



INSTITUTE OF ENGINEERING & MANAGEMENT

**SALT LAKE,
KOLKATA 700091**

DECENTRALIZED E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

SUBMITTED BY

Faizan Shakeel

*Thesis submitted for the partial fulfillment of
the requirements for the degree
of*
BACHELOR OF TECHNOLOGY



**COMPUTER SCIENCE AND ENGINEERING (IOTCSBT)
DEPARTMENT
INSTITUTE OF ENGINEERING & MANAGEMENT
MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY,
WEST BENGAL
2024**

DECENTRALIZED E-VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY



A thesis submitted by

Faizan Shakeel (Enrollment No-22021002017005)

Supervisor

Prof. Dr. Soumadip Biswas

Submitted for the partial fulfillment of the requirements for the degree of
Bachelor of Computer Science and Engineering (IOTCSBT)

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(IOTCSBT) INSTITUTE OF ENGINEERING & MANAGEMENT,
KOLKATA**

April 2024

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



CERTIFICATE

This is to certify that **“DECENTRALIZED E-VOTING SYSTEM USING BLOCKCHAIN TCHNLOGY”** is submitted in partial fulfillment of the requirement for the degree of Bachelor of Computer Science & Engineering by the following students:

Faizan Shakeel

(Enroll No-22021002017005)

Supervisor1
Prof. Dr. Soumadip Biswas

Head of the Department

Principal

Thesis Approval/ Dissertation Approval/Project Report Approval for B.Tech.

This thesis/dissertation/project report entitled **Decentralized E-voting System Using Blockchain** Technology by **Faizan Shakeel** is/are approved for the degree of Bachelor of Computer Science & Engineering.

Examiner(s)

1.....

2.....

Date:

Place:

ACKNOWLEDGEMENT

I wish to express my heartfelt gratitude to the all the people who have played a crucial role in the research for this project. Without their active cooperation the preparation of this project could not have been completed within the specified time limit.

I am thankful to my project guide **Prof. Dr. Soumadip Biswas** who supported me throughout this project with utmost cooperation and patience and for helping me in doing this Project.

I am also thankful to our respected Head of Department, **Prof. Dr. Moutushi Singh**, for motivating me to complete this project with complete focus and attention.

I am thankful to my department and all my teachers for the help and guidance provided for this work.

I extend my sincere thanks to my institute, the Institute of Engineering and Management, Kolkata for the opportunity provided to me for the betterment of my academics.

.....
(Signatures)

Faizan Shakeel (22021002017005)

Date:

TABLE OF CONTENTS

Article No.	Content	Page No
1.	INTRODUCTION.....	3
1.1	OVERVIEW.....	3
1.2	BACKGROUND.....	4
1.2.1	BLOCKCHAIN TECHNOLOGY	4
1.2.2	BLOCKCHAIN APPLICATIONS ACROSS DOMAINS.....	5
1.3	PROBLEM STATEMENT	5
1.3.1	KEY ISSUES.....	6
1.4	AIMS AND OBJECTIVES.....	6
1.5	METHODOLOGY.....	6
2.	LITERATURE REVIEW/BACK GROUND/ RESEARCH GAP ANALYSIS.....	9
2.1	RELATED WORK	9
2.2	IMPLEMENTATIONS OF BLOCKCHAIN BASED E-VOTING SYSTEMS	10
2.3	RESEARCH GAP AND ANALYSIS.....	11
3.	MATERIAL AND METHODS.....	12
3.1	SMART CONTRACT	12
3.1.1	VOTER REGISTRATION	12
3.1.2	VOTING CLIENT	13
3.2	BLOCKCHAIN NETWORK.....	13
3.3	DATA STORAGE AND RETRIEVAL	13
3.4	SECURITY AND PRIVACY.....	14
4.	SYSTEM REQUIREMENTS AND SPECIFICATION.....	15
4.1	SYSTEM REQUIREMENT SPECIFICATION.....	15
4.2	SPECIFIC REQUIREMENT	15
4.3	HARDWARE SPECIFICATION	15
4.4	SOFTWARE REQUIREMENTS	15
4.5	FUNCTIONAL REQUIREMENTS	16
4.6	NON- FUNCTIONAL REQUIREMENTS	16
4.7	PERFORMANCE REQUIREMENT.....	16

5. RESULTS AND ANALYSIS	17
5.1 BLOCKCHAIN PLATFORMS	17
5.2 CONSENSUS ALGORITHM	18
5.3 SECURITY AND PRIVACY TECHNIQUES.....	19
5.4 AUTHENTICATION AND IDENTITY VERIFICATION TECHNIQUES	21
5.5 ANALYSIS OF RESULTS.....	22
6. DISCUSSION AND CONCLUSION	23
6.1 DISCUSSION	23
6.2 CONCLUSION.....	25
7. SUMMARY, PUBLICATIONS AND FUTURE WORK	26
7.1 SUMMARY	26
7.2 FUTURE WORK	26
APPENDIX-A: FRONT COVER AND EDGE	27
REFERENCES	28

ABSTRACT

The integration of technology has become crucial in meeting diverse human needs. However, this surge in technological reliance has also brought forth new challenges, especially in democratic processes where trust in governments is dwindling. Elections play a pivotal role in modern democracies, determining leadership and the course of nations or organizations.

Yet, a substantial segment of society globally lacks trust in their electoral systems, posing a grave threat to democratic ideals. Major democracies such as India and the United States grapple with flaws like vote rigging, EVM hacking, election manipulation, and booth capturing.

The rise of blockchain technology presents a potential remedy to these challenges. Blockchain, renowned for its decentralization and transparency, holds promise in revolutionizing various industries. Expanding e-voting systems onto blockchain platforms could mitigate existing electoral system woes.

Blockchain's immutability, transparency, and security make it ideal for developing safer, cheaper, and more secure e-voting systems. Smart contracts, integral to blockchain, automate and enforce voting process rules, enhancing integrity and reliability. Ethereum, a widely adopted platform supporting smart contracts, stands out for such developments.

A robust e-voting system on blockchain must prioritize security, transparency, and voter privacy. The implementation and testing of an e-voting application as a smart contract on Ethereum using Solidity signifies progress towards these goals.

Leveraging blockchain for e-voting systems has the potential to bridge the trust deficit in electoral processes, fostering more secure, transparent, and credible democratic practices. Continued research, development, and adoption of blockchain-based solutions are imperative to fortify democratic values and ensure electoral system integrity worldwide.

.

Chapter-1

INTRODUCTION

1.1 OVERVIEW

Will of the people is a well-respected phenomenon for representation of opinion information of electoral bodies. These electoral bodies vary from the college unions to the parliaments. Over the years, 'vote 'has emerged as a tool for representing the will of the people when a selection is to be made among the available choices. The voting tool has helped improve the trust of people over the selection they make by a vote of majority. This has certainly helped in democratization of the voting process and the value of voting system to elect the parliaments and governments. In 2018, there are 167 countries out of little over 200 who have some kind of democracy; full, flawed, or hybrid etc. Since the trust of people is increasing in democracies it is important that they don't lose their trust in voting and voting system. By virtue of the emerging trust on the democratic institutions, the voting system emerged as a platform to help people to elect their representatives, who consequently form the governments. The power of representation empowers the people with a trust that the government shall take care of the national security, national issues like health and education policies, international relations, and taxation for the benefit of the people.

Blockchain technology has been recognized as a potential solution for secure and transparent e-voting systems. By leveraging the decentralization, immutability, and transparency of blockchain technology, e-voting systems can prevent fraud and manipulation, improve voter anonymity, and increase trust in the electoral process. Moreover, blockchain-based e-voting systems can reduce the cost and time associated with traditional voting systems.

Traditional voting mechanisms commonly rely on centralized entities, which can give the opportunity for vulnerabilities such as the tampering of results or electoral fraud. The decentralized and immutable features inherent in blockchain technology offer a promising solution to the vulnerabilities related to traditional and other e-voting approaches. Blockchain technology has the ability to create a tamper-proof and transparent platform for conducting e-voting. Blockchain-based e-voting systems provide secure, verifiable, and auditable voting procedures through the integration of cryptographic techniques and consensus protocols.

The growing interest in blockchain-based e-voting systems indicates the importance of a comprehensive and systematic evaluation of the current knowledge in this domain. One of the aims of this review is to identify the main benefits of e-voting systems based on blockchain technology through an in-depth review of the previous research. These benefits include heightened security, transparency, decentralization, and privacy. Additionally, we intend to identify the challenges and limitations that come with these systems, which include privacy and security concerns, scalability issues, and technical limitations.

1.2 BACKGROUND

1.2.1 BLOCKCHAIN TECHNOLOGY

A blockchain is a decentralized and distributed ledger made of a sequence of blocks linked to each other. Each block contains a list of transactions, and each transaction is a record of an event or action. The block header, which includes the previous block hash, timestamp, nonce, and Merkle root, identifies each block. The previous block hash links the current block to the previous one. The timestamp verifies the data in the block and assigns a time or date of creation for digital documents. The nonce, a number used only once, is a central part of the proof of work in the block. The Merkle root, a type of data structure frame for different blocks of data, stores all the transactions in a block by producing a digital fingerprint of the entire set of transactions. This structure provides assurance that once data are recorded in a block, they cannot be altered in the future without modifying all subsequently recorded blocks, making blockchain transactions immutable and secure.

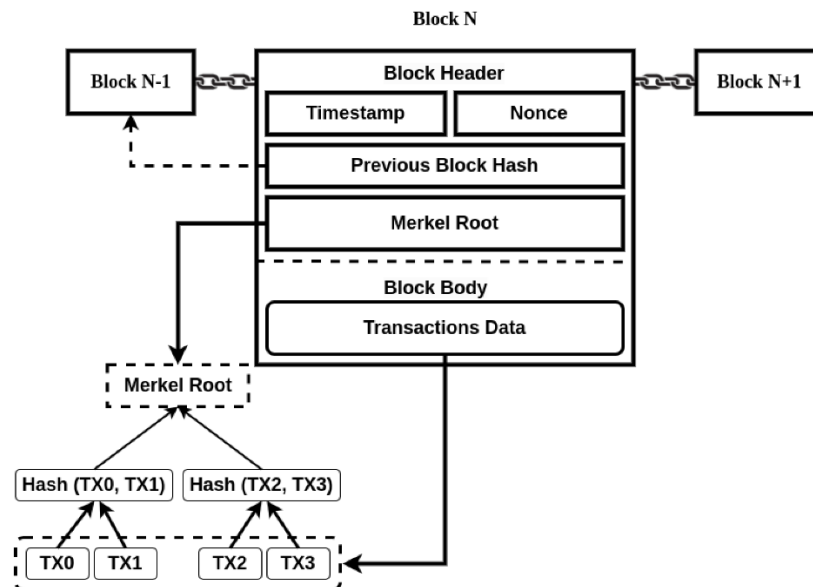


Figure 1. The blockchain structure

1.2.2 BLOCKCHAIN APPLICATIONS ACROSS DOMAINS

Blockchain technology has emerged as a revolutionary trend across various domains, and whereas blockchain technology application in e-voting systems attracts interest in enhancing electoral integrity and transparency, it is equally valuable in other domains, each with distinct requirements and objectives. This section aims to provide a comparison and analysis of blockchain applications in different domains such as healthcare, financial services, supply chain management, cloud computing, education, and IoT (Internet of Things) [4], highlighting their parallels and contrasts with their use in e-voting systems.

1.3 PROBLEM STATEMENT

As India is the second most populated country with 63.6% adults (who have the right to cast their vote), but the percentage of people voted is approximately 61% to 74%, ie only 18,27,936 has casted their vote out of 138 crore (2018 election). Among all of the reason for not participating in voting campaign, the most important one is the traditional method of voting is not convenient like, transportation is the main reason for not casting their vote.

The existing centralized voting systems are plagued by issues such as security vulnerabilities, lack of transparency, and restricted accessibility. To address these challenges, there is a need for the development of a decentralized voting system leveraging blockchain technology.

1.3.1 KEY ISSUES

- Centralized voting systems are vulnerable to hacking, fraud, and tampering with election results.
- Lack of transparency in the counting and recording of votes erodes public trust in the electoral process.
- Physical presence requirements in traditional voting systems create barriers for certain demographics, such as remote or disabled individuals.
- Traditional voting systems may not adequately address data privacy concerns related to the storage and handling of sensitive voter information.

1.4 AIMS AND OBJECTIVES

- Develop a decentralized system that employs cryptographic techniques to ensure the security and integrity of the voting process.
- Utilize blockchain technology to create a transparent and tamper-resistant ledger for

recording and verifying votes.

- Design an inclusive system that allows citizens to vote securely from any location, promoting accessibility for all eligible voters.
- Implement privacy-focused features to protect voter information while maintaining the anonymity of individual votes.
- Develop a user-friendly interface that enables seamless interaction with the decentralized voting system, ensuring a positive user experience.

1.5 METHODOLOGY

1. Initialization and Smart Contract Deployment:

The foundation of the system is laid with the deployment of a Solidity smart contract on a blockchain network. This contract, representing the rules and logic of the voting system, is instantiated with an initial state wherein voting is closed, and only the contract owner has the authority to make changes.

2. Candidate Registration:

The system allows administrators, recognized by the contract owner status, to register candidates through the "addCandidate" function. This function captures essential candidate details, such as name, age, and a unique identifier, ensuring a transparent and auditable candidate registry.

3. Allowlist Management:

To uphold the security of the voting process, an allowlist is implemented through the "addToAllowlist" function. This mechanism ensures that only authorized individuals, whose addresses are on the allowlist, can participate in the election. Administrators have the privilege to manage this list, reinforcing the system's commitment to secure and accessible voting.

4. Voting Period Commencement:

The voting process is initiated by the contract owner through the "startVote" function. This action opens the door for registered voters to cast their ballots, signaling the beginning of the democratic exercise.

5. Voter Participation:

Voters, utilizing their web3-enabled wallets, connect to the system by clicking the

"Connect Wallet" button on the user interface. This action authorizes them to participate in the voting process.

6. Casting Votes:

Once connected, voters access the candidate list through a dropdown menu populated by the "getCandidates" function. They can select their preferred candidate and cast their vote using the "vote" function. The system ensures the uniqueness of each vote, preventing multiple votes from a single address.

7. Real-time Vote Monitoring:

Throughout the voting period, the system provides real-time insights into the election's status through the "getCurrentVoteStatus" function. Users can access information on candidate popularity and overall voting trends, fostering transparency and confidence in the electoral process.

8. Vote Conclusion:

The contract owner, holding exclusive privileges, concludes the voting period using the "closeVote" function. This action seals the fate of the election, signaling the end of the voting phase.

9. Winner Determination:

With the voting phase concluded, users can employ the "getWinner" function to determine the victorious candidate. The system iterates through candidate votes, identifying the one with the highest count and declaring them the winner.

10. Results and Analysis:

The "results Section" of the user interface displays comprehensive information, including the winning candidate and overall vote status. Users gain insights into the election's outcome, reinforcing the system's commitment to transparency and verifiability.

Chapter-2

LITERATURE REVIEW

2.1 RELATED WORK

FREYA SHEER HARDWICK et. al[1] The author uses, the smart contracts and the PKIs for the verification and digital signatures for the first step of e-voting which is highly reliable and effective, also explains the e-voting using decentralized e-voting system with the voter privacy rights. The protocol has been designed to adhere to fundamental e-voting properties as well as degree of decentralization and allow the voter to change or update their vote.

Limitations: Implementing the changing or updating the vote, may leads to the less productive system, which increases the complexity of the algorithm, the effects the ongoing process of e-voting statistics.

ALI KAAN KOC et. al[2] Author clearly put forwards the idea of using Ethereum blockchain technique in the e- voting systems, this paper uses smart contracts for the verification and digital signatures of the blocks, which is safer, cheaper, more secure, more transparent and easier to use e-voting systems. The idea of using Ethereum blockchain and smart contracts for an e-voting is itself an high-minded, if implementation is successful, then e-voting will be secure enough to process all the voting through e-voting systems.

Limitations: Using smart contracts and Ethereum alone takes up to more storage.

NIR KSHETRI et. al[3] Authors explain the requirements and need of using blockchain effectively in the e-voting process, and provides a detailed survey for the e-voting technology in a certain region. It mainly put forwards the challenges faced before implementing blockchain based e-voting and the challenges to overcome by implementing blockchain technology in the e-voting.

Limitations: Author explains only the challenges to be faced by implementing blockchain technology, in e-voting but doesn't provide the solution for those issues.

SHEKHAR MISHRA et. al[4] In this paper, the author institutes about various authentication types like using biometric finger print using Aadhar card authentication, which enables the user to access the e-voting system using biometric finger print and verifies the Aadhar number for further processing of voting system.

Limitations: With only the biometric system with fingerprint doesn't provide enough security to the user.

Instead of only using only the fingerprint authentication, instead 3-step authentication and face recognition can be used to provide more security.

AMNA QUERESHI et. al[5] In this paper "Secure and Electronic polling system", the authors AMNA QURESHI, DAVID MEGÍAS, HELENA RIFA-POUS described Se-VEP, an e-polling system enabled by Internet which provides and protects the voter's integrity, security, voters unique details, poll integrity, third party breaching, prevention of double voting, fairness in election, and coercion resistance, and preventing devices with virus which change the users decision in voting and giving false results which leads to lot of problems.

RIFA HANIFATUNISA et. al[6] Author insinuates about, whole blockchain process and how it works in the process of e- voting, and explains how the hashing and Elliptic curve digital signature algorithm, provides the same amount of security as DSA but with smaller key length, allowing for faster calculations. This algorithm is a development of generalized digital signature algorithm using ECC algorithm in the digital signature generation process and its verification.

Limitations: Using Elliptic curve digital signature provides relatable security, with smaller storage and faster calculations.

2.2 IMPLEMENTATIONS OF BLOCKCHAIN-BASED E-VOTING SYSTEMS

Luxoft[1]: Luxoft Holding Inc., a global IT service provider of technology solutions, is developing an e-voting infrastructure that will enable the world's first consultative vote on blockchain in Zug, Switzerland. Hyperledger Fabric was used to create an authorized blockchain that included a network, applications, and algorithms. In order to allow voters to cast their ballots, Zug's digital ID registration app based on Ethereum was authorized through uPort. Luxoft announces its intention to open source this technology and creates a Government Alliance Blockchain to encourage blockchain use in public institutions [5].

Votem[2]: A company specializing in election management, its main product is the CastIron platform. This platform is built on blockchain technology and offers several distinctive features, including a distributed database, immutability, permission-based access, and an audit trail. Votem has successfully handled over 13 million voters, serving both government elections and

various associations in the United States and around the world. Notably, their track record boasts zero instances of fraud, compromise, attacks, or hacking, highlighting the security and reliability of their system [6].

Voatz[3]: A blockchain-based mobile voting tool that was launched in 2018 in West Virginia for overseas military voters participating in the 2018 midterm elections in the United States. Voatz includes biometric validation, such as fingerprints or retinal scans, so that voters validate their applicants and themselves on the application. A recent study found Voatz has major security flaws that allow attackers to monitor votes and edit or block ballots in large amounts [7].

POLYAS[4]: In the summer of 1996, Finland held the first POLYAS online election, with 30,000 voters participating in three languages. The company uses blockchain technology to offer an electronic voting system to the public and private sectors. Germany's Federal Office for Information Security granted the first online election certification in 2016. The online voting system satisfies anonymity, accuracy, singularity, verifiability, and auditability. In Europe and the USA, several important companies employ POLYAS to manage their electronic voting systems [8].

Polys[5]: An online voting system that increases confidence in the voting process and results. Because it is based on blockchain technology, it is secure and transparent. Both the voting procedure and the results are immutable. Transparent cryptographic techniques are employed on the top of the blockchain to protect voter anonymity. Voters can check at any moment to ensure that their vote is valid and unmodified [9].

DecentraVote[6]: A blockchain-based solution for virtual meetings was originally developed by a team at the iteratec location in Vienna. DecentraVote uses a public Ethereum network based on Proof of Authority consensus with permissioned validator nodes. The smart contract constructed a Merkle tree of all voting rights on-chain, and the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) generated a proof for every voting right off-chain. DecentraVote does not address national political elections [10].

2.3 RESEARCH GAP AND ANALYSIS

Our systematic analysis of Blockchain-based e-voting systems is guided by identified gaps in the current literature and specific objectives we aim to achieve. Despite ongoing research in this domain, existing studies often focus on the limitations of blockchain-based e-voting, lacking a comprehensive comparison with traditional and electronic voting systems in terms of benefits

and challenges. The primary objectives of this systematic analysis are therefore:

1. To conduct a comprehensive comparison of blockchain-based e-voting systems against traditional and e-voting systems, focusing on understanding their relative benefits and challenges.
2. To review and analyze the concrete implementation techniques of blockchain in e-voting systems, identifying how they address existing challenges.
3. To provide the potential implications of blockchain-based e-voting systems for addressing existing challenges in the blockchain-based e-voting systems.
4. To establish an up-to-date roadmap for future research, emphasizing areas that require further investigation in the rapidly evolving landscape of blockchain-based e-voting.

Chapter-3

MATERIAL AND METHODS

The proposed decentralized e-voting system leverages blockchain technology to provide a secure, transparent, and accessible platform for conducting elections. The system architecture consists of the following key components:

3.1 SMART CONTRACT

To provide easy access to students for thesis formatting, the text formatting styles are predefined which can be selected from the style section.

- The core of the system is a smart contract written in Solidity, a contract-oriented programming language for the Ethereum blockchain.
- The smart contract encapsulates the rules and logic of the voting process, ensuring transparency and immutability.
- Key functionalities of the smart contract include:
 - Candidate registration: Allows authorized administrators to add candidates to the election, capturing details such as name, age, and a unique identifier.
 - Allowlist management: Maintains a list of authorized voter addresses, ensuring that only eligible individuals can participate in the voting process.
 - Voting period management: Provides functions for the contract owner (administrator) to start and close the voting period.
 - Vote casting: Enables authorized voters to cast their votes for their preferred candidates through a secure and transparent process.
 - Winner determination: Implements the logic to determine the winning candidate based on the highest number of votes received.

3.1.1 VOTER REGISTRATION

- A secure and reliable process for registering eligible voters is necessary to maintain the integrity of the voting system.
- Voter registration can involve verifying identities through personal identification documents, biometric data, or other secure methods.
- Registered voters' addresses are added to the allowlist maintained by the smart contract, granting them the right to participate in the election.

3.1.2 VOTING CLIENT

- A user-friendly interface, such as a web application or a mobile app, is developed to facilitate interaction with the e-voting system.
- The voting client connects to the user's web3-enabled wallet (e.g., MetaMask) for authentication and transaction signing.
- Through the voting client, users can:
 - Connect their wallets to the system.
 - View the list of registered candidates.
 - Cast their votes for their preferred candidates.
 - Monitor the real-time voting status and results.

3.2 BLOCKCHAIN NETWORK

- The smart contract is deployed on a blockchain network, such as the Ethereum network.
- The choice of the Ethereum network is motivated by its widespread adoption, security features, and support for smart contracts.
- Initially, the smart contract can be deployed on a test network (e.g., Goerli Ethereum Testnet) for development and testing purposes.
- Once thoroughly tested, the contract can be deployed on the main Ethereum network for production use.

3.3 DATA STORAGE AND RETRIEVAL

- The blockchain serves as the immutable and transparent ledger for storing and retrieving

voting-related data, such as candidate information, vote counts, and election results.

- Private documents or sensitive information related to candidates or voters can be stored on a decentralized storage platform like IPFS (InterPlanetary File System) for added security and accessibility.

3.4 SECURITY AND PRIVACY

- Cryptographic techniques, such as digital signatures and hashing algorithms, are employed to ensure data integrity and secure communication between the voting client and the blockchain network.
- Voter privacy is maintained by separating the voter's identity from their vote, ensuring anonymity while preserving the integrity of the voting process.
- Potential threats, such as 51% attacks or Sybil attacks, are mitigated through appropriate security measures and consensus mechanisms implemented by the underlying blockchain network.

Chapter-4

SYSTEM REQUIREMENTS AND SPECIFICICATION

4.1 SYSTEM REQUIREMENT SPECIFICATION

A Software Requirements Specification (SRS) is a document that describes the nature of a project, software or application. In simple words, SRS document is a manual of a project provided it is prepared before you kick-start a project/application. This document is primarily prepared for a project, software or any kind of application.

4.2 SPECIFIC REQUIREMENT

Specific Requirements describes the external interface requirements, logical database requirements etc.

In this system following are the specific requirements:

- Merkel tools
- Block mining
- Web3 Enabled Wallet(i.e Metamask, Trust Wallet)
- Remix IDE
- Blockchain Explorer (<https://goerli.etherscan.io/>)
- Testnet ETHEREUM

4.3 HARDWARE SPECIFICATION

Processor	:	intel i3 or above
Ram	:	4GB
Hard Disk	:	16GB

4.4 SOFTWARE REQUIREMNTS

Operating System	:	Windows, Mac, Android
Backend	:	Solidity
Framework	:	Blockchain
Storage	:	IPFS

Front End : HTML, CSS, JavaScript

Other Requirements: Web3 Enabled Browser

4.5 FUNCTIONAL REQUIREMENTS

Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality.

In this system following are the functional requirements: -

- Voter's initial (biometric, identification) details have to be registered priorly.
- The details of the voter must be encrypted using smart contracts and blocks.
- The user has to determine the preferred political party and cast his/her vote accordingly.
- The application shows the real time results of the polling with show vote count option.

4.6 NON-FUNCTIONAL REQUIREMENTS

Non-functional requirements are the requirements which are not directly concerned with the specific function delivered by the system. They specify the criteria that can be used to judge the operation of a system rather than specific behaviors. They may relate to emergent system properties such as reliability, response time and store occupancy.

The non-functional requirements are:

- The project is not consuming more space and the processing is done quickly.
- Portable: the system can be used for all the operating system which support python

4.7 PERFORMANCE REQUIREMENT

These are the requirements which define how well the software system accomplishes certain functions under specific conditions.

Chapter-5

RESULTS AND ANALYSIS

E-voting systems based on blockchains use a variety of concepts and technologies to enable secure and trustworthy elections. Blockchain frameworks like Ethereum and Hyperledger Fabric, consensus algorithms like Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance, and privacy-enhancing techniques like homomorphic encryption and zero-knowledge proofs are among these technologies. Furthermore, authentication mechanisms such as biometric verification and identity management systems are critical in confirming voter legitimacy and maintaining the voting system's integrity.

In this section, we present a technology summary in five broader categories:

- Blockchain platforms
- Consensus algorithms
- Security and privacy techniques
- Authentication and identity verification techniques
- Analysis of Results

5.1 BLOCKCHAIN PLATFORMS

The blockchain frameworks and technologies domain includes a variety of platforms and tools used in the design and implementation of blockchain-based systems. Blockchain frameworks such as Ethereum, Hyperledger Fabric, Bitcoin, and Multichain provide the foundation required for developers to create decentralized apps.

Figure 2 includes a range of widely used blockchain frameworks, including the proposed blockchain e-voting systems context. In all of the frameworks mentioned, Ethereum is the most popular choice, as evidenced by the 34.91% portion of utilized frameworks. Although particular papers mentioned specific frameworks, there are further studies, and no specific blockchain framework is explicitly stated. Instead, they proposed customized systems that are based on the general concept of blockchain technology.

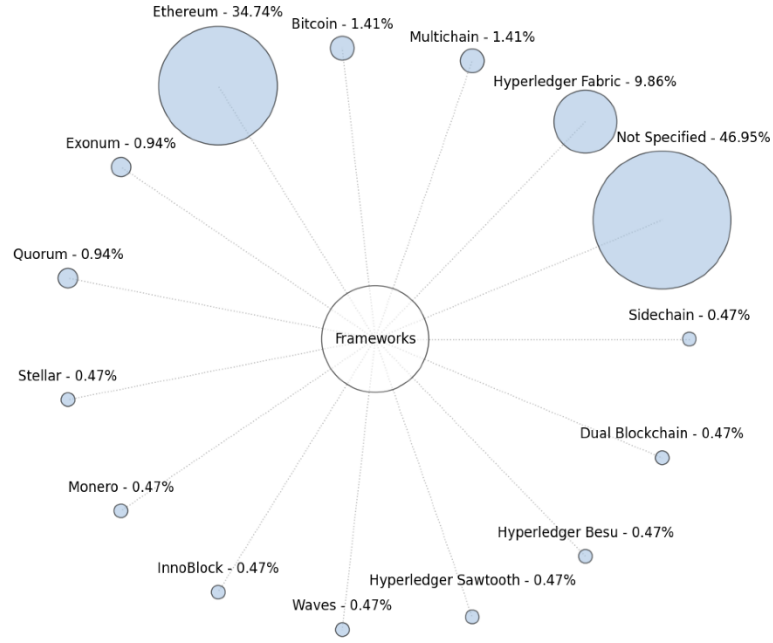


Figure 2. Blockchain frameworks distribution of proposed blockchain-based e-voting systems.

5.2 CONSENSUS ALGORITHM

The consensus algorithms that were mentioned are illustrated in **Figure 3**. Although a substantial number of papers do not explicitly mention the consensus algorithm used, it is reasonable to assume that for most proposed systems that use Ethereum as their framework, the consensus algorithm can be considered as Proof of Work (PoW). The following and most substantial protocol is referred to as “Proof of Work (PoW)”, resulting in approximately 5.2% portion of used consensus algorithms. In the following, we provide a brief definition for each of these consensus algorithms:

Consensus Algorithm	No. of Papers	Normalized (%)
Proof of Work (PoW)	11	100
Proof of Stake (PoS)	6	54.55
Proof of Authority (PoA)	6	54.55
Byzantine Fault Tolerance (BFT)	6	54.55
Practical Byzantine Fault Tolerance (PBFT)	4	36.36
Raft consensus algorithm	3	27.27
Delegated Proof of Stake (DPoS)	2	18.18
Crash Fault Tolerant (CFT)	1	9.09
Stellar consensus protocol (SCP)	1	9.09
Hybrid (PoC combined with PoS)	1	9.09

Normalized Percentage = $\frac{\text{Number of Papers in a Category}}{\text{Max Number of Papers in any Category}} \times 100$.

Figure 3. Adoption of consensus algorithms in blockchain-based e-voting systems

1. Proof of Work (PoW): Commonly used consensus algorithm, including Bitcoin. It is a technique that requires members, known as miners, to solve computationally demanding puzzles in order to secure the network and validate transactions [11].
2. Proof of Stake (PoS): a consensus process in which block creators (validators) are selected depending on their wealth or stake in the network, and their possessions act as a guarantee, inciting honesty and network security [12].
3. Proof of Authority (PoA): A consensus approach used with authorized entities or individuals as block validators. Unlike other consensus methods, PoA is based on a predetermined set of reliable validators who proved their credibility in the network [13].
4. Byzantine Fault Tolerance (BFT): A technique that obtains agreement among participants even in the presence of malfunctioning or malicious nodes. BFT consensus algorithms are designed for dealing with Byzantine failures, in which nodes behave unexpectedly and inconsistently [14].
5. Practical Byzantine Fault Tolerance (PBFT): A specific algorithm that provides BFT in distributed systems. A leader node is selected to propose a block of transactions, which the other nodes, called replicas, validate and agree on [15].

5.3 SECURITY AND PRIVACY TECHNIQUES

The use of blockchain-based e-voting systems needs to take security and privacy into consideration. Since it is decentralized and transparent, blockchain offers the possibility to boost the trustworthiness and credibility of e-voting systems. The use of security and privacy techniques in blockchain-based e-voting systems could assist in alleviating concerns about vote tampering, manipulation, and privacy violations.

Figure 4 shows the number of studies that deploy security and privacy techniques. Data collection covers a concepts and techniques. We list the number of publications and a normalized value in order to indicate the magnitude relative to other techniques.

Technique	No. of Papers	Normalized (%)
ZKP	24	100
HE	24	100
BS	16	66.67
RS	13	54.17
SS	3	12.50
QKD	2	8.33
MN	2	8.33
TLE	2	8.33
ML	2	8.33
CS	1	4.17
RoPO	1	4.17
PMS	1	4.17
BC	1	4.17
DP	1	4.17
PB	1	4.17

Normalized Percentage = $\frac{\text{Number of Papers in a Category}}{\text{Max Number of Papers in any Category}} \times 100$.

Figure 4. Distribution of security and privacy techniques in blockchain-based e-voting

As for the consensus protocols, we provide an overview of each of the techniques.

1. Zero-Knowledge Proofs (ZKPs): a cryptographic technique that enables one party to prove to another party the truthfulness of a statement or claim without disclosing any extra information [16,19].
2. Homomorphic Encryption (HE): a cryptographic technique that facilitates computations to be executed on encrypted data without the need for decryption [20,21,22].
3. Blind Signature (BS): a cryptographic method that enables a party to receive a valid signature on a message without disclosing the message's contents to the signer [23].
4. Ring Signatures: A cryptographic technique that offers anonymity and unlikability to the signer within a group (ring) of potential signers. In the context of cryptographic protocols, a ring signature allows the signer to generate a signature on a specific message, thus convincing the verifier that the message was signed by an entity within a specific group while at the same time obscuring the true identity of the singer [24].
5. Shamir's Secret Sharing Scheme (SS): a cryptographic method that enables the division of a secret into multiple shares that are distributed among participants [17].
6. Quantum Key Distribution (QKD): a method of establishing secure cryptographic keys between two parties that makes use of the concepts of quantum physics [25,26].
7. Mix Network (MN): This technique is used to protect the privacy of voters and the secrecy of votes. Through serving as a channel between voters and the authority responsible for counting the votes [27,28].
8. Time-lock encryption (TLE): in this technique, a time-based delay is added to the encoding of encrypted data [28].
9. Machine Learning (ML): By integrating machine learning and blockchain technology, along with deep learning algorithms, significant enhancements can be achieved in biometric ID authentication. This involves utilizing machine learning methods to analyze

facial features and verify the identities of users [18,29].

10. Circle Shuffle (CS): this method relies on a circular arrangement of votes, wherein each vote is assigned to a particular place in the circular structure [17].
11. Reputation-Based PayOff algorithm (RoPO): An incentive mechanism that is used in different decentralized systems to motivate players based on their reputation or performance history [30].
12. Proxy Multi-Signature Scheme (PMS): a variant of the common multi-signature method that includes the idea of a proxy or delegate to make signing on behalf of multiple individuals [31].
13. Bit Commitment (BC): a cryptographic technique in which one party (the committer) makes a commitment to another (the verifier) about a value without initially disclosing that value to the verifiers until the committee decides to reveal the committed value at a later time [32].
14. Differential Privacy (DP): It intends to maintain voters' sensitive data private while still allowing effective aggregate voting data analysis. It provides a structure for protecting voters' anonymity by adding random noise or perturbations to the data in a controlled manner [33].
15. Provenance-Based solution (PB): this solution involves tracking the origin and transformations of data (provenance) within the blockchain [34].

5.4 AUTHENTICATION AND IDENTITY VERIFICATION TECHNIQUES

In blockchain-based e-voting systems, reliable authentication and identity verification is important to protect the integrity and security of the voting process. Authentication and identity verification in blockchain-based e-voting systems play an essential duty in satisfying various important objectives, such as ensuring voter eligibility, preventing fraud, and maintaining vote secrecy.

1. Biometric authentication: This method uses an individual's unique characteristics to validate their authenticity. These qualities can include fingerprints, facial recognition, iris or retina patterns, and even voice.
2. OTP (One-Time Password): a password that can only be used for one login session or transaction, often used to give a higher level of protection to sensitive transactions or systems.
3. Aadhaar ID verification: the Unique Identification Authority of India (UIDAI) issues Indian residents a 12-digit Aadhaar number based on the resident's self-portrait, ten fingerprints, and two iris scans .

4. Multifactor authentication: this is the safety mechanism that requires multiple authentication methods from different categories to validate a user's identity for a login or other transaction.
5. Multi-step authentication: a security procedure that requires a user to provide extra evidence of identification when an additional level of assurance is required.
6. PKI-based X.509: PKI-based X.509 is a widely adopted standard that outlines how public key certificates are structured.
7. Unique IDs based on hash values: this method entails creating a unique identifier by applying a hash function to the biometric data, name, and date of birth of the voters.

Figure 5 summarizes the distribution of authentication approaches utilized in different research papers. According to the results, the biometric authentication approach is frequently addressed across different studies.

Technique	No. of Papers	Normalized (%)
Biometric Authentication	27	100
Aadhaar ID Verification	7	25.93
OTP (One-Time Password)	6	22.22
Multifactor Authentication	3	11.11
Multi-Step Authentication	3	11.11
PKI-based X.509	2	7.41
Unique Hash IDs	1	3.70

$$\text{Normalized Percentage} = \frac{\text{Number of Papers in a Category}}{\text{Max Number of Papers in any Category}} \times 100.$$

Figure 5. Distribution of authentication and identity verification techniques in blockchain-based e-voting papers.

5.5 ANALYSIS OF RESULTS

This study reviewed a variety of blockchain platforms in Section 4.1, including Ethereum, Hyperledger Fabric, Bitcoin, and Multichain, each offering unique capabilities crucial for e-voting systems. Platforms like Ethereum are notable due to their smart contract functionality, which allows the creation of complex voting protocols, thus enhancing security and transparency. The choice of platform plays a critical role in determining the scalability, security, and flexibility of the e-voting system [35].

In Section 4.2, we analyzed the consensus mechanisms employed in the blockchain

platforms, which are fundamental to the integrity and reliability of e-voting systems. Algorithms such as Proof of Work and Proof of Stake each bring different strengths and trade-offs in terms of security, energy efficiency, and processing speed. For e-voting systems, particularly on a national scale, selecting an appropriate consensus algorithm is critical, as it directly influences the system's ability to handle plenty of votes securely and efficiently while also preserving voter privacy.

The findings in Section 4.3 indicated the importance of incorporating advanced security and privacy techniques in e-voting systems. Techniques like homomorphic encryption and zero-knowledge proofs play a major role in ensuring that a voter's anonymity is maintained without compromising the transparency and verifiability of their vote. Implementing these techniques is essential for improving public trust in the electoral process.

Chapter-6

DISCUSSION AND CONCLUTION

The application turns out to be a success and the users can use their Web3 identity to vote. According to the application, every single voting request that is sent to the Smart Contracts required the transaction to be signed by the voter. Moreover, the voters need to abide by the rules that are defined in the Smart Contract so that the voters do not vote twice and the voter vote for the right candidates. This is to avoid any possible mutation by a third or direct party who is managing the system so that the result of the voting will always be transparent.

6.1 DISCUSSION

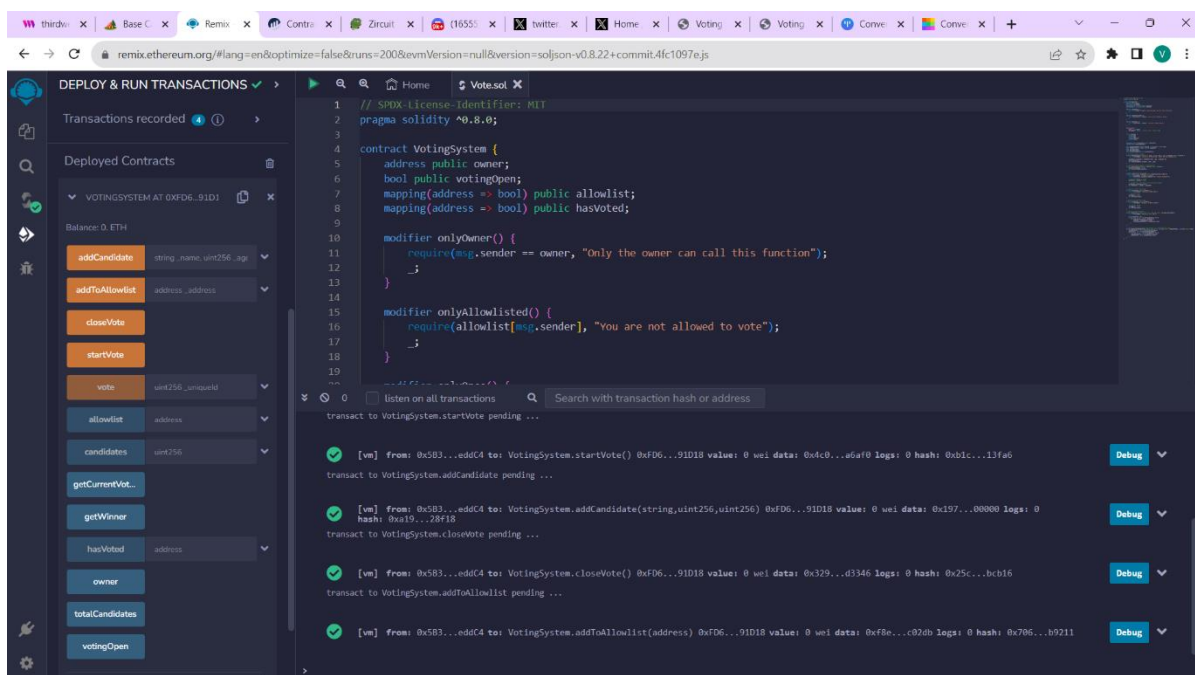


Figure 6. Deployed Contract in Remix IDE

In the above figure smart contract is deployed in remix ide on Ethereum Goerli Network. In Terminal 4 transactions are performed by the owner. These transactions are add candidates, add to allowlist, stat vote & close vote. After the transaction is successful a hash is generated.

In the above figure Orange buttons are write functions which can be performed only by the owner

of contract except vote function that is performed by allowed voter, Blue buttons are read only functions which can be accessed by both the parties.





















	0xec56a4129e...	<button>Close Vote</button>	10047228	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00005507
	0x686f57e2c39...	<button>Start Vote</button>	10047070	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00005498
	0x829b9e8a90...	<button>Add To Allowli...</button>	10046996	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00009525
	0xab9537c7cb...	<button>Add To Allowli...</button>	10046988	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00009525
	0x2480952d72...	<button>Add Candidate</button>	10046976	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00020549
	0x2853422996...	<button>Add Candidate</button>	10046967	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00023969
	0xc67c35fdc12...	<button>Close Vote</button>	10046951	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0
	0x9fd7e016db8...	<button>Add To Allowli...</button>	10046947	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0.00005545
	0x4b15bc6380...	<button>Add To Allowli...</button>	10046937	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0
	0xa6b02b92dfb...	<button>Start Vote</button>	10046927	120 days ago	0x9F7d30b2...96B2E4528		OUT	0xFD64d736...aF9891D18	0 ETH	0

Figure 7. Transactions are published on blockchain Explorer

In above Figure all transactions add candidates, add to allowlist, stat vote & close vote are published with their transaction hash and blocks which contain all the relevant information of particular block and transaction.

Transaction Hash:	0xa6b02b92dfb0c1ed8571e3915eb6e9e93bdb79adce767f5553aef4e446d53b52
Status:	Success
Block:	10046927 617082 Block Confirmations
Timestamp:	120 days ago (Nov-15-2023 08:40:12 AM +UTC)
Transaction Action:	Call Start Vote Function by 0x9F7d30b2...96B2E4528 on 0xFD64d736...aF9891D18
From:	0x9F7d30b29F587dcf61732244cEdB98396B2E4528
To:	0xFD64d736dD56261Dfc7780C49A08312aF9891D18
Value:	0 ETH (\$0.00)
Transaction Fee:	0.000000000000302434 ETH \$0.00
Gas Price:	0.000000011 Gwei (11 wei)

Figure 8. Start Vote Function transaction hash!

In above figure Start Vote function is executed by the Contract owner and that transaction is stored on blockchain explorer where everyone can see the details regarding that transaction, these transaction contains transaction hash which is unique, status of transaction, block number and

block confirmation number, timestrap , and transaction done by which address , gas fee etc.

6.2 CONCLUSION

The application that was implemented solved the original task of building a secure voting system. This application does not allow any mutations to the voting result, and it is the original goal of this application. The code from the application works well in real life, it is only required for the Smart Contracts to be on Mainnet, and an access to the government central database to check the validity of the social security numbers. One other way to do this project is to build a secure distributed system and provide restriction to the database so that only authorized personnel can access and query the database. Even that cannot prevent any mutation to the database because the authorized personnel can tamper with the vote result themselves and it defeats the purpose of the application in the first place. A background check is required to elect the trusted personnel to manage the database which stores the voting results, and even that is risky because there is no way to know if there is any outside influence on that person that could make him change his mind. With blockchain and Smart Contracts involved, the system can be decentralized and there is no need to worry about finding a trustworthy person to manage the database.

Chapter-7

SUMMARY, PUBLICATIONS AND FUTURE WORK

7.1 SUMMARY

The proposed framework provides complete security to the e-voting system, with the usage of Ethereum blockchain and smart contracts to provide added security to the system. Blockchain implementation prevents vote manipulation and provides privacy, integrity for voters to cast their vote. Smart contracts ensures that the voter can vote only once using his/her unique id (Aadhar number); with the convention of different security algorithms like SHA-256, Merkel hash and SMTP prototyping, enhances the security of the system. As a result, the voter is authorized to cast his/her vote from where ever they are; provides high security standards to the system and convenient and easier ways to vote.

The results show that blockchain technology has the potential to successfully implement e-voting systems. Transparency and auditability are seen as undisputed benefits. Security and privacy are, as would be expected for voting processes, the central properties. Here, the potential is seen in blockchain technology over other platform technologies, but whereas some specific aspects are acknowledged, both remain serious open problems, which their top rankings in the frequency lists for challenges and future directions show.

7.2 FUTURE WORK

- To the proposed existing system, additional biometrics (fingerprint, face authentication) can be added to enhance the security of the system.
- Three step authentications can also be used to provide more security to the system
- Deploy Decentralized voting System on Ethereum Mainnet Network to implement in real life.

REFERENCES

- [1] Paul Wackerow, August 16, 2022, this documentation is designed to help you build with Ethereum <https://ethereum.org/en/developers/docs/>
- [2] Solidity Documentation. (n.d.). Introduction to Smart Contracts. Retrieved from <https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html>
- [3] Ethers.js Documentation. (n.d.). Getting Started. Retrieved from <https://docs.ethers.org/v5/getting-started/>
- [4] Kong, X.; Wu, Y.; Wang, H.; Xia, F. Edge Computing for Internet of Everything: A Survey. *IEEE Internet Things J.* 2022, 9, 23472–23485. [Google Scholar] [CrossRef]
- [5] Luxoft. Available online: <https://www.luxoft.com/> (accessed on 18 November 2023).
- [6] Votem. Available online: <https://votem.com/> (accessed on 20 November 2023).
- [7] Voatz. Available online: <https://voatz.com/> (accessed on 20 November 2023).
- [8] Polyas. Available online: <https://www.polyas.com/> (accessed on 21 November 2023).
- [9] Kaspersky Box. Available online: <https://box.kaspersky.com/f/e68a161d8e7241909ea3/> (accessed on 21 November 2023).
- [10] Decentra. Vote. Available online: <https://decentra.vote/> (accessed on 25 November 2023).
- [11] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 14 May 2023).
- [12] King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012. Available online: <https://peercoin.net/assets/paper/peercoin-paper.pdf> (accessed on 19 August 2012).
- [13] Kovan—Stable Ethereum Public Testnet. Available online: <https://github.com/kovan-testnet/proposal/blob/master/README.md> (accessed on 14 May 2023).

- [14] Buchman, E. Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. Ph.D. Thesis, University of Guelph, Guelph, ON, Canada, 2016. [Google Scholar]
- [15] Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI 99), New Orleans, LA, USA, 22–25 February 1999. [Google Scholar]
- [16] Huang, J.; He, D.; Obaidat, M.S.; Vijayakumar, P.; Luo, M.; Choo, K.-K.R. The application of the blockchain technology in voting systems: A review. *ACM Comput. Surv. (CSUR)* 2021, 54, 1–28. [Google Scholar] [CrossRef]
- [17] Bartolucci, S.; Bernat, P.; Joseph, D. SHARVOT: Secret SHARe-Based VOTing on the Blockchain. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB '18), Gothenburg, Sweden, 27 May 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 30–34. [Google Scholar]
- [18] Cheema, M.A.; Ashraf, N.; Aftab, A.; Qureshi, H.K.; Kazim, M.; Azar, A.T. Machine Learning with Blockchain for Secure E-voting System. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 177–182. [Google Scholar]
- [19] Fatrah, A.; El Kafhali, S.; Haqiq, A.; Salah, K. Proof of Concept Blockchain-Based Voting System. In Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT '19), Rabat, Morocco, 23–24 October 2019; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–5. [Google Scholar]
- [20] Zhang, S.; Wang, L.; Xiong, H. Chaintegrity: Blockchain-Enabled Large-Scale E-Voting System with Robustness and Universal Verifiability. *Int. J. Inf. Secur.* 2020, 19, 323–341. [Google Scholar] [CrossRef]

- [21] Gupta, S.P.; Tripathi, A.M. E-Voting using Blockchain. *J. Physics Conf. Ser.* 2021, 1911, 1–14. [Google Scholar] [CrossRef]
- [22] Qu, W.; Wu, L.; Wang, W.; Liu, Z.; Wang, H. A Electronic Voting Protocol Based on Blockchain and Homomorphic Signcryption. *Concurr. Comput. Pract. Exp.* 2022, 34, e5817. [Google Scholar] [CrossRef]
- [23] Carcia, J.C.P.; Benslimane, A.; Boutalbi, S. Blockchain-based system for e-voting using Blind Signature Protocol. In *Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 01–06. [Google Scholar]
- [24] Kurbatov, O.; Kravchenko, P.; Poluyanenko, N.; Shapoval, O.; Kuznetsova, T. Using Ring Signatures For An Anonymous E-Voting System. In *Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 18–20 December 2019; IEEE: Piscataway, NJ, USA, 2022; pp. 187–190. [Google Scholar]
- [25] Verma, G. A Secure Framework for E-Voting Using Blockchain. In *Proceedings of the 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA)*, Gunupur, India, 8 September 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5. [Google Scholar]
- [26] Gupta, S.; Gupta, A.; Pandya, I.Y.; Bhatt, A.; Mehta, K. End to End Secure E-Voting Using Blockchain & Quantum Key Distribution. *Mater. Today Proc.* 2023, 80, 3363–3370. [Google Scholar]
- [27] Chaieb, M.; Yousfi, S. LOKI Vote: A Blockchain-Based Coercion Resistant E-Voting Protocol. In *Proceedings of the Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020*, Dubai, United Arab Emirates, 25–26 November 2020; Springer International Publishing: Cham, Switzerland, 2020. [Google Scholar]
- [28] Golnarian, D.; Saedi, K.; Bahrak, B. A decentralized and trustless e-voting system based on blockchain technology. In *Proceedings of the 2022 27th International Computer Conference, Computer Society of Iran (CSICC)*, Tehran, Islamic Republic of Iran, 23–24 February 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7. [Google Scholar]

- [29] Parmar, A.; Gada, S.; Loke, T.; Jain, Y.; Pathak, S.; Patil, S. Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 6–8 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5. [Google Scholar]
- [30] Li, M.; Luo, X.; Sun, W.; Li, J.; Xue, K. AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 4751–4756. [Google Scholar]
- [31] Luo, T. An Efficient Blockchain Based Electronic Voting System Using Proxy Multi-signature. In Proceedings of the 2021 3rd International Academic Exchange Conference on Science and Technology Innovation (IAECST), Guangzhou, China, 10–12 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 513–516. [Google Scholar]
- [32] Doost, M.; Kavousi, A.; Mohajeri, J.; Salmasizadeh, M. Analysis and Improvement of an E-voting System Based on Blockchain. In Proceedings of the 2020 28th Iranian Conference on Electrical Engineering (ICEE), Tabriz, Iran, 4–6 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–4. [Google Scholar]
- [33] Xu, Z.; Cao, S. Efficient Privacy-Preserving Electronic Voting Scheme Based on Blockchain. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 190–196. [Google Scholar]
- [34] Khan, K.M.; Arshad, J.; Khan, M.M. Empirical Analysis of Transaction Malleability within Blockchain-Based E-Voting. *Comput. Secur.* 2021, 100, 102081. [Google Scholar] [CrossRef]
- [35] Werth, J.; El Ioini, N.; Hajian Berenjestanaki, M.; Barzegar, H.R.; Pahl, C. A Platform Selection Framework for Blockchain-Based Software Systems Based on the Blockchain Trilemma. In Proceedings of the ENASE, Prague, Czech Republic, 24–25 April 2023; pp. 362–371. [Google Scholar]