University of the Philippines Manila
College of Arts and Sciences
Department of Physical Sciences and Mathematics

PriVote: An Anonymized and Secured Ethereum-based Internet Voting System

A special problem in partial fulfillment
of the requirements for the degree of
Bachelor of Science in Computer Science

Submitted by:

Mirai Reyes Yoshizaki

June 2023

Permission is given for the following people to have access to this SP:

Available to the general public	Yes
Available only after consultation with author/SP adviser	No
Available only to those bound by confidentiality agreement	No

ACCEPTANCE SHEET

The Special Problem entitled "PriVote: An Anonymized and Secured Ethereum-based Internet Voting System" prepared and submitted by Mirai Reyes Yoshizaki in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science has been examined and is recommended for acceptance.

Marbert John C. Marasigan, M.Sc. (*cand.*)
Adviser

EXAMINERS:

	Approved	**Disapproved**
1. Avegail D. Carpio, M.Sc.	_____	_____
2. Richard Byrann L. Chua, Ph.D, (*cand.*)	_____	_____
3. Perlita E. Gasmen, M.Sc. (*cand.*)	_____	_____
4. Ma. Sheila A. Magboo, Ph.D. (*cand.*)	_____	_____
5. Vincent Peter C. Magboo, M.D., M.Sc.	_____	_____
6. Geoffrey A. Solano, Ph.D.	_____	_____

Accepted and approved as partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science.

Vio Jianu C. Mojica, M.Sc.
Unit Head
Mathematical and Computing Sciences Unit
Department of Physical Sciences and Mathematics

Marie Josephine M. De Luna, Ph.D.
Chair
Department of Physical Sciences and Mathematics

Maria Constancia O. Carrillo, Ph.D.
Dean
College of Arts and Sciences

Abstract

The proposed system, PriVote, is an innovative and secure e-voting solution for Philippines Barangay SK elections. This web application is built on the Ethereum blockchain, utilizing digital signature technology to guarantee privacy and security for voters. With PriVote, users can register, cast their votes, and verify their votes while maintaining transparency and accuracy in the voting process. Smart contracts are employed to enforce voting rules, while digital signatures are used to provide integrity. PriVote is a potential solution to ensure secure and anonymous e-voting in Barangay SK elections.

Keywords: Keywords: e-voting system, Ethereum, blockchain, digital signature, privacy, security

Contents

List of Figures

List of Tables

I. Introduction

A. Background of the Study

The Sangguniang Kabataan (SK) has been utilizing traditional paper ballots and manual counting for its elections since 1991 [1]. With the rise of modern technology, there is a growing interest in exploring the use of internet voting methods to replace the traditional manual voting system. However, existing internet voting technologies present security risks, making them unsuitable for public elections. Alternatively, offline voting is significantly more expensive [2]. This has led to the development of centralized online voting systems that permit voters to cast their votes from home at their own convenience. However, centralized voting systems are susceptible to tampering, making the results unreliable.

Decentralized voting systems based on blockchain technology offer a potential solution to the security issues plaguing traditional and centralized voting systems. These systems use distributed ledger technologies (DLT) to create a transparent and secure voting system. In blockchain theory, a distributed ledger requires transactions between network participants to be accurately recorded in a shared ledger, with each transaction being timestamped and given a unique cryptographic signature, enabling each transaction to be tracked back to its corresponding historical record [3].

Despite the widespread use of decentralized voting systems, there are still concerns regarding their integrity and security. Therefore, it is necessary to incorporate certain internet properties to ensure the safety of the system. Our focus will be on four critical properties:

1. Tampering - by leveraging the use of Ethereum blockchain and digital signature, the system ensures the integrity of the election results.

2. Ballot confidentiality - only the voter themselves should know who they voted for

3. Individual verifiability - any submitted vote can be verified by the voter themselves.

4. Double spending - the system does not allow overvoting.

B. Statement of the Problem

The traditional paper-based voting system used in SK elections has been plagued with inefficiencies and issues such as legibility of handwriting and incorrect positioning of votes resulting in void ballots. Meanwhile, existing blockchain-based electronic voting systems carry security concerns, particularly with regards to anonymity and transparency [4, 5, 6].

To address these issues, the study propose the development of an internet voting system for SK elections using digital signature with blockchain. This will provide a more efficient and secure way of voting, ensuring both privacy and transparency. By using digital signature to encrypt the blocks, the problem of anonymity will be resolved, allowing for a tamper-proof and transparent voting process.

The system was developed using Ethereum blockchain and smart contracts to enforce voting rules. This system will be designed to guarantee the privacy of voters, prevent tampering, ensure ballot confidentiality, enable individual verifiability, and prevent double spending. The proposed system will be evaluated and tested for its effectiveness in handling SK elections.

The proposed internet voting system, utilizing digital signature with blockchain, presents a promising solution for secure and anonymous e-voting in SK elections, addressing the issues faced by the traditional paper-based voting system and existing blockchain-based electronic voting systems.

C. Objectives of the Study

The objective of this study is to develop a blockchain-based internet voting system that utilizes digital signature technology to address the security and privacy issues in the current manual process of SK elections. The system aims to provide a transparent and tamper-proof voting process while ensuring voter anonymity and confidentiality. The following functionalities will be implemented for the users of the system:

1. Allows the voter to
    (a) Register an account
    (b) Access their account using registered credentials
    (c) View the complete list of candidates and vote for their preferred candidate
    (d) View the results of the election only once the election has ended
    (e) Sign their votes via digital signature
    (f) View the election details
    (g) View their own profile
    (h) Logout of their account
2. Allows the voting authorities to
    (a) Verify and approve a voter's account
    (b) Setup an election wherein they can:
        i. Add candidates along with their position
        ii. Set the name of the election and its respective description
    (c) View the list of registered voters
    (d) Manage the election period
    (e) View the election details

(f) Begin a new election after an election has ended

(g) View their own profile

(h) Logout of their account

The proposed system aims to solve the issues of tampering, confidentiality, verifiability, and double spending in SK elections. The effectiveness and security of the system will be evaluated through an implementation and evaluation phase.

D. Significance of the Project

Automated systems have become an integral part of modern society, and e-voting is no exception. The use of an e-voting system for SK elections can drastically reduce the time and costs involved in manual vote counting and ballot printing. By leveraging Ethereum blockchain technology, the system ensures that data collected is tamper-proof and maintains its integrity. In addition, the use of digital signature technology ensures anonymity of voter data while maintaining transparency. Blockchain technology has proven to be a game-changer in various fields, including politics [7], carbon trading [3], and security [6]. By utilizing blockchain technology in our e-voting system, we aim to increase the security of SK elections and offer an efficient and reliable voting process for citizens.

The main reference, "Z-Halalan: A Blockchain-based Internet Voting System using Zero Knowledge Proof," [8] serves as an important foundation for this project, as it explores the use of online voting systems in a decentralized context. However, this study diverges from the main reference in several key aspects.

Firstly, our focus is on decentralized voting systems based on blockchain technology. While the main reference also utilizes blockchain, our study aims to further enhance security and transparency by leveraging the unique properties of blockchain technology, such as distributed ledger and consensus mechanisms. These features provide a tamper-proof and transparent voting process, ensuring the integrity of the election results.

Secondly, we incorporate digital signature technology to enhance privacy and ensure the authenticity of the voting process. By utilizing digital signature technology, we allow voters to securely sign their votes while maintaining anonymity. This not only protects the privacy of voters but also strengthens the trustworthiness of the entire voting system.

Lastly, this study specifically targets SK elections, which have their own unique requirements and considerations. SK elections involve a specific demographic and require tailored solutions to address their needs effectively. By focusing on SK elections, we can develop an internet voting system that is specifically designed to meet the requirements of this particular context.

In summary, while the main reference lays the groundwork for utilizing blockchain and zero-knowledge proof in an e-voting system, our project goes beyond by emphasizing decentralization, incorporating digital signature technology, and addressing the specific requirements of SK elections. These advancements contribute to the significance of our project in providing an enhanced, secure, and efficient voting solution for SK elections.

By incorporating these differences, our proposed internet voting system addresses the limitations of existing approaches and provides a tailored solution for SK elections, offering a secure, transparent, and efficient voting process for all participants.

E. Scope and Limitations

1. The scope of this study only includes non-weighted votes, which means that each voter's vote is considered equal regardless of their status or position.

2. The project does not consider extending voting time beyond what is required for SK elections.

3. The system will only be accessible to registered voters and voting authorities, and the registration process will be overseen by the voting authorities.

4. The system does not guarantee 100% security and privacy of the data since cybersecurity threats are constantly evolving. However, the application of blockchain and digital signature technology will significantly increase security and anonymity.

5. The system does not implement recasting of votes. Once the votes have been voted, there is no way for the voter to take back their votes.

6. Voters will be required to vote from physical polling stations to prevent coercion or external influence.

F. Assumptions

1. The study assumes that voters have a basic understanding of using the internet and a device (such as a computer or smartphone) to access the internet voting system.

2. The voters who register for the internet voting system will be able to generate and safeguard their own credentials for authentication.

3. The voting authorities who will be managing the system are capable of using the software and will be able to ensure the security of the system.

4. The voting authorities responsible for managing the voting system is trustworthy and acts with integrity throughout the process. This includes ensuring the fairness, transparency, and security of the voting system.

II. Review of Related Literature

A. Sangguniang Kabataan (SK) and SK Elections

The Katipunan ng Kabataan (KK) is a youth organization established under the Local Government Code of 1991 (Republic Act 7160) in the Philippines [1]. The primary role of the KK is to promote the welfare and interests of the youth at the barangay level. The Sangguniang Kabataan (SK) is the governing body of the KK and is composed of elected officials who represent the youth in their respective barangays. The SK is responsible for organizing programs and activities that address the needs and concerns of the youth, such as sports and recreation, education and employment, and community service. With the establishment of the SK and KK, the government seeks to empower the youth to actively participate in local governance and decision-making processes. By engaging the youth in these activities, the government aims to develop responsible and socially-conscious citizens who can contribute to the development of their communities. The SK and KK serve as an avenue for the youth to voice their opinions and ideas, and to make a positive impact on society.

The SK elections proceeds as follows [1]:

- The SK member who obtained the highest number of votes in the most recent election assumes the office of the Chairperson for the unexpired portion of their term.
- In the elected member refuses to assume the position or fails to qualify , the SK member who obtained the next highest number of votes shall assume the position for the unexpired portion of the term.

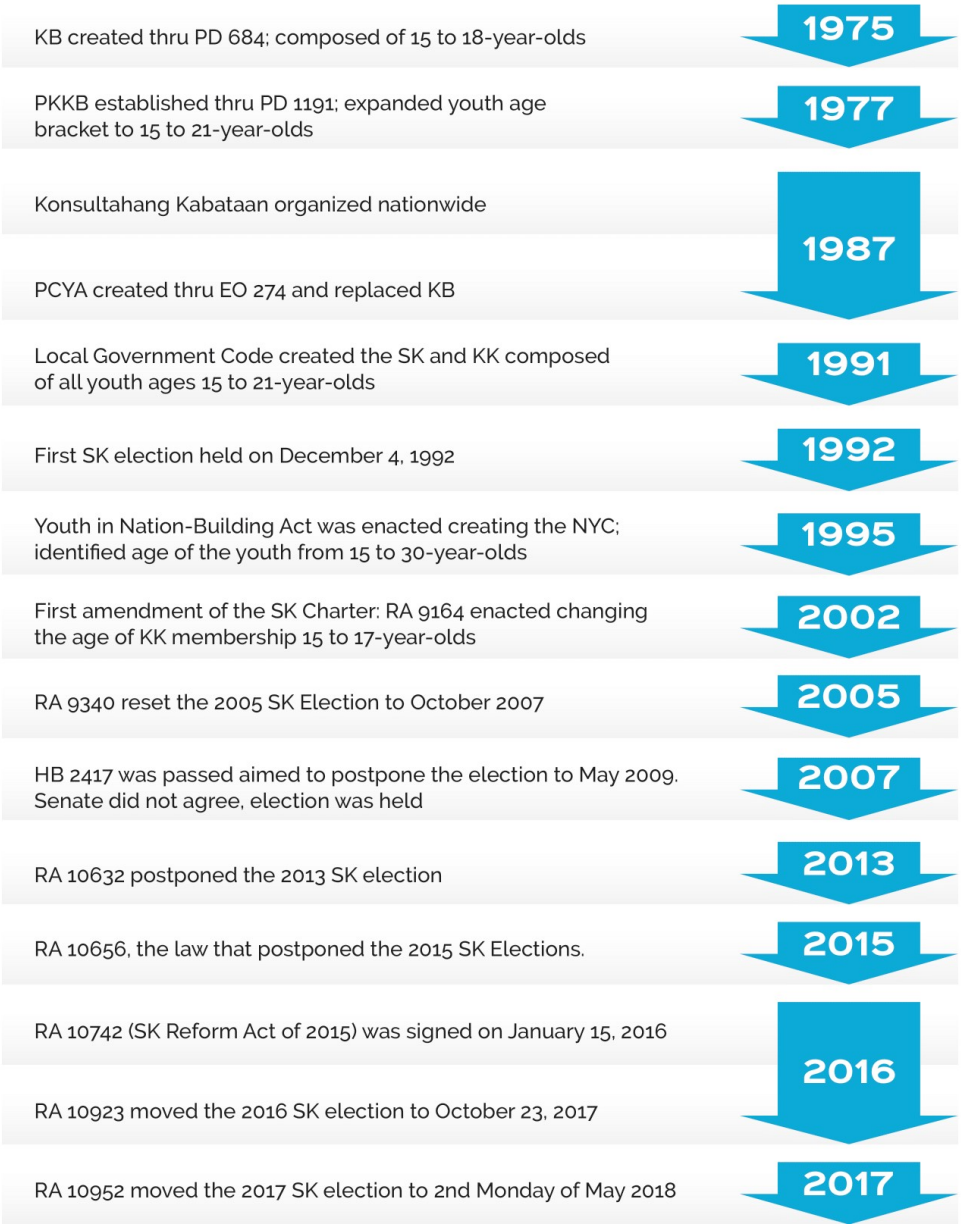

Figure 1: SK Historical Timeline

A..1 Sangguniang Kabataan (SK) Reform Act of 2015

The Sangguniang Kabataan (SK) Reform Act of 2015 (Republic Act No. 10742) was enacted to recognize and promote the youth's role in nation-building [9]. This law provides opportunities for the SK to engage in local governance and actively participate in the development of their respective communities [10].

Below are some of the provisions of the SK Reform Act of 2015 [9]:

- The age requirement for SK members was lowered from 15-17 years old to 18-24 years old, in order to ensure that SK members are more mature and

responsible in fulfilling their roles and duties [11].

- SK officials are mandated to undergo mandatory training programs to enhance their leadership skills, knowledge on public service, and ethical standards [9].
- SK officials are required to create and submit a comprehensive development plan for their respective barangays, which includes programs and projects for youth development, education, and employment [10].
- The SK is mandated to set up a grievance and feedback mechanism to ensure that the youth's concerns and issues are heard and addressed by the barangay officials [9].

A..2 Challenges and Issues in SK Election

Challenges and issues in SK Election include:

1. Lack of interest and participation - Many youth do not show interest in participating in the SK elections, which poses a challenge in achieving the youth's involvement in local governance [12].
2. Limited budget - There is a lack of funding allocated for SK programs and activities, which hinders the youth's capacity to initiate projects and programs beneficial for their communities [13].
3. Political influence and dynasties - The political influence of some families and political dynasties may affect the impartiality of SK elections and prevent the youth's equal representation in governance [14].
4. Lack of awareness and education - Some youth are unaware of the importance and potential of the SK in nation-building and local governance. This challenge highlights the need for education and awareness programs that emphasize the SK's significance in developing the youth's leadership skills and promoting youth participation in local governance [13].

A..3 Importance of secure and accurate voting in SK elections

Secure and accurate voting is essential in ensuring fair and legitimate SK elections. Any issues related to the security and accuracy of the voting process can lead to mistrust and dissatisfaction among the electorate, potentially undermining the legitimacy of the electoral process. The following are some of the reasons why secure and accurate voting is crucial for SK elections:

- Upholding democratic values: The SK elections are a vital component of the democratic process, and secure and accurate voting ensures that these elections are carried out in a fair and transparent manner [9].
- Ensuring Youth Representation: The SK elections serve as a platform for young individuals to participate in the democratic process and have their voices heard. Accurate and secure voting is crucial in reflecting the true will of the youth electorate [1].
- Preventing Election Fraud: Secure and accurate voting is necessary in preventing election fraud and irregularities, such as vote-buying, ballot stuffing, and manipulation of election results [15].
- Maintaining Public Trust: Accurate and secure voting helps to maintain the public's trust in the electoral process, ensuring that the SK election results are widely accepted by the youth electorate [16].

B. Evolution of Voting Technologies

B..1 History of voting technologies

The use of simple objects like rocks, shells, or pottery pieces for voting dates back to ancient times. However, more sophisticated voting methods were developed in the 19th century [17]. The paper ballot was the first voting method to gain widespread use in the United States. Voters marked a paper ballot with a pen or pencil until the late 1800s.

In the early 1900s, mechanical lever machines were developed. These machines had a lever for each candidate or measure, and voters would flip the lever to indicate their choice. Mechanical lever machines were used throughout the United States until the 1960s.

In the 1960s, punch card systems were introduced. Voters would punch holes in a card to indicate their choices, which would then be tabulated by a computer [18]. This method was used extensively in the 2000 United States presidential election and was fraught with controversy due to inaccuracies in the counting process [19].

In the wake of controversies surrounding the 2000 presidential election, many jurisdictions switched to optical scan systems, which involve voters marking their choices on a paper ballot that is then scanned and tabulated by a computer.

In recent years, there has been growing interest in internet-based voting systems. While some small-scale experiments have been conducted, the use of internet-based voting in national elections remains rare.

B..2 Emergence of electronic voting (e-voting) and internet voting

Voting is a method, by which a group, a meeting, or electorates, can make a collective decision or opinion [20]. The voting process involves casting of votes of the voter in a ballot which will then be processed by the system.

Conducting an electronic voting system must involve rigorous studying of the process itself and the security risks that come with it. As such, there have been developments and evolution with regards to voting as a means of addressing these security properties. One of these developments involve the rise of electoral voting.

Electoral voting or e-voting is an electronic means for casting and counting votes [21]. With the rapid development in the Internet and information technology, migration from traditional means to online means have also been progressing – one of these includes e-voting. The first remarkable progress of e-voting that was achieved was when punched-card ballots was first used in 1960's by applying internet technologies [22].

E-voting allows the voter to submit his/her/their vote electronically to the election authorities from any location. Commonly, the e-voting process starts when the voter registers their account in the system, after which a verification will be needed by the voting authorities to assure that the voter registered their true identity. After successful verification, the voter will then be allowed to cast their votes in the ballot - can be digital or paper ballot - which will then be submitted to the voting officials and be kept confidential. Once the voting period is done, the votes will be audited and will be released once results are finalized.

Electronic voting, similar to traditional voting, requires a number of properties to be fulfilled to be considered as an effective and secure system. Some of these include authentication, transparency, anonymity, integrity, security, privacy, mobility, fairness, and verifiability [23]. Although e-voting opens up a lot of new possibilities, it still poses a number of obstacles and challenges to overcome [7].

Internet voting or online voting is a more specific type of e-voting wherein it eliminates the need for printing of ballot papers and ope n polling stations [24]. When conducting internet voting, voters can vote in an election regardless of where they are as long as there is an internet connection. By doing so, voting can be done in remote places and voters do not have to travel to voting precincts to cast their votes. Current internet voting systems have posed security vulnerabilities some of which we will try to solve in this study.

C. Internet Voting Technologies

C..1 Advantages and disadvantages of internet voting

Internet-based voting, otherwise called online voting, provides remote options for voters to submit their ballots over the web [25]. This process results in more accessibility and convenience for voters located anywhere with an internet connection to cast their votes effortlessly. Besides this, internet voting allows for efficiency reporting by real-time vote counts that usually take less time than traditional counters do under observation. Furthermore, one major benefit could be

increased participation among eligible candidates due to its convenience factor [26, 27, 28]. The use of online voting systems by electoral agencies brings forth both advantages and drawbacks.

Proponents argue that it enhances accessibility since individuals nationwide can participate without geographical restrictions while reducing polling expenses through paperless balloting. However, others criticize these methods citing cybersecurity concerns posed by access controls placed on platforms via passwords since determined individuals may attempt to breach the system with fraudulent intentions potentially compromising ideals of fairness further raising suspicions about election outcomes [29].

C..2 Examples of internet voting systems used in elections around the world

Since 2005, Estonia has been utilizing i-Voting as an internet voting system in their elections [30]. Meanwhile, Scytl has also seen usage in several countries such as Switzerland, Australia, and the United States [31]. The government of Norway has conducted online voting tests using eValg during local and parliamentary elections. SMARTmatic was also utilized in the electoral processes of Venezuela, Brazil, and the Philippines [32]. The discussion surrounding internet voting for national elections has revealed a clear dichotomy between those who laud its convenience and potential for increased voter turnout, and those who emphasize its inherent vulnerabilities when it comes to security breaches and compromised voter anonymity. Consequently, while some nations have embraced the new technology, others maintain trust in established paper ballots as the standard means of conducting fair and transparent elections.

D. Security and Privacy Issues in Internet Voting

D..1 Types of security issues in internet voting

Internet voting has been associated with critical security challenges that need careful scrutiny before implementing such systems. Hackers can manipulate vote tallies by gaining unauthorized access while other types of cybersecurity threats include phishing scams, malware infections, insider attacks and denial-of-service (DoS) incidents [33].

Additionally, technological disruptions like computer bugs or communication breakdowns may interrupt voting procedures and errors in vote counting may ensue. The integrity and trustworthiness of election results through online voting are a major concern given the security issues associated with internet voting systems.

D..2 Effect of security issues on the integrity of election results

With technological advancements paving way for modernization in almost every aspect of our lives, internet voting systems are also becoming increasingly relevant. However, it's important to comprehend the security threats that come along with this innovation; cybercrimes like hacking, phishing or denial-of-service attacks pose a serious threat to these systems.

Thus secure internet-based voting processes are indispensable today. An alarming scenario arises when the security breach within an internet voting system is already corrected after it has been detected, yet it fails to remedy the crucial damage to the public's confidence in the democratic process[34].

As such, the integrity of elections can be at stake if security flaws persist since they not only threaten transparency but also accountability in how officials carry out their electoral duties. This emphasizes the need for secure, transparent, and accountable internet voting systems to maintain public trust and protect democracy [35].

D..3 Overview of existing security measures for internet voting

Several measures designed to enhance Internet voting system security include encryption when encoding data with a view to protecting it from unauthorized access. To restrict authorized people from accessing information, digital signatures are used and authenticated [36]. Moreover, in this regard, most systems require multifactor authentication which verifies whether an individual has permission through more than one verification method such as password combinations and biometrics [37]. To deter denial of service attacks from infiltrating the voting system, industry professionals recommend utilizing both firewalls and intrusion detection systems as effective preventative measures against unauthorized access [38].

Despite these implementations serving as critical safeguards towards bolstering overall platform security infrastructures, no system is entirely immune from potential exploitations or vulnerabilities.

Continuous monitoring and testing of the security measures is indispensable in today's world due to the persistent search for system vulnerabilities by malicious actors. This is critical to validate that the system is secure and any existing vulnerabilities are identified and addressed promptly.

E. Blockchain Technology

Blockchain technology served as the foundation of modern cryptocurrencies such that it heavily relied on the usage of cryptographic functions [39]. In blockchain, users make use of digital signatures to ensure secured transaction within the system through the use of public and private keys. Aside from security of transaction, there are other advantages of using Blockchain: (1) Immutable meaning it is difficult to tamper or alter a block in the network, (2) irreversible such that it prevents double spending, (3) distributed system wherein a copy of the ledger is present within all the members of the chain, (4) no central authority meaning it has a P2P system, and (5) resilient such that it is not prone to any sort of major

attacks [40].

E..1 Importance of Blockchain in Voting Systems

As an innovative solution that addresses existing challenges in voting mechanisms, blockchain proves to be reliable when it comes to ensuring the integrity of elections. Through its capacity to register each vote on its network, this technology offers an auditable election result record that resists manipulation or breaches. By having dependable verification methods like these at hand prevent fraudulent practices from deterring voters' trust in post-electoral procedures' legitimacy while cutting out mediators like third-party agencies for cost-efficiency. In 2018, the West Virginia Secretary of State's office executed a trial program aimed at enabling deployed military forces to cast their primary election votes in the state via a blockchain-enabled mobile voting platform [41].

F. Ethereum Platform

Ethereum is a blockchain-based software platform. It is an open platform for constructing decentralized applications atop blockchains; it defines a number of protocols for running arbitrarily sophisticated algorithms on the network. This code is executed on Turing-complete Ethereum virtual machines; these virtual machines are kept on each node in the network, and each issued instruction is executed on each node. Below are the following security properties by Ullah and Assim [42]:

- Decentralization: The fundamental element of Ethereum blockchain represents confidentiality in a decentralized system.
- Transparency: the data script in each node written and updated transparently with trusted source in blockchain system.
- Open Sourcing: All data tracking can be verified publicly, and people and new applications in the system are easy to create.

- Autonomous: Autonomy Chain Cloud of Ethereum Blockchain network controls the node by trusting a single head source for the entire system.
- Immutability: the transaction records are saved permanently and cannot be modified without having control on at least more than half of the nodes simultaneously.
- Anonymity: Ethereum blockchain technologies solved the trust problem between node and node, so data transfer or even transaction can be anonymous, only needing to know the person's blockchain address.

F..1 Ethereum Smart Contracts and Voting Systems

Ethereum Foundation [43] gives us an overview of what smart contract in Ethereum refers to:

Two types of accounts make up the Ethereum platform's core: (1) contract accounts and (2) externally owned accounts, which are often managed by human actors using private cryptographic keys. The code that will run on the virtual machines and control contract accounts can only be enabled by an account that is externally owned. Contract accounts implement **smart contracts**, which are typically made up of value tokens that can only be unlocked under specific circumstances. Solidity is a contract-oriented, statically typed, high-level language used to create smart contracts on, including but not limited to, the Ethereum virtual machine.

F..2 Ethereum-based Voting Systems

In the proposed e-voting system by Vemula et al. [4], they made use of CryptDB for storing election-related information. It not only provides security but also it allows various other operations on data without decryption. Another is a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. [5] We also have the Z-Halalan by Quiaoit [8] which is a privacy-preserving system that is built on the

Ethereum blockchain. It uses zero knowledge proof to provide anonymity to the voters by a coin. Lastly we have the e-voting system which focuses on smart contract such that it addressed some of the fundamental issues that legacy e-voting systems have, by using the power of the Ethereum network and the blockchain structure [6]

G. Digital Signature Scheme

Digital signature schemes enable individuals to sign messages using their private keys, providing a cryptographic proof of authenticity and integrity [44]. Each voter is assigned a unique private key, allowing them to digitally sign their ballots without revealing their personal identity. The signed ballots can be verified using the corresponding public keys, ensuring the authenticity and integrity of each vote.

G..1 Features and properties of digital signature scheme

Digital signature schemes possess several features and properties that contribute to the security and privacy of voting systems [45]:

- Anonymity: Digital signatures conceal the signer's identity, making it challenging to trace the origin of a message. In the context of voting, this anonymity protects voters' privacy and prevents coercion or intimidation based on their voting choices.

- Revocability: Digital signature schemes provide mechanisms to revoke individual signatures in case of illegal activities or misuse. If a voter's private key is compromised or if fraudulent behavior is detected, the corresponding signature can be revoked, ensuring the integrity of the election process.

- Resistance to Forgery: Digital signature schemes are designed to resist forgery, making it difficult for attackers to create valid signatures without access to the signer's private key. This property ensures that only legitimate

voters can generate valid signatures for their ballots, preventing unauthorized access to the voting system.

- Verifiability: Verifiability is a fundamental property of digital signature schemes, allowing anyone with access to the public key to verify the authenticity and integrity of a signed message. In the context of voting, this enables voters to independently verify that their ballots have been correctly signed and submitted, ensuring their trust in the system.

H. Synthesis

The proposed e-voting system discussed in [46] presents an innovative approach to address issues related to data integrity through the utilization of smart contracts and Solidity programming language. The study highlights the importance of comparing the identity of the ID and digital signature on the digital signature issuer's database to ensure the validity of the votes. The findings of the study demonstrate the potential of using blockchain-based e-voting systems for secure and reliable voting.

Furthermore, the Ethereum-based e-voting system presented in [47] utilizes digital signatures to ensure voter anonymity while preserving data integrity. The study shows that the proposed scheme is viable and can be implemented to provide secure and private voting for SK elections. The use of Ethereum blockchain technology offers a transparent and decentralized platform that allows for the creation of tamper-proof and immutable records of the voting process.

The synthesis of these two studies suggests that blockchain technology, particularly the use of Ethereum and digital signatures, can be utilized to develop a secure and reliable e-voting system for SK elections. By implementing the proposed schemes, issues regarding data integrity, voter anonymity, and security concerns can be addressed, leading to a more efficient and trustworthy election process.

III. Theoretical Framework

A. Overview of Sangguniang Kabataan (SK)

A..1 History and purpose of SK

The Sangguniang Kabataan (SK) is the youth council in the Philippines. It was established on 1991, by virtue of the "Local Government Code of 1991" [48]. The SK serves as a venue for the Filipino youth to exercise their leadership skills and participate in community-building initiatives.

A..2 Structure and functions of SK

Below are the functions of Sangguniang Kabataan (SK):

- Act as the official link between the youth, barangay, and local government council [49]
- Promote and protect the general welfare of the youth in the barangay
- Formulate policies and programs that will enhance the social, economic, cultural, intellectual, and moral development of the youth in the barangay [50]
- Participate in the planning and implementation of programs and projects of the barangay council for the benefit of the youth [51]

B. Sangguniang Kabataan (SK) Election

B..1 Electoral process and requirements

The SK electoral process involves several steps and requirements to ensure fair and democratic elections. As stated in the Republic Act No. 10742 or the Sangguniang Kabataan Reform Act of 2015, the SK election process includes the following:

- Preparations for the election, including the appointment of the Board of Election Tellers (BET) and the preparation of the list of voters.

- Campaign period where SK candidates are given the opportunity to present their platforms to the public.
- Election proper where voters cast their votes through secret ballot and the BET tallies the votes.
- Canvassing of votes where the results of the election are transmitted to the city, municipality or provincial board of canvassers.
- Proclamation of winners and submission of the results to the Commission on Elections (COMELEC).

Moreover, there are specific requirements for SK candidates as mandated by law. These include:

- Voters must be a Filipino citizen
- Voters must be of ages 16-30 years old
- Voters must be a registered voter in accordance to the COMELEC guidelines
- A voter will be then given a precinct number in which they can cast their votes
- During the voting period, the voter can cast their votes in their specified precincts
- Once voting period ended, the ballots will be collected and be subjected to manual voting per precincts
- There will be a second counting of votes to ensure that there the votes are counted correctly
- The votes per precinct will be consolidated and the final voting result will be released.

B..2 Challenges and issues in the current SK election system

The traditional SK Elections process involves manual procedures, from voting to vote tallying and counting. A sample SK ballot, illustrated in 2, reveals that the ballot lacks options for Sangguniang Kabataan members or Chairperson candidates. Consequently, voters must be aware of the candidates they intend to support, memorize their names, and the positions they seek to fill. Failure to do so will render their vote invalid. Additionally, the use of printed ballots can lead to various problems such as ballot stuffing, vote buying, and even simple errors such as miscounting. According to a report by the National Citizens' Movement for Free Elections (NAMFREL), the manual counting process has resulted in discrepancies between the number of ballots cast and the number of votes tallied, leading to doubts and questions about the accuracy of the election results [52]. Voter intimidation and vote buying have been identified as another major chal-

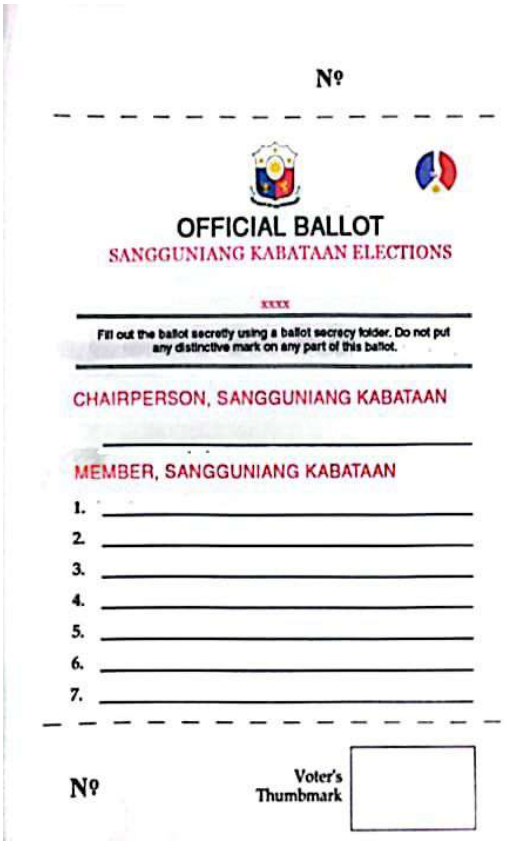

Figure 2: Sample 2017 SK Ballot

lenge in the SK election process. According to a report by [53], incidents of voter

intimidation and vote buying have been persistent problems in SK elections. Voter intimidation refers to any action aimed at discouraging or preventing a voter from casting his/her ballot freely. On the other hand, vote buying refers to the act of offering money or other material incentives to voters in exchange for their votes. These practices undermine the integrity of the election process and compromise the credibility of the results.

Moreover, the current system also suffers from a lack of accessibility, particularly for persons with disabilities (PWDs). The use of printed ballots and manual counting can be difficult for PWDs, who may require special assistance in order to participate in the election process [54].

B..3 Advantages and potential drawbacks of an internet-based voting system for SK elections

An internet-based voting system for SK elections has its advantages and potential drawbacks that should be considered before implementation. Some advantages of such a system include increased accessibility and convenience for voters, reduced costs and time associated with manual voting, and potential for faster and more accurate results [26]. However, there are also potential drawbacks such as security risks, lack of anonymity, and the potential for technical difficulties [55].

C. Internet-based Voting Systems

An internet-based voting system allows voters to cast their votes through the internet and transmit them to a central counting server. This can be done either through public computers, voting kiosks, or any internet-connected device accessible to a voter. To ensure the integrity of the voting process, certain properties must be upheld, including correctness, authenticity, completeness, non-immutability, verifiability, privacy, eligibility, and soundness. Specifically:

1. Correctness: The system must ensure that the voter's ballot reflects the candidate she intended to support.

2. Authenticity: The voter must be able to confirm that her ballot was recorded accurately.

3. Completeness: The public must be able to verify that all recorded ballots have been accurately counted.

4. Non-immutability: The system must prevent a voter from double voting.

5. Verifiability: The public should be able to verify that voters and the election records align.

6. Privacy: The system must guarantee that no unauthorized access occurs with the voter's account and/or vote.

7. Eligibility: Only qualified voters must be allowed to take part in the electoral process

8. Soundness:invalid ballots during the tallying phase must be disregarded.

C..1 Advantages and potential drawbacks of internet-based voting systems

While the internet-based voting system offers increased convenience and accessibility, it presents some potential concerns. Cyber attacks, hacking, and technical malfunctions are among the issues that can occur [56]. Ensuring voter information confidentiality and privacy also raises concerns [57]. Nevertheless, with adequate security measures and proper implementation, an internet-based voting system can enhance the accuracy and efficiency of the voting process.

D. Blockchain Technology

Blockchain technology is a unique form of distributed database communication that allows for the storage, verification, and auditing of transactions among peers on the network [58].

There are four fundamental characteristics of blockchain technology. Firstly, blockchain employs an append-only ledger that maintains a complete transactional history, and transactions cannot be overwritten like in traditional databases. Secondly, the technology is cryptographically secure, ensuring the integrity and verifiability of data within the ledger. Thirdly, the ledger is shared among multiple participants, enabling transparency and accountability throughout the network. Finally, blockchain is distributable, providing scalability for nodes and making it more resilient to cyber attacks.

The process by which blockchain operates is as follows [39]:

1. Users of the blockchain network submit prospective transactions to the network via various software tools like desktop or smartphone applications, digital wallets, or web services.

2. The software then transmits these transactions to one or more blockchain network nodes.

D..1 General Architecture of a block

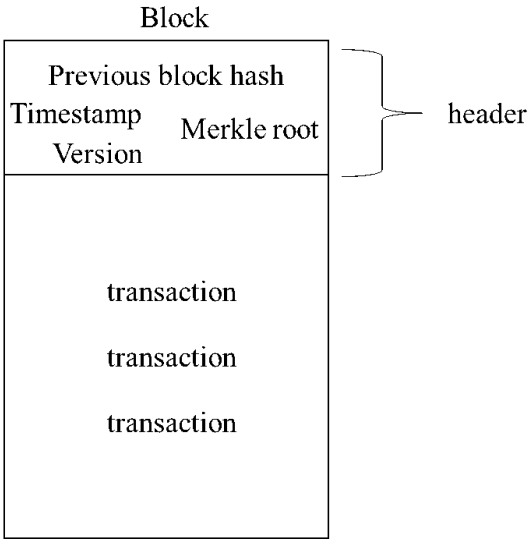

Figure 3: Composition of a Block

The Blockchain is formed by chaining together blocks that contain the hash digest of the preceding block's header, thereby creating a tamper-resistant system

[39]. Changing a previously published block would alter its hash, leading to unique hashes for all subsequent blocks due to the inclusion of the previous block's hash. This mechanism enables easy detection and rejection of changed blocks, ensuring the integrity of the system. In summary, the use of hash pointers to link blocks in a chain provides an immutable and secure distributed ledger, making Blockchain technology an appealing solution for various applications.

D..2 Composition of a block

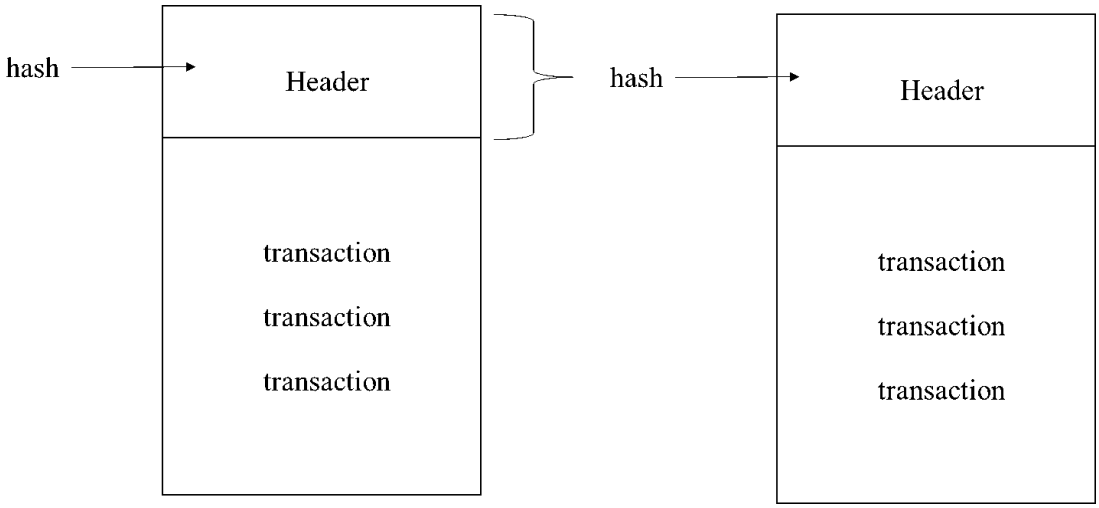

Figure 4: Linked blocks in a Blockchain

- Previous block's hash – A block is a linked list which includes transaction data and a hash pointer.
- Merkle root tree – A cryptographic hash of all the transaction in the block
- Timestamp – The time at which the block was created.
- Version – Current version of the block

D..3 Types of blockchain

Permission-less blockchain

This type of blockchain is public and transparent, allowing anyone to use it without any restrictions. People can operate node mining software, access wallets, and add

data to transactions as long as they follow the blockchain's rules.

Permissioned blockchain

Also known as a private blockchain, this type of blockchain is a closed ecosystem that requires authorization for people to join the network, view its history, or issue transactions.

Consortium or federated blockchain

This type of blockchain removes the authority of an individual and delegates power to a group of individuals forming a consortium or federation. Instead of granting power to a single entity, a group of people or organizations governs the blockchain network.

E. Ethereum Blockchain

The Ethereum blockchain is a decentralized platform where all participants are peers in a network of nodes [59]. Smart contracts are used to execute programs within the Ethereum blockchain. Unlike traditional centralized systems, Ethereum does not require a third-party intermediary, as there is no central authority that governs the chain.It employs a blockchain technology that stores and manages data in a distributed and secure manner, providing transparency, immutability, and tamper-resistance to the system. The use of smart contracts in Ethereum enables the automation of various processes, making it an ideal platform for developing decentralized applications and facilitating peer-to-peer transactions.

F. Digital Signature

The Digital Signature Signature Scheme is a cryptographic protocol that offers several benefits to internet-based voting systems. This scheme provides non-repudiation, integrity, and authenticity of ballots. If all the sginature is valid, then the verification of the vote, in terms of voting system, is also valid. However, if a signature is invalid, the verification as well as the vote itself becomes invalid. The Digital Signature Scheme is an effective technique to ensure the integry and

security of the voting process.

IV. Design and Implementation

A. Use Cases

There are two participants in the diagram below: Voter and Voting authorities. In summary, the voter can register for an account, cast a vote and view the full list of candidates. As for the voting authorities, they are able to approve and verify the voter's accounts and start and end an election.

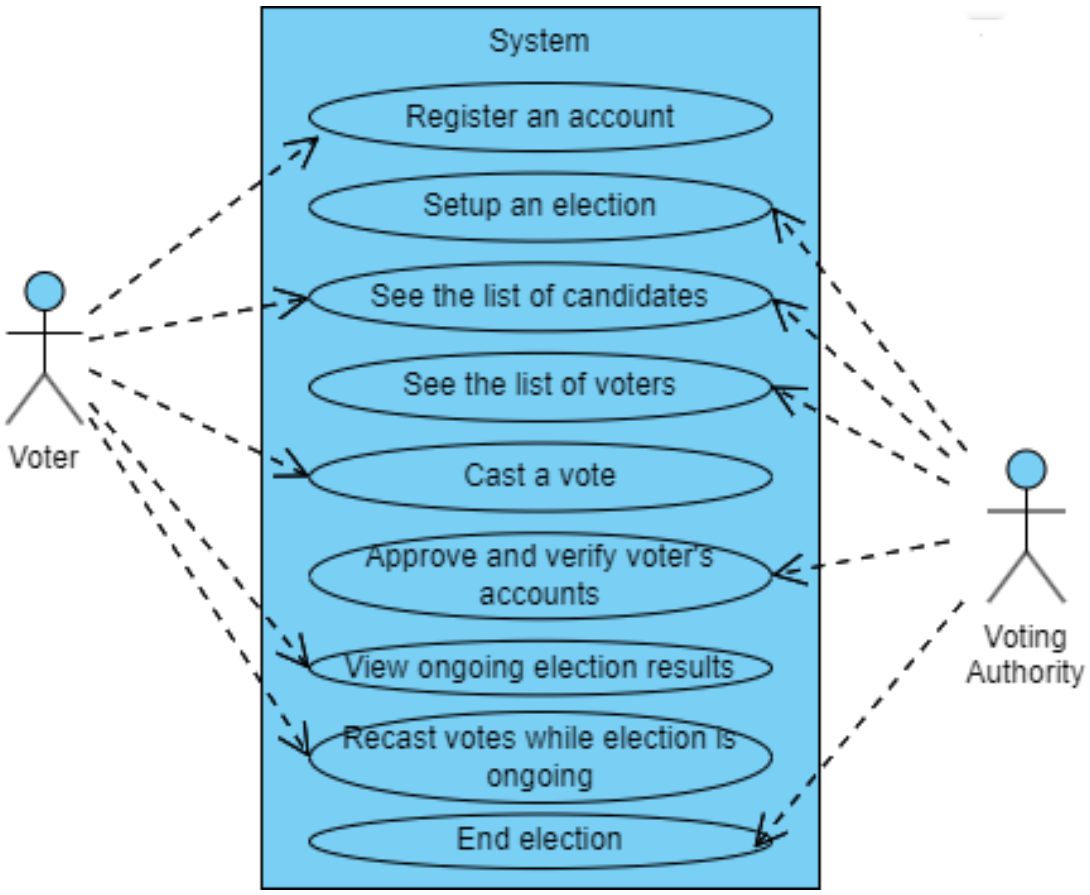

Figure 5: Use Case Diagram of the system

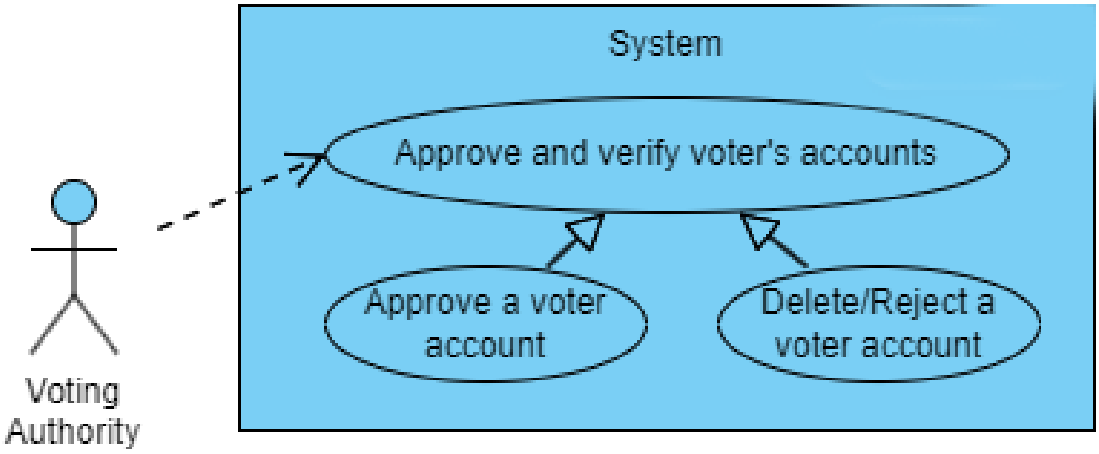

Figure 6: Use Case Diagram for Setting Up Voter List

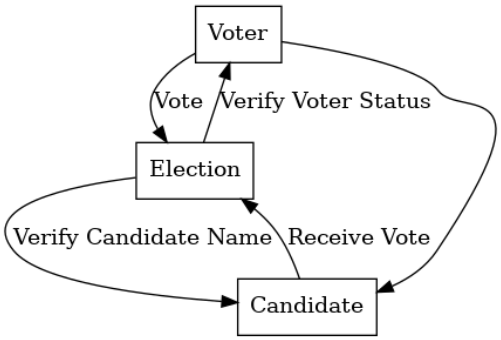

Figure 7: Use Case Diagram for Casting a Vote

Once a vote is received, the system verifies the validity of the digital signature to confirm that it has not been tampered with or forged. This verification process ensures the integrity of the vote and safeguards against unauthorized modifications.

Furthermore, the system checks if the candidate selected by the voter exists and is valid within the context of the ongoing election. This verification step ensures that votes are attributed to legitimate candidates and prevents any manipulation or misallocation of votes.

Upon successful verification of the digital signature and candidate validity, the vote is counted for the specific candidate. This step contributes to the overall tally of votes received by each candidate, allowing for an accurate representation of the voters' choices.

B. Database Design

The system utilized MySQL for the registration of voters, which is a commonly used and reliable database management system.

For the storage of votes, polls, and candidates, the system used blockchain. Blockchain technology can provide additional security and transparency due to its decentralized and immutable nature. Storing this sensitive information in a blockchain can help ensure the integrity and security of the data. Below is the database design.

Field name	Data type	Description
voter_id	Integer	Unique identifier for each USER
email	String	User's email address
first_name	String	First name of the USER
last_name	String	Last name of the USER
is_verified	Boolean	Indicates if voter has been verified by the voting authority
is_admin	Boolean	Indicates if user account is an admin
address	String	Address of the user
age	Integer	Age of the user
birthday	String	Birth date of the user
valid_id_type	String	Valid ID submitted by the user
valid_id_number	String	Valid ID number submitted by the user
blockchain_address	String	Blockchain address of the user

Table 1: User Database Table

Candidate - stores the information about a candidate

- candidateName - name of the candidate
- info - position of the candidate
- exists - boolean which determines if the candidate exists

Election - stores the information about the election

- name - name of the election
- description - description regarding the election
- started - boolean which determines if the election has started

- ended - boolean which determines if the election has ended

Vote - stores the information about a vote cast by a voter for a particular proposal

- voterId - unique identifier for the voter
- voterAddress - address of the voter
- voterName - name of the voter
- candidate - name of the candidate
- signature - digital signature of the voter

C. System Architecture

The system architecture for the proposed internet voting system was based on a blockchain-based decentralized approach. The system made use of Typescript to implement the web application.

The smart contract, a self-executing contract that are stored on the Ethereum blockchain, was built using Solidity programming language and implemented on the Ethereum blockchain. The contract served as the backbone of the system and was responsible for enforcing the rules and regulations of the voting process.

To ensure security and anonymity, the system employed the use of digital signature,particularly using the Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme. Digital signature allows voters to submit their votes without revealing their identities, while still ensuring that their votes are counted and verified.

The system consisted of several modules that work together to ensure the integrity and security of the voting process. The main modules are the voter module, the election module. The voter module is responsible for registering voters and issuing them unique identification numbers. The election module handles the creation of the election and submission and counting of votes.

D. Technical Architecture

- Intel Core i5 or AMD Ryzen 5 (or higher)
- RAM: 8 GB (or higher) if you have an HDD, 4GB if SSD
- Storage: 256 GB SSD (or higher)
- Graphics: Integrated or dedicated graphics card
- Operating System: Windows 10 or Linux
- Network Interface: Ethernet or Wi-Fi

V. Results

User login: The user (Voter or Voting Authority) can login using their email and password.

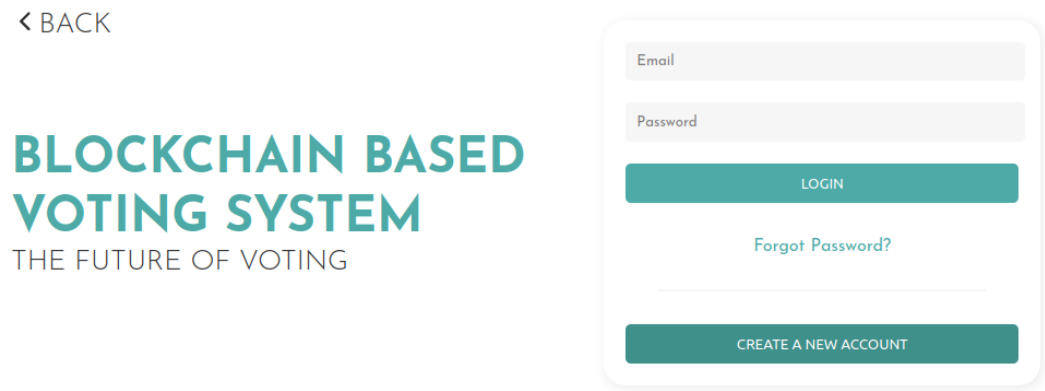

Figure 8: User login page

Voter Registration: These include fields for entering personal information, such as name, address, age, birthday, and identification details as well as their public blockchain address.

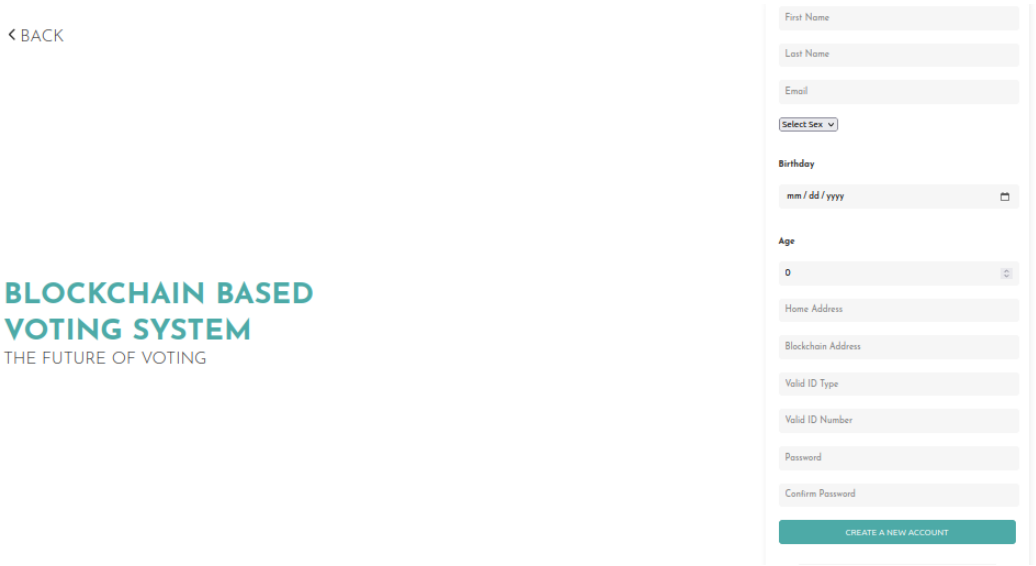

Figure 9: Voter registration page

User Profile: View the user's personal information. In this page, the user can also logout of their account.

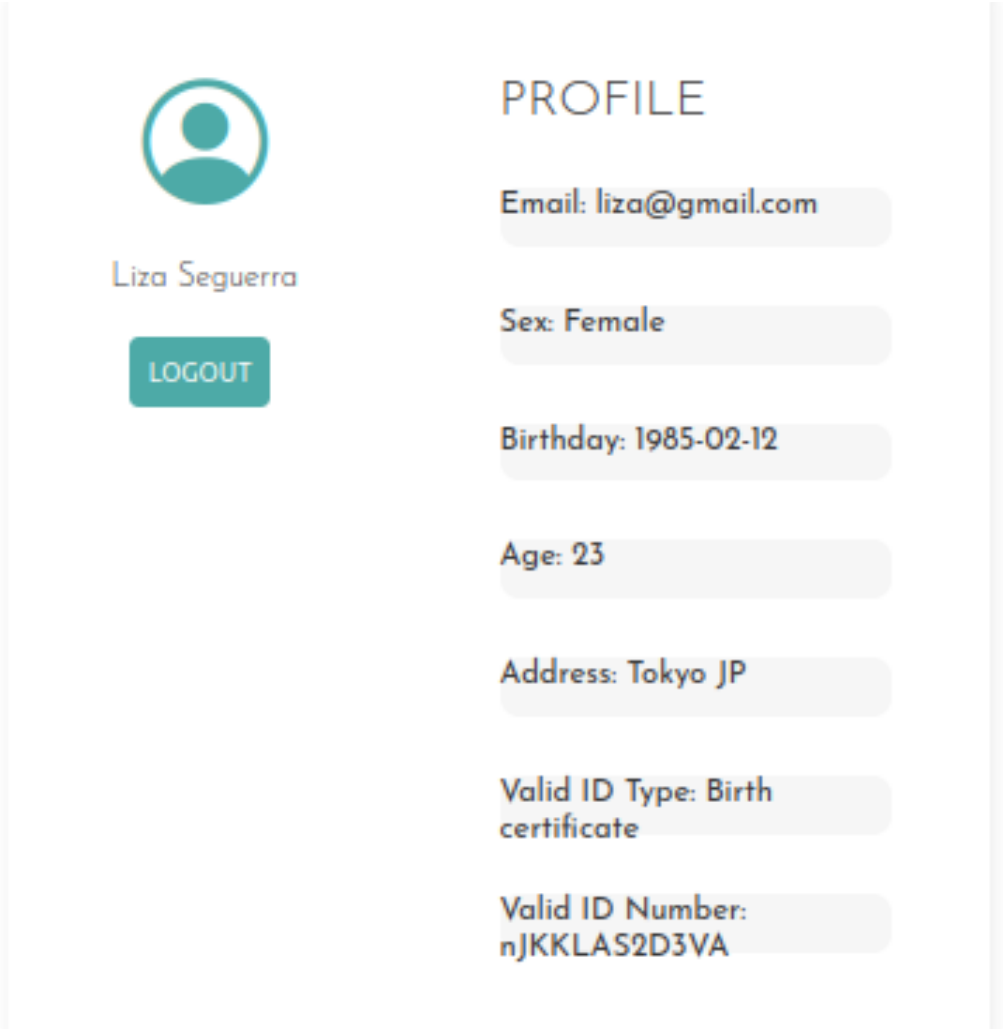

Figure 10: User profile page

Create Election: In here, the voting authority can start an election by inputting the Poll name, the description for the poll, and the Candidates and the respective position they are running for (Chairperson or Member).

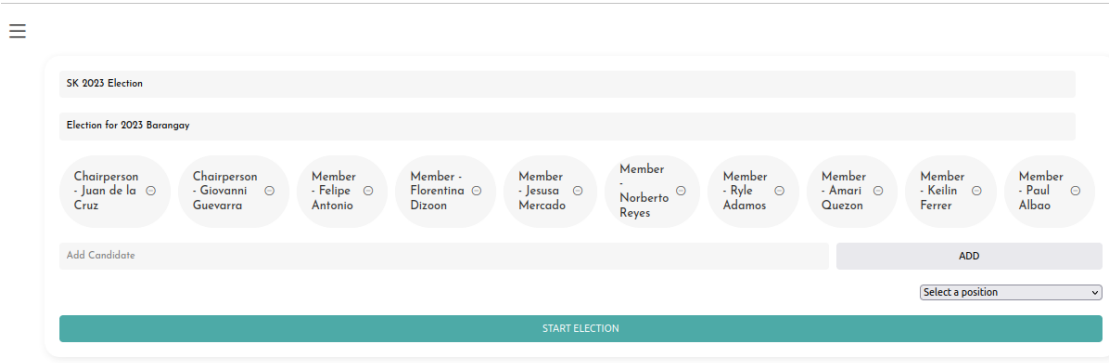

Figure 11: Voting Authority Dashboard - Create poll for election

Vote Submission: When there is an ongoing election, 12 will be the first thing that the voter will see. In here, the voter will need to enter their blockchain address. When properly inputted, the voter will now see the 13 wherein they can vote their preferred candidates. Once a Vote button is clicked it is disabled permanently during the course of the current election. Additionally, a voter can only vote one Chairperson candidate and atmost seven Member candidates.
When a voter inputted an incorrect blockchain address, their votes will not push through the network.

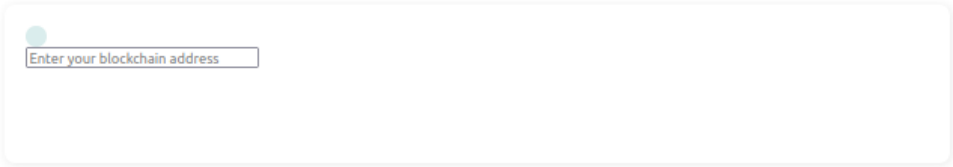

Figure 12: Voter Dashboard - Ongoing election

≡

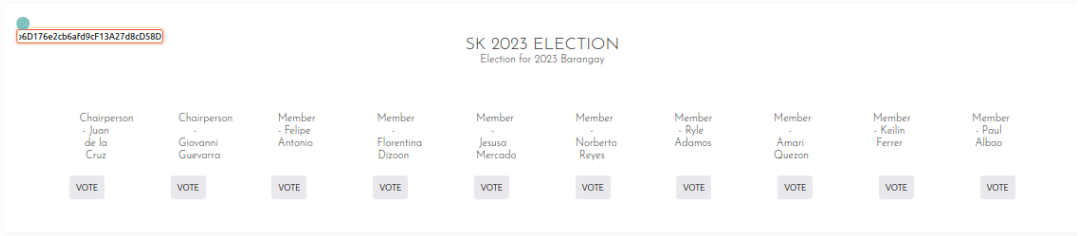

Figure 13: Voter Dashboard - Ongoing election (Inputted Blockchain Address)

Verification Portal: The Voting Authority can verify a newly registered Voter's account here. Every request for verification will display the voter's personal information. The Voting Authority can either verify or delete the request.

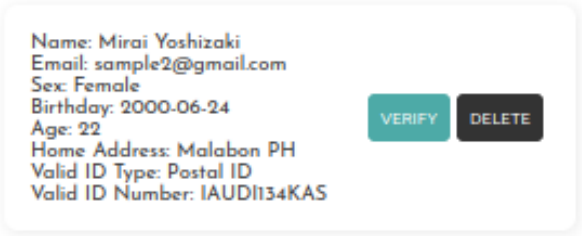

Figure 14: Verify voters

List of Voters: The Voting Authority can view the list of verified voters. Every voter along with their information will be displayed here.

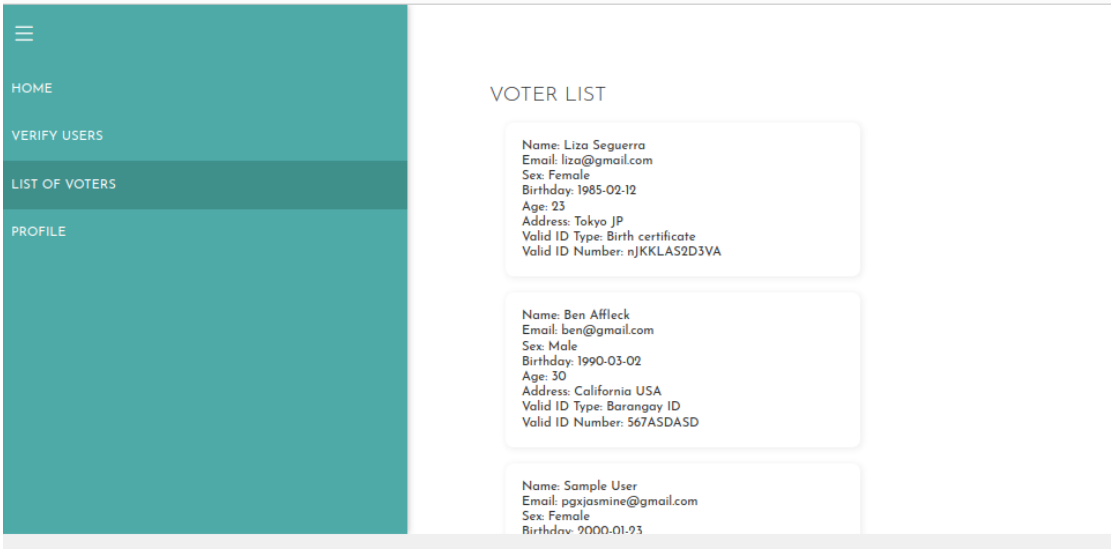

Figure 15: List of voters

Voting Authority Dashboard: This will be the view of the Voting Authority once an election starts. They are unable to view the current tally of the votes and will only be able to view the current candidates for that election. Additionally, they have the option to end the election on their own discretion.

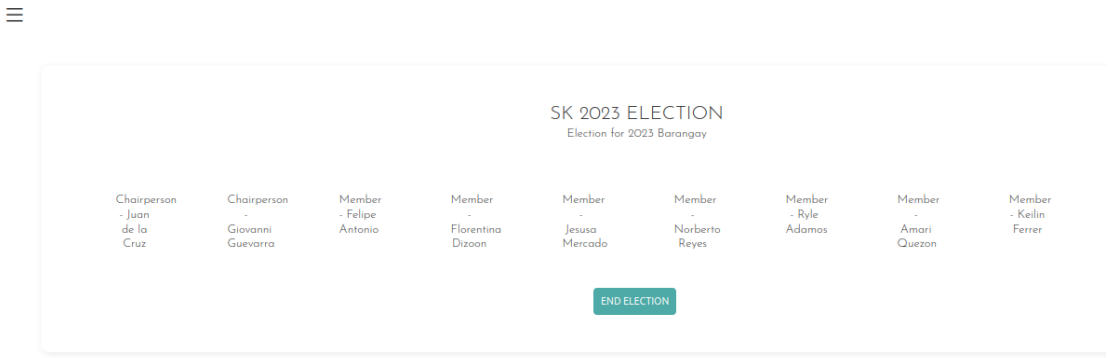

Figure 16: Voting Authority Dashboard - Ongoing election

Vote Results: Once an election is deemed as finished, the final tally of the recently concluded election can be viewed here.

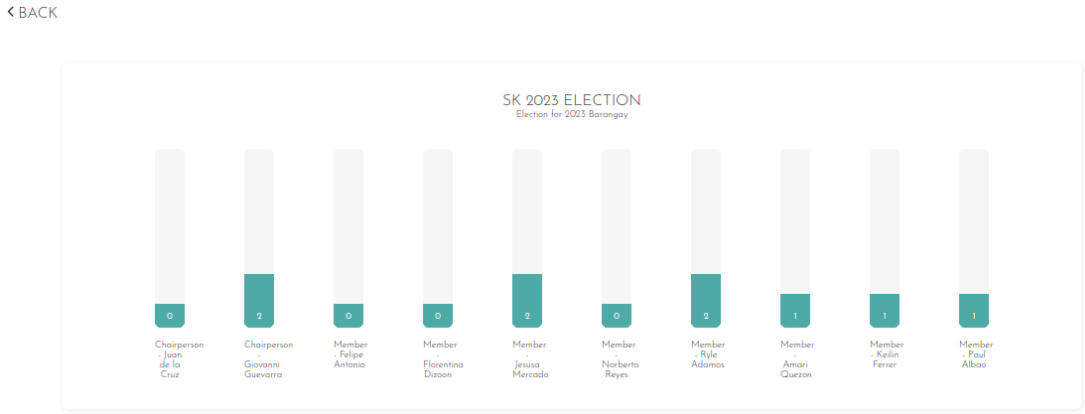

Figure 17: Vote Results for finished election

Election Ended: When an election ends, the voting authority can start a new election by clicking the 'Reset Election' button.

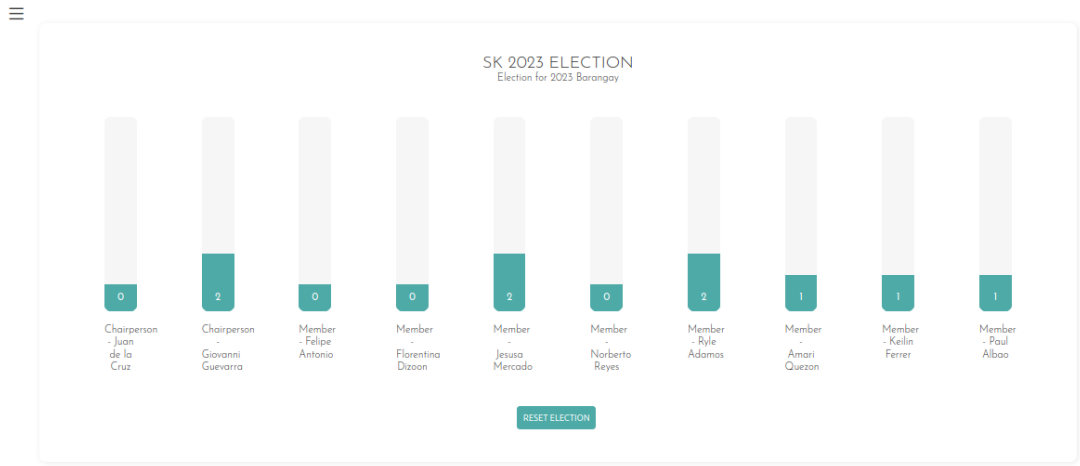

Figure 18: Voting Authority Dashboard - Finished Election

Deployed contract: The deployed contract can be accessed and reviewed through the Ganache interact interface.

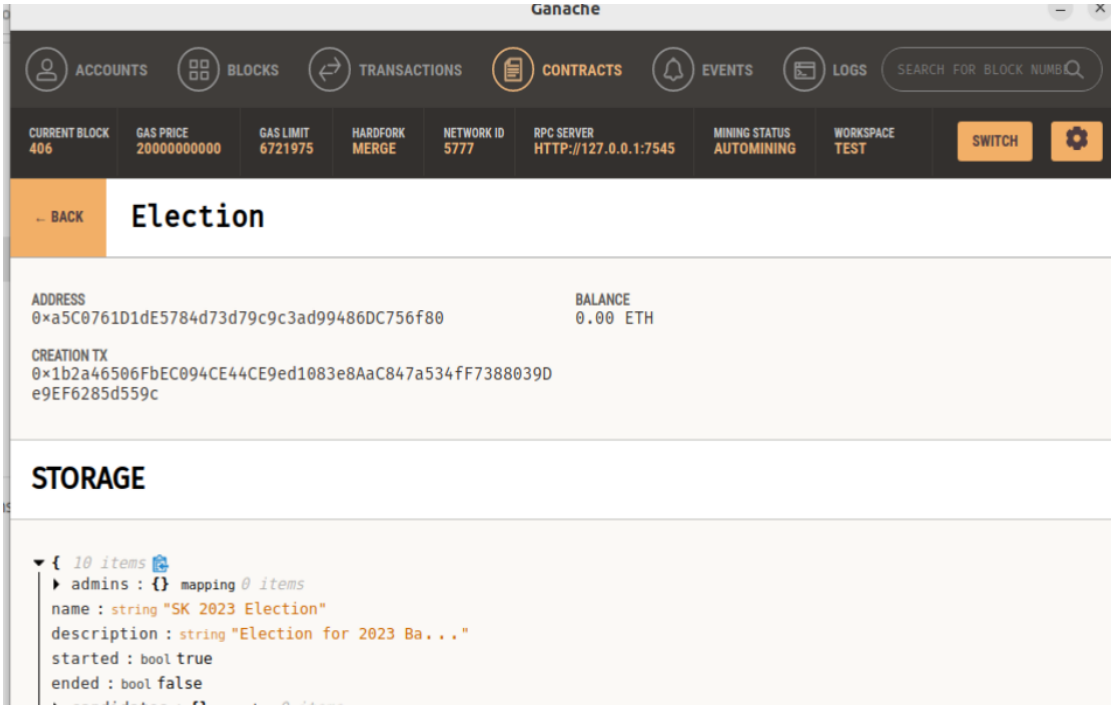

Figure 19: Deployed election contract

Ganache transactions: Throughout the implementation and testing phase, various transactions occurred in the Ganache environment. These transactions represent the interactions with our voting system, such as adding a new candidate, casting a vote, and ending an election. Each action triggered a new transaction recorded in Ganache, providing a transparent and traceable record of the system's operation.

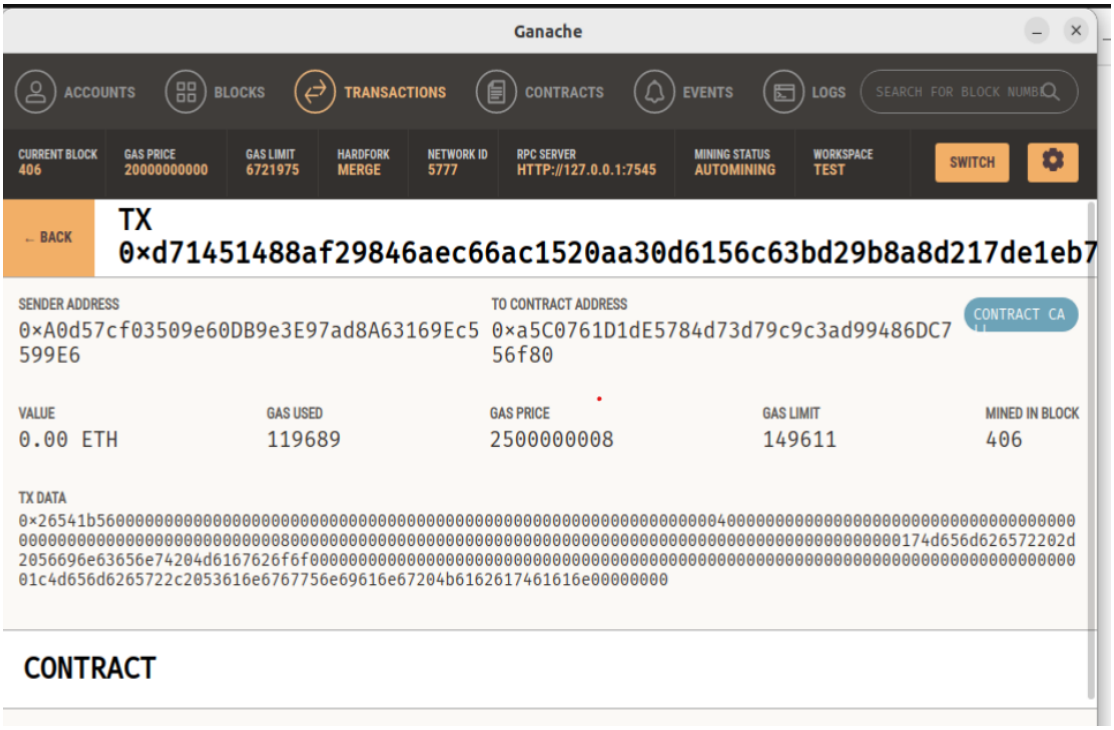

Figure 20: Deployed election contract

VI. Discussions

The developed Ethereum-based internet voting system using digital signature, was evaluated to assess its ability to fulfill objectives, address problems, and provide the anticipated significance. This section discusses these aspects along with the issues and challenges encountered during development and their resolutions, followed by a summary of the main contributions.

A. Objectives and Problem Addressing

Privote aimed to provide a secure and transparent voting mechanism using Blockchain technology and digital signature. The objectives were successfully met by implementing features such as user registration, vote casting, verification, and tallying. The system effectively addressed the problems of tampering, confidentiality, verifiability, and double spending in the voting process, providing an auditable and reliable platform.

B. Security Analysis

- Tampering - The integrity of election results and the prevention of manipulation are two of the primary objectives of our voting system. Utilizing the Ethereum blockchain allows us to take advantage of its decentralized and immutable nature. Each vote is recorded on the blockchain as a transaction, rendering it resistant to manipulation. Any attempt to alter or interfere with the voting data would necessitate consensus from the network, making it extremely secure and transparent.

  In addition, digital signatures play a crucial role in preventing manipulation. Every voter receives a digital signature that is affixed to their vote. This signature functions as cryptographic evidence of the vote's authenticity and prevents unauthorized alterations. Any modification of the vote would result in an invalid signature, signaling promptly that tampering has occurred.

- Ballot Confidentiality - Each vote is encrypted and stored on the blockchain as a secure and confidential entity. The use of ECDSA (Elliptic Curve Digital Signature Algorithm) cryptographic protocol guarantees that votes cannot be traced back to specific electors, protecting their privacy. The encryption process involves utilizing the public key of the voter to encrypt the vote before storing it on the blockchain. This ensures that only the corresponding private key possessed by the voter can decrypt and reveal the actual vote.

- Individual Verifiability: The voting system prioritizes individual verifiability, allowing voters to independently verify their cast ballots. When a voter casts their vote, it is accompanied by a digital signature generated using their private key and the ECDSA algorithm. This digital signature serves as cryptographic evidence of the vote's authenticity. By utilizing the ECDSA algorithm, the digital signature is mathematically linked to the specific vote and cannot be forged or tampered with. Voters can cross-reference their own digital signature with the blockchain's encrypted record of their vote, using their public key, to ensure that their vote has been accurately recorded and has not been altered by any unauthorized party. This transparency and verifiability inspire voter confidence, allowing them to have faith in the system and ensuring that their ballots are accurately tallied.

- Double voting/overvoting - The act of double spending, or casting multiple ballots, poses a serious threat to the integrity of any voting system. Our solution addresses this issue by leveraging the innate properties of the blockchain as well as the use of ECDSA.

  By design, the immutability and decentralization of the blockchain prevent duplicate ballots. Once a vote has been recorded on the blockchain, it becomes part of an immutable and transparent ledger, thereby eradicating the possibility of double spending. However, to provide an additional layer of security, we integrate digital signatures into the voting procedure to prevent double voting attempts.

During the voting process, each voter's ballot is accompanied by a digital signature generated using their private key and the ECDSA algorithm. This signature uniquely identifies the voter and ensures that only one vote per voter is cast. When a vote is received, the system verifies the signature's validity by using the corresponding public key associated with the voter. If the signature is valid, indicating that it was generated using the correct private key, the vote is accepted and recorded on the blockchain.

Any attempt to duplicate ballots would result in an invalid signature. The system checks the validity of each signature during the verification process. If an invalid or duplicate signature is detected, the vote is considered invalid and rejected. This mechanism prevents double voting by ensuring that only unique and valid votes are accepted, maintaining the integrity and fairness of the voting system.

C. Estimated Gas Consumptions

In order to estimate the gas prices for transactions in the voting system, Remix IDE and MetaMask environment were utilized. The Remix IDE provides a convenient development environment for Solidity smart contracts, while MetaMask acts as a digital wallet that interacts with the Ethereum blockchain.

To estimate the gas prices,several transactions were performed using Remix IDE and MetaMask. Below are the different transactions executed in the program along with their estimated gas consumptions:

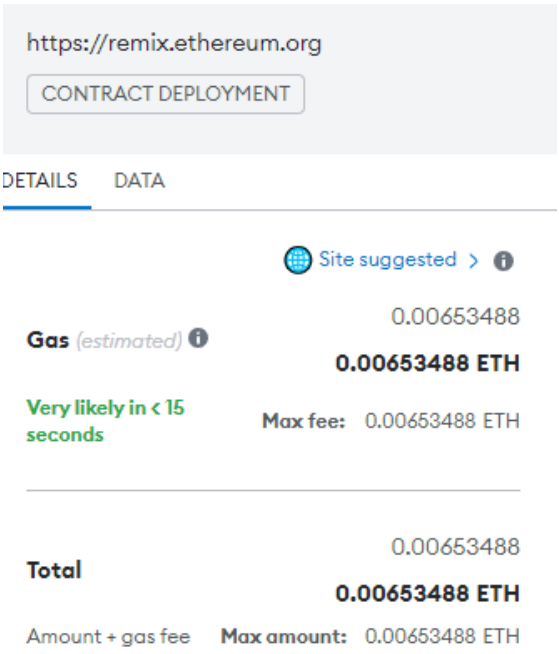

Figure 21: Contract deployment gas consumption

In 21, The deployment of the Election smart contract was initialized. The gas cost associated with deploying the contract is displayed in MetaMask, providing an estimation of the gas required for contract deployment.

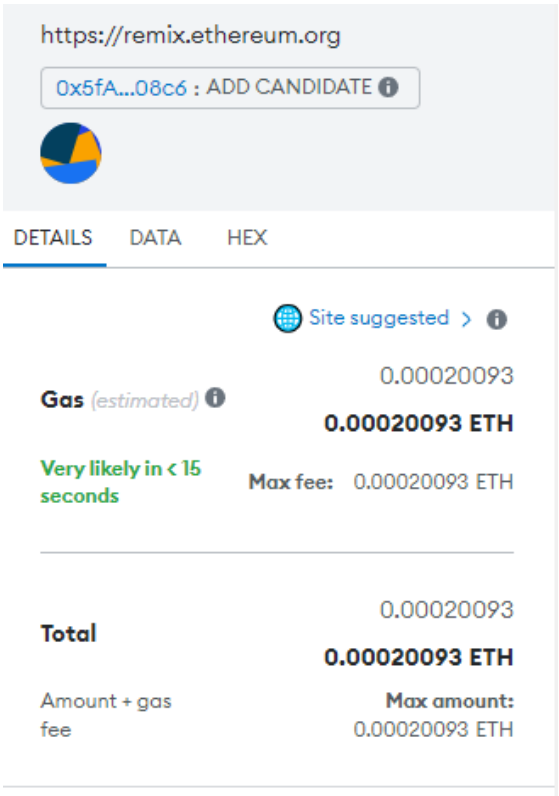

Figure 22: Add candidates gas consumption

The 22 shows the transaction for adding a candidate to the election. By invoking the appropriate function in the smart contract, the candidate's details, such as name and their running position, are recorded.

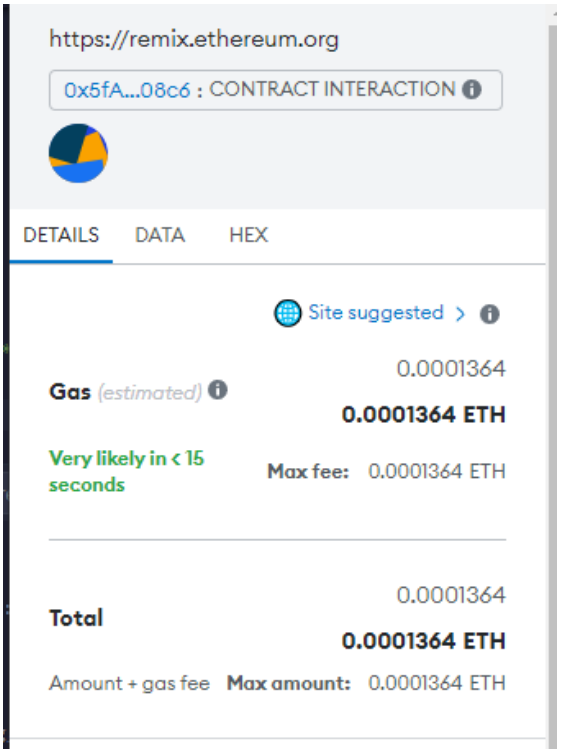

Figure 23: Set election details gas consumption

The transaction in 23 is setting the election details. This includes specifying the election name and corresponding details.

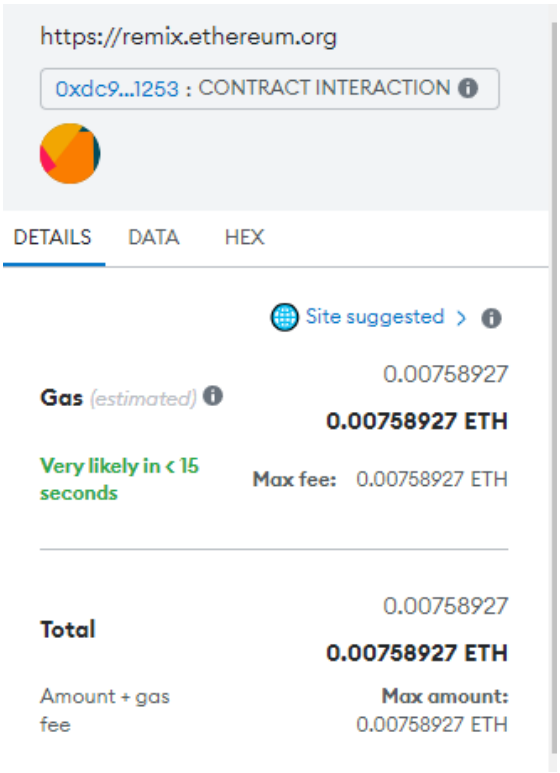

Figure 24: Voter registration page

The 24 depicts a vote transaction. By invoking the vote function, a voter casts their vote for a specific candidate.

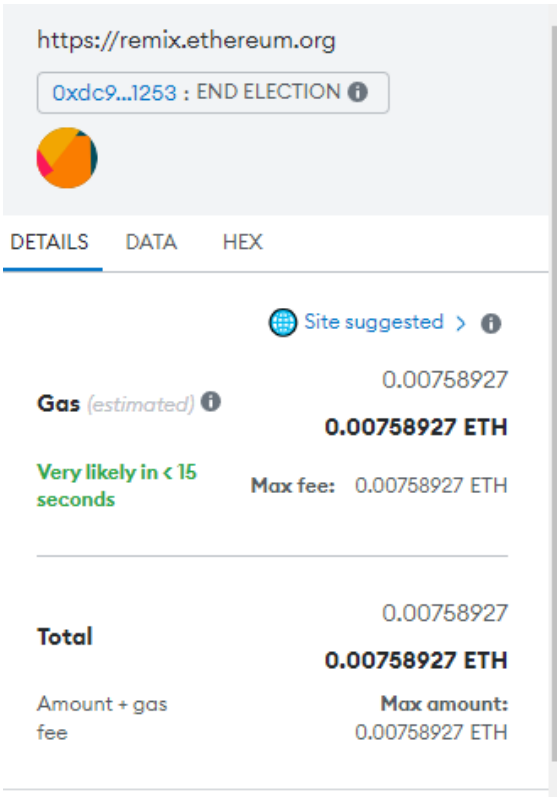

Figure 25: End election gas consumption

25 demonstrates the transaction for ending the election. By invoking the appropriate function, the election is concluded, and no further votes can be cast.

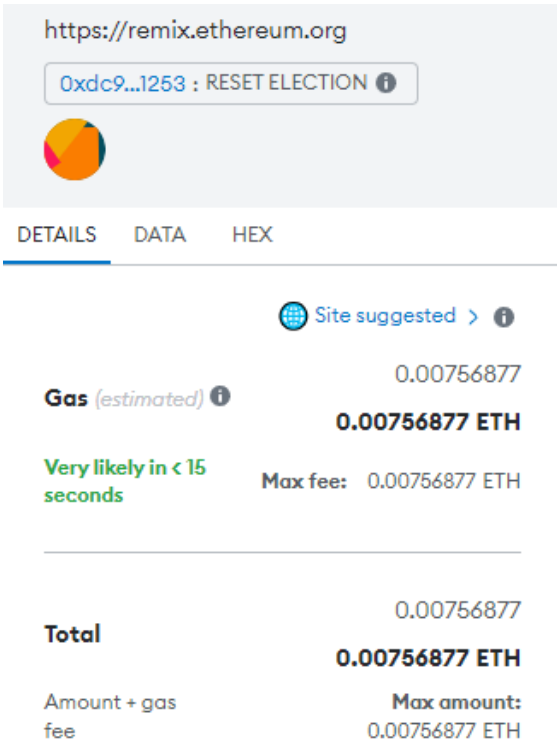

Figure 26: Reset election gas consumtpion

26 showcases the transaction to reset the election and start a new one. By calling the reset function, the smart contract is reset, clearing all previous data and allowing for a fresh election cycle.

By analyzing the gas costs for these additional transactions in the Remix IDE and MetaMask, we can estimate the gas consumption for various operations within the voting system. This estimation assists in optimizing gas usage and ensuring the efficient execution of the system on the Ethereum blockchain.

D. Casting the Vote with Digital Signature

When a voter casts their vote, it is accompanied by an ECDSA (Elliptic Curve Digital Signature Algorithm) digital signature that serves as cryptographic evidence of the vote's authenticity. The digital signature is unique to each voter and prevents unauthorized alterations or tampering with the vote. If any modification is attempted, the digital signature becomes invalid, indicating tampering has

occurred.

To ensure the integrity of the voting process, the system utilizes the ECDSA digital signature scheme. Below is the process of casting votes within the voting system:

- Vote Casting: When a voter casts their vote, they provide their voter ID, voter name, the candidate's name, and the digital signature generated using their private key.
- Signature Verification: The digital signature is verified using the ECDSA algorithm to validate the authenticity of the vote. The signature, along with the voter's public key and the hashed message (generated using the candidate's name and contract address), is used to recover the signer's address.
- Vote Recording: If the verification is successful, the vote is recorded in the smart contract as a transaction. The voter's ID is marked as voted to prevent duplicate voting.

By leveraging the ECDSA digital signature scheme, the voting system ensures that each vote is authentic, tamper-proof, and traceable back to the voter. The integration of ECDSA with the Ethereum blockchain provides an additional layer of security and trust in the voting process.

E. Significance

The developed system's significance was evident in its ability to enhance the security and privacy of the voting process. Digital signature played a crucial role in maintaining the anonymity of voters while ensuring the integrity of the cast votes. By leveraging Ethereum blockchain, the system achieved transparency, immutability, and decentralization, trust among participants. Additionally, the use of digital signature in the voting system introduces an additional layer of privacy protection and enhances the anonymity of voters, which may not be present in some previous studies.

F. Issues and Challenges

During development, several challenges were encountered, including user experience issues, integration complexities, and smart contract vulnerabilities. User experience issues were addressed through iterative design and usability testing. Integration complexities were managed by following best practices and leveraging established libraries and frameworks. Smart contract vulnerabilities were mitigated through extensive auditing and code review, ensuring robustness and security.

G. Contributions

The main contributions of Privote can be summarized as follows:

1. Development of an Ethereum-based internet voting system using digital signature, ensuring privacy, security, and trust in the voting process.

2. Implementation of key functionalities such as user registration, vote casting, verification, and tallying, leveraging smart contracts and decentralized storage.

3. Utilization of digital signature techniques to preserve voter anonymity while maintaining the integrity of the voting system.

4. Demonstration of the significance of blockchain technology in enhancing transparency and reliability in internet voting systems.

The developed system demonstrated its ability to fulfill objectives, address problems, and achieve significance in the context of an Ethereum-based internet voting system using digital signature. The encountered challenges were successfully overcome, and the system's unique features and contributions set it apart from existing references. Overall, this work contributes to the advancement of secure and trustworthy internet voting systems by leveraging blockchain technology and digital signature techniques.

VII. Conclusions

In conclusion, the paper focused on developing an Ethereum-based internet voting system using digital signature to address the problems of tampering, confidentiality, verifiability, and double spending in the voting process. The objectives were successfully achieved through the implementation of key functionalities such as user registration, vote casting, verification, and tallying, leveraging smart contracts and decentralized storage.

By utilizing digital signature, particularly ECDSA, the system ensured the privacy and anonymity of voters while maintaining the integrity and authenticity of the cast votes. The integration of the Ethereum blockchain provided transparency, immutability, and decentralization, contributing to a secure and trustworthy voting system.

Throughout the development process, various challenges were encountered, including user experience issues, integration complexities, and smart contract vulnerabilities. These challenges were effectively addressed through iterative design, usability testing, best practices in integration, and extensive auditing and code review.

This work distinguishes itself from previous references by incorporating digital signature techniques to enhance voter anonymity and by utilizing the Ethereum blockchain for transparency and decentralization. The system's significance lies in its ability to provide a secure and reliable voting platform that ensures the integrity of the voting process while protecting the privacy of voters.

In summary, the developed Ethereum-based internet voting system using digital signature successfully achieves the objectives of enhancing security, privacy, and trust in the voting process. The system's solutions address the problems of tampering, anonymity while ensuring verifiability, and trust, offering a robust and auditable platform for conducting elections. This work contributes to the advancement of secure and trustworthy internet voting systems, showcasing the potential of blockchain technology and digital signature techniques in revolutionizing the

voting landscape.

VIII. Recommendations

Based on the development and evaluation of the Ethereum-based internet voting system using digital signature, several recommendations can be made to further enhance the system and guide future research in this domain:

1. Enhance User Experience: Continuously strive to improve the user experience of the voting system. Conduct user testing and gather feedback to identify areas for improvement, such as intuitive interfaces, clear instructions, and simplified processes. User-friendly systems encourage higher participation and engagement in the voting process.

2. Scalability and Performance: As the number of participants and transactions increase, scalability and performance become critical. Explore optimization techniques and scaling solutions, such as sharding or layer-two solutions, to ensure that the system can handle a large number of voters without compromising efficiency and responsiveness.

3. Security Audits and Penetration Testing: Conduct regular security audits and penetration testing to identify and address potential vulnerabilities. This includes smart contract audits, network security assessments, and code reviews. Stay updated with the latest security best practices and actively address any identified weaknesses or risks.

4. Education and Awareness: Promote education and awareness campaigns to increase public understanding of blockchain-based voting systems and digital signature techniques. Address misconceptions and highlight the benefits of such systems in terms of transparency, privacy, and trust. This will foster trust and acceptance among stakeholders and the general public.

5. Regulatory Compliance: Stay informed about the legal and regulatory frameworks surrounding internet voting systems. Ensure that the developed system aligns with relevant laws, regulations, and guidelines related to elections,

data protection, and privacy. Collaborate with regulatory authorities and election commissions to ensure compliance and adherence to standards.

6. Collaboration and Interoperability: Encourage collaboration and interoperability among different blockchain-based voting systems. Standardization efforts and open protocols can facilitate seamless integration and information sharing, allowing for more comprehensive and inclusive voting processes.

7. Long-term Data Storage and Archiving: Develop strategies for long-term data storage and archiving of voting records on the blockchain. Consider the implications of storing sensitive voting data for extended periods and implement robust data protection measures to safeguard against unauthorized access or data loss.

8. Continuous Research and Development: As technology advances and new challenges emerge, it is crucial to foster continuous research and development in the field of blockchain-based voting systems. Explore emerging technologies, such as zero-knowledge proofs and homomorphic encryption, to further enhance privacy, security, and verifiability in the voting process.

9. By implementing these recommendations, the Ethereum-based internet voting system using digital signature can be further improved, making it more resilient, user-friendly, and trustworthy. Moreover, it will contribute to advancing the field of secure and transparent voting systems, ultimately paving the way for the widespread adoption of blockchain technology in elections.

IX. Bibliography

[1] N. Y. Commission, "Sangguning kabataan operations manual: A guide in reaffirming the role of the filipino youth in nation-building," 2017.

[2] B. Ahn, "Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting," *Sustainability*, vol. 14, no. 5, 2022.

[3] Y. Pan, X. Zhang, Y. Wang, J. Yan, S. Zhou, G. Li, and J. Bao, "Application of blockchain in carbon trading," *Energy Procedia*, vol. 158, pp. 4286–4291, 2019. Innovative Solutions for Energy Transitions.

[4] S. Vemula, R. Kovvur, and D. Marneni, "Secure e-voting system implementation using cryptdb," *SN Computer Science*, vol. 2, 05 2021.

[5] A. Benny, "Blockchain based e-voting system," *SSRN*, 2020.

[6] A. Koç, E. Yavuz, U. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," 03 2018.

[7] E. Aljarrah, "E-voting in jordan: Assessing readiness and developing a system," *Computers in Human Behavior*, vol. 63, pp. 860–867, 05 2016.

[8] R. J. D. Quiaoit, "Z-halalan: A blockchain-based internet voting system using zero knowledge proof," 2022.

[9] National Youth Commission, Jan. 15 2016.

[10] T. Ridon, "Challenge to youth: Break away from rotten system,"

[11] S. of the Philippines, "Bam urges youth to register for sk polls,"

[12] I. L. Rio, "Political involvement among the youth in barangays with lownumber of qualified voters during the 2007 sangguniang kabata-an election: Issues and concerns," 2016.

[13] L. I. Flores, R. Mendoza, J. Yap, and J. Valencia, "Advancing youth governance in the philippines: A narrative of the sangguniang kabataan and its road to reform," 02 2021.

[14] S. of the Philippines, "Sen. bam: Sk reform act sparks hope for an anti-political dynasty law," January 19, 2016.

[15] D. of Education, "Preserve the integrity of the elections, deped appeals to teachers," October 24, 2010.

[16] U. N. D. Programme, "Youth participation to sustain peace during electoral process," *Sustaining Peace during Electoral Processes (SELECT) Project*, 2023.

[17] L. R. Wislow, "Voting-machine," U.S. patent 963,105, July 5, 1910.

[18] J. P. Harris, "Data registering device," U.S. Patent 3,201,038, Aug. 17, 1965.

[19] V. V. Foundation, "Election systems sofftwares."

[20] B. A. A. Brian D. Silver and P. R. Abramson, "Who overreports voting?," *The American Political Science Review*, vol. 80, pp. 613–624, 2017.

[21] C. C. Craig Burton and S. Schneider, "vvote: Verifiable electronic voting in practice," *IEEE Security Privacy*, vol. 14, pp. 64–73, 2016.

[22] J. Göbel, P. Keeler, A. Krzesinski, and P. Taylor, "Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay," *Performance Evaluation*, vol. 104, 05 2015.

[23] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "Dvtchain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, p. 6855–6871, oct 2022.

[24] J. U, A. MJA, and S. Z, "Blockchain for electronic voting system-review and open research challenges," 2021.

[25] A. Kiayias, M. Korman, and D. Walluck, "An internet voting system supporting user privacy," in *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, pp. 165–174, 2006.

[26] R. M. Alvarez and T. E. Hall, *Point, click, and vote the future of internet voting*. Brookings Institution, 2004.

[27] W. D. Eggers, *Government 2.0 using technology to improve education, cut red tape, reduce gridlock, and enhance democracy*. Rowman amp; Littlefield Pub Inc, 2007.

[28] Y. Yao and L. Murphy, "Remote electronic voting systems: An exploration of voters' perceptions and intention to use," *EJIS*, vol. 16, pp. 106–120, 04 2007.

[29] K. Butterfield and X. Zou, "Analysis and implementation of internet based remote voting," in *2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 714–719, 2014.

[30] W. Drechsler and Ü. Madise, *Electronic Voting in Estonia*, pp. 97–108. London: Palgrave Macmillan UK, 2004.

[31] SCYTL, "About scytl - secure online voting and electoral innovation," Apr 2023.

[32] SMARTMATIC, "Our history - smartmatic."

[33] A. Al-Ameen and S. Talab, "The technical feasibility and security of e-voting," *International Arab Journal of Information Technology*, vol. 10, 07 2013.

[34] L. Carter and R. Campbell, "The Impact of Trust and Relative Advantage on Internet Voting Diffusion," *Journal of theoretical and applied electronic commerce research*, vol. 6, pp. 28 – 42, 12 2011.

[35] G. Schryen and E. Rich, "Security in large-scale internet elections: A retrospective analysis of elections in estonia, the netherlands, and switzerland," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 729–744, 2009.

[36] H. Hussien and H. Aboelnaga, "Design of a secured e-voting system," in *2013 International Conference on Computer Applications Technology (ICCAT)*, pp. 1–5, 2013.

[37] S. Hof, "E-voting and biometric systems?," in *Electronic voting in Europe - Technology, law, politics and society, workshop of the ESF TED programme together with GI and OCG* (A. Prosser and R. Krimmer, eds.), (Bonn), pp. 63–72, Gesellschaft für Informatik e.V., 2004.

[38] Q. R. S. Fitni and K. Ramli, "Implementation of ensemble learning and feature selection for performance improvements in anomaly-based intrusion detection systems," in *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, pp. 118–124, 2020.

[39] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *ArXiv*, 2019.

[40] R. Chatterjee and R. Chatterjee, "An overview of the emerging technology: Blockchain," 10 2017.

[41] A. Warner, "24 counties to offer mobile voting option for military personnel overseas," 2018.

[42] A. Ullah, S. Siddiquee, M. A. Hossain, and S. Ray, "An ethereum blockchain-based technology for data security of regulated electricity market," *Inventions*, vol. 5, pp. 1–14, 11 2020.

[43] E. Foundation, "Solidity."

[44] M. Li, "The advance of ethereum digital signature," *Highlights in Science, Engineering and Technology*, vol. 39, pp. 1159–1163, 04 2023.

[45] U. Patel, A. Patel, F. Suthar, and A. Patel, "The study of digital signature authentication process," vol. 1, pp. 38–43, 10 2019.

[46] I. Muchtadi-Alamsyah, M. Imdad, and S. Sutikno, "Group signature based ethereum transaction," *International Journal on Electrical Engineering and Informatics*, vol. 12, pp. 19–32, 03 2020.

[47] H. Yi, "Securing e-voting based on blockchain in p2p network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, 05 2019.

[48] Official Gazette of the Republic of the Philippines, "Local Government Code of 1991," *Official Gazette of the Republic of the Philippines*, p. 23, 1991.

[49] National Economic and Development Authority, "Ensuring People-Centered, Clean, and Efficient Governance," *Philippine Development Plan 2017-2022*, p. 55, 2017.

[50] Deparment of Interior and Local Government, National Youth Commission, "Joint Memorandum Circular No. 2017-01," p. 1, June 23, 2017.

[51] M. Lihgawon, "Kiangan sk provides sports equipment to sitios."

[52] N. C. M. for Free Election, "Namfrel position supporting the holding of barangay and sangguniang kabataan polls as scheduled on may 14, 2018,"

[53] C. P. Staff, "9 arrested for vote buying, more reports being validated — pnp,"

[54] P. A. V. Roxas, "Elderly man with disability fails to vote in bulacan,"

[55] G. Schryen, "Security aspects of internet voting," *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, 2004.

[56] K. Marky, M.-L. Zollinger, P. Roenne, P. Y. Ryan, T. Grube, and K. Kunze, "Investigating usability and user experience of individually verifiable internet voting schemes," *ACM Transactions on Computer-Human Interaction*, vol. 28, no. 5, p. 1–36, 2021.

[57] N. Kshetri and J. Voas, "Blockchain enabled voting," *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, 2022.

[58] H. Sheth and J. Dattani, "Overview of blockchain technology," *Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146*, Apr. 2019.

[59] P. M. Dhulavvagol, V. H. Bhajantri, and S. G. Totad, "Blockchain ethereum clients performance analysis considering e-voting application," *Procedia Computer Science*, vol. 167, pp. 2506–2515, 2020. International Conference on Computational Intelligence and Data Science.

X. Appendix

A. Source Code

```
//SPDX-License-Identifier: UNLICENSED
pragma solidity >=0.4.22 <0.9.0;

contract Election {
    mapping(address => bool) admins;
    string name; // name of the election. example: for president
    string description; // description of the election
    bool started;
    bool ended;

    constructor() {
        admins[msg.sender] = true;
        started = false;
        ended = false;
    }

    modifier onlyAdmin() {
        //require(admins[msg.sender] == true, "Only Admin");
        _;
    }

    function addAdmin(address _address) public onlyAdmin {
        admins[_address] = true;
    }

    /*****************************CANDIDATES SECTION*****************************/

    struct Candidate {
        string name;
        string info;
        bool exists;
    }
    mapping(string => Candidate) public candidates;
    string[] candidateNames;

    function addCandidate(string memory _candidateName, string memory _info)
        public
        onlyAdmin
    {
        Candidate memory newCandidate = Candidate({
            name: _candidateName,
            info: _info,
            exists: true
        });

        candidates[_candidateName] = newCandidate;
        candidateNames.push(_candidateName);
    }

    function getCandidates() public view returns (string[] memory) {
        return candidateNames;
    }

    function getCandidateInfo(string memory _candidateName) public view returns (string memory) {
    require(candidates[_candidateName].exists, "No such candidate");

    return candidates[_candidateName].info;
}


    /*****************************CANDIDATES SECTION*****************************/

    /*****************************ELECTION SECTION*****************************/

    function setElectionDetails(string memory _name, string memory _description)
        public
        onlyAdmin
    {
        name = _name;
        description = _description;
        started = true;
        ended = false;
    }

    function getElectionName() public view returns (string memory) {
        return name;
    }

    function getElectionDescription() public view returns (string memory) {
        return description;
    }

    function getTotalCandidates() public view returns (uint256) {
        return candidateNames.length;
    }

    /*****************************ELECTION SECTION*****************************/
```

```
/*****************************VOTER SECTION*****************************/

struct Vote {
    string voterId;
    string voterName;
    string candidate;
    bytes voterSignature;
}
Vote[] votes;
mapping(string => bool) public voterIds;
string[] votersArray;
string[] chairpersonArray;
string[] memberArray;

function vote(
    string memory _voterId,
    string memory _voterName,
    string memory _candidateName,
    bytes memory _signature
) public {
    require(started == true && ended == false);
    require(candidates[_candidateName].exists, "No such candidate");
    // require(!voterIds[_voterId], "Already Voted");

    Vote memory newVote = Vote({
        voterSignature: _signature,
        voterId: _voterId,
        voterName: _voterName,
        candidate: _candidateName
    });

    bool checkVoted = verify(msg.sender, address(this) , _candidateName, _signature);
    require(checkVoted == true, "Verify signature failed");

    votes.push(newVote);
    voterIds[_voterId] = true;
    votersArray.push(_voterId);
}

function getVoters() public view returns (string[] memory) {
    return votersArray;
}

function getChairpersonVoters() public view returns (string[] memory) {
    return chairpersonArray;
}

function getMemberVoters() public view returns (string[] memory) {
    return memberArray;
}

/*****************************VOTER SECTION*****************************/

function getVotes() public view onlyAdmin returns (Vote[] memory) {
    return votes;
}

function getTotalVoter() public view returns (uint256) {
    return votersArray.length;
}

function endElection() public onlyAdmin {
    require(started == true && ended == false);

    started = true;
    ended = true;
}

function resetElection() public onlyAdmin {
    require(started == true && ended == true);

    for (uint32 i = 0; i < candidateNames.length; i++) {
        delete candidates[candidateNames[i]];
    }

    for (uint32 i = 0; i < votersArray.length; i++) {
        delete voterIds[votersArray[i]];
    }

    name = "";
    description = "";

    delete votes;
    delete candidateNames;
    delete votersArray;

    started = false;
    ended = false;
}

function getStatus() public view returns (string memory) {
    if (started == true && ended == true) {
        return "finished";
    }

    if (started == true && ended == false) {
        return "running";
    }
```

```
        return "not-started";
    }

    /********************** PROCESS VERIFY SIGNATURE ************************/
    function getMessageHash(
        address _to,
        string memory _candidateName
    ) public pure returns (bytes32) {
        return keccak256(abi.encodePacked(_to, _candidateName));
    }


    function getEthSignedMessageHash(bytes32 _messageHash) public pure returns (bytes32) {
        return keccak256(abi.encodePacked("\x19Ethereum Signed Message:\n32", _messageHash));
    }


    function verify(address _signer, address _to, string memory _candidateName, bytes memory signature) public
        bytes32 messageHash = getMessageHash(_to, _candidateName);
        bytes32 ethSignedMessageHash = getEthSignedMessageHash(messageHash);

        return recoverSigner(ethSignedMessageHash, signature) == _signer;
    }

    function recoverSigner(bytes32 _ethSignedMessageHash, bytes memory _signature) public pure returns (address
        (bytes32 r, bytes32 s, uint8 v) = splitSignature(_signature);
        return ecrecover(_ethSignedMessageHash, v, r, s);
    }

    function splitSignature( bytes memory sig ) public pure returns (bytes32 r, bytes32 s, uint8 v) {
        require(sig.length == 65, "invalid signature length");
        assembly {
            // first 32 bytes, after the length prefix
            r := mload(add(sig, 32))
            // second 32 bytes
            s := mload(add(sig, 64))
            // final byte (first byte of the next 32 bytes)
            v := byte(0, mload(add(sig, 96)))
        }
    }

    /********************** FINISH SIGNATURE **********************/
}
```

XI. Acknowledgment

I would like to express my sincere gratitude to my thesis adviser, Mr. Marbert John C. Marasigan, for their invaluable guidance, expertise, and unwavering support throughout the entire research journey. Their profound knowledge, insightful feedback, and constructive criticism have played a crucial role in shaping the direction and outcomes of this thesis. Their dedication to academic excellence, patience, and commitment to my growth as a researcher have been instrumental in the successful completion of this project. I am truly grateful for their mentorship and the invaluable lessons I have learned under their guidance.

I would also like to extend my heartfelt appreciation to the Department of Science and Technology - Science Education Institute (DOST-SEI) for their financial support in the form of the thesis allowance. This support greatly facilitated the completion of this project by alleviating financial constraints and enabling me to dedicate more time and resources to the research process.

Furthermore, I would like to express my deepest gratitude to Kush, Kaye, Ada, and all of Sonder for their unwavering support, understanding, and encouragement throughout this endeavor. Their presence and constant support kept me grounded and motivated during the challenges encountered along the research journey. Their belief in me and their willingness to lend a helping hand whenever needed were invaluable, and I am forever grateful for their presence in my life.

To everyone mentioned above and to those who may not be explicitly named, but have contributed in their own unique ways, I offer my sincerest appreciation. Your support, encouragement, and love have been instrumental in the successful completion of this project.

Thank you all from the bottom of my heart.