electronics

Article

Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections

Robin Singh Bhadoria [1,*], Arka Prabha Das [2], Abul Bashar [3] and Mohammed Zikria [3]

[1] Department of Computer Engineering & Applications, GLA University, Mathura 281406, Uttar Pradesh, India
[2] Indian Institute of Information Technology (IIIT) Bhopal, Bhopal 462003, Madhya Pradesh, India
[3] College of Computer Engineering and Science, Prince Mohammad Bin Fahd University, Al-Khobar 31952, Saudi Arabia
* Correspondence: robin19@ieee.org

Abstract: A democratic election is a crucial event in any country. Therefore, the government of the country is concerned with creating more competitive and fairer elections. This paper discusses the survey and scope of Blockchain technology adoptions in conducting elections. A distributed digital ledger is used in the Blockchain technology that is utilized for recording transactions happening between two parties. Ledger conducts this processing in an efficient and effective manner with latest secure mechanism of encryption algorithms. Therefore, the data stored in several blocks in each transaction is secure, transparent, and tamper-proof, which ultimately improves the transparency and voter confidentiality. This paper demonstrates how the benefits of the Blockchain technology such as immutability, transparency and end-to-end verifiability can be utilized by the national governments around the world to ensure fair democratic elections. In short, we aim to present a rigorous mechanism of a Blockchain based e-voting system, its efficiency based on different consensus algorithms and the overall progress and analysis based on some critical parameters to anticipate the feasibility of the successful implementation of the proposed e-voting system.

Keywords: Blockchain technology; e-voting system; smart contract; distributed ledger; transparency and confidentiality

Citation: Bhadoria, R.S.; Das, A.P.; Bashar, A.; Zikria, M. Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections. *Electronics* **2022**, *11*, 3359. https://doi.org/10.3390/electronics11203359

Academic Editor: Hamed Taherdoost

Received: 6 September 2022
Accepted: 29 September 2022
Published: 18 October 2022

1. Introduction

The most common means of vote casting is through ballot papers. This method has been widely criticized because of fraudulent voting and booth capturing witnessed across various countries worldwide. Thus, manually casting the vote has been replaced with electronic machines to record the vote for individual citizens of the country. The machines saved paper costs and reduced time and replaced the manual exercise involved in conventional counting and resulted in dumping of fake votes. Such voting machines introduced more transparency and verifiability to its voters [1].

Even after all these replacements, several concerns still remain for voters. The Distributed Ledger Technology (DLT) can be combined with such voting machines to make the electoral process more robust and error-free. DLT is secured and immutable through the use of complex encryption algorithms. In simple terms, Blockchain is defined as a distributed database whose copy is issued to everyone involved in the transaction process [2]. One can add records in the database but cannot alter them. Therefore, data stored inside the Blockchain is secure, transparent, and tamper-proof.

A distributed digital ledger is used in Blockchain technology that is utilised for recording transactions happening between two parties. This task is achieved by the ledger in a very efficient manner. In creating chain of blocks, each block comprises of data and its associated hash value of previously created block in such a chain [3]. The data stored inside such blocks may depend on the type of Blockchain, especially its version. "Hash"

is the second element that is always unique, very similar to a human fingerprint that can be identified amongst trillions of hands. Hash is calculated just after the creation of a block and the Hash identifies the block along with its contents. Any manipulations in the block will automatically cause changes in its associated hash value [4]. Thus, the role of hash is very significant in identification of any block, if it is modified. This gives unique characteristic for Blockchain, and each block is linked or chained in sequence to one another. The first block is an initial block, and thus it does not have any hash value and is also known as the *genesis block*. When anyone tries to modify or alter the data in any block, the hash value associated with the blocks also gets modified which helps in identification of such block and make it as "*invalid*". This scenario makes a chain of blocks as more secure and immutable.

The conceptualization of Blockchain Technology is creating a number of records, namely blocks, that hold data and its associated generated hash value (always *unique*). It creates a distributed ledger that keeps a record of all data for every transaction [5]. Three major pillars of the Blockchain are immutability, decentralized and transparency. Such a technique is also known as Distributed Ledger Technology (DLT) as demonstrated in Figure 1.

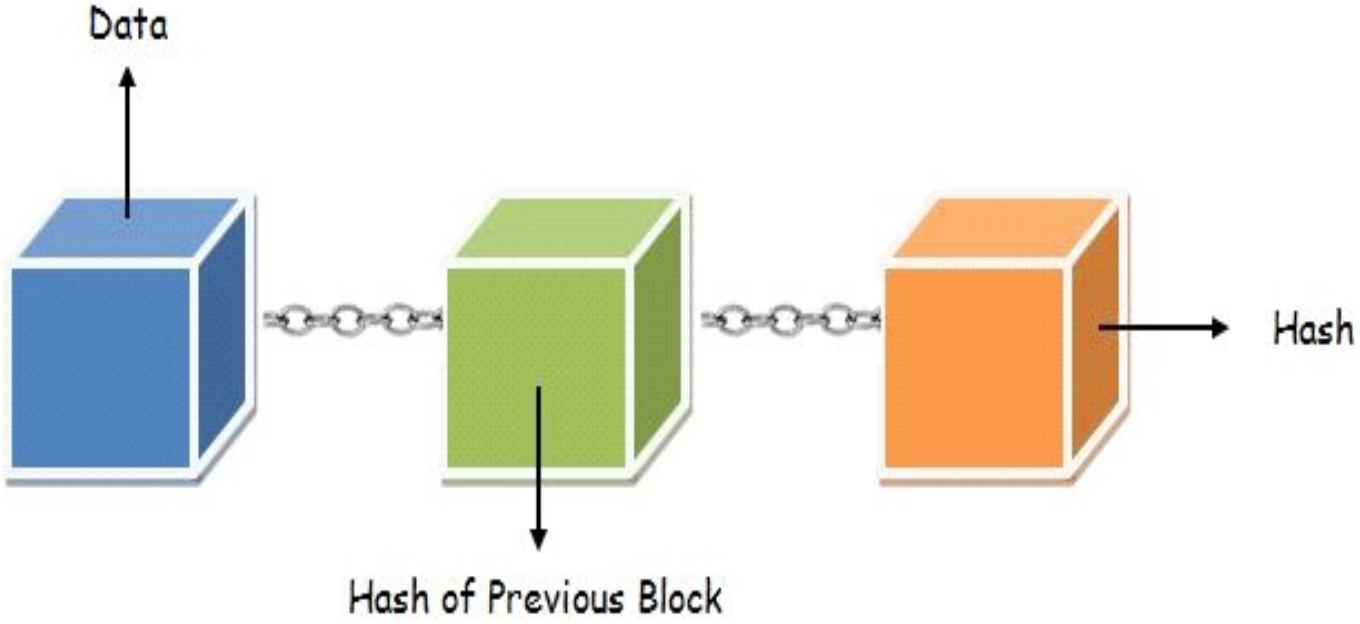

Figure 1. Blockchain based Traceable Certificates in a Distributed Ledger.

1.1. Three Pillars of Blockchain Technology

1.1.1. Decentralization

The need of the decentralized system can only be understood when we are aware about the vulnerabilities of a centralized system that is used in a traditional fund transfer system. Banks and client-server model are examples of the centralized system in which bank as a central authority controls the entire transaction process [6].

To address such limitations, the idea of a decentralized system is introduced in which data has been utilized to store, record and synchronize transactions at different nodes. In decentralization, every node can make transaction associated with the data. Blockchain Technology has been established with the aid of distributed networks, digital signature and encryption/decryption techniques from the security domain. A decentralized system uses peer-to-peer (P2P) networks in which every node can own the copy of the complete data in the chain of blocks [7].

1.1.2. Transparency

Generally, Blockchain transactions are not encrypted. Current block stores the hash of the previous block. The encryption technique is used in Blockchain which ultimately secures the data. Thus, this characteristic enables Blockchain technology to maintain transparency and privacy in the entire network nodes of peer connection. The identity of an individual node is kept hidden through the use of complex cryptographic unique alphanumeric characters and usually symbolized only by its public identifier/address [8].

1.1.3. Immutability

This term is used to depict something that has entered into the chain of blocks and can never be modified or altered in anyway. Even though the data can be added to the chain, but already existing blocks of data cannot be altered. Due to cryptographic hash function, such property is exhibited by Blockchain Technology. Moreover, hashing is a methodology or technique in which the input data length is a variable quantity whereas the output length is fixed [9].

2. Role of Blockchain in Overall Governance

Blockchain can not only be utilized in elections but can also be used to improve overall governance by incorporating it in property registry systems [10], public sector banking [11], healthcare [12] and building smart cities [13]. All the sectors which are prone to cyber-crimes can be made secure with the help of Blockchain. Thus, the novelty of the proposed research lies in developing theoretical approach for sustainable development of the society on the basis of the Blockchain-based Traceable Certificates. The major benefits of Blockchain adoption specifically into an e-Election can be listed below [14]:

- The first benefit that Blockchain can bring about is transparency. Decentralized ledger of Blockchain records result—in accuracy and safety thus ensuring trust at every stage of the voting process;
- Immutable public ledger enables the tracking and counting of votes while being visible to everyone. This feature of Blockchain provides legitimacy of the voting;
- Blockchain and its distributed ledger provides an unhackable system as there is no involvement of fallible or corruptible central body;
- Blockchain allows for anonymity during voting by providing private keys to the voters. These applications of such private keys keep the votes polled by the voters anonymous;
- Processing time is reduced in Blockchain because results can be gathered and processed quickly soon after the completion of the voting phase.
- Blockchain as an Ultimate Solution for Securing Elections

This idea of Blockchain in conducting secure election has previously been implemented by companies such as Agora and Polys but the former was not able to justify its presence and had a controversy with the Sierra Leone government while the latter never achieved scalability in any state election. There have been several challenges which need to be kept in mind while designing system for e-Election conduction [14,15]:

- Difficulty in integration with legacy systems;
- Complexity and lack of Blockchain talented personnel;
- Lack of scalability;
- Lack of interoperability;
- Lack of good governance;
- Lack of user experience and education.

Several noteworthy attempts have been made recently, but none of them have achieved the scalability which is required for Blockchain based voting to be successful as depicted in Table 1 [16,17].

Table 1. Adoption of Blockchain Technology in e-Election and the reported vulnerabilities.

Year	Country	Consequences
August, 2018	Tsukuba, Japan	Tested only for social purposes but not for elections. (State Sponsored)
November, 2018	West Virginia, USA	All vulnerabilities are not covered. (Boston based Voatz named app)
March, 2018	Sierra Leone	Officially not accepted. (Switzerland based company name Agora)
June, 2019	Russia	Moscow City election conducted
June 2020	African Nations	Flexibility and adequate security to the election procedure.

Due to the presence of the above-mentioned properties and after looking at the frauds that occurred in digital electoral systems as discussed in Table 2, it is recommended that the Blockchain technology is used in Electronic Voting Machines to make them more intelligent and secure [18,19].

Table 2. Consequences of electoral frauds in various countries.

Country	Issue
India	Booth capturing and rigging
United States of America	Rigging via hacking
Russia	Ballot stuffing
United Kingdom	Proxy voting
Nigeria, South Africa	Voter impersonation and booth capturing
Germany	EVMs have been prone to hacking
Netherlands	EVMs lack of transparency
Ireland	EVMs lack of transparency and trust

The perception associated with the casting of a vote by authorized voters can be visualized in Figure 2, that justifies the usage of Blockchain technology in such a system [20,21]. When a fraud voter penetrates the system through fake credentials it can immediately be reported at the zonal office by authorities. Such malicious activities can easily be determined through Blockchain technology [22]. The first block called *genesis block* is created with legitimate data associated with transaction identity, source/destination address, voter/candidate details, etc.

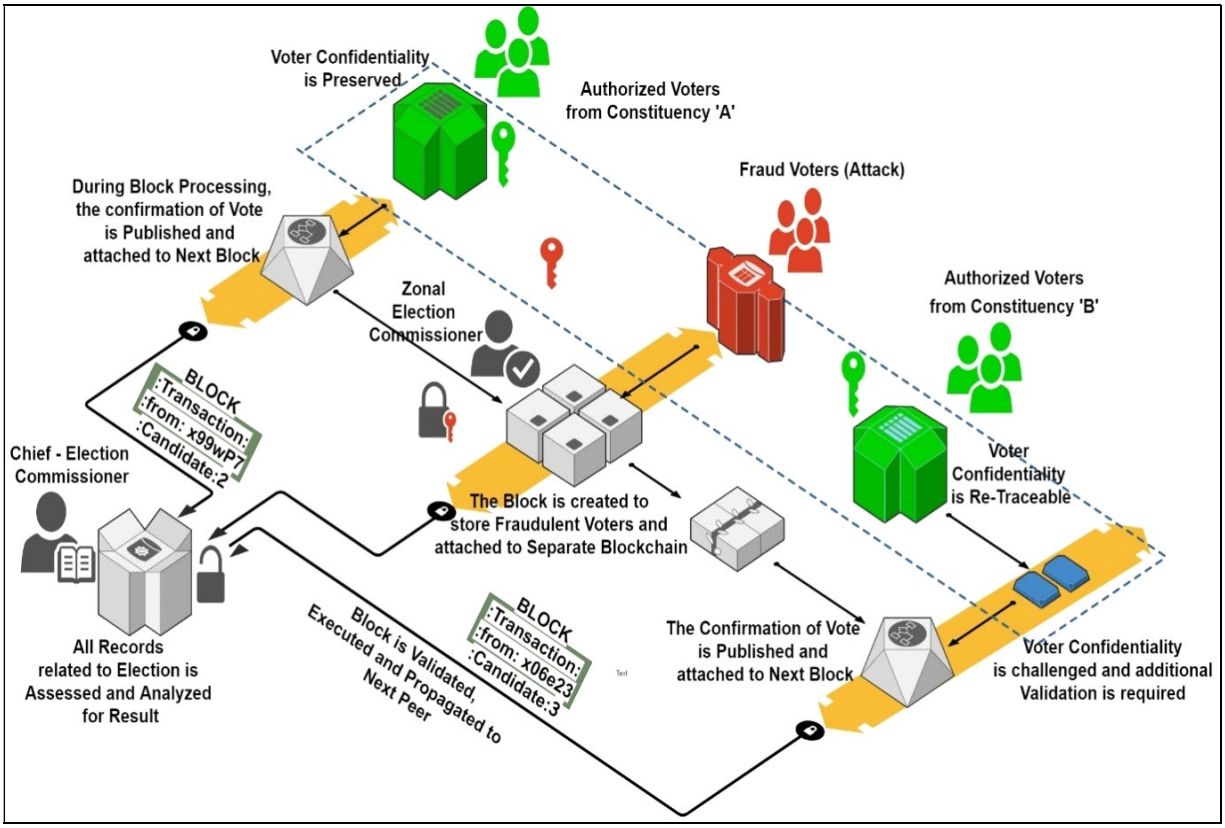

Figure 2. Casting of Electronic Vote through Blockchain based Traceable Certificates.

3. Material & Methods

Before studying the working of Blockchain technology in electronic voting, it is important to know the vulnerabilities in today's election in detail. Several parameters may influence any e-voting processes that are as follows [23,24]:

Hacked voter registration databases: Cyber-attack on voter's registration database can also threaten people's ability to vote. A registration database consists of information such as voter's name, phone number, address, etc. Such information is known as Personally Identifiable Information (PII). Hackers can exploit the stored information by selling it on the dark web and use it to target potential voters with disinformation and to gain benefits.

Hacked voting hardware: Any type of electronic device or software used in the machine is subject to cyber-attacks. Results stored in these devices can be vulnerable to hacking. Hackers need only one single point to breach an entire model of the voting machine. Attackers may also inject malware into machines developed by reputed companies to cause a dangerous effect on the votes of millions of voters [25,26].

Compromised election reporting systems: Reporting systems could be manipulated to announce false results. If automated data streams are used to inform the results to news organizations, then attackers may manipulate data streams and trick news organizations to announce the wrong winner. In this context, highly realistic fake videos can be created announcing bogus winners using Generative Adversarial Networks (GANs). It is a type of Neural Network used to carry out unsupervised learning. GANs can be utilized by attackers to fabricate audio, video, and image content, which seem realistic and plausible.

Post-election audits: The procedure used to count the votes and the equipment are checked for their correctness. If any bug or error is found during the audit, election officials are informed, and they can act as a deterrent against fraud. However, experts believe that voting machines that only record votes electronically are not suitable for ensuring election integrity.

A glimpse of Election Security: There are three stages in an election process: pre-election, election, and post-election. There are several steps that are followed in an election process, as shown in Figure 3. The process also contains several vulnerabilities which need to be identified to prevent future attacks.

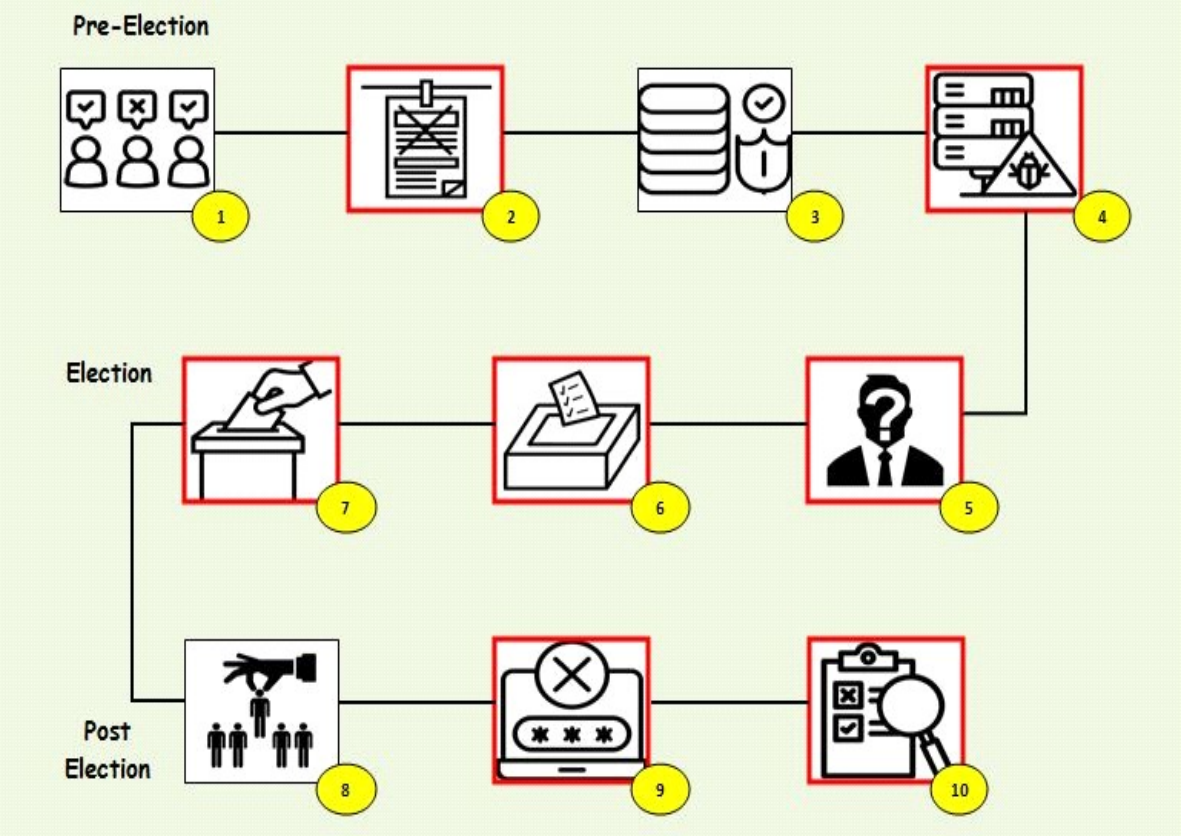

Figure 3. Election process and its vulnerabilities.

Sept.1 Voter forms a political opinion;
Sept.2 Disinformation campaign against the voter;
Sept.3 Voter enters their name in a voter registration database;
Sept.4 Hackers attack the voter registration database and alter the records;
Sept.5 Voter is unable to find their record because of altered voter record;
Sept.6 If a voter casts a vote, their vote could be changed by a hacked voting machine;
Sept.7 Voter's vote could be miscounted due to tampering caused in the machine;
Sept.8 A winner is declared;
Sept.9 Reporting systems are compromised to spread alternative results;
Sept.10 Mismatch in the results causes dispute over election's integrity which prompts a post-election audit that can be vulnerable to inaccuracies.

Steps shown in Figure 3 as highlighted into red color rectangular depicts the vulnerabilities and possible breach into security [27].

3.1. Consensus Protocol for a Common Understanding in Generating Certificates

There is a need for a common point of understanding in a decentralized consensus mechanism. This can be termed as Proof of Work (PoW) in which a certain procedure is used to validate the transaction in a given peer-network and creates a new block for consortium Blockchain [28,29]. Consensus is a kind of agreement that must be taken up by each participating node in consortium. There can be major algorithms for consensus protocol for different features as depicted in Table 3.

Table 3. Various Consensus Algorithms with Major Features.

Feature	Proof of Work (PoW)	Byzantine Fault Tolerance (BFT)	Proof of Capacity (PoC)	Proof of Burn (PoB)	Proof of Stake (PoS)
Consistency	Y	Y	Y	Y	N
Scalability	Y	Y	Y	Y	Y
Partition Tolerance	N	Y	N	N	N
Efficient	N	Y	N	Y	Y

3.2. Algorithms for Voting & Publishing Schemes

During the processing of each block after the casting of the vote by the authorized voter using Blockchain based election, the data associated with the elected candidate and voter itself is stored within the block. Such block is published and attached to the next block that creates a chain in series [30,31]. The smart contract is created by the chief election commissioner (administrator) in respective blocks.

If a voter wishes to REGISTER for casting their vote, then the voter must ensure to SETUP for predefined system software possessed by Chief Election Commissioner ed authority) [32]. The voter should use CREDENTIALS to cast their vote through e-ballot. This can be recorded with a digital signature with mentioned VALIDITY. The job of a legitimate voter is specified in Algorithm 1.

Algorithm 1: Voting Scheme for individual voters

Voting Scheme for individual voters
Initially, SETUP the device as per the requirement of system software
If the Voter is not REGISTERED then
Use CREDENTIALS to REGISTER with verification
Cast a Vote with DIGITAL SIGNATURE
VALIDITY of the e-ballot for particular session END

After casting a vote by the authorized voter, it is the duty of the election commissioner (administrator) to PUBLISH the vote [33]. This should be verified first by VALIDATE and then APPEND it to the next block in the series. This process is depicted in Algorithm 2.

Algorithm 2: Publish Scheme for Vote by Election Commissioner

Publish Scheme for Vote by Election Commissioner
Firstly, CHECK the VALIDITY for the e-ballot
If VALIDITY is FALSE then
e-ballot can be CANCELLED
Otherwise,
e-ballot can be PUBLISHED and APPENDED to the next block

3.3. Blockchain as the Solution to Vulnerabilities

Let us understand how Blockchain affects the voting process as shown in Figure 4 [34,35].

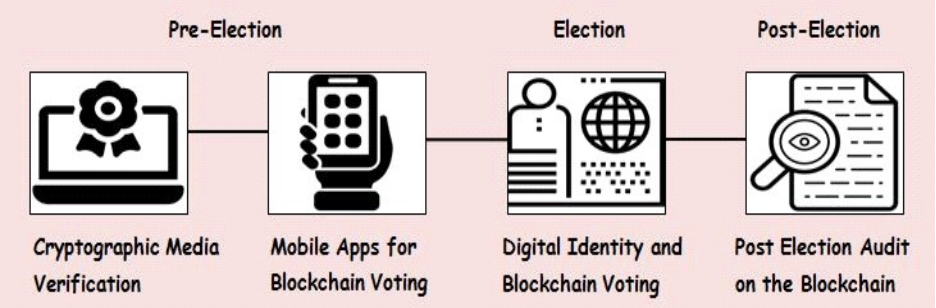

Figure 4. Securing Election Process through Blockchain based Traceable Certificate.

- Cryptographic Media Verification: Cryptographic techniques would help to determine the trusted and accountable sources of information. Voters would only consume the information that is stamped with a unique cryptographic identifier. In this work, the practice of "Cryptographic media verification" is based on previous existing unique cryptographic identifier created by authorized persons (in the government).
- Mobile Apps for Blockchain Voting: Voting through mobile apps would increase voter's participation in an election process and adding Blockchain to the application would help in securing mobile internet voting.
- Digital Identity and Blockchain Voting: Biometric identity such as iris and face data has been used to match a voter's identity with his/her identity stored in the voter's registration database at the time of his or her registration. This technique has been adopted to verify the identity of the person.
- Post-Election Audit on the Blockchain: Each voter would be allowed to examine each ballot to confirm the accuracy of the counted votes without revealing his or her identity.

4. Use of Blockchain in Electronic Voting for Certificates

Indian electoral arrangements currently utilize the EVM (Electronic Voting Machine), wherein the person casting his vote presses a button corresponding to the candidate they wish to vote. However, there have been recent modifications after the emergence of VVPAT (Voter Verified Paper Audit Trail) through which the voter can also verify whether his vote has been received by the candidate to whom he has casted his vote to [36]. The addition of VVPAT to EVM has simplified the process but added some serious issues regarding security. To remove these bottlenecks, Blockchain would prove to be an effective solution. Once Blockchain is induced in this electoral process, the threats of booth capturing would no longer exist, and the results would be full of trust [37].

To reform the electoral process in the biggest democracy is not easy, but in the long run it would be beneficial. To begin with, the Chief Election Commission of India should devise a Blockchain-based electronic voting system. All eligible voters must be allowed to vote only after their biometric verification is successful. Once verified, voters must select the candidate to whom they want to vote for, and this vote would be converted to a block [38]. This block will then be verified and will contain all the information necessary such as the candidate who received the vote, identity of the voter (into hidden format such as ****), timestamp, etc. This would then become an indispensable part of the Blockchain. Similarly, all the voters would then follow the same process and create such blocks. The duty of the Chief Election Commission would then be to verify the identity and display it for everyone to see. Since blocks are connected via the hash of the previous block, changing any one block would lead to tampering of the complete information which is not possible.

The process of casting vote and counting the votes of a particular candidate into peer of network, there must be a set of specific functions (RANGE) as mentioned in Algorithm 3. These functions can rely on a particular smart contract generated between e-voter and the corresponding candidate as discusses in Algorithm 3.

Algorithm 3: Smart Contract for e-Voters and Candidate Function

```
Add Candidate into the Peer Network
ADD Candidate as per the requirement of system software
IF CONFIRM e-voter COUNT does not exceed the RANGE
CREATE or APPEND the COUNT
END IF
CHECK the VALIDITY for the e-Voter
If VALIDITY is FALSE then
e-voter can be CANCELLED
Otherwise,
CAST the vote and APPENDED it to the next block
Increment the vote COUNT
```

Case Study: Indian Electoral System

India has a vibrant electoral democracy governed by the Constitution of India through which fundamental rights and the country's citizen duties can be configured. Such elections are conducted by distinct roles from the election commission of India [38]. As such conducting elections in India is a tedious and cumbersome process because the country holds the position of the world's most populated democracy. Indian states have been subjected to allegations from various political and non-political organizations regarding malfunctioning of the currently used system for elections i.e., VVPAT (Voter Verified Paper Audit Trail) and EVM (Electronic Voting Machine) [39,40].

These systems have been upgraded and made better than the ballot paper system to reduce paper wastage and time; however, it has also brought some severe issues with it such as being prone to electronic faults, hacking, etc [41,42]. Moreover, transportation of these machines from a central control unit to polling stations has led to wear and tear. Thus, to avoid all these added issues security personnel trained Election Commission officials, etc. are appointed to take care of the machine. However, with the emergence of Blockchain technology, expenditure on such avoidable factors would decline. This will improve the overall governance and the electoral process of the country. The Indian government spent about 3426 crore INR for conducting elections in 2014 [43] which witnessed a 131% rise in the costs as compared to the 2009 elections.

For any voting system, there can be a number of parameters that need to be considered while designing an automated, secure and trusted e-voting system [44]. Firstly, it should majorly focus on events such as register (create), poll, validity, verify and publish. This can be well-conceptualized from three-point of views, i.e., voter's view, candidate's view and chief election commissioner's view as depicted in Figure 5 [45].

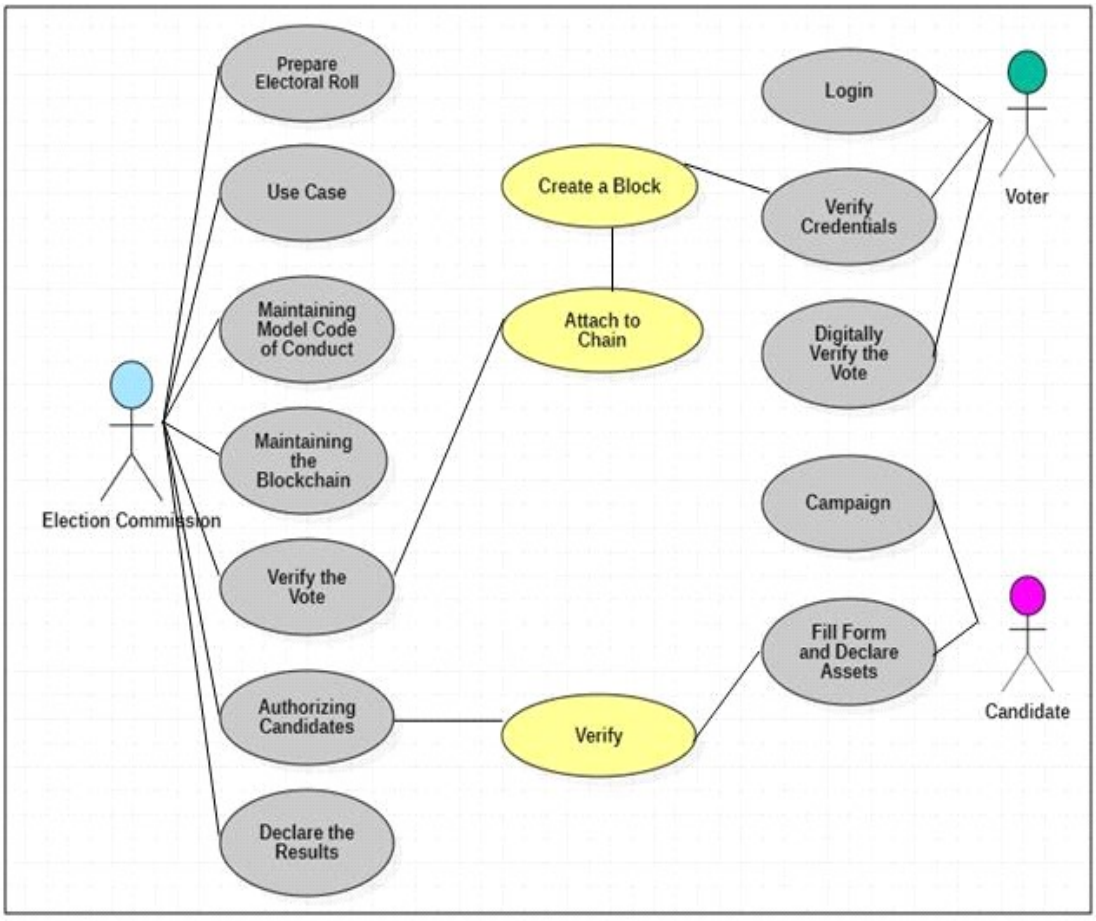

Figure 5. Use case for e-Electoral Voting System.

5. Results & Discussions

Decentralization with security and privacy-preserving features can be of primordial importance for its application in activities of mass participation as a general election [46,47]. The statistical analysis of different parameters of any public Blockchain should be considered in order to facilitate the process more efficiently. One of the key challenges which is ubiquitous to such public Blockchain is the cost of deployment. However, in this case the principal aim is to achieve optimized security and reliability. In Ethereum Blockchain, all the programmable transactions require some charges for ensuring safety in the networks and to overcome computational challenges. All operations such as computations, smart contract deployment and storage on the EVM require fees to complete the tasks. In our case with some initial fluctuations, we have observed throughout consistency in the chain length and the transaction energy dissipation. However, the charges are expected to increase with the deployment of more complex smart contracts, which in turn would result in making the entire process comparatively expensive, as shown in Figure 6.

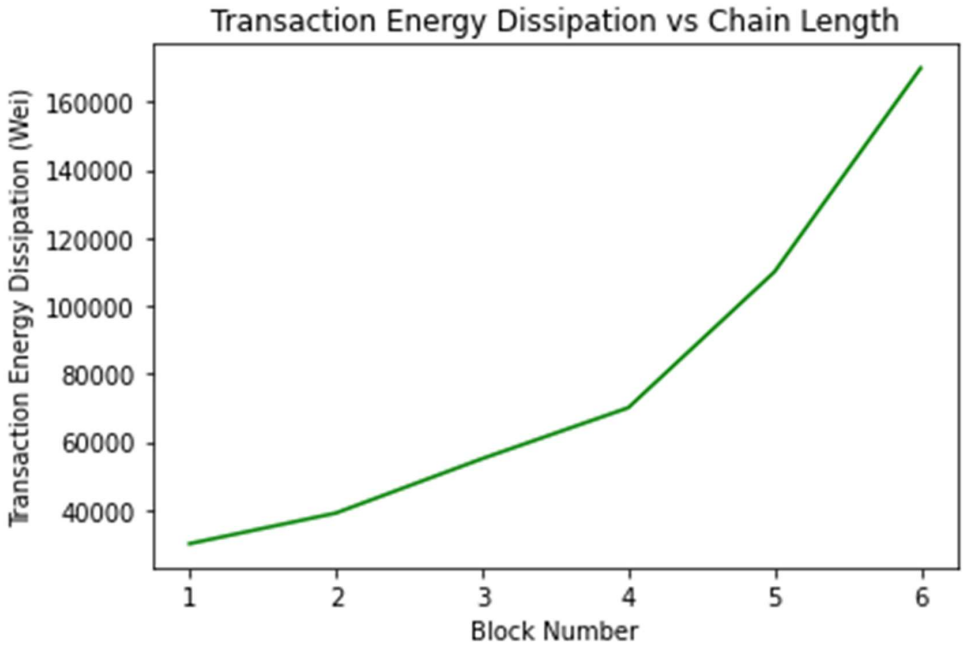

Figure 6. Comparison of transaction energy dissipation and block number.

Block time is the length of time it takes to create a new block in a Blockchain. In an election process block time could be one of the decisive factors for the successful implementation and adoption of such a system. We have observed that the block time is expected to increase exponentially with the chain length by measuring it at an interval of one block, as shown in Figure 7. One of the main factors which influences the block time is the difficulty level of the network. In Ethereum homestead released Blockchain the level of difficulty is calculated using the following procedure: where//denotes integer division and 2** denotes the two to the power operation. The int function returns the largest integer less than or equal to a given number:

$$block\_time = current\_block\_timestamp - parent\_block\_timestamp \quad (1)$$

$$\begin{aligned} current\_block\_difficulty = {} & parent\_block\_difficulty + (parent\_block\_difficulty/2048) \\ & * \max(1 - (block\_time/10), -99) \\ & + \mathrm{int}(2 * *((current\_block\_number/100000) - 2)) \end{aligned} \quad (2)$$

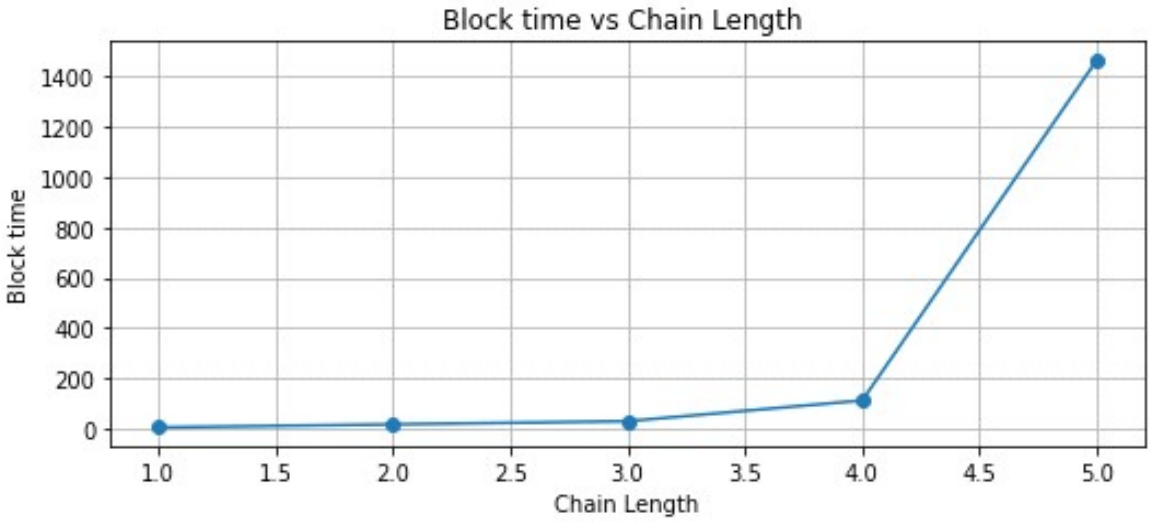

Figure 7. Comparison of block time and chain length.

The proposed mechanism can be deployed to any other Blockchain with lower gas fees to make the process more cost effective, provided it is open-source, reliable and meets the protocol and security standards for the execution of a general election. We have also made an attempt to estimate the variation of throughput (transactions per second, tps) and average latency of the Blockchain with the send rate (tps). Transaction throughput may be defined as the measure of how fast a Blockchain can process a particular transaction. Blockchain network latency is the time between submitting a transaction to a network and the first confirmation of acceptance by the network. An analysis of such parameters can be a decisive factor, particularly when the chain length is very large. In our case we have found a strong correlation in the variation of throughput and average latency with the send rate (tps) of the chain. We evaluated the performance of the system over different transaction sending rates (10–130 tps). Although the average latency showed a steady increase with the increase in the transaction send rate, the throughput increased till the transaction send rate increased to 100 tps and then the growth rate slowed down, as shown in Figure 8.

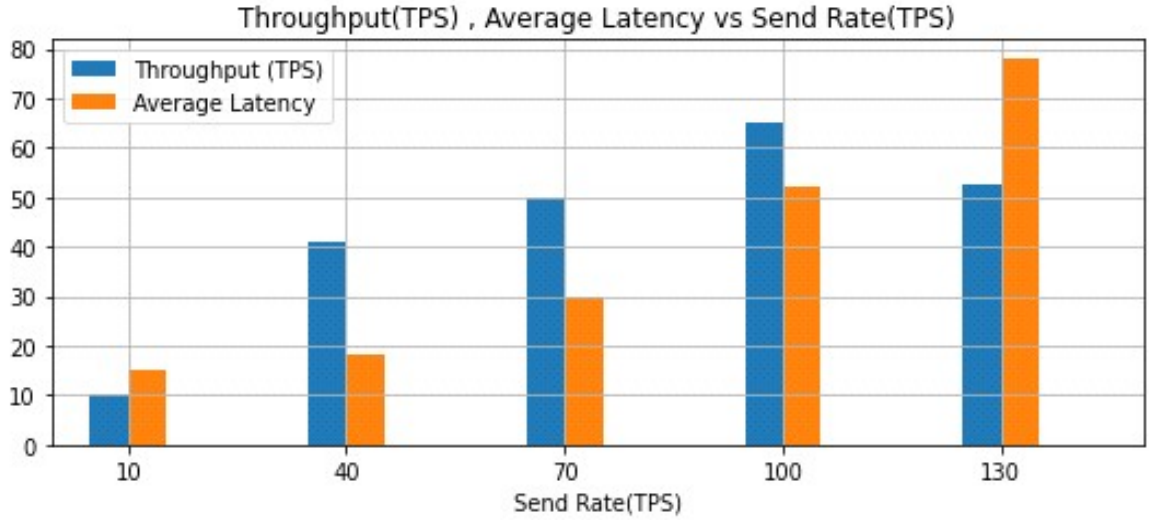

Figure 8. Variation of throughput and average latency with the send rate.

So, the analysis of the system over the aforementioned parameters reveals that adoption of decentralization for an event of mass participation such as an election process is a viable option. As from the point of feasibility of cost, it is clear that although the process

has dependency on gas fees, the cost is economical and governments and organizations would find it affordable.

Overall, the system performed as per our expectations. The accuracy over varying transaction send rates (tps) over the network has been found to be considerably better in comparison to the existing centralized voting system, as shown in Figure 9. The analysis shows strong correlation with the desired outcomes in terms of cost and security, and we conclude that the adoption of Blockchain based traceable certificates in democratic elections would ensure transparency, confidentiality and security of the process.

Figure 9. Measure of accuracy with the send rate.

Analyzing the Feasibility of Proposed Mechanism for Achieving ESG-Goals in the Context of a Democratic Society

The proposed mechanism is dependent on factors such as the block processing time (for syncing with other nodes) and transactions processing time of the network used. The following chart represents the gas used for the network transactions in the proposed system. A and V represents the operations dependent on the administrator and the voters, respectively.

Table 4 discusses the parameters that affects the public blockchain networks over cost of development of the system. The total cost of implementing the system would be attained by adding the costs for deploying, maintaining and monitoring the system across public or enterprise blockchains.

Table 4. Cost comparison for different blockchain networks over consensus algorithms.

Networks	Affecting Parameters for Cost Issues	Consensus Algorithms
Ethereum	high gas fee	PoW or PoS
Hyperledger Fabric	data storage in private database, reliance on authorized organizations	CFT or BFT
Stellar	small circulation, risks of volatility	BFT
Quorum	low scalability	Practical BFT
Hedera Hashgraph	not open-source, partially decentralized	Asynchronous BFT

However, the system can be made more efficient through the use of more low-cost networks. The possibility of the development of more energy efficient and scalable private

networks and protocols in future would further enhance the feasibility of the usage of the system. Further, a second layer can be used on top of a main network with high gas cost networks, for faster response and low gas cost. Transaction verification mechanisms such as the Proof-of-Work consensus protocol require high processing power and hence are energy consuming which might negatively impact the climate change mitigation efforts since a considerable proportion of electricity is obtained from combustible fossil fuels worldwide [48–50].

6. Conclusions

This article presents the need for a secured voting system based on the Blockchain technology. Such a technology has a bright future and would capture the market in the coming years through its security features such as immutability, transparency, distributed nature and end-to-end connection through smart contracts. For events such as elections, voter's confidentiality and transparency are the major characteristics in a democratic country. To conduct such an election through online or digital means, Blockchain technology plays a vital and prominent role in securing this event. Our observations reveal that the implementation of the Blockchain technology in elections would not only be feasible but also will be very effective in terms of both cost and security. The government should ensure the choice of consensus algorithms, parameters such as block size, difficulty of the chain etc. based on the number of voters and available time. The smart contract is a legal event or action which would get automatically executed whenever it is intended to be included by its developers. Such contract binds the integrity of the voter with the created block and would then append it to the next processing block to form the sequence or chain which would be immutable. This guarantees confidentiality and transparency for voter's rights. Strong network connectivity and reliable hardware infrastructure and software services for mining, security, processing power and memory would be required to maintain the constant throughput in the Blockchain during the entire electoral process. There is a strong possibility of an exponential rise in block time with the increase in the difficulty of the chain if power consuming consensus algorithms such as Proof-of-work are used. In this regard, it should be noted that the consensus algorithm goes towards achieving enhanced security, transparency and scalability. In 'Proof-of-work', the primary intention is to mine the coin whereas in 'Proof-of-stake', the intention is to validate the transaction. For more energy efficient mechanisms, such as the 'Proof-of-stake' can be also used, however, in case of 'Proof-of-stake' mechanism, inconsistencies in the governance issues remain such as excessive influence of validators with maximum holdings on transaction verification, possibilities of induced centralization in the process through double spending etc. Additionally, certain security challenges such as advanced spear phishing attacks on the voters by cybercriminals, threat of natural disasters which might bring in severe interruptions in the process, hardware vulnerabilities etc., continue to exist. We conclude that the proposed Blockchain based e-voting system would, however, be effective in achieving integrity and security in any democratic election around the world.

Our future work would comprise of a more comparative evaluation of the system over various private networks and thorough an analysis of performance through its implementation using different consensus algorithms. Based on our findings from this paper, we also aim to investigate the possibility of a dedicated Blockchain which would meet the criteria for the low consumption of energy and security standards to become more relevant for its implementation in a real national election.

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

Funding: This research was funded by Cybersecurity Center, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia with grant number PCC-Grant-202121.

Data Availability Statement: The data used to support the findings of this study have been retrieved from: US Election 2020Race to Presidential Election 2020 by County (URL: https://www.kaggle.com/datasets/unanimad/us-election-2020) (accessed on 27 August 2022) and Indian Election Dataset: State and National Level Election Data from 1977–2015. (https://www.kaggle.com/datasets/awadhi123/indian-election-dataset) (accessed on 27 August 2022).

Acknowledgments: The work conducted in this research has received the grant from Cybersecurity Center, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia (https://pmu.edu.sa/cybersecurity/) (accessed on 27 August 2022) under Project Number: PCC-Grant-202121.

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

References

1. Zaghloul, E.; Li, T.; Ren, J. *d*-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting. *IEEE Internet Things J.* **2021**, *8*, 16585–16597. [CrossRef]
2. Nakamoto, S. Bitcoin: A Peer-To-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 5 June 2022).
3. Park, S.; Specter, M.; Narula, N.; Rivest, R.L. Going from bad to worse: From Internet voting to blockchain voting. *J. Cybersecur.* **2021**, *7*, tyaa025. [CrossRef]
4. Hu, W.; Li, H. A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. *Alex. Eng. J.* **2020**, *60*, 491–500. [CrossRef]
5. Dinh, T.N.; Thai, M.T. AI and Blockchain: A Disruptive Integration. *IEEE Comput.* **2018**, *51*, 48–53. [CrossRef]
6. Eyal, I. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. *IEEE Comput.* **2017**, *50*, 38–49. [CrossRef]
7. Febriyanto, E.; Triyono; Rahayu, N.; Pangaribuan, K.; Sunarya, P.A. Using Blockchain Data Security Management for E-Voting Systems. In Proceedings of the 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, 23–24 October 2020; pp. 1–4.
8. Shabnam, S.; Sayyad, F. Voting Using Blockchain Technology. In *Intelligent Computing and Networking*; Springer: Singapore, 2021; pp. 285–291.
9. Mustafa, M.K.; Waheed, S. An E-Voting Framework with Enterprise Blockchain. In *Advances in Distributed Computing and Machine Learning*; Springer: Singapore, 2021; pp. 135–145.
10. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A Survey on the Scalability of Blockchain Systems. *IEEE Netw.* **2019**, *33*, 166–173. [CrossRef]
11. Khalfan, M.; Azizi, N.; Haass, O.; Maqsood, T.; Ahmed, I. Blockchain Technology: Potential Applications for Public Sector E-Procurement and Project Management. *Sustainability* **2022**, *14*, 5791. [CrossRef]
12. Singh, L.; Kumar, A.; Singh, Y. Internet of Healthcare Things (IoHT) and Blockchain: An Efficient Integration for Smart Health Care Systems. In *Healthcare and Knowledge Management for Society 5.0*; CRC Press: Boca Raton, FL, USA, 2021; pp. 135–149. [CrossRef]
13. Rejeb, A.; Rejeb, K.; Simske, S.J.; Keogh, J.G. Blockchain technology in the smart city: A bibliometric review. *Qual. Quant.* **2022**, *56*, 2875–2906. [CrossRef]
14. Maesa, D.D.F.; Mori, P. Blockchain 3.0 applications survey. *J. Parallel Distrib. Comput.* **2020**, *138*, 99–114. [CrossRef]
15. Umeh, J. Beyond Bitcoin and the Blockchain. *ITNOW* **2018**, *60*, 48–49. [CrossRef]
16. Abayomi-Zannu, T.P.; Odun-Ayo, I.; Tatama, B.F.; Misra, S. Implementing a Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria. In *Proceedings of the First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*; Springer: Singapore, 2020; pp. 857–872. [CrossRef]
17. Alvi, S.T.; Uddin, M.N.; Islam, L.; Ahamed, S. From Conventional Voting to Blockchain Voting: Categorization of Different Voting Mechanisms. In Proceedings of the 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 19–20 December 2020; pp. 1–6. [CrossRef]
18. Rubtcova, M.; Pavenkov, O. Implementation of Blockchain technology in electronic election in Sierra Leone. In Proceedings of the 2018 Conference: "Re-Thinking Regions in Global International Relations", Davao City, Philippines, 23–24 March 2018; Volume 23.
19. Pawlak, M.; Poniszewska-Marańda, A. Trends in blockchain-based electronic voting systems. *Inf. Process. Manag.* **2021**, *58*, 102595. [CrossRef]
20. Khan, K.M.; Arshad, J.; Khan, M.M. Empirical analysis of transaction malleability within blockchain-based e-Voting. *Comput. Secur.* **2020**, *100*, 102081. [CrossRef]
21. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A Survey on Blockchain for Information Systems Management and Security. *Inf. Process. Manag.* **2020**, *58*, 102397. [CrossRef]

22. Hassan, N.U.; Yuen, C.; Niyato, D. Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions. *IEEE Ind. Electron. Mag.* **2019**, *13*, 106–118. [CrossRef]
23. Taş, R.; Tanrıöver, Ö.Ö. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. *Symmetry* **2020**, *12*, 1328. [CrossRef]
24. Li, C.; Xiao, J.; Dai, X.; Jin, H. AMVchain: Authority management mechanism on blockchain-based voting systems. *Peer—Peer Netw. Appl.* **2021**, *14*, 2801–2812. [CrossRef]
25. Baudier, P.; Kondrateva, G.; Ammi, C.; Seulliet, E. Peace engineering: The contribution of blockchain systems to the e-voting process. *Technol. Forecast. Soc. Chang.* **2020**, *162*, 120397. [CrossRef]
26. Yang, X.; Yi, X.; Nepal, S.; Kelarev, A.; Han, F. Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Futur. Gener. Comput. Syst.* **2020**, *112*, 859–874. [CrossRef]
27. Sadia, K.; Masuduzzaman, M.; Paul, R.K.; Islam, A. Blockchain-Based Secure E-Voting with the Assistance of Smart Contract. In *IC-BCT. 2019*; Springer: Singapore, 2020; pp. 161–176. [CrossRef]
28. Alam, M.; Yusuf, M.O.; Sani, N.A. Blockchain technology for electoral process in Africa: A short review. *Int. J. Inf. Technol.* **2020**, *12*, 861–867. [CrossRef]
29. Li, K.; Li, H.; Wang, H.; An, H.; Lu, P.; Yi, P.; Zhu, F. PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains. *Front. Blockchain* **2020**, *3*, 11. [CrossRef]
30. Kshetri, N.; Voas, J. Blockchain-Enabled E-Voting. *IEEE Softw.* **2018**, *35*, 95–99. [CrossRef]
31. Benabdallah, A.; Audras, A.; Coudert, L.; El Madhoun, N.; Badra, M. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access.* **2022**, *10*, 70746–70759. [CrossRef]
32. Specter, M.A.; Koppel, J.; Weitzner, D. The ballot is busted before the Blockchain: A security analysis of voatz, the first internet voting application used in us federal elections. In Proceedings of the 29th {USENIX} Security Symposium ({USENIX} Security 20), Boston, MA, USA, 12–14 August 2020; pp. 1535–1553.
33. Dimitriou, T. Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting. *Comput. Netw.* **2020**, *174*, 107234. [CrossRef]
34. Pawade, D.; Sakhapara, A.; Badgujar, A.; Adepu, D.; Andrade, M. Secure Online Voting System Using Biometric and Blockchain. In *Data Management, Analytics and Innovation*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 93–110. [CrossRef]
35. Roh, C.H.; Lee, I.Y. A study on electronic voting system using private Blockchain. *J. Inf. Process. Syst.* **2020**, *16*, 421–434.
36. Wolchok, S.; Wustrow, E.; Halderman, J.A.; Prasad, H.K.; Kankipati, A.; Sakhamuri, S.K.; Yagati, V.; Gonggrijp, R. Security analysis of India's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security, Chicago, IL, USA, 4–8 October 2010; pp. 1–14.
37. Krishnamurthy, R.; Rathee, G.; Jaglan, N. An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices. *Wirel. Netw.* **2019**, *26*, 2391–2402. [CrossRef]
38. Soni, Y.; Maglaras, L.; Ferrag, M.A. Blockchain Based Voting Systems. In *European Conference on Cyber Warfare and Security*; Academic Conferences International Limited: Athens, Greece, 2020; pp. 241–248.
39. Goyal, M.; Kumar, A. Sustainable E-Infrastructure for Blockchain-Based Voting System. In *Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings*; Scrivener Publishing: Beverly, MA, USA, 2021; p. 221. [CrossRef]
40. 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.
41. Schaub, M.; Phares, H.B. Cryptocurrency value changes in response to national elections: Do they behave like money or commodities. *Appl. Econ. Lett.* **2019**, *27*, 1135–1140. [CrossRef]
42. Rathor, S.; Agrawal, A.; Yadav, D.P. The Efficient use of Blockchain for Reducing Frauds in Parental Property Distribution. In Proceedings of the 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 28–29 February 2020; pp. 46–49.
43. Peck, M.E. Blockchain world—Do you need a blockchain? This chart will tell you if the technology can solve your problem. *IEEE Spectr.* **2017**, *54*, 38–60. [CrossRef]
44. Ma, X.; Zhou, J.; Yang, X.; Liu, G. A Blockchain Voting System Based on the Feedback Mechanism and Wilson Score. *Information* **2020**, *11*, 552. [CrossRef]
45. Rathor, S.; Agrawal, A. A robust verification system for recruitment process by using blockchain technology. *Int. J. Blockchains Cryptocurrencies* **2020**, *1*, 389–399. [CrossRef]
46. Huang, J.; He, D.; Obaidat, M.S.; Vijayakumar, P.; Luo, M.; Choo, K.K.R. The Application of the Blockchain Technology in Voting Systems: A Review. *ACM Comput. Surv. CSUR* **2021**, *54*, 1–28. [CrossRef]
47. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Futur. Gener. Comput. Syst.* **2019**, *105*, 13–26. [CrossRef]
48. Hussain, A.A.; Emon, M.; Tanna, T.A.; Emon, R.I.; Onik, M.; Hassan, M. A Systematic Literature Review of Blockchain Technology Adoption in Bangladesh. *Ann. Emerg. Technol. Comput. AETiC* **2022**, *6*, 1–30. [CrossRef]

49. Seifelnasr, M.; Galal, H.S.; Youssef, A.M. Scalable open-vote network on ethereum. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 436–450.
50. Jain, P.K.; Pamula, R.; Yekun, E.A. A multi-label ensemble predicting model to service recommendation from social media contents. *J. Supercomput.* **2021**, *78*, 5203–5220. [CrossRef]