**E-voting protocols used in different countries**

The SIVP protocol can be implemented in Colombia [1] to ensure a fair and transparent voting process. The protocol provides a method to avoid fraud and assure the accuracy of election results. The article introduces the Secure Internet Voting system (SIVP), a novel voting system based on blind signatures and public key cryptography that assures votes are anonymous and cannot be traced back to the voter. The protocol also includes a method for validating each voter and ensuring that only qualified voters may vote. Eligibility, democracy, privacy, verifiability, correctness, fairness, robustness, receipt-freeness, and coercion resistance are all provided by the protocol. The protocol ensures eligibility, democracy, privacy, verifiability, correctness, fairness, robustness, receipt-freeness, and coercion resistance. The research compares the computational burden of SIVP to that of other voting protocols and concludes that, despite the addition of extra security measures, it is not excessively high.

The work also examines the security needs of electronic voting systems and describes the SIVP protocol's nomenclature and technique of creation. The various phases of the SIVP protocol are detailed, and a security analysis of SIVP is provided, as well as a comparison to comparable e-voting protocols. The SIVP protocol may also be used to boost voter turnout by making it simpler for people to vote.  
  
The Secure Internet Voting Protocol (SIVP) contains six consecutive phases: announcement, registration, authentication, voting, encryption, decryption, and tally up.

* The electoral authority announces the election and gives information about the candidates and the voting procedure during the announcement phase.
* Eligible voters are enrolled and given a unique identification during the registration process. The registration authority checks each voter's eligibility and gives a digital certificate to each voter.
* Voters are authenticated during the authentication step using their identify and a password. The authentication center confirms the voter's identification and issues a token that permits the person to vote.
* During the voting round, individuals voted anonymously. The vote is received by the voting center and encrypted using a homomorphic encryption method.
* The encrypted votes are delivered to the tally center during the encryption phase, where they are decoded using a threshold decryption algorithm.
* The encrypted votes are decoded and tabulated to decide the winner during the decryption phase. The findings are posted on a bulletin board accessible to the public by the tally center.
* Finally, during the verification process, independent organizations and trustees confirm the integrity of the election and the accuracy of the results.

SIVP has various security properties, including eligibility, democracy, privacy, verifiability, correctness, fairness, robustness, receipt-freeness, and resistance to coercion. SIVP's security has been assessed using formal techniques and simulations, and the findings suggest that it is resistant to a variety of threats, making it a viable alternative for secure online voting.

**Critical Opinion:** The paper proposes the use of the Secure Internet Voting system (SIVP) in Colombia, highlighting how its use of public key cryptography and blind signatures can guarantee elections' security, fairness, and openness. By highlighting SIVP's eligibility verification, computational efficiency, and potential to increase voter turnout, the research presents SIVP as a reliable and secure option for election procedures.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

The study [2] dives into blockchain e-voting systems that have been accepted and deployed in elections by several nations, with an emphasis on the registration process used.

In 2015, Australia launched blockchain e-voting during the State General Election of New South Wales, with around 280,000 residents voting using an app called Scytl. After completing the registration procedure, the voter registers with authorities, obtains their voter ID, and selects a 6-digit pin. After casting their vote, they enter the system with their ID and PIN and receive a 12-digit receipt number. To authenticate their vote, the voter uses their ID, PIN, and receipt number to get the information.  
Estonia is the first country in the world to implement electronic e-voting in elections.It requires the Internet as well as an Electronic National Identification Card for authorization, encoding, and signatures. Voters must download the voting program, verify with their electronic ID, and then vote from a list of candidates if they are eligible.

Polyas is used in Germany for democratic elections. Polyas is the only e-voting software provider whose e-voting technology has been approved by the German Federal Office for Information Security. In 2011, Norway implemented e-voting for regional elections. The program is somewhat decentralized and anonymous. Due to cyber-attack worries, the nation discontinued the use of e-voting platforms.

In 2014, Russia launched e-voting for over two million individuals. Russia also made use of Waves' blockchain-based e-voting technology. The system employs a Proof of Authority-based crash fault tolerance consensus method. Smart contracts are used to save voting process rules, registration information, and vote verification.

Sierra Leone embraced Agora as their e-voting system for the election for president in 2018, making it the first time blockchain technology was employed in a presidential election.

In South Korea, around 9,000 citizens voted in 2017 for a Blockchain project that used a smart contract based on blockchain technologies.

Switzerland held municipal balloting utilizing Luxoft-developed e-voting technology. The bulk of their national voting procedures from state-wide elections and referendums use the Swiss e-voting system. The suggested system is a mobile phone application that confirms via Short Message Service (SMS). Voters insert their ID into the e-voting website and follow the instructions to cast their vote; they enter a PIN and match a security symbol to the one they got in the mail. If the two match, the vote is accepted by the system. Following that, individuals input PIN numbers, the name of the referendum, and the response (positive or negative).

**Critical Opinion:** The study evaluates blockchain-based electronic voting systems' global adoption, emphasizing on registration processes. Noteworthy implementations include Australia's use of Scytl for state elections, Estonia's pioneering use of Electronic National Identification Cards, and Russia's deployment of Waves' blockchain technology. Despite outcomes, challenges such cyberattacks forced Norway to abandon electronic voting, revealing the convoluted nature of e-voting adoption throughout the world.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

The study [3] indicates that blockchain technology has the potential to alter the way elections are conducted and gives insights for scholars and practitioners interested in this field.

Tsukuba City in Ibaraki Prefecture, Japan, employed blockchain and My Number cards for the first online voting validation test in August 2018, according to Jun Huang and Debiao. The government urged residents to use innovative technology to generate new ideas to benefit society, and in the final voting phase, they employed a blockchain-based voting system to choose the final supported works from the contenders. The legitimate voters were identified using the My Number card.

The report additionally addresses the application of blockchain technology in the 2018 presidential election in Sierra Leone. The National Electoral Commission recorded and verified the votes cast in the election using a blockchain-based voting technology. The approach was developed to prevent fraud and preserve the voting process's openness. It further addresses the usage of blockchain technology in the 2019 Moscow City Duma election. To enable residents to vote remotely, the government adopted a blockchain-based voting system. The technology was created to protect the voting process's security and authenticity.

**Critical Opinion:** The study highlights how blockchain technology has the ability to completely change election processes and provides insightful information for professionals as well as scholars. Through case studies in Moscow, Sierra Leone, and Japan, it illustrates how blockchain technology may be effectively used to improve vote security, thwart fraud, and promote transparency in election processes.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

Using blockchain technology, this study [4] presents a privacy-preserving e-voting system that allows score voting. The method is built on the Ethereum blockchain to enable safe and private voting in the digital era. The system is made up of multiple modules, including a registration module, a balloting module, a tally module, and an authentication module, and it employs a variety of cryptographic approaches to protect the voting process's secrecy and integrity. The system enables score voting, a form of voting system in which voters award a score to each candidate rather than choosing a single candidate. This enables voters to express their choices more precisely, potentially leading to more representative election results.

The system is built on the Ethereum blockchain, an open-source system that allows developers to create and deploy distributed applications. Because all transactions are recorded on a public register that is available to all participants, the adoption of blockchain technology assures that the voting process is transparent and tamper-proof. The registration module enables voters to register for the election and assigns each voter a unique identification. Voters may cast their ballots using a safe and user-friendly interface thanks to the voting module. The tallying module gathers votes and computes election results autonomously. The verification module enables participants to validate the voting process and confirm that the results are correct. The system is examined using an empirical assessment on the Ethereum blockchain, which demonstrates that it can withstand workloads of up to 10,000 transactions transmitted at a rate of 200 per second before experiencing substantial performance decreases. Increased voter engagement, enhanced election integrity, and lower costs associated with traditional voting methods are all possible benefits of establishing a privacy-preserving e-voting system.

**Critical Opinion:** In order to ensure anonymity in score voting, this paper proposes an Ethereum-based blockchain-based electronic voting system. By utilizing cryptographic techniques across its modules, the system permits accurate voter expression, ensures transparency, and may provide advantages over conventional approaches such as improved election integrity, more voter participation, and lower costs.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------  
  
According to the study [5], present voting methods are vulnerable to fraud, manipulation, and assaults, particularly in light of the ongoing epidemic. Because of their online nature, electronic voting systems are more vulnerable to security flaws. The proposal explains how blockchain technology, which is a distributed information storage system, addresses these difficulties by offering an encrypted and autonomous network. The use of blockchain technology ensures that each individual vote is encrypted and recorded in a distributed ledger transaction. It becomes immutable and impervious to alteration once it has been recorded. The use of blockchain technology to enable e-voting assures transparency, efficiency, and dependability.

The paper provides a thorough knowledge of blockchain technology and how it operates. Haber and Stornetta initially proposed the technique as a concept in 1991, with the goal of producing electronic paper timestamps. Blockchain technology is a distributed network that depends on node consensus rather than a single body for control. As a result, all historical records of transactions are unalterable, guaranteeing the immutability required in voting systems. The authors then outline the key components of blockchain technology that make it suitable for electronic voting. Cryptographic algorithms, decentralized networks, peer-to-peer transactions, and smart contracts are among them. The Elliptical Curve Digital Signature Algorithm, for example, ensures that each vote is encrypted and signed with a unique signature.

The article describes the many blockchains that might be utilized in an e-voting system, including public, private, and consortium blockchains. The writers clinically outline the benefits and drawbacks of each variety. For example, public blockchains provide more security and decentralization, but consortium blockchains may provide greater speed and anonymity. Finally, the authors describe how several consensus methods might be used to maintain the integrity of the electronic voting system. Proof of Work (PoW), Proof of Burn (PoB), Proof of Stake (PoS), and Proof of Authority (PoA) are all defined.

**Critical Opinion:** The paper emphasizes crucial blockchain elements such cryptographic algorithms, decentralized networks, and consensus techniques while pointing out flaws in the present voting procedures and arguing in favor of using blockchain technology to improve electronic voting's transparency and dependability. The authors evaluate different blockchain types, including public, private, and consortium, highlighting their attributes for secure and decentralized electronic voting systems.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

Aqua [6], a novel blockchain-based e-voting system proposed in the study, aims to address the constraints of previous e-voting systems. Aqua is built on the Ethereum blockchain and uses smart contracts written in Solidity. The system has three major components: a front-end that provides a user experience to voters, a back-end that handles the act of voting, and an intelligent contract that stores voting data and implements the voting process rules. The Aqua system passes through multiple steps, including startup, voting, counting, and outcomes, with various individuals contributing at each level.

The authors used a variety of technologies to develop Aqua, including Hardhat, Ethers.js, HTML-PHP, CSS, and JavaScript. The article describes the implementation in full, including the technologies employed. The authors conducted numerous experiments to validate the Aqua system's usefulness, including a performance test and a security study. The results of these studies revealed that Aqua is a potential option for performing safe, transparent, and efficient e-voting operations. Overall, the Aqua system provided in the study makes an important addition to the field of e-voting systems and has the potential to be extended and enhanced further in the future.

**Critical Opinion:** The Aqua system, a novel blockchain-based e-voting solution proposed in the study, overcomes previous limitations by utilizing the Ethereum blockchain and Solidity smart contracts. Aqua is made up of voting-centric and user-oriented components. It goes through several phases, and experimental validations confirm that it can be used for safe and effective electronic voting. The study validates Aqua as a significant contribution to the field, poised for future expansion.  
  
—--------------------------------------------------------------------------------------------------------------------------------------------------------------  
  
For Jordan's parliamentary elections, the paper [7] demonstrates an electronic voting system based on blockchain technology. The suggested system is built on digital contracts, which are self-executing contracts in which the conditions of the buyer-seller agreement are explicitly written into pieces of code. The smart contracts are built on the Ethereum blockchain, which is a platform that is decentralized for developing decentralized apps that offers a high level of security, transparency, and immutability. Two smart contracts are developed to aid the e-voting process, with the first responsible for installing the second smart contract. The first contract is directly related to the district and is in charge of establishing the district structure (votingDistrict), whilst the second contract is the actual eVoting contract.

When the government wants to add a new district, it calls the first contract's createDistrict function, which then produces a new copy of the subsequent contract on the Ethereum distributed ledger. Smart contracts for the e-voting system are written in the computer language Solidity. The Web3 framework, React library, Infura -API, and Metamask Ethereum wallet are all used in the e-voting Ethereum application. To establish a voting process, the electronic Ethereum-based voting system (EBVS) takes the following phases. The EBVS voting system includes two smart contracts: the votingDistrict smart contract and the eVoting smart contract. The votingDistrict contract is in charge of installing the eVoting smart contract and keeping track of all deployed eVoting smart contract instances by recording the addresses of the deployed instances in an array. The manager/government will add as many districts as they like to the votingDistrict smart contract using the createDistrict function, and a new district will be generated as an instance of the eVoting smart contract.

Using the smart contract votingDistrict, all persons entitled to vote in a given district are assigned to that district. Throughout the preparation phase, each citizen must create a Metamask storage account, an Ethereum wallet, and decide which public address he or she will use throughout the voting process. There are two methods for adding voters: The first step is for the voter to visit the identification verification office and verify the blockchain address. In this situation, a voter is added to the blockchain immediately in a single transaction. The second method is to add a list of pre-registered voters in a certain district all at once. Each Ethereum address is a voter.

When voting begins, each voter votes using his or her address. The voter's identity must remain anonymous in order to safeguard the voter's privacy. When the government adds voters, the eVoting smart contract first checks to see if the voter has already been added and if the voter's Identity or residence has never been used before. It also determines if the wallet balance connected with the voter address is zero. This phase is essential to demonstrate the accuracy of the system (the number of tokens in each balance must exactly equal the maximum number of candidates). When a voter is added to the system, the government transfers several tokens from the government wallet that exactly match the maximum number of candidates in their district. Each token represents one vote and only one contender. No one else has the authority to add voters; the activity of adding voters is rigorously supervised by the government smart contract.

**Critical Opinion:** For Jordan's parliamentary elections, the study suggests a blockchain-based electronic voting system that uses Ethereum smart contracts for security and transparency. The votingDistrict and eVoting smart contracts are the two that make up the system. The former creates instances of the latter for every district, while the government smart contract oversees token-based verification to guarantee voter anonymity and accuracy.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------  
  
The paper [8] suggests that the Independence National Electoral Commission use blockchain-based voting in Nigeria's general election to address present voting concerns. The Technology-Organization-Environment hypothesis was employed in the study to explain this assertion. When an established technology is no longer capable of delivering its advantages, another innovation must be adopted. Given all of the challenges surrounding elections in Nigeria, it is clear that citizens would want to adopt an invention that is transparent, trustworthy, safe, and irreversible.

Blockchain technology has the potential to fix present voting challenges in Nigeria and build a more transparent and credible electoral system. All of these difficulties will be greatly minimized, if not totally eliminated, by blockchain technology. When residents vote from the comfort of their own homes, for example, ballot box snatching, ballot papers, and the transit of critical election materials are all avoided. Even if a person is bribed to vote in favor of a candidate, the candidate cannot force the person to vote for him, and the election result cannot reveal the person's vote.

The report suggests that INEC interacts with blockchain professionals from the Stakeholders in Blockchain Technology Association in Nigeria (SIBAN) and A and D Forensics, who would set out and build the structures and recommend the necessary equipment. These specialists will also install, test, and validate the system in chosen places across the country's six geopolitical zones before presenting and certifying it for use in general elections. INEC should also undertake voter education to bridge the information gap for citizens, hold awareness seminars, and promote the usage of blockchain widely. Education is required since blockchain is a new technology that requires everyone to be familiar with how it performs and what it can achieve when deployed. Finally, the study believes that the use of blockchain polling will assist INEC in developing a more transparent, reliable, secure, and irreversible electoral system. The study offers strategies for INEC to properly use this technology, such as consulting with blockchain specialists, performing voter education, and holding awareness seminars.

**Critical Opinion:** The paper proposes that the Independence National Electoral Commission (INEC) in Nigeria use blockchain-based voting to address current voting challenges, with an emphasis on transparency and security. The study recommends INEC's engagement with stakeholders, education initiatives, and nationwide system installation, with the goal of establishing a transparent, reliable, and secure electoral system.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

Turkey's [9] planned blockchain-based e-voting system is intended to alleviate the shortcomings of traditional paper-based elections. The suggested approach attempts to protect the confidentiality and privacy of votes and voters while also expediting the counting and announcement of results. While some nations have adopted e-voting, blockchain-based election systems are still in the works, according to the report. To achieve the highest level of security, privacy, and data integrity, the system employs blockchain distributed ledger technology, notably Ethereum blockchain. There are three levels to the system: application, network, and consensus.

The suggested system's application layer is in charge of the user user experience chain, the Application Programming Interface and smart contracts. The user interface enables voters to participate in elections through an easy-to-use platform, while the blockchain API enables the application to connect to the blockchain network to save and access votes and other necessary data. The smart contracts serve as self-executing and autonomous contracts that operate on the blockchain and contribute to the election's integrity.

The network layer is the system's second layer, connecting two sorts of users: voter clients and communication servers. Individual voters cast their votes via the user interface via a secure internet connection as voter clients. Communication servers make data transfer between ballot terminals and the public ledger network more safe and secret. The proposed system's last layer is the unanimity layer, which uses the Ethereum blockchain to reach consensus on the legitimacy of votes. Because the system employs a consensus approach, the votes cast by the citizens are verified, authenticated, and secure. Additionally, the consensus layer guarantees that every vote gets recorded and that the final total is visible and accurate.

The research also examines the proposed system from many perspectives, such as security, confidentiality, credibility, and scalability. According to the article, the suggested system tackles these concerns by including features such as ballot confidentiality, dual-factor authentication, quadruple encryption, and recovery from disasters.

**Critical Opinion:** Through Ethereum blockchain technology, Turkey's blockchain-based e-voting system aims to improve election processes by prioritizing vote confidentiality and privacy. The system's multi-layered approach ensures a secure user experience, strong data integrity, and dependable consensus, while features like dual-factor authentication and quadruple encryption address concerns about security, confidentiality, credibility, and scalability.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

The paper [10] offers a blockchain-based e-voting method. It aims to overcome the shortcomings of traditional elections by offering an anonymous electronic voting system with security, anonymity, privacy, and auditability. The suggested system is made up of multiple components, including algorithms, a registration procedure, a voting process, and an administrative panel. The system's algorithms are based on the SHA-256 cryptographic hashing method. This algorithm is used to convert messages into a 256-bit hash result. This method is used by the system because it can generate fixed-length outputs from arbitrary-length inputs and is resistant to crashes and preimage assaults. The registration procedure is the initial stage of the proposed system. The system checks to see if the user is already in the records and qualified to vote. After being authenticated, the user is given a one-of-a-kind hashed address to use for voting. Voters can only vote once, and they must visit the system's voting page to do so within the voting time. The system logs them out once the vote is over, and outcomes are revealed.

**Critical Opinion:** The paper outlines a blockchain-based e-voting method that overcomes traditional election constraints by ensuring anonymity, security, and auditability. Using SHA-256 cryptography, the system uses unique hashed addresses for authenticated voters, limiting each user to one vote and revealing results after voting.  
  
—--------------------------------------------------------------------------------------------------------------------------------------------------------------

Elfattal [11] examines research articles on electronic voting systems published in the Scopus database from 2000 to 2022 in five countries: the United States, India, China, the United Kingdom, and Germany, to find patterns and challenges related to e-voting in each nation.

According to the study papers, the United States is a leader in the creation and deployment of e-voting systems. The US government spends extensively in the study and development of e-voting systems, mostly in response to the country's concerns and difficulties. The authors found that the HAVA program, which was launched following the 2000 presidential elections, had a substantial influence on the acceptance and deployment of e-voting systems in the United States. Numerous studies concentrated on the development of voting machines that are electronic and technologies that improve the way people vote online in the United States. Security and privacy concerns about e-voting technologies have additionally been addressed in the country.

The authors discovered that research articles in India focused on increasing the access of electronic voting platforms to India's varied population. Citizens in India can vote via an Automated Voting Machine or virtually via the web under the country's e-voting system. The authors stated that the Indian online voting system is frequently criticized for security, dependability, and accuracy difficulties. Many research papers have been written to improve the privacy and reliability of India's e-voting system in order to avoid fraud and hacking. The researchers who conducted this study discovered a scarcity of literature on digital voting systems in China. Nonetheless, the nation has been making investments in the development and implementation of e-voting technologies. According to the study papers, the Chinese government has failed to ensure openness and justice in the electronic voting process, with claims of election irregularities circulating. This lack of openness has slowed the country's adoption of e-voting technology.

The United Kingdom has been dabbling with limited forms of e-voting, such as internet voting, postal voting, and voting via electronic equipment. The authors discovered that electoral supervisors in the United Kingdom are cautious to use e-voting systems owing to safety, precision, and the possibility of system failure. To increase public faith in the system, research articles focused on increasing safety and visibility of voting systems in the United Kingdom. In its municipal and legislative elections, Germany has used e-voting equipment. The authors discovered that study articles concentrated on different features of the electronic voting system, such as safety, openness, and privacy issues. Germany has been extremely dismissive of e-voting systems and has created an individual verification method for the country's electronic voting devices. The study report examined several features of electronic voting platforms in each nation, emphasizing variations in adoption caused by a variety of reasons. According to the report, the key challenges related with e-voting systems in various nations include worries about safety, accountability, convenience, and system accuracy.

**Critical opinion:** Author examines research on electronic voting systems from 2000 to 2022, identifying the United States as a development leader influenced by the HAVA programme. India prioritizes accessibility, China faces transparency challenges, the United Kingdom investigates e-voting cautiously, and Germany prioritizes safety and privacy. The study highlights various adoption challenges across nations, such as concerns about safety, accountability, convenience, and system accuracy.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

Building an e-voting system in Libya [12] is a hard task that must be carefully considered to guarantee that it runs successfully while offering optimum privacy, security, and openness. The primary goal of an e-voting system is to make the voting process more accessible to those who live in remote places or are unable to vote in person. Although not commonly used in Libya, given the country's relative lack of democracy, revolution, and unpredictable administration, e-voting has potential as a method of modernizing the voting process in order to make it easier, more productive, and credible.

The issues involved in the electronic voting process, which may be classified into three main groups: safety, vote verifiability, and laws and regulations, guide the design of e-voting systems. Because an e-voting system has to safeguard all data, involving voter annulment, cryptography protocols, key management, and the use of blockchain applications, security is a critical factor. Election systems must also be enabled to verify that all votes given are valid and that voter identities are validated, ensuring that they match the criteria for voter eligibility. To do this, the report suggests that e-voting systems incorporate a security matrix that allows for data protection, user identification, and secure communication in all elements of the operation and control procedures. Other criteria include clear audit trails, which enable voters to validate their votes and guarantee that they were correctly tallied using verifiability functions such as zero-knowledge proofs.

When constructing e-voting systems, the legal framework relevant to polls must also be addressed. Legal frameworks are a set of laws and norms that regulate elections in each nation, generally adapted to their individual needs, culture, and history. As a result, e-voting systems must adhere to legal frameworks, requirements, and rules. Online voting, for example, may be prohibited or discouraged owing to electronic theft or concerns about voter rights. Hence, e-voting advocates need to work closely with the security and legal teams to guarantee the legal compliance and operate within the constitutional limits and national context. To combat data fraud, the report advises that e-voting systems be interoperable with and integrated with traditional voting systems. This will ensure the correctness and validity of the vote results, as well as give a trustworthy and comprehensive record of all transactions connected to registration of voters, the casting procedure, recording, and validation.

**Critical Opinion:** Implementing an e-voting system in Libya presents challenges that require meticulous attention to ensure success while maintaining privacy, security, and transparency, while also providing a potential avenue for modernization despite historical democratic challenges. The design considerations, which emphasize security measures, compliance with legal frameworks, and interoperability with traditional voting systems, highlight the importance of collaboration between e-voting advocates, legal, and security teams in order to address concerns and maintain electoral integrity.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

The author [13] believes that e-voting can help Zimbabwe overcome election-related problems in the past. The adoption of e-voting technologies with little human intervention can make the election process more inclusive. By reducing human mistakes and increasing voting accuracy, electronic voting technologies reduce voter intimidation. By allowing people to vote surreptitiously and independently, the approach maintains the impartiality of the political process. E-voting systems allow for faster tabulation and analysis of results, promoting electoral stability and confidence among citizens. E-voting may also be scaled up or down to fit growing electorates and specific socioeconomic or territorial requirements.

E-voting networks, on the other hand, must be developed with rigorous protections to assure their reliability and safety. Capacity-building and training initiatives are required to improve the distribution of skilled ICT staff and expert personnel across all industries. Zimbabwe's government should develop a comprehensive legal framework outlining the standards, norms, and procedures for electronic voting. The regulatory framework should ensure the fairness of the voting process, protect voters' privacy, and handle any possible problems.

The author proposes a five-point strategy for adopting electronic voting systems in the Republic of Zimbabwe:

1. Legislative Foundation: The Zimbabwean government should adopt a comprehensive legal framework outlining the standards, norms, and procedures for electronic voting. This legal structure should assure the equity of the voting process, protect voters' privacy, and handle any possible problems.

2. Public Participation: The author advises that the Zimbabwean government involve all required partners in the planning and implementation of e-voting systems. Candidates for office, civil society groups, election administration organizations, and technical professionals are all included. Open conversations and debates with a diverse audience will aid in the formation of trust and consensus.

3. Trial Tasks: Before ramping up deployment, the author advocates evaluating the feasibility, reliability, and safety of the system for electronic voting on a small scale. Before expanding up the implementation, pilot programs will detect and fix any scientific or operational difficulties.

4. Member Training and Knowledge: The author recommends that thorough voter education programs be launched to ensure that individuals are versed in the positive aspects of electronic voting and how to utilize it correctly. Voter registration, voting procedure confidentially, and the overall integrity of the system should be prioritized.

5. Safety Mechanisms: Finally, the author advises implementing robust security measures to safeguard the computerized voting system. This comprises capacity-building and training initiatives aimed at increasing the allocation of skilled ICT human resources and expert personnel across all industries.

The author suggests that e-voting can alleviate many of Zimbabwe's election-related difficulties. Zimbabwe's government should establish a robust legal framework, enlist all essential partners, and carry out experimental initiatives. The author suggests that the e-voting system be tested for feasibility, reliability, and security. Finally, broad voter education campaigns should be implemented, together with robust security measures to ensure that the system adheres to democratic values.

**Critical Opinion:** According to the author, implementing e-voting in Zimbabwe can address historical election-related issues by increasing inclusivity and reducing human errors, thereby reducing voter intimidation. To ensure success, the author proposes a five-point strategy that emphasizes the importance of legislative foundations, public participation, trial tasks, member training, and robust safety mechanisms, with the goal of establishing a secure, inclusive, and transparent electronic voting system aligned with democratic values.

—--------------------------------------------------------------------------------------------------------------------------------------------------------------

The FLEP methodology [14] is an electronic voting protocol implemented in France for the 2022 French parliamentary election for foreign nationals. The authors highlight two major flaws in the FLEP protocol that have an impact on both the validity of the voting process and the confidentiality of the votes that were cast. By hijacking a hacked voting device, attackers can possibly infiltrate the balloting server and fake votes or change voter intentions. The authors' study demonstrates how the FLEP protocol's dependence on an accurate ballot client presupposition and validating voters are flaws that expose the system to attack.

To address these difficulties, the authors suggest important protocol modifications, with the goal of creating an end-to-end verified e-voting system. The proposed solutions might be classified as either technological or societal. Technical fixes include the addition of authorized boot procedures as well as reliable platform modules to the current voting software. They also suggest a double cryptographic encryption and signature system, whilst social solutions aim to regulate and improve the protocol's deployment process by adding monitoring and inspection requirements. According to the authors' study, the lack of explicit security proofs indicates that the FLEP protocol, as well as any e-voting protocols that use it, are vulnerable to prospective attacks, necessitating additional studies into practical solutions. To improve e-voting security, the authors advocate increased contact between academics and practitioners.

The authors' findings have significant consequences for elected officials, regulators, and academics engaged in the design, development, or auditing of electronic voting systems. They emphasize the need for verifiability in electronic voting systems, which is possible only through formal authenticity processes. The article identifies design and implementation flaws within the FLEP protocol and suggests technological and social solutions. Their work contributes significantly to accelerating the creation of secure voting platforms by detecting potential weaknesses and giving real recommendations that might safeguard the election process's integrity and privacy.

**Critical Opinion:** The FLEP methodology used in the 2022 French parliamentary election for foreign nationals reveals critical flaws, prompting the authors to advocate for significant technological and societal changes to improve protocol security. The lack of explicit security proofs emphasizes the need for additional research and collaboration to strengthen e-voting systems against potential attacks and ensure verifiability.

—-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Citations /References: Use **APA** format

1. Satizábal, C., Páez, R., & Forné, J. (2022). Secure Internet Voting Protocol (SIVP): A secure option for electoral processes. Journal of King Saud University-Computer and Information Sciences, 34(6), 3647-3660.
2. Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting Meets Blockchain: A Survey. IEEE Access, 11, 23293-23308.
3. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. ACM Computing Surveys (CSUR), 54(3), 1-28.
4. Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M., & Almusali, M. (2023). Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain. Applied Sciences, 13(2), 1096.
5. Chaubey, A., Kumar, A., Pandey, V., Bhushan, B., & Purohit, P. (2023). Leveraging Secured E-Voting Using Decentralized Blockchain Technology. In Data Analytics for Internet of Things Infrastructure (pp. 265-290). Cham: Springer Nature Switzerland.
6. Karanikolas, N., Kaklamanis, C., & Nikolopoulos, S. (2023). AQUA: A blockchain based multi-winner e-voting system.
7. Malkawi, M., Yaseen, M. B., & Habeebalah, D. (2023). Ethereum Blockchain Based e-voting System for Jordan Parliament Elections. Appl. Math, 17(2), 233-241.
8. Eghe-Ikhurhe, G. O., Roni, N., Bonsu, M. O. A., & Chen, X. (2023). The relevance of blockchain based voting adoption in governance structure: evidence from Nigeria. International Journal of Economics, Commerce and Management, 11(1), 1-21.
9. Bulut, R., Kantarcı, A., Keskin, S., & Bahtiyar, Ş. (2019, September). Blockchain-based electronic voting system for elections in Turkey. In 2019 4th International Conference on Computer Science and Engineering (UBMK) (pp. 183-188). IEEE.
10. Al-Maaitah, S., Qatawneh, M., & Quzmar, A. (2021, July). E-voting system based on blockchain technology: A survey. In 2021 International Conference on Information Technology (ICIT) (pp. 200-205). IEEE.
11. Elfattal, S., Awad, M., & Ben Abderrahmen, S. (2023). E-voting in Literature: Analyzing Nations’ Interest. In Proceedings of the Central and Eastern European eDem and eGov Days 2023 (pp. 41-46).
12. Khalifa, S. S., Ejmaa, A. M. E., Najih, A. M. A., & Zneen, M. A. A. M. (2023). Designing a framework for blockchain-based e-voting system for Libya. Computer Science and Information Technologies, 4(3), 191-198.
13. Tom, T. (2023). E-voting, Information Gap, and The Digital Divide in Zimbabwe. Technium Soc. Sci. J., 45, 284.
14. Debant, A., & Hirschi, L. (2023). Reversing, Breaking, and Fixing the French Legislative Election {E-Voting} Protocol. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 6737-6752).