Global Survey and Comparative Analysis of Contemporary E-Voting Protocols: A Cross-Country Perspective

1st Jorge Flores
40224380
CIISE
Concordia University

2nd Fatemeh Montajabiha
40200002
CIISE
Concordia University

3rd Saloomeh sayad azari
40185290
CIISE
Concordia University

4th Dymphna Thomas
40267079
CIISE
Concordia University

5th Avin Vincent
40265132
CIISE
Concordia University

6thLikitha Reddy
40265131
CIISE
Concordia University

7th William Coker
40260832
CIISE
Concordia University

8th Jagadeesh Bavineni
40219221
CIISE
Concordia University

9th Rahimeh Afshari
40243548
CIISE
Concordia University

10th Kimia Ghasemi
40224378
CIISE
Concordia University

***Abstract*—In this report we will review past and current efforts in the area of e-voting, analyzing his challenges and how different technologies have been trying to address them. Also, we will review experiences of using the approaches that have been applied. In each technology, we will describe, also, the current security analysis with respect to specific attacks. We will go in-depth with some real-world experiences that could present interesting cases of e-voting.**

As is possible to appreciate when someone reads the different protocols and experiences, the task of defining a completely secure protocol for electronic voting is very difficult, not only from the technical point of view but from the political and organizational perspective. In that sense, our main effort in this report is to try to find a tendency in the different approaches to electronic voting that will allow us to give an informed opinion about the question of whether it will be a valid protocol that will be generally accepted, at least for an important period, or that this is an, more and more, elusive objective. In conclusion of this search, we think that the search for a definitive approach is still far from being achieved.

We have separated the protocols and experiences in an imaginary "pre- and post-blockchain word". The use of blockchain, for real or "fancy" reasons, is a definitive moment especially for this kind of problem, so, in our opinion, add some simplicity at the hour of reviewing so many cases. We have found that, despite initial suspicion, all the protocols analyzed that are based on blockchain decided to do this because of the unique characteristics of the blockchain proposal.

***Index Terms*—Keywords: E-voting Protocols, Blockchain, attacks, security analysis**

I. Introduction

Electronic voting (e-voting) is a significant technological advancement in electoral processes, bringing together the realms of digital technology and democratic practices. This report provides a comprehensive review of the e-voting landscape, assessing its development and the numerous challenges it faces. The discussion includes a thorough examination of the technological infrastructure used in e-voting systems, with a focus on cryptographic methods and security protocols that are critical for maintaining the integrity and confidentiality of votes.

The first chapters lay the groundwork by explaining the fundamental principles of electronic voting and emphasizing its critical role in modern democracies. Following sections provide an in-depth examination of blockchain technology, a pivotal innovation proposed to improve the security and transparency of electronic voting systems. This report examines the practical applications of e-voting through a comparative study of various global cases, drawing lessons from various international experiences.

A. Th evolution of non-traditional voting schemes

If we move ahead of what we can consider "traditional voting", that is a vote with a ballot in a voting booth, the first and popular alternative that we need to consider is postal voting. Postal voting is still used in many elections around the world and is considered the standard against e-voting must be compared. Also, in the same category, we have telephone and fax voting. Why postal, telephone, and fax voting are a standard to be compared? Because they offer a way to extend democracy to places and moments different than the traditional voting and, in that way, can achieve major participation and in that way more representativity: many people who would be unable to vote through traditional ways will be able to participate in the democratic process using other ways. Following the same logic, e-voting can offer the democratic process major advantages more than cost or convenience (like electronic voting could be) [1]. In this report, we will explore mainly internet-based e-voting, because delivers a true opportunity to extend the benefits of postal, telephone, and fax voting in terms of extension of places and time and also could provide improvements in the fair conditions of the election process.

B. Theoretical framework

1) Mathematics behind e-voting protocols

- Elliptic curves: can be used for secure and efficient cryptographic operations offering very high levels of security.
- Cryptographic hash functions: play a crucial role in e-voting protocols by providing security and integrity to various aspects of the system.
- Public Key Encryption Schemes: They are very important, providing a foundation for secure communication, authentication, and confidentiality.
- Homomorphic Encryption: It allows one to make specific calculations in the encryption result of the voting, getting results without needing to decrypt the individual votes.
- Digital Signature Schemes: Provides integrity in the public-key setting, authenticating the messages or data that are part of the process.
- Blind Digital Signature Schemes: Allows to ensure the anonymity of protocol participants.
- Commitment Schemes: They are like digital envelopes that guarantee privacy as long as the envelope has not been opened. In addition, there is a bind between the sealer (committer) and the message.
- Secret Sharing: Allows the protection of the key, dividing it into different partners and defining a threshold of participants needed to decrypt the secret.
- Zero-Knowledge proofs: It allows the check that no one can vote twice at the same time that the vote remains private.

C. E-voting online, pre-blockchain history

From the Second World War, mainly pushed by the democratization movement, efforts toward general availability and perfectibility of the democratic process have encountered technical possibilities, and, in particular, the internet offers great promise in that goal. [2]

First, many theoretical protocols were proposed, but mainly those efforts rested in the academic world.

After this, a practical approach emerged from private companies and governments. The political race was ignited when President Bill Clinton ordered an investigation on the matter in 1999. Sadly, the events of the Bush versus Gore election put doubts over certainties in the role of machines in the election

and the trials of internet voting were moved outside the U.S. [1]

II. Main challenges

What makes electronic voting a harder process than e-banking for example? More than the fact that e-banking has problems and is subject to attack and fraud, is the special characteristics that e-voting needs that make this kind of project so challenging.

As an e-voting mechanism, it is necessary to achieve the goals of authentication, anonymity/privacy, and verifiability/auditability. In other words, we need that, for example, to be able to assure the voter that his vote was considered. His option was recorded correctly, and, at the same time, be able to assure him that his vote was anonymous, and there was no way that someone could coerce him with the vote. These objectives look, at first sight, as a contradiction. The fact that the voter receives some kind of paper or receipt is achieved when the voting is done in the voting booth using an electronic machine (which is called DRE = Direct recording voting, instead of REV = remote electronic voting), but in remote e-voting the issue of how to deliver assurance to the voter it has been matter of discussion.

Another aspect that is challenging is the possibility of fraud because any interference in the way of impersonation, communication intersection, tampering, or even the hack of the counting services at the end of the process can be used as fraud methods.

Also, being the process executed remotely, the concern of coercion is similar to the cases of postal, telephone, and fax. Electronic voting protocols need to address this issue. [3]

Even before considering blockchain as a technology interesting for electronic voting, there were three requirements that are very related.

One is End-to-end verifiability, which is the capacity of the system to offer the voter the verification that their own vote has been cast as intended. Another characteristic is Web Bulletin Boards (WBBs) for posting all the cast ballots in a medium where anyone can see the information. WBBs are used in channels that are secured and where all the ballots are shown in encrypted form. The last one is the use of a homomorphic tally, allowing algebraic operations in the group of ballots without the need for decryption.

III. Literature Reviews

Use of e-voting protocols in the world In terms of adoption, we can find, in general terms, a prudent approach from many different countries: there are some who have been promoting the use of electronic voting, especially looking to avoid fraud. Other countries are analyzing electronic voting, especially using reports from expert commissions. There are also, small-scale adoptions and large-scale adoptions. In these cases, we also explore what kind of criticism and attack these experiences have experienced.

A. The Nedap/Groenendaal ES3B electronic voting system, experiences in the Netherlands, portions of Germany, and France

The Nedap/Groenendaal ES3B electronic voting system, which is used in the Netherlands, portions of Germany, and France, has come under fire, particularly in Ireland, where its usage has been suspended. In this research, [6] investigates system vulnerabilities, and also raising concerns about the reliability of Direct Recording Electronic (DRE) voting devices.

The broad usage of the Nedap ES3B in the Netherlands, combined with its suspension in Ireland, emphasizes the importance of assessing the security and dependability of electronic voting systems. This article investigates realistic attacks on the Nedap ES3B, disclosing all probable flaws that could jeopardize the validity of the election results.

The ”Screen and Keyboard Man-in-the-Middle Attack” is one of the attack scenarios outlined, in which a small board is installed inside the device’s enclosure and can intercept and modify data between the computer and the display or keyboard. This raises the possibility of undetectable vote manipulation with limited access before elections. Another

source of worry is the inclusion of a microcontroller in the ballot memory module, which allows for manipulation after votes have been cast, jeopardizing the entire integrity of the voting process.

[6] strongly opposes the reliance on obscurity for security and calls into question security methods that limit auditability. It focuses on the potential clash between the objectives of concerned voters and manufacturer-oriented security features. Furthermore, the failure to examine potential insider attacks and reliance on DRE systems are cited as major problems.

Because of the observed design flaws, the Nedap ES3B system is more vulnerable to exploitation by malevolent actors. While both attackers and governments might possibly exploit its weaknesses, the practicality of attacks and the type of vulnerabilities make hostile attackers more likely to compromise the system, particularly given quick pre-election access.

In conclusion, the Nedap ES3B is said to be insufficiently secure for use in elections. The current Dutch e-voting requirements have been criticized for putting too much emphasis on security against various attacks. [6] advocates for new legal requirements addressing basic computer security and independent verification to ensure election results are legitimate. This analysis broadens the scope of potential attacks beyond specific vulnerabilities in the Nedap ES3B to fundamental questions about the security, transparency, and verifiability of electronic voting systems, urging for a comprehensive approach to election protocols.

B. Clash Attacks on the Verifiability of E-Voting Systems

[7]The paper investigates the vulnerability of electronic voting (e-voting) systems to a new attack known as the ”clash attack.” This attack has the potential to jeopardize the integrity of the voting process, particularly in systems that use receipt verification mechanisms. It has been tested on four different e-voting systems, some of which have been used in actual elections. The paper emphasizes the potential risks posed by the clash attack and provides insights into its applicability across various e-voting configurations. The goal is to raise awareness about this threat, which will lead to the development and implementation of strong countermeasures or the explicit articulation of trust assumptions in future e-voting systems. The Wombat voting system was utilised in a genuine college election in Israel. Voters use an ID card to enter the system, cast encrypted ballots, and then post the results on a public bulletin board. In the context of Wombat, where identical receipts are issued, enabling undetected manipulation, the collision attack is illustrated. The clash attack in Wombat focuses on producing duplicate receipts for voters with comparable selections. Countermeasures including pre-printing serial numbers on receipts and putting in place processes for clerks to recognise and handle duplicate receipts are suggested as ways to lessen the impact of this attack. One popular electronic voting system that is available in multiple varieties is Helios. We discuss the original variation, variants with detachable names and versions with aliases. We describe the clash attack vulnerabilities of these variations. Rival browsers and message boards are exploited by the collision attack in Helios versions with detachable names, which publishes duplicate votes. When voters with similar choices are given the same alias, it could lead to a clash attack against the alias version. Modifications to random coin usage and alias issuance procedures are among the countermeasures. The VAV (Vote, Audit, Verify) voting system—a variation on the Three-Ballot system—is presented in this paper. Voters are issued three ballots. Each ballot lists the candidates in a predetermined sequence, with one candidate designated as ”A” and the rest as ”V.” Simple ballots' serial numbers are altered as part of the clash attack against ThreeBallot and VAV, allowing for manipulation. Verifiability is highlighted as being important, and a countermeasure with pre-printed serial numbers is proposed. The research highlights differences in trust assumptions and attack techniques between the previously reported attack and the clash attack. A pre-printing of serial numbers countermeasure that complies with Wombat is suggested. The study adds to a deeper comprehension of the weaknesses and advantages of the electronic voting

system, with a careful consideration of both verifiability and accountability.

C. Security and Reliability of Webb County's ES&S Voting System and the March '06 Primary Election

[8] Dan S. Wallach's comprehensive approach evaluates the security and dependability of Webb County's ES&S voting system, focusing on the ES&S touchscreen systems used during the March 2006 Primary Election. The investigation included data collection via observations and data copying, which revealed potential vulnerabilities in the electronic voting infrastructure. The initial step of the Threat Analysis report is to look into possible risks to the voting process. It highlights the vulnerabilities to malicious firmware installations and reverse engineering, as well as the dangers of software manipulation throughout the pre-election and election stages. It is advised to use stronger passwords and to install more security features. During an election, the possibility of machine tampering and ballot stuffing increases. The paper discusses accessibility issues as well as the risk of sophisticated attacks. Concerns about poll worker-induced ballot stuffing are raised, emphasizing the importance of strong security measures to prevent fraudulent activities. The Tabulation System may be subject to software and data tampering. The ES&S tabulation systems have centralized tampering risks, necessitating an "air gap" defence and strict physical access controls. The vulnerabilities also raise concerns about data corruption in event logs and voting logs, prompting recommendations for data protection measures such as system lockdown and digital signatures during transmission. The report examines the mechanisms used to collect and transmit votes, highlighting the flaws in PEBs and CompactFlash cards. Procedural errors, such as incorrectly tabulating "test" votes, are discussed, as are suggestions such as incorporating sanity checks and rejecting votes cast after the election date has passed. While both malicious attackers and governments could potentially exploit the vulnerabilities in Webb County's ES&S voting system, the practicality of attacks and the nature of identified vulnerabilities make it more likely that the system will be compromised by malicious attackers. In conclusion, [8] the paper emphasizes the serious security flaws in Webb County's ES&S voting system. It makes useful recommendations to improve the voting infrastructure's security, transparency, and dependability. To maintain public trust and ensure the integrity of democratic processes, robust security measures and transparency in electronic voting systems are emphasized. Critical Opinion: We see a shared vulnerability in the overall security of the Nedap ES3B, contactless smartcard systems, and Webb County's ES&S voting system, which is the reliance on outdated security paradigms. Recent technologies, such as blockchain, are frequently viewed as election security saviors. Although blockchain holds promise, its widespread application to election protocols remains a contentious issue. The immediate need for strengthened legal requirements, independent verification, and transparency trumps the current industry hype surrounding specific technologies. To defend democratic processes and maintain their integrity, an all-inclusive commitment to modernizing election systems and improving security measures is required.

IV. SIVP in Colombia

The SIVP protocol can be implemented in Colombia [9] to ensure a fair and transparent voting process. The protocol provides a method to avoid fraud and assure the accuracy of election results. [9] 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.

[9] 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.

V. Efforts in Libya

Building an e-voting system in Libya [20] 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 more 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 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 the registration of voters, the casting procedure, recording, and validation.

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.

VI. Zimbabwe experience

The author in [21] 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:

- 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.
- 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.
- 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.
- Member Training and Knowledge: The author rec-

ommends 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.

- 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.

According to the author in [21], 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.

VII. Problems with the popular neo-vote system

[28] delves into a critical examination of the Neovote online voting system, shedding light on the significant security and privacy concerns plaguing this widely utilized platform. Neovote, adopted by numerous companies and institutions for conducting internal elections, has faced scrutiny regarding its susceptibility to vulnerabilities and its failure to ensure the privacy and integrity of the voting process. Through a detailed exploration, the study highlights various flaws within the Neovote system. It elucidates the inadequacies in maintaining the confidentiality of voter information, potential loopholes allowing multiple votes, and the lack of mechanisms to guarantee the integrity of the overall electoral process. The analysis dissects the discrepancies between the system's claimed compliance with regulations and the actual implementation, ultimately calling into question the reliability and trustworthiness of this online voting platform.

The paper rigorously examines Neovote's code structure, revealing instances of code re-use from obsolete libraries and the absence of end-to-end verification processes. These inadequacies not only pose a threat to the privacy of voters but also open avenues for potential attacks that could compromise the legitimacy of the entire voting process. The broader implications of this study reach beyond Neovote's specific issues, advocating for enhanced regulatory frameworks to govern the use of online voting systems. It underscores the necessity for greater transparency, verifiability, and adherence to stringent security standards in technological advancements within democratic processes.This analysis serves as a clarion call for policymakers to reevaluate existing regulations and enforcement mechanisms. It emphasizes the need to prioritize security, privacy, and verifiability in online voting systems to uphold public trust and confidence in democratic practices.

The study reveals multiple vulnerabilities in Neovote, particularly concerning privacy and security. From inadequate registration procedures to the absence of end-to-end verifiability, the system falls short of ensuring voter privacy and the integrity of the electoral process. The analysis exposes flaws in the code structure, instances of code reuse from outdated libraries, and failures in ensuring end-to-end integrity checks. Moreover, the absence of code transparency and verifiability mechanisms leaves the system susceptible to potential attacks that could compromise the authenticity of the vote.

[28] presents a thorough and critical examination of the Neovote system, highlighting substantial concerns regarding

its adherence to established regulations and security best practices. The revelation of code reuse, obsolescent libraries, and the absence of end-to-end verification mechanisms showcases significant vulnerabilities. These vulnerabilities not only compromise the privacy of voters but also cast doubt on the reliability and authenticity of the entire electoral process. The discussion on legal and regulatory constraints underscores the importance of regulatory bodies and enforcement mechanisms to ensure the integrity of online voting systems. The paper rightly advocates for better guidelines and standards to govern the use of such technologies, emphasizing the need for transparency and verifiability to maintain trust in the electoral process.

This analysis serves as a crucial wake-up call for policymakers, urging them to reevaluate existing regulatory frameworks and enforcement mechanisms, ensuring that technological advancements in voting systems prioritize security, privacy, and verifiability. It also underlines the responsibility of for-profit entities like Neovote in upholding stringent security standards, especially when their systems play a critical role in democratic processes. The findings of this paper not only raise serious concerns about the Neovote system but also emphasize the broader need for comprehensive regulations that ensure the integrity of online voting systems, crucial in maintaining public trust and confidence in democratic processes.

VIII. Active and passive attacks

Ballot secrecy in online elections is studied for active attacks, but passive attacks on message lengths are less explored. Volkamer and Krimmer's requirement for e-voting protocol messages raises concerns. The study tested if ballot confirmation pages leak voter selection information, with Montreal-based Simply Voting being the only vendor with publicly accessible demonstrations. [34]

The system involves ballot-casting, verification, and review processes, but potential side-channel attacks, such as length-based attacks on voter selections, have been observed in the Voatz system.[2] Voatz's system allows explicit, uncompressed candidate names, while Simply Voting uses fixed-length IDs. The length and value of a candidate's name can affect confirmation page size and potentially leak information under certain conditions.

SwissPost and Neuvote systems avoid transmitting confirmation pages over the internet by generating them on the client side in JavaScript. This prevents network activity and no correlation between candidate name length and network response length. To mitigate length-based fingerprinting attacks, padding is added to ensure a fixed response length. However, this method has limitations and could slow page load times. Simply Voting has implemented a mitigation by adding random padding bytes to their ballot confirmation pages, resulting in a 25% accuracy in prediction strategies. Ballot secrecy headers can be compromised when a voter abstains, resulting in unique TLS record lengths.

In a real-world mayoral election, a model based on network-observed TLS record length of voters' vote confirmation page predicted the chosen candidate with 83% accuracy. In complex ballots, it outperformed random guessing. However, limited information could be collected for significant subgroups of ballots. This performance discrepancy is unlikely to be explained by sample variation, according to validation. It is difficult to obtain voter demos, and firms should not require lengthy internal considerations to answer to requests. The industry should follow Simply Voting's lead and provide free demos.

[34] explores the issue of ballot secrecy in online voting settings, highlighting the potential for exploitation by network observers. A novel attack on encrypted ballot confirmation pages was demonstrated in a recent Canadian mayoral race .A testing system was developed, consisting of a Client Application and a Server Application, to simulate an online voting system. The system simulates an election where voters can vote for one or more offices, with each ballot representing an actual HTTP request. In reality, a voter's choice correlates with the TLS record length of the ballot confirmation page.

SwissPost and Neuvote systems are better because avoid

transmitting confirmation pages over the internet by generating them on the client side in JavaScript. There is no Internet activity, no correlation between candidates. Padding is used for length-based fingerprinting attacks; however, it has disadvantages such as huge response size and content reliance. A solution could be to display candidate names as fixed-length images.

IX. Current blockchain-based voting protocols

A. Blockchain proposals

There are general reasons why blockchain is an alternative, especially if we remember the characteristics described in pre-blockchain efforts like bulletin boards and end-to-end verifiability.

Blockchain, as data that is built out of a chain of data packages, offers even better characteristics than a bulletin board. A block contains a timestamp, a hash value of previous transactions as well as a nonce which is a random number used to verify the hash. The integrity of the blockchain is guaranteed by the structure described. Also, every block is validated by the nodes in the network applying some kind of cryptographic mechanism (like authority-based or storage-based).

The functionality of the blockchain can be extended with the use of smart contracts, which are computerized transactions that enforce the terms of an agreement. Functionality located in smart contracts is executed in very specific conditions and their results are logged in the form of an immutable transaction [4]

Despite the fact that blockchain offers great characteristics to add to an e-voting protocol, it also a "hype" ("a situation in which something is advertised and discussed in newspapers, on television, etc. a lot in order to attract everyone's interest" according to the Cambridge dictionary), so we need to be very cautious about the true nature of so-calling "blockchain-based e-voting protocols". We will review in the next chapter some examples and we will try to assess their real nature.

X. Analysis of Blockchain Solutions for E-Voting: A Summary

In response to the evolving landscape of elections, [30] probes the intersection of electronic voting (e-voting) and blockchain technology. E-voting, aimed at enhancing voter turnout and accessibility, encounters challenges in ensuring security and transparency. The application of blockchain within e-voting emerges as a compelling solution, promising heightened integrity and trust in electoral processes.

[30] systematically dissects various blockchain-based e-voting applications, categorizing their features into four thematic domains: voter authentication, voting encryption, resistance to attacks, and security properties. It offers an extensive exploration of blockchain technology, delving into its implementation nuances, consensus protocols, and the emergence of smart contracts.

The comprehensive analysis of [30] concludes by shedding light on the limitations and potentials of blockchain-infused e-voting systems. It highlights scalability as a pivotal challenge, emphasizing the need for systems to efficiently handle millions of votes within strict timeframes. The paper critically dissects the vulnerabilities of current applications, addressing concerns regarding security, voter identification, decentralization, and the digital divide.

While acknowledging the promise of blockchain in fortifying voting processes, [30] refrains from presenting blockchain as a panacea. It underscores the necessity of complying with fundamental legal principles in voting, addressing technological and human-related constraints, and navigating the political, financial, and ethical implications of deploying e-voting systems.

[30] strength lies in its comprehensive analysis, meticulously dissecting various blockchain-based e-voting implementations. By providing a structured comparison and dissecting their technical features, the paper enables readers to comprehend the nuanced challenges and potentials of these systems.

However, despite its meticulous analysis, the paper might

benefit from further exploration into the practical implications of these systems in real-world scenarios. While addressing scalability and technical limitations, a deeper investigation into user experience, potential societal impacts, and regulatory challenges could render the analysis more holistic.

The paper effectively highlights the complexities and trade-offs inherent in implementing blockchain solutions for e-voting, but additional insights into potential mitigations for the identified vulnerabilities or experimental outcomes could enhance its practical applicability and relevance in shaping future e-voting landscapes.

XI. Blockchain in integrity

In a global landscape where technological advancements continually intersect with democratic processes, the paper serves as an exploration into the pivotal nexus of electronic voting (e-voting) and the transformative capabilities of blockchain technology. Elections, fundamental to democratic systems, demand utmost integrity and trust in their processes. However, in many regions, especially developing countries, challenges persist in ensuring the credibility and fairness of electoral practices due to inadequate civic identification systems and governance issues. The paper systematically navigates these complexities by spotlighting the promise and potential of blockchain technology in fortifying the integrity of voting processes. It investigates the multifaceted applications of blockchain in e-voting, dissecting two distinct streams: one that directly integrates blockchain into e-voting systems and another that employs blockchain as a supporting mechanism, bolstering integrity without intrusively altering the existing voting processes. Through meticulous analysis, the paper delineates how blockchain-based voting systems offer verifiable, auditable, and transparent processes, ensuring voter anonymity while eliminating reliance on centralized authorities. This exploration underscores the crucial role of blockchain's cryptographic algorithms and consensus mechanisms in safeguarding voting processes against external threats, thereby fostering decentralized, secure, and transparent electoral systems.

[29] outlines the crucial role of blockchain technology in bolstering the integrity of voting processes. It discusses two streams of blockchain application in e-voting: one employing blockchain directly for e-voting and another utilizing blockchain as a non-intrusive supporter or third-party verifier in the voting process. Blockchain-based voting systems ensure individual voting verification, auditability, anonymity, and transparency while eliminating the reliance on a trusted third party. The integrity of these systems relies on cryptographic algorithms and blockchain's consensus mechanisms, offering decentralized, secure, and transparent voting processes.

Moreover, the paper emphasizes the importance of electoral integrity, asserting that public confidence in electoral and political processes is fundamental. It highlights the necessity of strengthening the independence of election officials, judges, and courts to ensure impartial and transparent electoral systems. Additionally, the discussion emphasizes the global significance of electoral integrity, not limited to transitioning democracies but extending to established democracies facing varying dimensions of integrity challenges.

[29] provides an insightful analysis of the role of blockchain in maintaining voting integrity. It effectively outlines the challenges in electoral integrity faced by developing countries, such as the absence of robust civic identification systems and governance issues affecting integrity maintenance. By proposing blockchain as a solution, the paper presents a comprehensive framework that accommodates various scenarios, including direct implementation of blockchain in e-voting systems or using it as an integrity layer around existing systems.

However, while [29] advocates for blockchain as a solution to integrity issues, it also acknowledges the complexities. Integrating blockchain into the existing legal framework, ensuring third-party audits, and addressing sustainability concerns arising from dependence on foreign suppliers or licensed software poses significant challenges. Moreover, the paper rightly points out that while blockchain offers potential solutions, it's not a

panacea and requires meticulous consideration and adaptation to diverse electoral contexts.

Overall, the paper makes a compelling case for the integration of blockchain technology to fortify voting integrity. It effectively navigates through the complexities and nuances of electoral integrity issues while offering a robust framework for blockchain-based solutions, showcasing the potential to address these critical challenges in the electoral and voting processes.

XII. Verify-your-vote proposal based on blockchain

[31] presents "Verify-Your-Vote" (VYV), an innovative online voting system utilizing Blockchain technology. It aims to ensure secure and verifiable elections by leveraging robust cryptographic primitives and a transparent bulletin board system. Eligibility verification, voter identification, vote privacy, receipt-freeness, fairness, and individual and universal verifiability are only a few of the many features that VYV provides. The protocol's architecture prioritizes voter privacy and integrity while highlighting security and trust in the voting process.

The research in [31] introduces the VYV protocol, showcasing its novel approach to online voting. By scrutinizing various existing systems like TIVI, Follow My Vote, Open Vote Network, and Agora, the paper demonstrates that VYV provides enhanced security and privacy features compared to its counterparts. The VYV protocol utilizes Blockchain technology, a public bulletin board, and cryptographic primitives to ensure a persistent view for voters, securing the election process from eligibility validation to result verification. The study substantiates the system's robustness through security analyses and formal verification using ProVerif, confirming its ability to maintain vote privacy, authentication, and coercion resistance while enabling scrutiny of the voting process.

While [31] offers an intricate analysis of the VYV protocol and its security measures, some aspects could be further elaborated. The paper occasionally assumes familiarity with advanced cryptographic concepts, potentially alienating readers not well-versed in this domain. A more detailed explanation or supplementary material on these concepts would enhance accessibility and understanding. Additionally, while the security analyses using ProVerif are informative, practical implementation challenges or real-world feasibility studies could add depth to the paper. Exploring the scalability and practical applicability of VYV in diverse election scenarios would augment its practical relevance.

[31]'s comprehensive exploration of cryptographic primitives and formal verifications establishes the robustness of the VYV protocol. However, expanding on real-world use cases, potential challenges in deployment, and considerations for large-scale implementation would provide a more holistic view. Addressing these aspects would solidify the paper's contribution, making it more accessible and impactful for a broader audience interested in secure e-voting systems.

XIII. Blockchain experiences in Real Life

A. Russian Internet voting protocol

The elections of 2021 in Russia have been the target of two papers that we analyzed in this survey. The special political situation of Russia, the big deployment used in that year, and the fact that many important exponents in the area of cryptographies and mathematics came from that area of the world make it very attractive to study the particularities and deployments in e-voting in that election event.

Two main protocols were deployed in the Russian 2021 elections: one developed by Kaspersky Lab and the Department of Information Technologies of Moscow and the other developed by Rostelecom and Waves Enterprise, which was used in six federal districts of Russia.

In the next area, we analyze [4] and [1] who review extensively the second one.

B. Russian Federal e-Voting - General ideas

Even when information and data about the protocol are relatively scarce, some authors have been exploring and putting

together different sources to try to show an integrated scheme of the protocol that was used.

To describe the protocol, first, we can talk about the participants: Voter, Organiser, Internal Observer, External Observer, Election Observer, and Keyholders.

The voter is someone who has the right to vote and is included in a list form by accessing a web portal for Russian citizens. It is important to notice that someone who votes through e-voting can't vote in person. The voters can vote using a mobile application. During the authorization phase, the voting device generates a key pair for the GOST signature scheme.

The organizer is someone who coordinates the e-voting process. It generates the organizer key pair and the final encryption key that encrypts all the votes.

The internal observer is a participant who observes all the processes, inspecting individual nodes of the blockchain and also conducting the auditing process.

The external observer is similar to the internal observer but accesses a web page (that was down during the elections)

Election observer is a combination of internal and external observers.

Key Holders are very important and particular participants of the process: they are who hold shares of the *very important* organizer's secret key.

In terms of process, we have a vote collector, which is a component that allows the voter to cast the vote, interacting with the blockchain and adding encrypted votes. The tallier uses the blockchain and decryptor components. The decryptos has a Hardware Security Module (HSM).

C. Process

The first step called the setup phase, is the generation of multiple keys from the Organiser and Registrar. In this step, the secret key of the organizer is split and distributed, the blockchain receives smart contracts with the information of the election, and the final key is composed of the organizer and teller's secret keys making them mutually dependent in the final result.

The second step, the authorization phase, is related to identifying the voter as someone who can vote using a multifactor e-mail mechanism. In terms of cryptography, the device generates a key pair and the voter is added to the voter list.

The voting phase, step three, utilizes proofing to prove that a bitstring contains correct values and uses smart-contract functionality to validate the vote. The addition of their vote can be validated by the voter on a web page.

The tallying phase, step four, is done by reconstructing the secret key from the shares and summing the ciphers in the blockchain by parts at the end of the aggregate votes. It is important to notice that is not possible to decrypt the transactions containing individual votes using publicly available information.

The final step, the audit phase, verifies the list of voters, the number of cast votes, and blind signatures, and the uniqueness of transactions related to voters.

D. Security Analysis

The main criticism of the process is that it doesn't enable the voter to verify that their vote was published in the blockchain in the way that he marked and also is not possible to know if the vote was altered in the way to the blockchain. So, basically, the process doesn't provide any form of individual verifiability.

A further criticism is based on the fact that opposing past ideas, the secret key of the organizer is not composed of different keys generated by trusted participants but generated by the organizer and then split.

XIV. Other analysis in Russian-based election protocols

[5] performed the security analysis based on nine defining criteria [24], The results from his study infer that the voting system cannot assure a voter to cast-as-intended verifiability as voters cannot confirm if their digital ballot choices were cast

correctly. Although voters can verify their voting transaction in the Blockchain retrieval, they cannot ensure that their vote remains unaltered, and this lacks the recorded-as-cast verifiability. The decryption of individual votes from the Blockchain is impossible due to the publication of only a portion of the secret key after the tallying phase. [1] This allows a malicious voter who controls the voting device to alter the casted vote and the encryption scheme encrypts the falsified vote and this attack goes unnoticed since the voter can only verify his vote casting but not the actual contents of it after it has been cast.

Additionally, the following attack depicts how a malicious government can tie a voter's identity to a cast voted, [24] Collaboration between the Vote Collector and the Registrar during the authorization phase could result in the Voter's IP address and browser metadata being stored by a corrupt Registrar. In the same way, this data may also be recorded by the Vote Collector during the voting phase. As a result, the Vote Collector receives information of the Voter's encrypted vote together with IP address and metadata, and the Registrar obtains knowledge of the Voter's identity, IP address, browser, and device details. The attackers can tie an encrypted vote to the voter's identity by cross-referencing this data. But to decode each vote, it is necessary to compromise the Organiser and Decryptor (HSM module) in addition to the Registrar and Vote Collector (which a malicious government can easily do during the setup phase).

XV. Other experiences of Blockchain in the world

The study [10] 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).

The study [10] 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.

XVI. Specific attacks on the swiss post protocol

From [25] paper we appreciate that global parameters are created by the trusted setup (SDM) at the beginning of the system. Through the SetupTally protocol, the electoral board and mixing control components (CCMs) collaboratively generate a public key while exchanging a secret key. Voters get voting cards with voter credentials and verification codes generated by the trustworthy print office and CCRs using the SetupVoting protocol, which also contains the cryptographic data (CMtable) required for return code recovery with CCRs. Voters receive voting cards during the voting phase, and they cast votes using a web-based client that is relayed to CCRs over an untrusted server. Voters receive jointly computed return codes that are derived from valid votes. After voters verify it with a ballot casting key, CCRs verify its authenticity by working together to compute and return a vote cast return code. Unconfirmed votes are then eliminated during the Tally Phase, and CCMs hosted by Swiss Post mix and partially decrypt the encrypted votes in order. Auditors use VerifyVotingPhase and VerifyOnlineTallyPhase to confirm the evidence provided by control components. The last mix and decryption is finished by the canton CCM, and auditors use VerifyOfflineTallyPhase to confirm the proofs. In this paper we use the terms CCM and mixer interchangeably.

XVII. Lack of signature validation - Attack on individual verifiability

[25] found a vulnerability in the authentication phase of the protocol specifically in 'validateSignature' and 'validateChoiceCodesEncryptionKey' methods. These tests confirm that the input is signed, but they don't confirm the signer's identity. The adversary can infer the identity of authorised parties since they have valid signing keys. Additionally, the system does not verify that the keys are utilised for the intended purpose or that the subject field of the linked X.509 certificate matches the expected party. This vulnerability is further discussed by swisspost in their Gitlab issues board [26], The election's public key is supplied exclusively to the voting server during the configuration phase, signed by the administration board secret key, and is not directly received by the control components from the setup component. For zero-knowledge proof verification, which is essential for individual verifiability, the Return Codes control components (CCR) during the voting phase require the election public key ELpk. It is possible for a malicious voter to offer authentic Choice Return Codes for an invalid vote by taking advantage of the lack of sufficient checks.

XVIII. Attack on individual privacy

The decryption process occurs in a single round, starting with mixer1 mixing and partially decrypting the list of ballots. Subsequently, mixer2, mixer3, and mixer4 continue this process sequentially. This involves auditors in two stages: first, they act as an intermediate spot check before the offline CCM4's involvement. If mixer1, mixer2, and mixer3 provide consistent data, auditors prompt the Election Board to reveal the final part of the decryption key to mixer4. Finally, auditors verify the correct decryption performed by mixer4. [27] found a vulnerability that can exploit two functionalities of the protocol, no verification at the CCM's level and producing relatively small-scale results than the handled ballot sizes. The

potential threat actor for the described attack is a malicious insider or a malicious government agent among the Control Components (CCMs) or the Voting Server. Specifically, the attack involves collusion among three dishonest CCMs and a dishonest Voting Server.

The attack goes as follows [27], after obtaining the k ballot boxes for decryption, an evil Mixing component1 creates an additional one, Bk+1, which just holds an individual's ballot. After that, mixing component1 submits the k+1 ballot boxes to Mixing component2 in the usual manner. Genuine, mixing component2 combines and decrypts the k + 1 boxes, then sends the results to mixing component3, who repeats the process. The malicious Mixing component3 eliminates elements corresponding to Bk+1 before providing the data to the auditors. Auditors find this to be accurate, which leads to the disclosure of the Electoral Board's secret Mixing componet4 key. In the end, Mixing component4 (malicious) works with Mixing component1 and Mixing component3 to finish decoding Alice's ballot. Crucially, the k "valid" ballot boxes can be decrypted by Mixing component4 covertly. Because the dishonest Voting Server may be aware of the relation between ballots and voters (e.g., IP address), this attack enables three conspiring dishonest CCMs and a dishonest Voting Server to discover an individual's vote and, consequently, the vote of any voter of their choice. By adding malicious ballot boxes, [27] the attack can be expanded to discover the votes of several voters while staying undiscovered unless the additional boxes cause the process to delay. Since all communications go through the dishonest Voting Server, Mixing component3 (working with CCM2) may also be truthful.

XIX. Proposal extension to the Swiss protocol

Cryptographic end-to-end verifiability helps detect election integrity violations, but individual verifiability is challenging for voters. A study by [32] showed that QR-code-based code voting should be used in certain elections as it avoids reliance on trustworthy clients and positively affects manipulation detection rates. Studies on verifiable voting systems have shown mixed results on their effectiveness in e-voting systems. A code-voting approach aims to reduce trust in vote secrecy, but limited evaluations have been conducted.

The Swiss voting system uses a postal service to send voters an individual code sheet, which contains an initialization code, check codes for each voting option, confirmation code, and finalization code. The system generates an election-specific election key pair for each voter, with the private key deduced from the initialization code.

Researchers at E-Vote-ID 2021 proposed an extension of Switzerland's verifiable voting scheme to improve vote secrecy. However, they did not evaluate (two groups with video and without video) its effectiveness in manipulating voters. A user study found that 65% of those receiving the video detected manipulation, while 75% and 63% of those not watching the video detected it. The researchers discuss ways to increase detection rates. [32][33]

Online voting for political elections usually involves using verifiable voting systems, which guarantee vote confidentiality only in cases where the voting client is reliable. This problem can be solved by code voting, which offers a workable improvement to the current approach that can improve manipulation-detection effectiveness without compromising usability. According to this research, code-voting verifiable voting schemes may be an acceptable solution since simple steps like scanning QR codes can take the place of difficult human voting code entry steps. Although the analysed technique has a greater manipulation-detection efficacy, there is still potential for improvement. The study in [32] comes to the conclusion that increasing manipulation-detection efficacy requires a close examination of alternative interventions and a focus on verifiability.

This paper focused on cryptographic end-to-end for election integrity violations. Also, evaluate and detect manipulation in electronic voting and attacks. with using a QR code base in the code voting system. They use of blockchain technology in e-voting to address voters between voters. In real they used the

Swiss voting system and E-Vote-ID 2021 to detect manipulation of voting and Improve that system with descriptive video. for the swiss system, voting uses a postal and send code sheet which is a private code for one person. The system became easier using a QR code and scanning with a camera. Then improve with descriptive video.

The E-Vote-ID-2021 proposal outperforms the original system in detection manipulation rates of course, this system improved to description of video and participation divided to video and no video But No significant differences were found between the no-video-group and video-group. It is better to use E-Vote-ID-2021 proposal.

XX. Ethereum efforts

Using blockchain technology, this study [12] 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.

In order to ensure anonymity in score voting, [12] 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.

XXI. Blockchain's based Aqua

Aqua [14], 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 in [14] 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.

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.

XXII. Jordan's parliamentary elections

[15] displays a voting platform based on the technology of blockchain for Jordan's legislative elections. The proposed system is based on digital binding agreements, which are autonomous agreements in which the buyer-seller contract conditions are expressly put into code. The smart contracts are developed on the Ethereum blockchain, which serves as an open-source system for constructing decentralized apps with an elevated level of privacy, reliability, and inviolability. Two digital contracts are created to help with the electronic voting process, with the first tasked with implementing the second. The first contract has a direct relationship to the local and is responsible for creating the district framework, while the supplementary contract is the real eVoting agreement.

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.

For Jordan's parliamentary elections, the study [15] 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.

XXIII. Nigeria's experience

[16] 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.

[16] 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.

XXIV. Turkey's planned blockchain-based e-voting system

Turkey's [17] 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 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 safer and secret. The proposed system's last layer is the unanimity layer, which uses the Ethereum blockchain to reach a 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 [17] 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.

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.

XXV. Scopus database

Elfattal [19] 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.

Author in [19] 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.

XXVI. Additional protocols based on blockchain

The paper [18] 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.

The paper [18] 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.

XXVII. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy

Technology has significantly impacted social life, with the internet providing easy access to resources and services. Blockchain technology, a keystone of cryptocurrencies, is a game changer in many technologies and services due to its immutability property and decentralized architecture. One potential application of blockchain is in e-voting schemes, providing a decentralized architecture for open, fair, and independently verifiable voting. This paper proposes a new e-voting protocol that uses blockchain as a transparent ballot box, adhering to fundamental e-voting properties and offering decentralization. The paper highlights the pros and cons of using blockchain for this proposal, providing a roadmap for blockchain technology to support complex applications.

Blockchain technology, a distributed network of interconnected nodes, allows users to remain anonymous and has the potential to make e-voting more acceptable and reliable. Its distributed ledger contains the full history of transactions, and no single authority controls the network. [35][36]

The proposed e-voting protocol uses a blockchain-based system to allow voters to change their minds and cancel votes. It uses a transparent ballot box as a network of equals, with each voter acting as a node. A Central Authority verifies eligibility using application-dependent methods. Ballots are digital representations of physical ballots, sealed if not revealed. The protocol has three phases: initialization, preparation, voting, and counting. The protocol ensures eligibility, privacy, fairness, and verification of election results, with a blind signature scheme preventing party identification. Centralization and fraud prevention are key concerns.

[35] evaluates the potential of blockchain technology in e-voting to address the lack of enthusiasm among young tech-savvy people. It suggests an e-voting mechanism and provides performance metrics. The article also covers the difficulties encountered by the blockchain platform in implementing complicated applications such as e-voting. It proposes two potential future directions for improving the underlying blockchain technology for e-voting and other related applications.

[35] Proposes a new e-voting protocol using blockchain for a transparent ballot box, adhering to e-voting principles, offering decentralization, and allowing voter update within permissible voting periods. I mean the paper presents a detailed protocol or system architecture that leverages blockchain technology to ensure security, transparency, and accuracy in electronic voting. for implementation, they used Ethereum blockchain API and used GAS for expenses. Blockchain applications maximize profits by determining transactions worth above computational cost, preventing mining overtaken by mining nodes. But Ethical concerns arise when charging voters for voting rights.

It shows the importance of decentralization in an e-voting system and trust in electronic voting systems.in conclusion, e-voting mechanisms, including blockchain-based schemes like BitCongress, Follow My Vote, and Tivi, offer promising solutions for secure and efficient voting processes. It can improve the security of the voting system.

XXVIII. Risks in blockchain based protocols

The study [11] 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.

The study [11] 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.

According to another study [13], 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.

This study 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.

This study 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.

XXIX. Other efforts

A. FLEP methodology experience in France

The FLEP methodology [22] 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.

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.

B. Specific attacks for the FLEP experience

The French legislative e-voting protocol specification [23] is not completely open but briefly provides data about practical deployment and overall functionality. Debant and Hirschi [D2] Reverse engineered the specification working and their description mainly focused on the newly found channel attacks in FLEP.

C. Lack of correspondence between voters to their ballots

[22] found a vulnerability with the FLEP system which lacks the correspondence of voter's receipts to their ballots. The FLEP system ensures election integrity by using the receipts. To ensure their ballots have been placed in the voting box accurately, voters can choose to send a server a copy of their receipts. Then a third party verifies the decryption zero-knowledge proofs (ZKPs) to ensure the accuracy of the election results.

These procedures act as protections against manipulating any one vote or the election's total result. The authors [22] observed a nuance in the JavaScript code of the FLEP voting client. In particular, the voting client's computation of the ballot references may not match the ones that are provided to the voter. Since the references of the voting servers are not converging with the voting clients in all the instances a malicious actor can exploit the channel attacks.

An attacker who gains access to the communication channel can alter the election results by modifying and discarding the votes. This disrupts the individual verifiability characteristic of the protocol.

XXX. iVote and Voatz protocols

This section will seek to detail voting protocols deployed in actual elections, namely iVote protocol which was in March 2015 for the state election for New South Wales, Australia [39]. Additionally, Voatz protocol will be discussed, which was used in 2018 and in state, federal as well as municipal elections in West Virginia, Utah, Denver and Oregon, and used in 2016 Utah Republican Convention and Massachusetts Democratic Convention [41]. Furthermore, vulnerabilities and attacks on said protocols will be explained including, depending on the attack, its corresponding threat actor (e.g., malicious voter, malicious government). It is also important to understand that due to the sensitive nature of the data being used in the voting applications, the vulnerabilities discovered and discussed are limited to public data and replications of the original voting application.

A. Vulnerability of iVote Protocol

The protocol iVote as previously mentioned was used in state election in New South Wales, Australia and accounted for 5% of total votes for the entire election and was developed by Scytl partnered with New South Wales Electoral Commission (NSWEC) [39]. Security experiments and analysis were executed by a team of researchers named, [39] from University of Michigan and University of Melbourne, respectively. They discovered two downgrade-to-export attacks that the iVote protocol is vulnerable to, namely FREAK attack (Factoring RSA Export Keys) and Logjam attack.

B. FREAK Attack

The scope of their experiments was limited to publicly available data including client-side HTML, CSS and JavaScript and due them invalid voters they were limited to the login page https://cvs.ivote.nsw.gov.au and the test website, https://practise.ivote.nsw.gov.au/ that the public could practice voting on. Also, both websites were inspected and had virtually the same client-side code. For secure web distribution, iVote, employs HTTPS. The SSL Test performed by Qualys SSL Labs certified that the principal iVote HTTPS server was secure against known vulnerabilities. An external web server on the other hand, https://ivote.piwikpro.com which also imports and executes JavaScript from the Piwik tool when iVote is loaded, was discovered to be insufficient in SSL

settings, obtaining a 'F' grade. The server also supports 512-bit RSA and ephemeral Diffie-Hellman key exchange ciphersuites [39].

The FREAK attack, which stands for Factoring RSA Export Keys, is a TLS vulnerability that was made public on March 3, 2015, less than two weeks before the election. Due to setup issues on the Piwik server, it was vulnerable to FREAK, and a network-based man-in-the-middle attacker [38]. FREAK exploits the flaw in export-grades of 512-bit RSA keys supplied by the TLS protocol, which is a legacy feature of 1990s-era US cryptography export limitations. An attacker could trick browsers into employing export-grade RSA (which has reduced cryptographic entropy), get the RSA private key by factoring the 512-bit public key, and modify the contents of the connection if a server supported it, which Piwik does. The attacker initiates the attack by intercepting the browser's TLS CLIENT HELLO message and sending a substitute message to the server pretending that the browser wants to use export-grade RSA. In export-grade RSA modes, the server issues a temporary 512-bit RSA public key to the client and signs it with a node chosen by the client using the public key from the normal X.509 certificate. The client validates the certificate chain from the server's X.509 certificate to a trusted root certificate authority, then uses the temporary RSA key to encrypt session key information that will be used to safeguard the connection for the lifetime of the connection. The attacker's main objective in establishing a connection is to convince a voter's browser that they are ivote.piwikpro.com by utilizing the server's signature and an RSA public key [39]. Nadia Heninger demonstrated how to factor 512-bit RSA keys in 7 hours for under $100 using open-source tools and Amazon EC2 [43].

After factoring the key, the attacker can intercept the user's connection, note the nonce of the client, and issue a request to the legitimate Piwik server with the same nonce, posing as a signature oracle. The Piwik server changes its temporary key every hour, making factoring the key difficult. However, by maintaining a long-lived TLS connection and repeatedly invoking client-initiated renegotiation, the server may be forced to utilize the same temporary RSA key for extended periods of time [39]. Several browsers namely Internet Explorer, Safari, and Chrome for Mac OS and Android were vulnerable to this attack until a patch was published March 10 and voting on iVote commenced March 16 so many users might still be browsing on vulnerable browser versions [44].

C. Logjam Attack

All widely used browsers were vulnerable to the downgrade-to-export Logjam attack, which was launched against the ivote.piwikpro.com server. This attack targets ephemeral Diffie Hellman (DHE) cipher suites and is enabled by a vulnerability in the TLS protocol rather than a client-side implementation issue. A man-in-the-middle attacker can compel browsers to utilize export-grade Diffie-Hellman with parameters that an attacker can break, gain session keys, and intercept or unilaterally modify the contents of the connection if the server supports it. The Logjam attack used open-source software to complete the pre-computation step for three more popular 512-bit values of p, each occupying about a week of wall-clock time by using idle cycles on a cluster [37]. After precomputation, the researchers were able to break individual key exchanges based on those values in roughly 90 seconds using a single 24-core machine. The same sort of attack would be possible against Piwik's system, allowing them to attack all iVote sessions from any browser for a set up-front cost for the precomputation. Another flaw was that the NSW web server delivered the iVote application using a secure HTTPS configuration, which then loaded extra JavaScript from an unsecured external server, ivote.piwikpro.com. An attacker who intercepted communications between the voter's browser and the PiwikPro server may alter this JavaScript, allowing them to insert arbitrary malicious code into the iVote application. A proof-of-concept demonstration was created to show how an attacker may control the iVote system by exploiting the FREAK or Logjam vulnerabilities. The attack made use of

vulnerabilities in the Piwik server to substitute code loaded from ivote.piwikpro.com with malicious JavaScript that might alter the functioning of the iVote web application at will. The malicious code was introduced into critical components of the iVote client code, which used AngularJS to execute worker JavaScript threads that performed cryptographic operations. As these signals were delivered to the worker script that performed the encryption, the malware intercepted them and changed the intended vote to a different one. This altered the vote transmitted to the iVote server, exposing the voter's intended vote and authentication credentials to the attacker's command-and-control server [39].

D. Vulnerability & Attacks of Voatz Protocol

As previously mentioned, the Voatz protocol was used in 2018 for state, federal as well as municipal elections in multiple states and again in elections in 2016. But it is not without Its vulnerabilities. A team of researchers from Massachusetts Institute of Technology (MIT), namely Michael A. Specter, James Koppel and Daniel Weitzner ran a security analysis limited to a cleanroom environment and a replica of the original Voatz application and its infrastructure so not to affect actual Voatz server. They discussed that the vulnerabilities could be perpetrated by 3 types of adversaries:

An attacker that is controlling a user's device, An attacker controlling Voatz's API server, An attacker that can intercept network activity between the voter's device and the API server but has no further access.[41]

An attacker with root capabilities can deactivate Voatz's host-based safeguards, allowing them to steal the user's vote, disclose her secret ballot, and exfiltrate her PIN and other authentication data. The Zimperium SDK, which is included with Voatz, is configured to detect debugging and other efforts to change the app, as well as collect intelligence on any malware it discovers. It would have recognized the researcher's security analysis, blocked the app from functioning normally, and notified the API server of said activities by default. However a bypass can be accomplished by altering Zimperium entry points to prevent the SDK from running. The hooking tools in the Xposed Framework allowed the researcher to redirect control flow [41].It is also crucial to remember that this was only possible if there was no out-of-band communication between Zimperium and Voatz. This claim is supported by the fact that neither the app's analysis nor Zimperium's description contain any mention of this service. Even in the event that the device is not online, a remote attacker can directly impersonate the user and access Voatz's servers by using the PIN and other login credentials that are not stored in secure storage but rather pass through the application's memory. The PIN and the remainder of Voatz's login credentials can be anonymously obtained by an attacker with root access to the device [41].

The researchers created a program that intercepts and logs every communication between the device and the server prior to encryption with SKaes (which is a 256-bit symmetric key used in the TSL handshake between Voatz server and application) and data encryption and storage in the local database. This allows the researchers to view the user's raw PIN as well as other authentication data in plaintext. Offline attacks can exploit Voatz's database, as it only requires the user's PIN to unlock limited to exactly 8 numeric characters with unlimited attempt as inputting the PIN. This implies only 100,000,000 possible PINs. Additionally, Voatz does not allow PINs with three consecutive digits, removing 5% of PINs before beginning the exploit. This attack would result in quickly relearning the PIN, retrieving the user's PIN, login information, and vote history all at once. The researchers constructed a prototype of this technique and demonstrated that an attacker can brute force the key on a 3.1GHz 2017 MacBook Pro in about two days [41].

An attacker can employ a stealth UI modification attack to change the application to submit a desired vote while still displaying the same UI as if the app logged the user's contribution. This is due to a vulnerability of the application feature that allows for voter spoiling which enables a voter to cast a new vote that invalidates all prior votes [41]. A variant

of this attack affected the Estonia e-voting system with similar results [42].

The protocol is also vulnerable to server attacks, as the analysis indicated that no assurances are made against the API server actively changing the user's vote via a MITM (Man-In-The-Middle) attack. A salt is also required to unlock the database, which is stored in plaintext on disc in the application's shared preferences file. If the server conducts cryptographic procedures such as AES encryption, it may decrypt the user's vote before sending it to any external log via the SKaes and convincingly re-encrypt any value provided to the log. Even if is not symmetric key available to the server, the application is vulnerable to a MITM attack, as access to the unencrypted TLS stream would have to be enabled if a for example a Hardware Security Module (HSM) is employed for cryptographic operations [41].

There is no public key authentication as part of the device handshake, and the device provides evidence to the effect that these interactions are ever registered on the blockchain. The server can terminate the connection before the HSM and arbitrarily impersonate the user's device by repeating the whole device handshake between Voatz server and application and all subsequent communication back to the blockchain via the HSM. The hypothetical HSM, which has the TLS keys necessary to terminate the connection and executes all cryptographic activities, is capable of launching attacks against the user. An attacker having access to the user's network activities, but no key material can determine how the user voted. The software specifically leaks the length of the plaintext, which can allow an attacker to identify, at the very least, who candidate the user voted for. The flaw originates from how a ballot is transmitted to the server after a user has finished making their choice. In a vote submission, the "choices" list containing users' choice, as well as the entirety of the metadata given by the server about that candidate. As a result, the length of the ciphertext varies greatly depending on the voter's choices. Attackers might also deduce the voter's preferences by evaluating the length of the packet that corresponds to the actual vote submission, with the remainder consisting of other protocol requests involved in vote casting and user maintenance. This issue is exacerbated by Voatz's extra encryption. Data is gzip-compressed at the application layer before being encrypted over TLS in Voatz's version, which may have provided some privacy if the compression alone was sufficient to mask the size discrepancies between plaintexts. However, because Voatz encrypts incoming data before the system applies gzip, this step is made insignificant, and the length of the final packet's ciphertext remains proportionate to the size of the plaintext [41].

The Voatz app is a privacy invading application that gathers information from users such as email, physical address, birth date, IP address, picture, device model, OS version, and language choice. It also asks for permission to read GPS data on the initial login. Voatz's use of third-party code comprises more than 22 libraries from 20 suppliers, including more than 22 from separate companies namely Jumio, Zimperium, Amazon AWS, Realm DB, Google Firebase / Crashlytics, gson, protobufs, zxking, Square OHTTP & Retrofit, Datatheorem's Trustkit. Overseas military voters have been reported to use the application, implying that information revealed about users might possibly supply rivals with knowledge on US military deployments. The user's IP address can convey location information, allowing organisations like Jumio, Crashlytics, and Zimperium to infer troop deployments [41].

Additionally, due to the application not requiring voters to re-enter their PIN upon login and does not notify users of re-voted or spoilt ballots, it is vulnerable to coercive attacks. If a voter becomes unconscious, an attacker with physical access to the device and the user's fingerprint might simply vote on their behalf. This susceptibility is especially crucial in instances of domestic violence [40].

XXXI. Conclusion

So, what is our opinion about the applicability of e-voting with the current set of protocols and general conditions? A

direct answer is that currently there are no conditions to apply this in general elections.

One can argue that e-voting is applied with restrictions in Canada and the US, but the key here is the words "with restrictions" because the impact of a problem with e-voting is controlled because of the minimum percentage of the general population who vote through this process. The consequences of a failed e-voting election would be disastrous for the country that hosted that process. This is an argument that is delivered at the beginning of this document precisely differentiating e-voting from online banking.

From the strict security point of view, and like the "Working Group Statement on Developing Standards for Internet Ballot Return" said in 2022 [45], there are key aspects that are not be resolved and are critical to the security of an e-voting event:

Currently, there are no conditions

- End to End Verifiability is not completely achieved and we are far from this: End to End verifiability would allow voters to verify that their cast votes have been correctly registered and have been counted correctly, but is a technology not widely deployed and neither fully tested. Different protocols analyzed in this document have shown that this is a characteristic not achieved, and the Russian elections are a very good example.
- There is, still, a great prominence of malware on the client side. Like in Voatz's case, even safeguards fail to detect client-side control attacks. Another example not involving malware is the FLEP voting protocol.
- Targeted denial of service attacks: despite the fact of multiple efforts in the internet community, there are still techniques and infrastructure that allow this. This is not directly mentioned in the reports analyzed but is a permanent issue with any approach to e-voting.
- Lack of deployment of digital credentials: mentioned as a weak point in the registration process, is needed to avoid this kind of vulnerability. The process of validation through e-mail, message codes, and even MFA has inherent difficulties and risks.
- Apparent contradiction between verifiability and no-coercion: as we have mentioned in the report, these are two objectives that are very difficult to achieve at the same time and are translated in reality to the absence of a direct voter-verifiable ballot of record.

  With these aspects not resolved, the sagest answer is to wait for more mature trials and applications of technology that permit to address the topics described.

References

[1] Gibson, J. P., Krimmer, R., Teague, V., Pomares, J. (2016). A review of e-voting: the past, present and future. Annals of Telecommunications, 71, 279-286.

[2] Horster P, Michels M (1995) Der vertrauensaspekt in elektronischen wahlen. In: Trust Center. Springer, pp 180–189

[3] Tarasov, P., & Tewari, H. (2017). The future of e-voting. IADIS International Journal on Computer Science & Information Systems, 12(2).

[4] Buck, M. (2022). Security analysis of the Russian federal remote e-voting scheme (Bachelor's thesis).

[5] Vakarjuk, J., Snetkov, N., & Willemson, J. (2022, June). Russian federal remote E-voting scheme of 2021–protocol description and analysis. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference (pp. 29-35)

[6] Gonggrijp, R., & Hengeveld, W. J. (2007). Studying the Nedap/Groenendaal ES3B voting computer.

[7] Kusters, R., Truderung, T., & Vogt, A. (2012, May). Clash attacks on the verifiability of e-voting systems. In 2012 IEEE Symposium on Security and Privacy (pp. 395-409). IEEE.

[8] Wallach, D. (2006). Security and Reliability of Webb County's ES&S Voting System and the March 06 Primary Election.

[9] 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.

[10] Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting Meets Blockchain: A Survey. IEEE Access, 11, 23293-23308.

[11] 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.

[12] 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.

[13] 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.

[14] Karanikolas, N., Kaklamanis, C., & Nikolopoulos, S. (2023). AQUA: A blockchain based multi-winner e-voting system.

[15] Malkawi, M., Yaseen, M. B., Habeebalah, D. (2023). Ethereum Blockchain Based e-voting System for Jordan Parliament Elections. Appl. Math, 17(2), 233-241.

[16] 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.

[17] 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.

[18] 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.

[19] 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).

[20] 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.

[21] Tom, T. (2023). E-voting, Information Gap, and The Digital Divide in Zimbabwe. Technium Soc. Sci. J., 45, 284.

[22] 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).

[23] Voxaly.(2023, February 22). VOXALY_LEG2023_Verifiabilites_Specifications_publiques_v2.04.docx – C0 - 2/69 - V. Voxaly.

[24] Vakarjuk, J., Snetkov, N., & Willemson, J. (2022, June). Russian federal remote E-voting scheme of 2021–protocol description and analysis. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference (pp. 29-35).

[25] Haines, T., Pereira, O., & Teague, V. (2022, September). Running the Race: A Swiss Voting Story. In International Joint Conference on Electronic Voting (pp. 53-69). Cham: Springer International Publishing.

[26] https://gitlab.com/swisspost-evoting/e-voting/e-voting/-/issues/1

[27] Cortier, V., Debant, A., & Gaudry, P. (2021). A privacy attack on the Swiss Post e-voting system (Doctoral dissertation, Université de Lorraine, CNRS, Inria, LORIA).

[28] Blanchard, E., Gallais, A., Leblond, E., Sidhoum-Rahal, D., & Walter, J. (2022, September). An Analysis of the Security and Privacy Issues of the Neovote Online Voting System. In International Joint Conference on Electronic Voting (pp. 1-18). Cham: Springer International Publishing.

[29] Adeshina, S. A., & Ojo, A. (2019, December). Maintaining voting integrity using blockchain. In 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 1-5). IEEE.

[30] Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for E-voting: A systematic literature review. IEEE Access.

[31] Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019). Verify-your-vote: A verifiable blockchain-based online voting protocol. In Information Systems: 15th European, Mediterranean, and Middle Eastern Conference, EMCIS 2018, Limassol, Cyprus, October 4-5, 2018, Proceedings 15 (pp. 16-30). Springer International Publishing.

[32] Kulyk, O., Volkamer, M., M¨ uller, M., Renaud, K.: Towards improving the efficacyof code-based verification in internet voting. In: Bernhard, M., et al. (eds.) FC2020. LNCS, vol. 12063, pp. 291–309. Springer, Cham (2020). https://doi.org/10. 1007/978-3-030-54455-3 21

[33] Kulyk, O., Ludwig, J., Volkamer, M., Koenig, R.E., Locher, P.: Usable verifiable secrecy-preserving e-voting. In: Electronic Voting: 6th International Joint Conference, E-Vote-ID. University of Tartu Press (2021)

[34] 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. Federalelections. In: 29th USENIX Security Symposium (USENIX Security 2020), pp. 1535–1553 (2020)

[35] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085263

[36] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375

[37] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., & Zimmermann, P. (2015). Imperfect forward secrecy: How diffie-hellman fails in practice. Proceedings of the ACM Conference on Computer and Communications Security, 2015-October, 5–17. https://doi.org/10.1145/2810103.2813707

[38] Beurdouche, B., Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., Strub, P. Y., & Zinzindohoue, J. K. (2017). A messy state of the union: Taming the composite state machines of TLS. Communications of the ACM, 60(2), 99–107. https://doi.org/10.1145/3023357

[39] Halderman, J. A., & Teague, V. (2015). The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9269, 35–53. https://doi.org/10.1007/978-3-319-22270-7_3

[40] Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., Manthorne, C., Churchill, E. F., & Consolvo, S. (2017).

Stories from survivors: Privacy & security practices when coping with intimate partner abuse. https://research.google/pubs/pub46080/

[41] Specter, M. A., Koppel, J., Weitzner, D., Specter MIT, M. A., Koppel MIT, J., & Weitzner MIT, D. (2020). The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. In arXiv. https://www.usenix.org/conference/usenixsecurity20/presentation/zhou-jie

[42] Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the estonian internet voting system. Proceedings of the ACM Conference on Computer and Communications Security, 703–715. https://doi.org/10.1145/2660267.2660315

[43] Valenta, L., Cohney, S., Liao, A., Fried, J., Bodduluri, S., & Heninger, N. (2016). Factoring as a Service. Financial Cryptography, 9603 LNCS, 321–338. https://doi.org/10.1007/978-3-662-54970-4_19

[44] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, & J. A. Halderman. (2015, March 3). Tracking the FREAK Attack. https://freakattack.com/

[45] Alvarez, M., Garcia, M., Benaloh, J., Herrera, R., Bones, A., Brady, H. E., . . . Weatherford, M. (2022). Working Group Statement on Developing Standards for Internet Ballot Return. Berkeley: Berkeley, Public Policy, The Goldman School.

Contributions

Members	Task
Jorge Flores40224380, Fatemeh Montajabiha40200002 , Saloomeh Sayad azari 40185290	Research of recent academic publications that introduce/analyze voting protocols (starting from recent conferences)
Rahimeh Afshari40243548 , Kimia Ghasemi40224378 , Likitha Reddy 40265131, Avin Vincent 40265132	Research of voting protocols used in practice in various countries
William Coker40260832 , Jagadeesh Bavinemi40219221	Attacks on voting protocols both from malicious voters and malicious government
Jorge Flores 40224380, Fatemeh Montajabiha 40200002	Abstract, Conclusions, General Structure