Internet Voting Security could Make it Worse. Available online: https://theconversation.com/blockchains-wont-fix-internet-voting-security-and-could-make-it-worse-104830 (accessed on 3 April 2020).
114. Goodman, R.; Halderman, J.A. Internet Voting is Happening Now. Available online: https://slate.com/technology/2020/01/internet-voting-could-destroy-our-elections.html (accessed on 15 July 2020).

115. Park, S.; Specter, M.; Narula, N.; Rivest, R.L. Going from Bad to Worse: From Internet Voting to Blockchain Voting. Available online: https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf (accessed on 17 July 2020).
116. Bull, C.; Gjøsteen, K.; Nore, H. *Faults in Norwegian Internet Voting*; TUT Press: Lochau, Austria; Bregenz, Austria, 2018; pp. 166–169.
117. Pathak, A.; Wasay, A.; Singh, C.; Bhavan, R.; Umale, J. Design and implementation of a secure and robust voting system based on blockchain. *Int. J. Adv. Res. Ideas Innov. Technol.* **2018**, *4*, 869–875.
118. McCorry, P.; Shahandashti, S.F.; Hao, F. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. In *Financial Cryptography and Data Security*; Kiayias, A., Ed.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10322, pp. 357–375, ISBN 978-3-319-70971-0.
119. Mercer, R. Privacy on the Blockchain: Unique Ring Signatures. *arXiv* **2016**, arXiv:161201188.
120. Roopak, T.M.; Sumathi, R. Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology. In Proceedings of the 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 5–7 March 2020; pp. 71–75.
121. Juno Bella Gracia, S.V.; Raghav, D.; Santhoshkumar, R.; Velprakash, B. Blockchain Based Aadhaar. In Proceedings of the 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 21–22 February 2019; pp. 173–177.
122. Domestic and Overseas Voters Gender Statistics. Available online: http://www.ysk.gov.tr/doc/dosyalar/docs/24Haziran2018/2018CBMV-SecmenCinsiyet.pdf (accessed on 18 August 2019).
123. Xu, J.J. Are blockchains immune to all malicious attacks? *Financ. Innov.* **2016**, *2*, 25. [CrossRef]
124. Wang, S.; Wang, C.; Hu, Q. Corking by Forking: Vulnerability Analysis of Blockchain. In Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 829–837.
125. Saad, M.; Spaulding, J.; Njilla, L.; Kamhoua, C.; Shetty, S.; Nyang, D.; Mohaisen, A. Exploring the Attack Surface of Blockchain: A Systematic Overview. *arXiv* **2019**, arXiv:190403487.
126. Ramezan, G.; Leung, C.; Jane Wang, Z. A Strong Adaptive, Strategic Double-Spending Attack on Blockchains. 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; pp. 1219–1227.
127. Vegendla, A.; Duc, A.N.; Gao, S.; Sindre, G. A Systematic Mapping Study on Requirements Engineering in Software Ecosystems. *J. Inf. Technol. Res.* **2018**, *11*, 49–69. [CrossRef]
128. Kosar, T.; Bohra, S.; Mernik, M. A Systematic Mapping Study driven by the margin of error. *J. Syst. Softw.* **2018**, *144*, 439–449. [CrossRef]
129. Silva, R.A.; de Souza, S.D.R.S.; de Souza, P.S.L. A systematic review on search based mutation testing. *Inf. Softw. Technol.* **2017**, *81*, 19–35. [CrossRef]