Blockchain based E-Voting System using Smart Contracts

M.Tech Thesis

Submitted in partial fulfillment of
the requirements for the award of the degree
of
Master of Technology by Research
in
Department of Software Engineering
by

Chirag Nagar (24/RSE/010)

under the guidance of

Dr. Divyashikha Sethia
Associate Professor
Department of Software Engineering



DEPTT. OF SOFTWARE ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY, DELHI
May 2025



DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

CANDIDATE'S DECLARATION

I, Chirag Nagar, hereby certify that the work which is being presented in the thesis entitled Blockchain based E-Voting System using Smart Contracts in partial fulfillment of the requirements for the award of the Degree of Master of Technology by Research, submitted in the Department of Software Engineering, Delhi Technological University is an authentic record of my own work carried out during the period from January 2026 to May 2026 under the supervision of Dr. Divyashikha Sethia.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other Institute.

Candidate's Signature

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

Signature of Supervisor

Signature of External Examiner



DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

CERTIFICATE BY THE SUPERVISOR

I hereby certify that Chirag Nagar (Roll No. 24/RSE/010) has carried out their research work presented in this thesis entitled "Blockchain based E-Voting System using Smart Contracts" for the award of Master of Technology by Research degree in Software Engineering, Delhi Technological University, Delhi under my supervision. The thesis embodies results of original work, and studies are carried out by the student himself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

Date: 21.05.2026

Dr. Divyashikha Sethia
Associate Professor
Dept. of Software Engineering
Delhi Technological University
New Delhi, India



DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to **Dr. Divyashikha Sethia**, Associate Professor, Department of Software Engineering, Delhi Technological University, for her invaluable guidance, encouragement, and continuous support throughout the course of this research. Her profound knowledge, insightful suggestions, and constant motivation have been instrumental in the successful completion of this thesis.

I would also like to acknowledge the Department of Software Engineering, Delhi Technological University, for providing a conducive academic environment and the necessary resources that facilitated the completion of this work.

I am deeply thankful to the faculty members and my fellow peers at the Department of Software Engineering, Delhi Technological University, for their valuable suggestions, encouragement, and constructive feedback during the course of this research.

Finally, I would like to express my heartfelt gratitude to my parents, family members, and friends for their unconditional support, patience, and encouragement, which have been a constant source of strength and inspiration throughout this journey.

Place: Delhi

Date: 21.05.2026 Chirag Nagar

Blockchain based E-Voting System using Smart Contracts

Chirag Nagar

ABSTRACT

The rapid development of digital technologies has markedly influenced key areas, including electoral systems, where there is an increasing need for solutions that ensure security, transparency, and resistance to tampering. This study introduces a blockchain-based electronic voting system designed to mitigate the shortcomings found in traditional and current e-voting approaches, such as voter fraud, data tampering, and insufficient transparency.

Firstly, the study proposes the Smart Contract Optimization and Performance Enhancement System (SOPES), a novel methodology intended to enhance the efficiency and reduce costs associated with blockchain applications. SOPES employs several advanced optimization strategies, including improvements in memory access, variable packaging, mapping and array structuring, as well as the removal of unnecessary code. These enhancements collectively result in approximately a 33% performance improvement, leading to lower gas costs and faster execution. By addressing core challenges in blockchain environments, particularly high transaction fees and limited scalability, this optimization framework contributes to making smart contract deployment more viable from both technical and economic perspectives.

Secondly, the optimized smart contracts developed through SOPES are applied to construct a low-cost blockchain-based electronic voting system that aims to overcome the weaknesses of existing digital voting methods. Leveraging blockchain's inherent characteristics—such as decentralization, immutability, and cryptographic security—the system promotes transparency, prevents fraudulent voting activities, and counters data manipulation. Key electoral functions including voter authentication, ballot casting, and vote counting are automated via these optimized contracts, thereby reducing reliance on manual processes and operational resources. Moreover, the integration of advanced cryptographic protocols supports voter anonymity while maintaining auditability, thereby providing a secure and privacy-respecting voting environment suitable for large-scale electoral implementations.

This report addresses significant deficiencies in blockchain-based voting systems, particularly regarding scalability, energy consumption, and user experience, by proposing a comprehensive and adaptable framework applicable to various electoral scenarios. The findings demonstrate that optimized smart contracts in conjunction with blockchain technology enhance the security, transparency, and dependability of electoral processes. By incorporating cost-effective and performance-driven mechanisms, the system offers promising feasibility for practical deployment while sustaining resilience against potential security threats. In summary, the proposed solution constitutes a meaningful step forward in modernizing electoral infrastructure, reinforcing confidence in democratic procedures, and fostering a voting environment characterized by greater security, transparency, and inclusiveness.

Contents

Certificate i

Candidate's Declaration ii

Acknowledgement iii

Abstract iv

Contents v

List of Figures vii

List of Tables viii

1 Introduction 1
- 1.1 Background . . . 2
  - 1.1.1 Electronic Voting System . . . 3
  - 1.1.2 Blockchain . . . 3
  - 1.1.3 Applications of Blockchain . . . 4
  - 1.1.4 Security Considerations in Blockchain . . . 5
  - 1.1.5 Challenges in E-Voting System . . . 5
  - 1.1.6 Advantages of Blockchain E-Voting System . . . 6
  - 1.1.7 Research Gaps . . . 7
- 1.2 Problem Statement . . . 7
- 1.3 Research Objectives . . . 7
- 1.4 Report Layout . . . 8

2 Technical Background 9
- 2.1 Blockchain Technology . . . 9
  - 2.1.1 Architecture of Blockchain . . . 10
  - 2.1.2 Advantages of Blockchain . . . 11
- 2.2 Etherum . . . 12
  - 2.2.1 Architecture of Etherum . . . 12
  - 2.2.2 Advantages of Etherum . . . 13
- 2.3 Smart Contracts . . . 14
- 2.4 E-Voting Systems . . . 14
  - 2.4.1 Structure of E-Voting System . . . 15
  - 2.4.2 Security and Privacy issues in E-Voting System . . . 15
- 2.5 Blockchain and Smart Contracts in E-Voting Systrem . . . 15

2.6 Cryptographic Measures 16
2.7 Smart Contract Cost Optimization 16

3 Optimizing Smart Contracts for Low Gas Consumption 18
3.1 Background 18
3.2 Motivation 19
3.3 Related Works 19
3.4 Architecture of SOPES (Smart OPtimizer for Ethereum Smart contracts 21
3.5 Results 23

4 Proposed Blockchain E-Voting System 26
4.1 Background 26
4.2 Motivation 27
4.3 Related Works 28
4.4 Methodology 30
4.5 Architecture of Blockchain E-Voting Proposed Solution 31
4.6 Identity Verification 32
4.7 Consensus Mechanisms 33
4.8 Scalability of System 33
4.9 Integration with Traditional System 34
4.10 Integration with Blockchain 34
4.11 Workflow of the Voting Transaction 34
4.12 Results and Discussion 37

5 Conclusion and Future Work 40

6 Publications and Presentations 41

Author's Profile 44

List of Figures

1.1 Flow of a Blockchain Transaction [1] 2
1.2 Comparison of Different types of Voting systems [1] 3

2.1 Block Architecture of a Single Block in Blockchain [2] 10
2.2 Structure of an Etherum blockchain node [3] 12

3.1 Architecture of SOPES (Smart Optimizer for Ethereum Smart Contracts) 21
3.2 Comparison of Different Models with proposed SOPES Tool 24

4.1 Architecture of Proposed Blockchain based E-Voting Solution 31
4.2 LoginPage of Proposed Blockchain based E-Voting Solution 35
4.3 Verification Page of E-Voting Solution 35
4.4 Voting parties 36
4.5 Hash Generation of Voted Party 36
4.6 Live Results Page 37
4.7 Transaction Hash and Block Genrartion in Blockchain 37
4.8 Comparison of SOPES based Blockahin Evoting system with different models) 38

List of Tables

3.1 Comparison of Features in Gas Optimization Tools 20
3.2 Comparison of Gas Optimization Tools for Deployment Cost 24
3.3 Comparison of Gas Optimization Tools for Execution Cost 25
3.4 Comparison of Gas Optimization for Execution Cost 25

4.1 Comparison of Features in Blockchain-Based E-Voting Systems 29
4.2 Comparative Analysis of Smart Contract Gas Consumption and Optimization Efficiency 39

Chapter 1

Introduction

With the beginning of the new age it has become increasingly important that we have safe, clear and rapid election systems. The very traditional voting methods had many years of guaranteed trust but have been criticised due to voter fraud, manipulation, and less reliable logistically. Electronic voting systems were introduced to make the voting process more technologically optimal. Serious central governance issues existed in those systems, leading to a lack of transparency and potential cybersecurity problems. From the above shortcomings, blockchain technology presented a path through which such a better electronic voting system could come on board, primarily through the effective use of economically efficient smart contracts.

Blockchains [4] were first invented as the understructure for cryptocurrencies like Bitcoin. It has evolved to serve many purposes beyond financial and monetary exchange. Decentralized [5] in nature, its immutability and other cryptographic protections make blockchain technology highly suited to alleviate some inherent weaknesses in traditional voting systems. Blockchain technology protects the votes during an election using a nearly tamper-proof distributed ledger, making it verifiable and transparent. It considerably reduces the opportunity for electoral fraud because manipulations of the records can require impossible computational resources and the acceptance of most network participants. A core element of a blockchain-based electronic voting system is the use of smart contracts [6], which are self-executing pieces of code on the Blockchain that systematically enforce established regulations. This eliminates intermediaries and allows interoperability among parties in trustless operations. In an electronic voting scheme, voting processes such as voter registration, casting, and counting votes can be automated using smart contracts. These contracts can ensure that all the steps in a process are executed transparently, securely, and free of human interference, thus minimizing the chances of errors and malpractices.

Although smart contracts have various advantages, it are often criticized for their high computational costs that may hamper scalability and widespread adoption for large-scale applications like national elections. Here, cost optimization becomes important. Optimized smart contracts [7] designed with caution in such a manner that the system can balance functionality and economic efficiency so the extensive application of the system can be achieved. Optimization techniques include gas usage minimization, essentially transaction cost minimization, and off-chain computation to reduce on-chain execution. A blockchain-based e-voting [8] architecture that relies on economically efficient smart contracts offers several advantages.

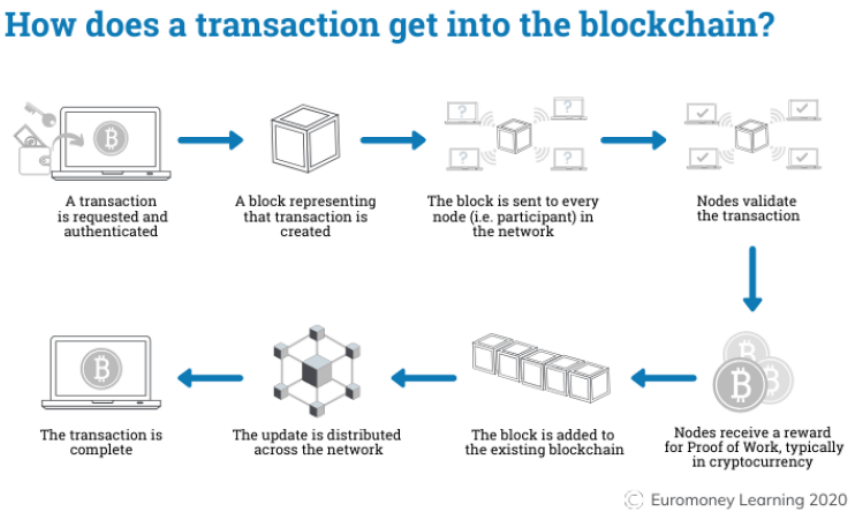


Figure 1.1: Flow of a Blockchain Transaction [1]

The application of a blockchain electronic voting system entails various difficulties. The issues associated with scalability, voter anonymity, and compliance with regulations have often been an impediment for blockchain-based technologies like Ethereum, which allow for smart contract execution. The current paper addresses the problem of blockchain electronic voting systems, their implementation, and the potential effects, both technical and economic, that arise from such implementation.

1.1 Background

The electronic voting systems (e-voting) are expected to be substituted for the traditional paper ballots by providing certain benefits such as being cheap, speed in reporting the results and provide access for voters [7]. But the e-voting systems face various challenges that include the risk to be attacked in the cyber-security sphere [9], issue with voter anonymity and not able to maintain an audit trail. These kind of problems demand an appropriate solution from a technology point of view in terms of security and performance.

In fact, blockchain technology was first proposed as a component for cryptocurrencies and the potential impact in various fields is greatly emphasized since it has peculiar characteristics like decentralization [4], immutability and transparency. When applied in the voting process, blockchain, as presented in Fig. 1.1, provides an immutable ledger suitable for storing votes.Moreover, through innovative contracts-self-executing software running on the Blockchain, it is possible to automatize and enforce many important aspects of the voting process, including verifying voters and aggregating results. These technologies all respond to the major concerns against the fraud, distrust, and inefficiency of the currently available e-voting systems.

This study aims to build sophisticated electronic voting systems that are both technically sound and financially viable for implementation across different socio-economic contexts by integrating blockchain technology with cost-effective smart contracts [5]. This section draws attention to the need for a paradigm shift in electronic voting methods and lays the platform for exploring Blockchain as a transformative force within the elections.

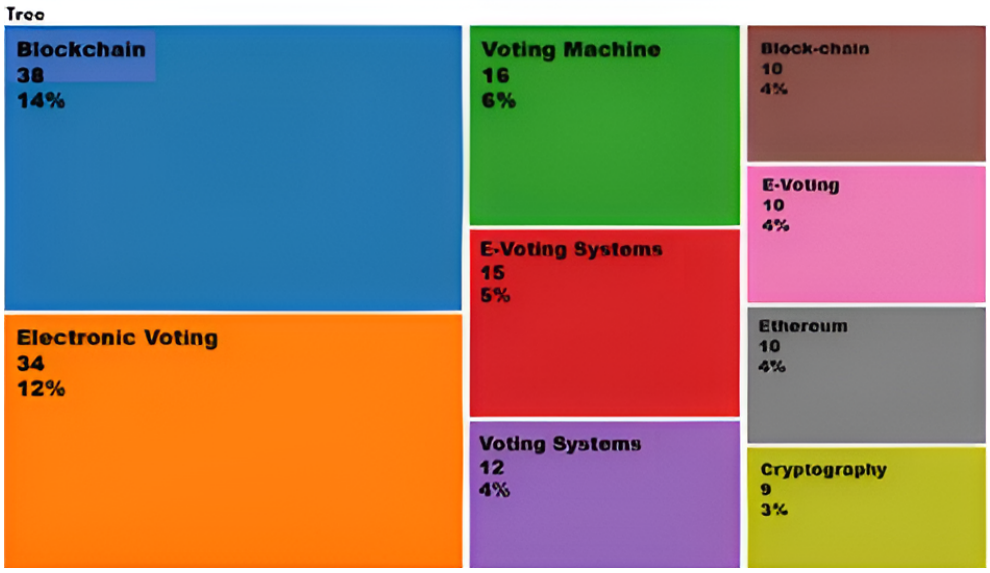


Figure 1.2: Comparison of Different types of Voting systems [1]

1.1.1 Electronic Voting System

The electronic voting system (e-voting) [5] is one of the modern ways elections are conducted. These systems use digital technologies that help cast, count, and distribute votes. In India, mainly EVMs have been used to implement the process of e-voting by replacing the paper ballot system, which was time-consuming, in the late 1990s [7]. It was a landmark moment in India's electoral machinery. It addressed vote duplication, invalid votes, and managerial crises, as millions of ballots were handled within one of the world's biggest democracies.

EVMs developed and designed by the ECI brought more efficiency to the voting process. The machine is portable, user-friendly, and does not require a network to work, thus making it suitable for deployment even in remote and rural areas. Recent evidence of this success came in the general elections in India, and over 600 million voters cast their ballots seamlessly using EVMs shown in Fig. 3.2. Critics have demonstrated that the system has no end-to-end verifiability; EVMs are standalone systems with no mechanism providing clear and transparent independent auditability.

This is a very transformative opportunity to integrate blockchain technology into the framework of India's e-voting. All security issues could be solved using blockchain technology by providing an immutable, decentralized ledger for recording and verifying votes. For instance, Indian voters outside India can vote securely with blockchain-enabled platforms and thus need not physically visit polling stations. Additionally, it can automatically authenticate voters, thus allowing real-time vote counting while ensuring accuracy and trustworthiness in a blockchain with smart contracts-based voting.

1.1.2 Blockchain

It was initially presented in 2008 [9] as the underlying framework for the cryptocurrency called Bitcoin, but it has since become a revolutionizing innovation with applications beyond cryptocurrencies. At its core, Blockchain operates as a decentralized ledger [10] distributed with the record of transactions to be safe, immutably, and transparently recorded. Unlike conventional centralized systems, Blockchain operates on a peer-to-

peer network where each network participant, a node, has equally matched access to a copy of the same record. Such a decentralization mechanism ensures higher security, transparency, and trust. As such, Blockchain is the best solution to problems in banking and finance, health, supply chain management, and electronic voting.

The basic unit in a blockchain is called the "block." It is a virtual container holding information, the essence of information about a given transaction. These blocks are chained together in permanent sequence via complex mathematical algorithms [8] into a chain protected in this way. Once that block is placed into the chain, no information it contains can be altered or deleted without the network's unanimous consent. Immutability is a fundamental property that makes Blockchain reliable for data integrity in applications.

Another feature of Blockchain is that it features privacy for voters and still has mechanisms to verify. Advanced cryptographic [4] techniques utilizing zero-knowledge proofs [9] and hashing allow Blockchain to anonymously identify the voters while creating mechanisms to verify the authenticity of votes. Therefore, there is a critical need to balance privacy and transparency in maintaining democratic integrity in an e-voting system. The implementation of blockchain technology in the system of e-voting can positively affect its security, efficiency, and transparency and thus significantly impact the functioning of democratic institutions. With the development of this technology, it is possible that it will not only change the election process but also have an impact on the very structure of governance and civic participation worldwide.

1.1.3 Applications of Blockchain

- ***Cryptocurrency and Digital Payments***: The blockchain technology is the core technology that drives the operation of cryptocurrencies like Bitcoin and Ethereum. It enables users to conduct financial transactions directly between each other without using any intermediary organization such as a bank.

- ***Supply Chain Management*** :The Blockchain provides end-to-end visibility and traceability in logistics operations. It allows for the real-time tracking of items from the source to their final destination, as exemplified by applications in industries like food, pharmaceuticals, and high-end fashion.

- ***Healthcare*** : Blockchain technology provides a secure method of sharing medical records, thus ensuring that patients' privacy is maintained while allowing healthcare professionals to access the most current data.

- ***Voting Systems*** : Blockchain technology helps improve the process of conducting elections, providing a platform for voters to cast their votes anonymously, transparently, and without any risk of vote rigging, as illustrated by several trials conducted across different countries.

- ***Digital Identity Management*** : Blockchain technology allows for secure and decentralized identity verification, giving people the ability to have more control over their personal information. Examples of use cases include digital identification, passports, and access control.

- ***Financial Services and Banking*** : Blockchain technology can improve banking operations by facilitating quick and secure transactions across international borders

and lowering transaction costs and risks of fraud.

- ***Insurance*** : Blockchain makes the insurance industry more efficient and transparent because blockchain technology streamlines claim processing and provides a fraud-proof system for recording contract details.

- ***Real Estate*** : Using blockchain technology can improve the efficiency of real estate transactions since it records real estate ownership securely and helps prevent fraud related to land titles.

- ***Energy Trading*** : Using blockchain allows for the development of a decentralized energy market whereby energy producers trade directly with consumers at lower costs.

1.1.4 Security Considerations in Blockchain

The blockchain technology is known for the inherent security features that it comes equipped with; nevertheless, it possesses certain vulnerabilities, particularly with respect to its application within areas such as e-voting. Ensuring that it works effectively in such scenarios demands a thorough assessment of the blockchain network structure, possible attacks, and effective measures for mitigating the identified threats.

The consensus algorithm is one of the key parameters that affects the security of blockchains [11]. To resolve the issue that the shared database remains consistent, Algorithms like PoW [12] and PoS [7] work in the way that ensure that no unauthorized operation on the database is performed. But even if the necessary measures are taken, not all threats can be avoided. A 51% attack is also a possible scenario when an attacker is controlling over 51 percent of computation power or stake resources.

Another point we should note down is the usage of smart contracts. Automating contracts make our actions to be more efficient, but vulnerabilities that caused by poor implementation or insufficient testing may be exploited by anyone. It may cause wrong behavior, money lost or technical issues. Particularly in cases such as electronic voting where minor errors can jeopardize the entire procedure.

Privacy is one of the biggest challenges in the application of blockchain technology. Even though the openness of blockchain is one of its core building blocks, it can be problematic when it conflicts with the privacy concerns involved in voting. This dilemma is being actively addressed through highly secure cryptographic techniques including zero-knowledge proof, ring signature, and homomorphic encryption.

1.1.5 Challenges in E-Voting System

Though e-voting systems are valued a great deal owing to the easy, efficient, and accessible approach that it offers to the election, still it has got numerous problems regarding e-voting which need to be properly solved. By the application of newer techniques like block chain, another problem arises.

- ***Security Risks***
  Despite their advantages like easy access, high efficiency and convenience electronic voting (e-voting) systems have several problems to overcome in order to become a trustworthy, secure and credible voting mechanism. Further difficulties that the

implementation of high tech technology, like the blockchain, would bring to e-voting require the application of innovative solutions for an optimum combination of security, transparency and user-friendliness.

- ***Voter Privacy and Anonymity***
  In this regard, there is the issue of finding the right balance between the need to maintain voter secrecy and the need to have some level of openness within the voting process. It may be important for a system to have room for audit and verification, but it is just as critical that it remains impossible to link any vote to its respective voter.

- ***System Integrity and Trust***
  The adoption of electronic voting machines by the electorate largely depends on the credibility of the technology. Malfunctioning of the technology due to such issues as loss of votes, malfunction, or even manipulation results in a lack of confidence among voters concerning the election process. Therefore, it becomes essential to adopt tampering technologies along with test procedures.

- ***Cost Considerations***
  Electronic voting systems carry considerable costs, which range from development to maintenance and security. The costs include software development costs, purchase of hardware, training of staff, and security upgrades. These expenses can present major problems, particularly in areas with limited resources.

- ***Auditing and Verification***
  The process of validating votes while maintaining the anonymity of voters is inherently difficult. Although blockchain technology offers advantages such as transparency and immutability, the application of blockchain technology also comes with some technical difficulties and high costs.

1.1.6 Advantages of Blockchain E-Voting System

One important feature of using blockchain technology in electronic voting is safety, efficiency, transparency, and privacy of the system [10]. The primary concern behind this feature is increased security since the blockchain uses cryptography in voting and stores all votes safely; thus, it becomes highly resilient to attacks and frauds. The decentralized nature of the technology minimizes risks for traditional centralized voting processes.

Transparency [4] and immutability [9] constitute another major benefit. The use of blockchain ensures that all votes are stored in immutable ledger and become irreversible after being added to the chain. Thus, one can monitor all processes during electronic voting in real-time mode; this helps guaranteeing that votes will not be altered. The properties of blockchain technology assure that results of voting will be accurate and credible, and voter's privacy will be guaranteed.

Another benefit of using the blockchain technology is efficiency. Traditional voting systems require some expenses like purchasing paper for making ballots, organizing voting centers, and hiring people who will count votes manually. The blockchain approach to voting will eliminate many costs associated with these procedures and make the voting process cheaper and faster.

1.1.7 Research Gaps

Despite the benefits that have been realized from e-voting using blockchains, there are certain research issues that need to be tackled to ensure that the effectiveness of such voting processes is increased, particularly with regard to smart contracts.

- ***Scalability and Performance***: The first of these issues relates to the scalability of the process. An increase in the number of voters might lead to blockchain congestions which, in turn, might limit the transaction speed.
- ***Interoperability***: To enhance the efficacy of e-voting, smart contracts need to be effectively incorporated into existing voting frameworks and complementary technologies.
- ***Security and Privacy***: Even though blockchains are immutable and clear, voter anonymity is still a challenge. The current trend involves trying to create cryptographic methods that allow for the verification process while maintaining voter anonymity.
- ***Legal and Regulatory Framework***: There are certain legal issues about whether smart contracts can be used effectively in e-voting, as well as issues about the auditability and accountability of smart contracts.

1.2 Problem Statement

E-voting solutions promise a convenient and secure way of conducting voting compared to traditional methods; however, various hurdles need to be overcome in order to implement them. First, there is a need for costless voting for both the elector and the election body, which faces huge costs related to managing elections. Identity verification must be guaranteed, meaning that instead of verifying IDs, it would be necessary to use digital identities protected by the blockchain system. Additionally, the high costs involved in using smart contracts call for the implementation of cheaper systems. Lastly, while blockchain offers data integrity and transparency, there is also a need to protect voter privacy.

1.3 Research Objectives

The goal of this project is to create an electronic voting mechanism with the use of Blockchain technology, where the smart contract will be implemented in a way that will be optimized for minimum costs and computing power.

- **Objective 1: Optimizing Smart Contracts for Low Gas Consumption**
  The goal is to create a decentralized, open, and secure election system via the application of blockchain technology and smart contracts, with a gas optimization rate of about 33% and thus lower operational costs. It will be built such that the entire process of voting, from casting the votes to counting them, becomes more efficient, scalable, and economically feasible. In addition, the model is designed in such a way that there are zero costs incurred by the voters, with the costs being taken care of by the relevant authority.

- **Objective 2: Proposed Blockchain E-Voting System**
  The other target would be the creation of a solid infrastructure to authenticate and verify voters through the use of blockchain-based technologies, such that the voting process would be open only to those who have been allowed to vote while protecting their privacy. In the context of using advanced cryptographic algorithms in the infrastructure, the purpose would be to strike a balance between privacy, trustworthiness, and security without sacrificing usability and accessibility.

1.4 Report Layout

The rest of the report is structured as follows: Chapter 2 discusses the technical background of the study. Chapter 3 reviews the relevant literature on the subject matter. Chapter 4 provides an overview of the methodology of the blockchain voting idea. Chapter 5 introduces the suggested blockchain e-voting system. Chapter 6 examines methods that would help optimize smart contracts to minimize gas expenses. Chapter 7 describes the prototype design of the e-voting application. Finally, Chapter 8 concludes the paper.

Chapter 2

Technical Background

2.1 Blockchain Technology

Starting from the creation of Bitcoin [11] in 2008 by Satoshi Nakamoto to address the issue of double spending in digital payment systems, Blockchain has evolved into a highly secure and revolutionary technology. Initially designed as the backbone for Bitcoin, Blockchain is now recognized as a foundational framework for various applications beyond cryptocurrencies. While Bitcoin, Ethereum [1], Hyperledger Fabric [2], and Solana [2] are some of the most well-known blockchain-based platforms, the technology itself is far more versatile. Blockchain operates as a distributed ledger, securely storing an ever-growing list of records called blocks. These blocks are sequentially linked, each containing its data, the hash of the previous block, and a unique cryptographic hash of its own. The first block of any blockchain, called the genesis block, sets the foundation for the chain.

These blockchains use one-way cryptographic hash functions; once information is hashed, it is impossible to recover the original information. Additionally, if a block of data changes slightly, the entire hash would change, and consequently, all the hashes from the succeeding blocks down have to be compromised. This characteristic makes it very difficult to alter blockchain data, hence maintaining integrity. Besides, the blockchain entries are spread on a decentralized network of peer-to-peer nodes. Therefore, The system is highly resistant to tampering and data loss. This redundancy ensures that transparency is realized because all the nodes that participate in the network access the same data. One of the most popular features of Blockchain is its ability to realize consensus in a decentralized environment. Distributed consensus protocols include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) [3], and Proof of Authority (PoA), all enabling consensus among the majority of nodes that a transaction is valid before it can be entered in the Blockchain. Such a consensus process eliminates the need for a central governing authority and ensures the system's integrity. Using public and private keys in blockchain technology brings transparency and security to the system. Public keys work like account numbers; one has a unique account number in the network, yet all users can access it. Private keys represent cryptographic signatures that authenticate a transaction and must be confidential. These keys, as a whole, provide legitimacy and help in gaining ownership during the transactions process. Private keys are the main keys that provide access and control to the public address; having access to the private key means total control over the account. In many blockchain environments, the use of smart contracts is seen, which can be referred to as computerized programs where the terms of the contract are embedded.

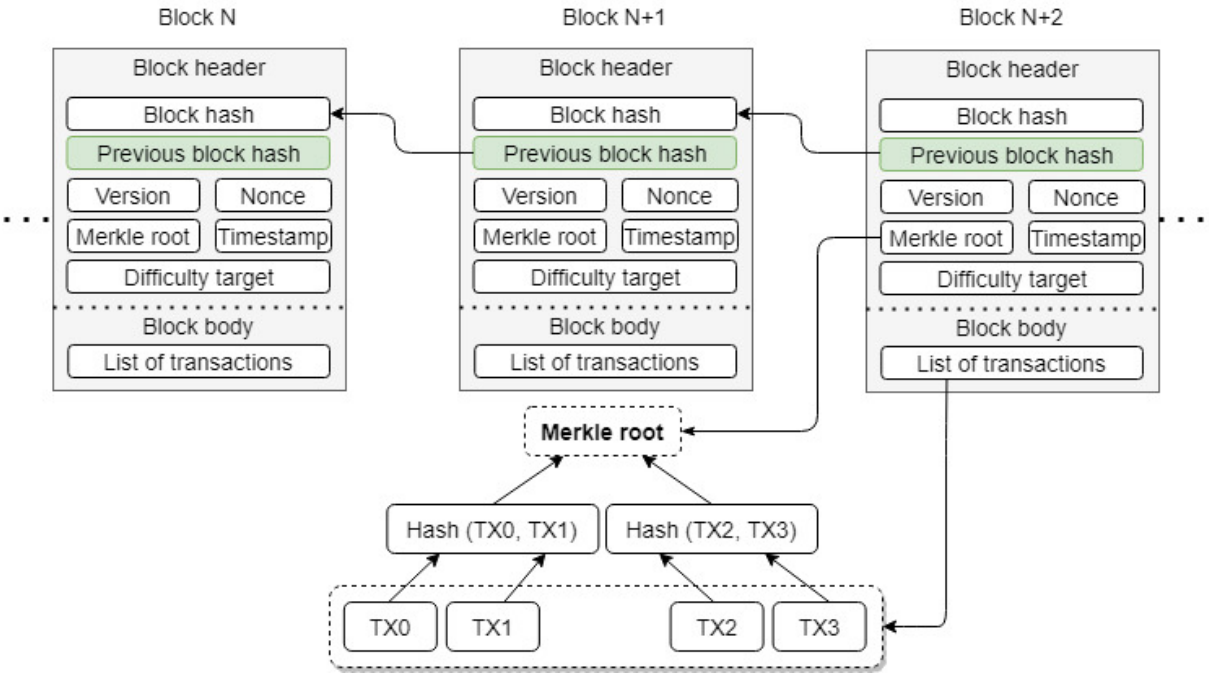


Figure 2.1: Block Architecture of a Single Block in Blockchain [2]

In spite of all the advancements made, there are a number of barriers that still pose hindrances to the extensive use of the technology. Some of the main challenges include the problem of scaling, huge energy usage, and lack of awareness among users. However, the continuous advancements in technology are increasingly overcoming such hurdles.

2.1.1 Architecture of Blockchain

As stated in various sources, blockchain technology [11] is known for having a distributed and decentralized [10] database design that helps in handling information among different nodes on the network without the need for any centralized control. It exhibits qualities such as immutability, transparency [9], and permanence of data, among others. In essence, blockchain technology refers to a connected series of blocks in a chain format that contains all parts needed for system consistency. Blockchain uses a peer-to-peer network design where nodes work together, validate each other, and have an entire copy of the ledger on their systems.
Each block in the Blockchain has a detailed shown in structure 2.1 designed to ensure security and connectivity:

1. **Header**

   - *Block Hash*: A unique identifier generated using cryptographic algorithms. This hash secures the block's data and serves as its digital fingerprint.
   - *Previous Block Hash*:Binds the current block to the previous block, hence creating an unbreakable chain. Any change to a block invalidates the hashes after it.
   - *Timestamp*: Captures the precise time of block creation, ensuring chronological order in the chain.

- Nonce: This is a nonce used to verify the validity of a block in proof-of-work systems.
- *Merkle Root*: A cryptographic hash of all transactions in the block, used to verify the transaction without accessing the whole data set.

2. **Body**
   - *Transactions*: The success of any blockchain application mainly depends on the consensus protocols that help to achieve a consensus on whether the block is valid or not among the various nodes. The ledger is mainly made up of the information that is deemed to be valid.
3. **Consensus Mechanism**
   The process of validation and inclusion of blocks to the blockchain depends on consensus algorithms like Proof of Work or Proof of Stake. They help achieve a consensus within the network and prevent any malicious attacks.
4. **Peer-to-Peer Network**
   Ledger copies maintained on all the nodes improve transparency, enhance security, and increase resilience in the network.

2.1.2 Advantages of Blockchain

Given its transformative potential, blockchain technology is positioned to become a critical component in the development of secure and efficient digital infrastructures going forward. :

1. ***Decentralization*** : Functioning as a peer-to-peer network without intermediaries such as banks or authorities, blockchain makes operations more cost-efficient and safer because it lacks single points of failure.
2. ***Transparency*** : In a distributed ledger, data can be accessed uniformly by all the nodes, thus building trust and creating visibility and traceability of transactions.
3. ***Security*** : To ensure the security of information, blockchain uses cryptography. Every block has the hash of the previous block, so any change will destroy the chain, ensuring integrity of the information stored in the blockchain.
4. ***Immutability*** : As information in blockchain is immutable, it cannot be changed or deleted after adding to the blockchain. This property makes it reliable because once the information is added to the blockchain, no one will be able to make changes to it. It is very useful when it comes to keeping records of some transactions.
5. ***Cost Efficiency*** : Through the removal of middlemen and automation of work process, blockchain technology can reduce costs greatly. The smart contract, which consists of pre-defined rules for execution, plays an important role in saving cost and time.
6. ***Improved Efficiency*** : Blockchain also facilitates process optimization through real-time data sharing and minimizes reconciliation efforts. For example, cross-border payment transactions that traditionally require days can be completed within minutes under this framework.

2.2 Etherum

Ethereum [2] is an open-source, decentralized blockchain that is very well known for its facilitation of smart contracts, which enables the efficient creation of DApps [1]. Its native digital currency, Ether (ETH), is one of the most used digital assets, making Ethereum the second most popular Blockchain in the world after Bitcoin. Besides its functionality as a cryptocurrency, Ethereum also allows the creation and trading of NFTs [4] and uses the ERC-20 token standard. This allows developers to develop tokens in a smart contract that can be sent to publicly defined addresses, permitting regulated and secure transaction implementation throughout the blockchain application.

Initially, Ethereum depended on the Proof of Work (PoW) consensus mechanism [11] for transaction validation and block mining. Mining is one of the primary blockchain processes that includes validating transactions, creating new blocks, and adding to the chain. According to the work cited below, miners [6] are important players in the network, who ensure the integrity of data and are rewarded for their contribution. The consensus algorithms, such as proof of work (PoW) and proof of stake (PoS), limit mining capabilities to the nodes only. Under PoW, miners with more computational power have a greater chance of winning while mining the transactions, but the approach requires much more energy to perform and is vulnerable to attacks. In PoS networks, nodes that stake some cryptocurrency to mine transactions are allowed, providing more reliable and efficient networks. Another notable feature of PoS is that miners can be penalized in case of any malpractice, thus adding to the credibility of the system.

2.2.1 Architecture of Etherum

Ethereum architecture [2], as outlined in the referenced article [2], represents a well-structured framework that enables the development of DApps and smart contracts with the objective of achieving decentralized operations and providing security and efficiency guarantees. The architecture 2.2 of Ethereum consists of several levels [11], elements, and interdependencies, all of which enhance the performance of the entire system. Ethereum operates in a decentralized manner, wherein each node holds an entire copy of the blockchain and takes part in the consensus and validation process. An essential part of the Ethereum platform is represented by the Ethereum Virtual Machine (EVM), which acts as a decentralized computing environment responsible for executing smart contracts. The EVM has a Turing-complete design, enabling computations in the system.

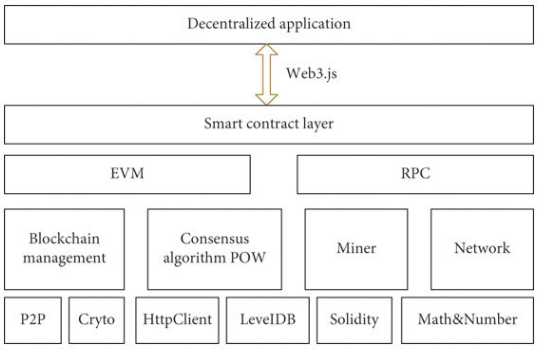


Figure 2.2: Structure of an Etherum blockchain node [3]

The smart contracts on the Ethereum blockchain are self-executing programs that implement the rules governing a contract through programming logic. The program runs on its own based on the pre-set rules. Its benefit is that this framework ensures trustless trades because we no longer have an intermediary to guarantee that both parties will comply.

The blockchain technology of Ethereum is made up of a 2 layer system. This consists of a layer of execution and layer of consensus. Whereas the execution layer is responsible for transaction management, the consensus layer guarantees agreement on the state of the blockchain among the nodes. This system helps the overall scalability of the Ethereum network. Adhering to the architectural tenets outlined above will facilitate interoperability and consistency in implementation. The key characteristics of the Ethereum blockchain architecture include decentralization, programmability, and scalability.

2.2.2 Advantages of Etherum

Several benefits characterize Ethereum, making it one of the most popular blockchain projects among both developers and end-users. Versatility of Ethereum is provided through its advanced capabilities and efficient architecture.

1. ***Decentralization*** : Since the platform operates on a worldwide network of nodes, there is little need for central servers, and the system is available all the time, without single points of failure or possibility of censorship.

2. ***Smart Contract Functionality*** : The platform allows the creation of self-executing contracts with predetermined conditions, thus promoting automation of transactions without intermediaries. Such contracts have many use cases, such as decentralized finance, logistics, and gaming.

3. ***Ethereum Virtual Machine (EVM)*** : Thanks to the Turing-completeness of the Ethereum Virtual Machine, developers can execute any type of computations, as well as develop DApps with arbitrary logic.

4. ***Transition to Proof of Stake (PoS)*** : Ethereum 2.0's shift to PoS reduces energy consumption, making the network environmentally sustainable. PoS also enhances security by penalizing malicious actors and rewarding honest validators.

5. ***Interoperability*** :Ethereum allows interaction and coordination with the blocks of other networks, providing better opportunities for developing decentralized technologies.

6. ***Security*** : Decentralization of Ethereum and PoS make it less vulnerable to external attacks, including the possibility of 51

7. ***Scalability Improvements*** : Through future upgrades like sharding and rollups, Ethereum hopes to become more scalable, reducing transaction fees and increasing throughput.

2.3 Smart Contracts

As mentioned above, the key operational concept of smart contracts [8], according to previous research, is referred to as deterministic logic, which means that a certain transaction or action is carried out once the predefined conditions have been met. In case of meeting such conditions, the transaction will be verified by all nodes of the blockchain network. It should be noted that each node acts independently, which helps to prevent any interference of a third party into the transaction process since smart contracts are executed in an absolutely autonomous manner.

The execution of smart contracts usually involves trigger mechanisms coded into the smart contract itself. For instance, a blockchain-enabled voting system might feature a smart contract capable of automatically tallying votes and generating results, hence maintaining integrity and transparency [6]. Smart contracts can also communicate with other technological systems, such as APIs, and AI to support advanced functionalities making them feasible in many sectors including secure and reliable voting systems. The Solidity programming language is an optimized and specialized programming language used to develop smart contracts in Ethereum network. The language borrows elements from various programming languages, providing a systematic syntax for blockchain programming.

The architectural [9] structure of Solidity conforms to the Ethereum Virtual Machine (EVM). The EVM runs the compiled bytecode of smart contracts in a uniform way throughout the nodes of the network. Scientists and developers use Solidity to perform functions like verification of votes, control over access, and transaction handling. Solidity is capable of complex data structures such as mappings and arrays. Besides, Solidity provides options like decreasing memory space and choosing more efficient data structures and loops in order to optimize the cost of execution known as gas efficiency. Gas optimization is crucial in scaling since it can minimize the costs of implementing contracts. Low-level operations, custom modifiers, and libraries allow Solidity code to be modularized. Therefore, gas efficiency can not only minimize the costs but also increase scalability and accessibility, which is crucial in blockchain-based voting systems as each transaction involves paying some fee to the network. Therefore, smart contracts and Solidity are, in reality, the technological base of blockchain-based voting systems with a good foundation for making voting processes transparent, efficient, and tamper-proof.

2.4 E-Voting Systems

An e-voting system, or electronic voting [2], uses electronic technologies to cast and count votes in elections. This system is designed to make the voting process more efficient, secure, and accessible while preserving the integrity of elections. It has different components, such as voter registration, casting of votes, verification of votes, and tabulation of results, all done electronically. It makes it easier for voters who are far away or have disabilities to vote. The incidence of human error is reduced, and counting is sped up. Blockchain technology or cryptography also makes it hard for malicious people to manipulate or interfere with the system.

2.4.1 Structure of E-Voting System

1. **Voter Registration** : In electronic voting (e-voting) systems, voter registration is generally conducted online through submission of identification data to confirm eligibility, which is stored securely for verification purposes.

2. **Vote Casting** : Votes are cast electronically via secure interfaces such as websites or mobile applications, where voters select candidates or options; selections are then securely recorded.

3. **Result Tabulation** : The vote counting begins automatically after the closure of polls and usually helps in faster sharing of results compared to traditional techniques.

2.4.2 Security and Privacy issues in E-Voting System

Security and privacy are the main issues that need to be addressed when implementing electronic voting systems. Despite offering more convenience and wide availability, electronic voting systems are vulnerable to several cyber-attacks that can affect the credibility of the entire process.

1. ***Cyberattacks*** : Despite being more convenient and available to many voters, such systems are vulnerable to cyber attacks that include hacking, malicious attacks, and even Distributed Denial of Service (DDoS) attacks that can influence the election results.

2. ***Data Privacy*** : Preservation of voters' privacy and protection of votes without connecting them to any voters is another important aspect since breaches lead to lack of trust that can influence voter turnout.

3. ***Authentication*** : Inadequate authentication processes, which include use of passwords or biometrics, expose the system to possible intrusions. Hence, the use of two-factor or multi-factor authentication is necessary for better results.

4. ***Data Integrity*** : It is also necessary to protect votes from interference during transmission and transfer using blockchain technologies to make sure that the data will not be altered in anyway.

5. ***System Vulnerabilities*** : Unfixed software or weak security measures can pose great risks for the security of the process.

2.5 Blockchain and Smart Contracts in E-Voting Systrem

There are several approaches to using blockchain technology for voting processes to increase transparency and minimize chances of manipulations. Most blockchain-based systems utilize smart contracts to record votes and perform counting, which increases accuracy and impartiality of elections. Due to the distributed [4] and immutable [9] nature of blockchain technology, this method allows minimizing the involvement of intermediaries in the process and securely storing data about the voters and their ballots. It should be

mentioned that voters do not pay for the use of this technology directly; the expenses related to its implementation, such as transaction costs and deployment fees, are covered by the election committee.

Voter identity [11] is still the system's core. To validate each vote, individuals must identify with a government-issued ID. Several studies have considered the best attributes of a voting system. These attributes include verifying that voters are eligible, preventing double voting, maintaining voter privacy [9], ensuring fairness in the process, and ensuring that all valid votes are counted. The vote cast must be verified by the voter that it has indeed been cast and recorded. Blockchain can make the system more transparent and secure, but challenges remain, such as coercion, which can occur even with the protections of the technology. In Electronic Voting Systems (EVS) [3], the problem of receipt-freeness—where voters cannot show how that voted—depends on trusted third parties. However, Blockchain can lessen the need for these third parties by securing the whole voting process. Another key point in blockchain voting systems is to keep costs low while getting more people to vote. Such a blockchain voting system can include more people and reduce barriers to participation as transaction fees for voters are zeroed. The organizing committee can cover all the costs.

2.6 Cryptographic Measures

Cryptography is vital in securing electronic voting (e-voting) systems by ensuring votes' confidentiality, integrity, and authenticity. Several cryptographic techniques are employed to protect sensitive voter data and prevent malicious attacks.

1. ***Encryption*** : Encryption is used to protect the confidentiality of votes. When a voter casts a vote, it is encrypted to ensure that no one, including election officials or hackers, can read or alter it during transmission. Symmetric and asymmetric encryption methods.

2. ***Digital Signatures*** : Digital signatures ensure the authenticity and integrity of the vote. When voters cast their vote, it is signed with their private key, verifying their identity and ensuring the vote has not been tampered with.

3. ***Hashing*** : Hashing ensures data integrity by converting data into a fixed-length string (hash). In e-voting, the vote is hashed and stored in a blockchain or secure database. If any part of the vote is altered, the hash value changes, making tampering easily detectable.

4. ***Zero-Knowledge Proofs (ZKPs)*** : ZKPs allow for verification of vote validity without revealing the content of the vote. This is important for preserving voter anonymity while ensuring the vote is legitimate.

5. ***Homomorphic Encryption*** : This allows for processing encrypted votes without decrypting, ensuring privacy during tallying while enabling accurate results.

2.7 Smart Contract Cost Optimization

The project focuses on cost optimization of the e-voting system [5] that promises to provide high security and operational efficiency. It mainly focuses on reducing costs in-

curred during developing and deploying a secure and efficient voting platform. It reduces server costs while increasing the system's availability by spreading data over multiple nodes. Besides this, smart contracts also provide voting automation through verifying and counting votes, eliminating human interference and reducing the costs associated with administration and labor. Scalability [6] is needed to deal with millions of transactions without escalating costs. Cloud architecture self-tunes towards the dynamic resource requirement with minimal cost escalation. Cryptographic technologies combine optimum security measures with cost by encrypting and hashing, protecting data against unauthorized alteration, and not spending expensive money on periodic external audits. Besides these concepts, the design and the structure of the smart contracts affect a lot in the cost efficiency. For example on the Ethereum's blockchain, each of the transaction executed on the blockchain requires the gas value according to the complexity. In the words of software engineers, optimization techniques like skipping non-essential computation, using appropriate data structures like map instead of array in order to have an O(1) search complexity, excluding high-memory intensive operations etc. Module contracts systems which move frequently changed codes out of chain (cite:ct4) or use proxy would minimize deployment cost and also the cost of interaction with smart contracts. Batched transactions include bundling of transactions offline into one online transaction so that the total gas consumed is reduced.

Chapter 3

Optimizing Smart Contracts for Low Gas Consumption

3.1 Background

These are self-executing computer protocols implemented within the blockchain framework, especially the Ethereum network, designed to facilitate the performance, validation, and enforcement of virtual agreements. The immutable and transparent nature of these protocols offers benefits associated with trust, dependability, and automation. Nevertheless, for these protocols to perform their functionalities, computing power is consumed in terms of gas and compensated in the form of the network's indigenous coin like Ether on Ethereum. Gas serves two purposes, namely, to reward validators for performing computations and prevent exploitation of the network's computing power.

The price of gas depends mostly on the complexity of computations and the usage of the memory space required for a particular contract. Since all smart contracts run on-chain, architectural optimization becomes important in order to minimize gas fees, which in turn increases cost-effectiveness and scalability. Poor coding leads to expensive transaction fees that limit the useability of the system. With the increase in popularity of dApps and varying prices of gas, optimization becomes crucial for both developers and users. There are several elements that affect the price of gas such as choices regarding data structure, memory usage, looping, interactions between contracts, and opcodes. Writing to the blockchain's memory requires higher fees compared to reading. Modifications made to dynamic data structures such as arrays and mappings may significantly raise the cost of gas.

With the increase in applications based on the Ethereum blockchain network, especially in critical sectors like online voting systems, there is an urgent need for efficient and effective smart contract development. The problem of gas optimization is one of the major issues that must be addressed in this regard, since it affects the cost of transactions and scalability. The existing solutions to this problem include GASOL, SoliS, and SmartChecker, which utilize heuristics, symbolic techniques, and static code analysis to detect inefficient code patterns.But the above approach either may generate unstable optimization, be contract specific, utilize additional computing power or restrict the developer autonomy. To alleviate the problem, this paper offers a new framework named SOPES Tool (Smart Optimizer for Ethereum Smart Contracts) as shown in Figure 3.1.

3.2 Motivation

With the advent of Dapps and with the increased implementation of blockchain technologies into diverse sectors, smart contracts become an essential element for secure computation. In contrast with the other benefits that they offer, one of the main hindering factors to their broader adoption in particular networks like Ethereum, is the unpredictable cost in gas for executing a smart contract. A more complicated contract, a transaction with significant computation, interaction with numerous nodes may end up with high gas costs.

It's not only the convenience problem, but it has to do with user experience, accessibility, and the business model. Gas fees play a considerable role in the operational cost of applications in areas where demand is extremely high, such as in DeFi apps, electronic voting platforms, supply chains, token-based economies, and others. At times of congestion, the costs associated with the process may be prohibitive, prompting the developer to weigh functionality against cost considerations. For blockchain applications in the public sector, including the use of e-voting, energy distribution, and digital identities, cost optimization becomes imperative in order to achieve scalability and judicious use of resources.

There may not be any existing methods that have standard or automatic procedures for reducing gas usage. Many tools are provided for writing efficient contracts, but most of these techniques involve a lot of manual work, expert knowledge, and experimentation. At the same time, there needs to be a careful balance between the efficiency and other factors such as correctness and security. Therefore, the motivation for this report is driven by the urgent need to:

- Reduce financial barriers to smart contract adoption through systematic gas optimization.
- Enhance user experience by lowering transaction costs.
- Offer developers tangible feedback and automated tools to simplify the optimization process, without impacting functionality or security.

In this research, we aim to investigate and derive efficient gas optimization methods to make smart contract systems more practical, cheap, available and more easily adoptable in the normal digital structure.

3.3 Related Works

The Ethereum platform is one of the best-known blockchain systems due to its ability to incorporate smart contracts that have the property of Turing completeness, which allows for DApps [12] to perform functions independently without any third party. The EVM [7] supports these smart contracts using computing power measured in gas.Execution of smart contracts incurs costs based on opcode execution [10], data storage [4], and contract complexity [11], and hence gas optimization is an important line of research. Various methodologies and optimization models minimize gas costs and optimize execution efficiency while ensuring contract integrity.

Existing gas optimization tools have introduced various techniques intended to lower computational loads. GASOL [10], a heuristics-based optimizer, uses formal verification

Tools	Loop Summary Optimization	Dynamic Optimization	Variable Storage Optimization	Memory Calling Optimization	Syntactic Modifier	Variable Packaging	Mapping Array Creation	Remove inefficient code	Summary of optimization
BlockSim [7]	✓	×	✓	×	×	×	×	×	×
TBA [12]	✓	✓	×	×	×	×	×	×	×
ESCAT [5]	✓	✓	×	×	×	×	×	×	×
sOptimize [11]	✓	×	×	×	×	×	×	×	×
SAFEVM [10]	✓	✓	×	×	×	×	×	×	×
SOL [4]	✓	✓	✓	×	✓	×	×	×	×
SolOSphere [9]	✓	✓	✓	×	✓	×	×	×	×
GaSaver [6]	✓	✓	×	×	×	×	×	×	×
GASOL [8]	✓	✓	×	×	×	×	×	×	×
SOLIS [13]	✓	✓	×	×	×	×	×	×	×
Proposed SOPES	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 3.1: Comparison of Features in Gas Optimization Tools

techniques to detect inefficiencies and refactor contracts to minimize gas consumption. SoliS [4] leverages symbolic execution to analyze smart contract logic, detect unnecessary computations, and optimize storage allocation. SmartChecker [13], a static analysis tool, provides developers with diagnoses of gas-inefficient Solidity [11] patterns and recommends changes to improve gas efficiency. Other optimization techniques, discussed briefly in TABLE 3.1, involve loop summary optimization, which prevents redundant iterations through summarizing recurring calculations; dynamic optimization, which changes contract execution flows based on runtime information to reduce gas-consuming operations; and variable storage optimization, which reduces gas consumption by optimal management of contract state variables, favoring memory over storage [9] wherever possible. Though these tools yield varying degrees of gas reduction, it have increased costs due to increased execution times, added complexity, or limitations on applicability.

The proposed SOPES tool outperforms these current solutions by incorporating bytecode-level compression, dynamic opcode [6] restructuring, and storage-aware execution, providing a 33% savings in gas fees over conventional optimization tools. In contrast to prior models, which emphasize stand-alone optimization methods, it also incorporates static and dynamic analysis, providing complete contract refinement without compromising execution efficiency. By minimizing computational redundancies, state management

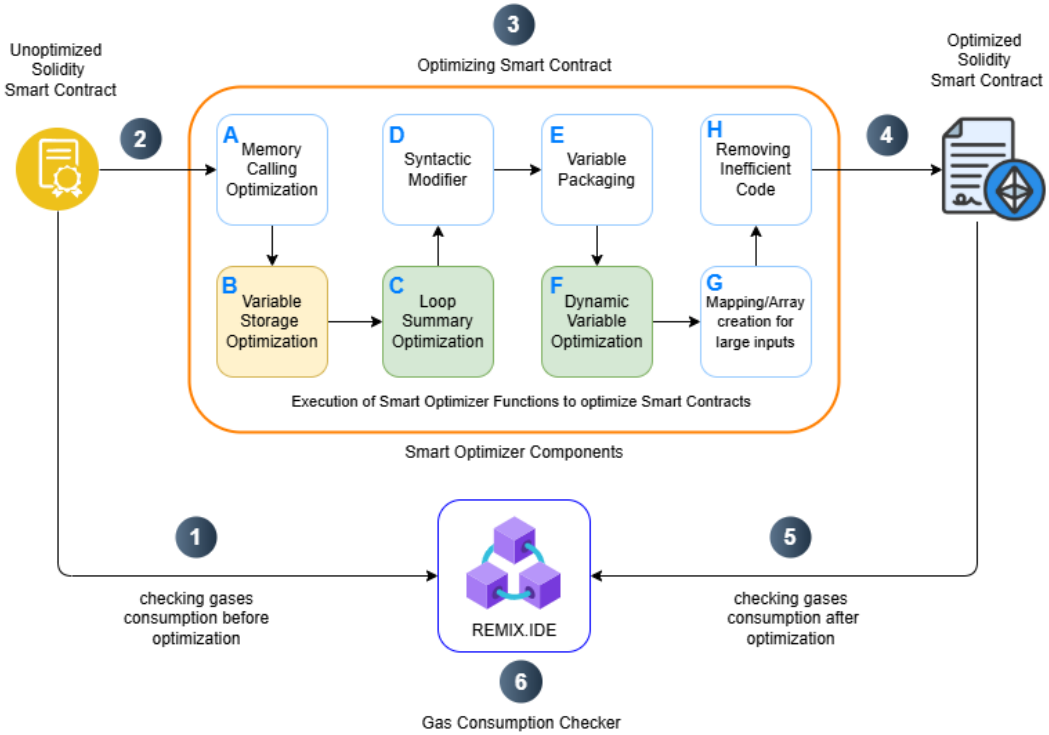


Figure 3.1: Architecture of SOPES (Smart Optimizer for Ethereum Smart Contracts)

optimization, and execution logic restructuring, the proposed solution considerably enhances transaction throughput and contract deployment expense. The integration of SOPES improves Ethereum's efficiency.

3.4 Architecture of SOPES (Smart OPtimizer for Ethereum Smart contracts

The proposed SOPES tool architecture is designed to integrate seamlessly with the existing Ethereum development ecosystem. It leverages REMIX.IDE—Ethereum's official web-based integrated development environment (IDE)—to simulate and monitor gas consumption across different deployment stages. The SOPES workflow is executed in a six-phase pipeline:

1. REMIX.IDE simulates the Ethereum on the testnet chain for gas consumption evaluation.

2. The proposed SOPES tool optimizes writing and deployment on REMIX.IDE (built by Ethereum developers) to record deployment, transaction, and execution costs in gas units.

3. SOPES follows eight algorithmic procedures, each addressing key optimization functionalities by memory calling, variable storage optimization, loop summarization, syntactic modifiers, variable packaging, dynamic variable optimization, mapping, and removing high-cost functions.

4. SOPES, tested again on REMIX, produces low-cost, gas-efficient, and optimized smart contracts.IDE.

5. REMIX.IDE executes the optimized version, logs gas costs, and compares it with the original.

6. Gas consumption is analyzed and tested on the testnet network on REMIX.IDE.

The SOPES framework overcomes such limitations using bytecode compression at bytecode level [6], rearranging opcode and realizing the operations at the time of runtime. Thus it costs much less gas than traditional techniques. Unlike approaches focusing on incremental enhancements, SOPES combines both static and dynamic analysis for effective contract optimization while preserving efficiency. A detailed explanation of the features and functionalities of SOPES components:

A. *Memory Calling Optimization*: One key approach used in SOPES is decreasing the usage of the costly storage methods provided by Ethereum's blockchain. Since memory access is relatively cheaper compared to the other two approaches, the use of memory for the transfer of transient data results in the reduction of costs. Using memory and calldata, especially for passing arguments to functions, helps to decrease gas costs.

B. *Variable Storage Optimization*: The SOPES ensure efficiency in the use of gas when declaring and accessing variables by optimizing the packing of variables and using efficient storage formats. The immutable nature of some variables ensures that they cannot be changed during execution, while several variables can be stored in one storage location.

C. *Loop Summary Optimization*: In order to decrease the load on computation in relation to the number of runtime loop iterations, SOPES utilizes mathematical and state caching methods to consolidate the impact of the loops before executing them. This will avoid duplicative computations, minimize unnecessary memory utilization, and optimize gas-hungry functions that often appear in smart contracts.

D. *Syntactic Modifier Optimization*: The tool also improves the optimization of function modifiers and loop structures by incorporating inline assembly and unchecked statements, resulting in more efficient control flow management. The result is contracts that consume less computational resources by removing unnecessary stack manipulations and checks.

E. *Variable Packaging*: The technique of data-type packing involves grouping several small data types such as uint8, bool, and uint16 in a single uint256 storage slot. The advantage of packing data types is that maximum use is made of the slot and gas consumption minimized.

F. *Dynamic Variable Optimization*:The SOPES framework optimizes the management of often-used variables through the use of memory and call information rather than contract storage. This technique utilizes lazy loading and in-place calculation methods for more efficient handling of conditional statements and loops.

G. *Mapping/Array Optimization*: Mappings are preferable to dynamic arrays for large databases due to the former's access time efficiency (O(1)). SOPES improves storage architecture through the transformation of declarations and access methods, minimizing the need for iterations and lookups.

H. *Remove Inefficient Code*: The major advantage of SOPES is that it removes the unnecessary or outdated coding sections, such as extra conditionals, unnecessary state variables, and repeated functions. It replaces the repeated looping process on the blockchain with batching, which increases efficiency and reduces cost.

I. *Optimization Summary Generator*: Lastly, the SOPES software includes a novel optimizer summary that produces a readable API result showing the effect on gas consumption caused by each change. The diagnostic utility allows developers to conduct a line-by-line analysis, helping them make decisions about the benefits vs. costs of adopting best practices.

In terms of testing its effectiveness and ability to scale, the SOPES framework was used as part of the development process for a blockchain-based voting system. Through its optimization capabilities that include memory and storage management, loop summarization, and bytecode restructuring, the use of SOPES resulted in less gas being consumed during the deployment and execution of contracts. As a result, it became possible to cast votes, perform identity checks, and track votes efficiently while reducing the costs involved.

3.5 Results

The effectiveness of SOPES in terms of lowering the amount of gas usage has been proven through extensive benchmarks of SOPES using existing optimization solutions such as GASOL [10], SoliS [4], and SmartChecker [13]. The findings show that SOPES lowers gas fees by about 33%, which means that SOPES outperforms previous solutions in the sense that improvements were only marginal at best. The analysis is carried out by considering the different types of gas used by smart contracts, as well as bytecode optimization, opcode optimization, and dynamic variables management. It was found that there is significant improvement in the use of SSTORE [4] and SLOAD [8] operations.

The performance assessment, as illustrated in the comparative TABLE 3.2, 3.3, 3.4 and in Fig 3.2, highlights the superior efficiency of proposed SOPES optimization tool.

The contracts optimized using the SOPES methodology have shown an obvious decline in their transaction execution costs especially in the cases where loop operations, function modifiers, and storages are used intensively. Contrary to existing optimizations that handle the problem from a one-sided perspective, SOPES offers a comprehensive methodology that seeks to solve inefficiencies from both the source code level and the bytecodes level [6]. The removal of unnecessary function calls, storage changes, and bad management of variables makes it possible to reduce the gas and increase the transaction execution speed. Besides, reorganizing mappings and arrays makes sure that there are no expensive loop operations since constant-time lookup is possible. Graphical evidence also supports this claim.

Through the incorporation of loop summary optimization, dynamic opcode manipulation, and optimized use of memory space, SOPES shows itself to be scalable, economical,

Contract	Original	Optimized (GASOL)	Saved (GASOL)	Optimized (SOPES)	Saved (SOPES)	Difference
Bubble Sort	519,024	534,594	(-15,570)	406,063	112,961	128,531
Calculator	1,124,579	1,158,316	(-33,737)	638,095	486,484	520,221
If-else	1,015,968	1,015,968	—	813,763	202,205	202,205
Prime Checker	782,616	813,920	(-31,304)	490,717	291,899	323,203
Factorial	889,698	907,491	(-17,793)	354,345	535,353	553,146
ERC-20 Token	1,566,786	1,528,453	15,667	1,233,917	332,869	348,536
Yield Farming	1,044,805	1,086,597	(-41,792)	823,060	221,745	263,537
Staking	818,553	818,553	—	593,381	255,172	255,172
Endless Loop	149,582	157,061	(-7,479)	52,442	96,148	103,627
String Concat	515,585	451,364	25,779	397,607	117,978	143,757
2D Array Search	382,850	390,507	(-7,657)	306,979	75,871	83,528
Selection Sort	491,064	505,795	(-14,739)	389,375	101,689	116,428
Insertion Sort	633,442	639,776	(-6,334)	502,966	130,476	136,810
Merge Sort	603,688	621,798	(-18,110)	481,834	121,854	139,964
Quick Sort	487,964	492,843	(-4,879)	387,601	100,357	105,236
Sum of Arrays	439,083	452,255	(-13,172)	292,080	147,003	160,175
Palindrome	721,828	736,326	(-14,436)	25,475	335,936	410,789
Square Num	342,302	239,649	9,217	173,319	57,113	66,330
Matrix	423,252	423,252	—	155,371	267,881	267,881
KYC Verify	1,150,442	1,230,972	(-80,530)	761,054	389,388	469,918
Avg Gas Saved				**74,929**		

Table 3.2: Comparison of Gas Optimization Tools for Deployment Cost

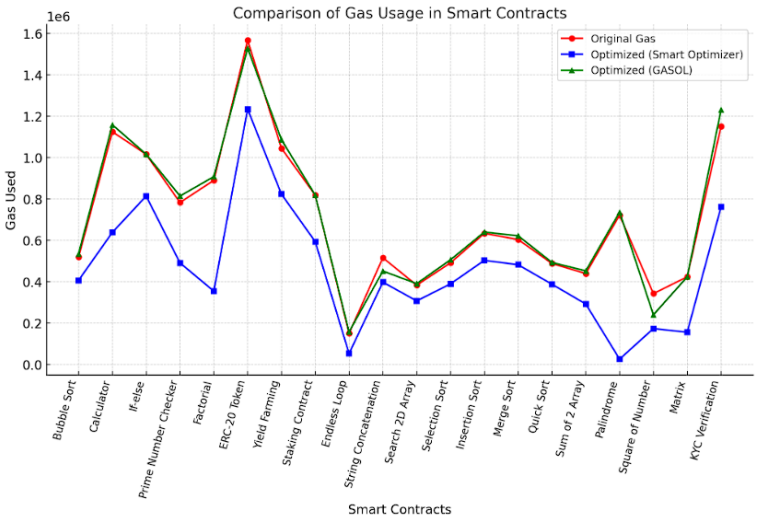


Figure 3.2: Comparison of Different Models with proposed SOPES Tool

and better performing in relation to smart contracts. Studies reveal that traditional optimization strategies are capable of reducing gas payments by 5%–10%, while SOPES is known to bring down these payments by up to 33% as shown in Fig. 3.2.

Contract	Original	Optimized (GASOL)	Saved (GASOL)	Optimized (SOPES)	Saved (SOPES)	Difference
Bubble Sort	451,325	4,60,350	(-9,025)	352,034	99,291	1,08,316
Calculator	9,77,894	10,17,009	(-39,115)	5,54,865	4,23,029	4,62,144
If-else	8,83,450	8,83,450	—	7,16,315	1,67,135	1,67,135
Prime Checker	6,80,535	7,21,367	(-40,832)	4,26,710	2,53,825	2,94,657
Factorial	7,73,650	7,81,386	(-7,736)	3,08,126	4,65,524	4,73,260
ERC-20 Token	13,62,422	13,89,670	(-27,248)	10,62,690	2,99,732	3,26,980
Yield Farming	9,08,526	9,53,952	(-45,426)	7,08,651	1,99,875	2,45,301
Staking	7,11,785	7,11,783	(-9,104)	45,586	84,485	93,589
String Concat	4,48,334	4,66,267	(-17,933)	3,49,702	98,632	1,16,565
2D Array Search	3,32,913	3,42,900	(-9,987)	2,66,331	66,582	76,569
Selection Sort	4,27,012	4,39,822	(-12,810)	3,55,978	71,034	83,844
Insertion Sort	5,50,819	5,56,327	(-5,508)	4,54,753	96,066	1,01,574
Merge Sort	5,24,946	5,35,444	(-10,498)	4,18,198	1,05,960	1,16,458
Quick Sort	4,24,316	4,28,559	(-4,243)	3,39,453	84,863	89,106
Sum of Arrays	3,81,811	3,89,447	(-7,636)	2,53,982	1,27,829	1,32,072
Palindrome	6,27,676	6,46,506	(-18,830)	3,03,021	3,24,655	3,43,485
Square Num	2,30,375	2,72,397	(-42,022)	1,56,293	44,082	86,104
Matrix	3,68,045	3,68,045	—	95,905	2,72,140	2,72,140
KYC Verify	10,00,384	14,18,448	(-50,019)	6,61,786	3,38,598	3,88,617
Avg Gas Saved			**73,318**			

Table 3.3: Comparison of Gas Optimization Tools for Execution Cost

Contract	Original	GASOL Opt.	GASOL Saved	SOPES Opt.	SOPES Saved	Diff.
Bubble Sort	3,69,803	3,77,739	(-7,936)	2,84,749	85,054	92,990
Calculator	8,60,494	8,94,913	(-34,419)	4,67,097	3,93,397	4,27,816
If-else	7,70,828	7,70,828	—	6,20,103	1,50,725	1,50,725
Prime Checker	5,82,611	5,41,828	(-40,782)	3,46,584	2,36,027	2,76,809
Factorial	6,56,052	6,23,393	(-6,560)	2,34,350	4,21,702	4,28,262
ERC-20 Token	12,01,098	12,25,119	(-24,021)	9,36,857	2,64,241	2,88,262
Yield Farming	7,94,820	8,34,561	(-39,741)	6,12,012	1,82,808	2,22,549
Staking	6,13,329	6,13,329	—	4,23,198	1,90,131	1,90,131
Endless Loop	71,521	75,812	(-4,291)	24,382	47,139	51,430
String Concat	3,68,890	3,83,645	(-14,755)	2,84,046	84,844	99,599
2D Array Search	2,57,989	2,65,728	(-7,739)	2,03,812	54,177	61,916
Selection Sort	3,46,984	3,57,393	(-10,409)	2,80,916	66,068	76,477
Insertion Sort	4,62,097	4,71,339	(-9,242)	3,72,809	89,228	98,470
Merge Sort	4,31,952	4,40,591	(-8,639)	3,33,852	98,100	1,06,739
Quick Sort	4,31,952	4,40,591	(-8,639)	3,33,852	98,100	1,06,739
Sum of Arrays	4,31,952	4,40,591	(-8,639)	3,33,852	98,100	1,06,739
Palindrome	4,31,952	4,40,591	(-8,639)	3,33,852	98,100	1,06,739
Square Num	1,36,581	1,43,410	(-6,829)	1,01,070	35,511	42,340
Matrix	3,46,841	3,46,841	—	94,301	2,52,540	2,52,540
KYC Verify	3,46,841	3,46,841	—	94,301	2,52,540	2,52,540
Avg Gas Saved			**72,124**			

Table 3.4: Comparison of Gas Optimization for Execution Cost

Chapter 4

Proposed Blockchain E-Voting System

A blockchain-based electronic voting system [7] proposes a secure, transparent, and economically feasible approach for contemporary electoral processes by leveraging advances in blockchain technology combined with smart contracts. This model addresses core issues surrounding traditional voting methods, such as security, voter authentication, economic viability, and outcome disclosure, without compromising accessibility and usability.

The process would begin with identity authentication to ensure that only eligible voters participate, which means that each voter must be authenticated using their government-issued identification documents. After verification, unique credentials are given to voters to store on a blockchain. Added security in the voting procedure, including OTP verification, ensures that only verified voters can vote without fraud and unauthorized access. It ensures that operation is efficient with scalable levels, making the tasks manageable for a significant population of users. Since there are no barriers to the participation process, voting is free, ensuring that no voter incurs losses by voting. After each vote, the member is given a receipt, just as in the case of everyday transactions.

This is based on the security, decentralization, and immutability provided by the Ethereum blockchain [5]. Such a system ensures anonymity by the voters but keeps outcomes of votes transparent by using advanced cryptic methods [4], zero-knowledge proofs [8], and homomorphic encryption. Votes get counted in real time, allowing for live results observation and maintaining voter anonymity at the same time. Such a system of blockchain-based electronic voting not only re-engineers voting process but also ensures its security, transparency, and efficient functioning so that this technology can be scaled in the future.

4.1 Background

The research work under study seeks to explore the development and deployment of an electronic voting system (e-voting) [ct6] that uses enhanced smart contracts along with modern web technologies that integrate secure and tamper-proof voting processes into the blockchain. The fundamental idea is to overcome current voting systems (paper based and centralized digital systems) by implementing the blockchain technology.

Conventional electoral processes may have problems like lack of transparency, hackable, manipulatable, ineffective at counting, unable to include all possible voters, costly. Whereas, there are numerous benefits to use electronic voting systems.However, they pose several risks and problems, such as data security issues, voter verification, privacy concerns, and reliance on centralized authorities.

In order to solve these problems while maintaining the validity of electoral processes in the real world, the proposed system makes use of blockchain technology as a decentralized ledger where recorded transactions are immutable, traceable, and resistant to tampering. Once a vote is entered into the blockchain, it becomes untouchable and cannot be altered.

4.2 Motivation

However, no matter what model a democratic society implements, there is one thing that makes it effective – the integrity and security of voting infrastructure. The traditional models of elections that used either paper ballots or centralized electronic voting proved their vulnerability, which included possibilities of voting frauds, technical difficulties, manipulation, and low access. All these factors show that voting process needs better solutions, which could guarantee more reliable and transparent outcomes.

Blockchain voting is one of the new solutions proposed to solve all of the above-mentioned problems. Blockchain technology provides a good solution for organizing voting as it possesses decentralization, immutability, and transparency, which are needed to ensure safe elections. Voting data saved on a distributed ledger that requires network-wide approval before any change occurs would provide a highly secure infrastructure for votes.

Despite all these benefits, there still are several limitations in implementing blockchain for voting, which include scalability issues, gas costs, and user interface concerns. Smart contracts play an important role as they would be responsible for enforcing the election rules within the blockchain. Nevertheless, inefficient smart contracts may cause high gas costs, which would make implementation difficult and less scalable. Thus, making sure that smart contracts do not consume too much gas is an important task in implementing blockchain voting solutions.

This report is motivated by the desire to:

- Enhance trust in electoral outcomes by eliminating reliance on centralized authorities.
- Prevent election fraud through immutable, transparent vote recording.
- Enable secure remote voting that expands accessibility to disenfranchised populations, such as those abroad or with mobility constraints.
- Reduce election costs by streamlining processes via smart contract automation.
- Provide real-time auditing without compromising voter privacy.

4.3 Related Works

A blockchain technology is one of the most recent innovations that have been considered a promising solution to some of the current problems related to modern voting processes. The characteristics of decentralization, immutability, and transparency have made blockchain technology a very promising tool for improving elections [10]. However, even though there is a lot of potential in e-voting technology, a range of issues remain, such as lack of efficiency [9], security, and accessibility issues. This part of the paper aims at discussing current research in this field.

Whether paper-based or electronic, traditional voting systems face several issues that limit their effectiveness and reliability [11]; public trust in these systems has been greatly diminished due to security issues such as vote manipulation, ballot tampering, and unauthorized access. In addition, the high costs associated with producing, distributing, and managing electoral staff have been a significant cost burden [12]. Accessibility is also a concern because logistical barriers deny those in remote areas, along with people with a disability, the right to cast their votes. Hence, such challenges require safe, transparent [7] yet cost-effective alternatives, leading the researchers to explore block-based voting systems.

Blockchain technology can attribute decentralization, security, and transparency to the voting system. The immutability ledger ensures that tampering and deleting the recorded votes are impossible. This virtually solves the common problem facing traditional systems [8]. Most importantly, Blockchain offers stakeholders a mechanism for auditing the voting without compromising confidentiality. Despite all these benefits, however, integration of blockchain technology in electoral systems has challenges like scalability [10], anonymity, and transaction fees that must be overcome for it to be a viable replacement.

The blockchain framework uses smart contracts as self-executing algorithms. An important part of the automation of electoral processes is through smart contracts, which automate several components: voter registration documentation of votes cast counting of votes cast. A significant reduction in human interference and, hence, a decrease in errors is achieved with increased operational efficiency. Moreover, smart contracts make the system more transparent because it applies predetermined regulations to all parties involved. However, existing implementations tend to have high gas fees in public blockchains, particularly Ethereum [10], and hence financially unviable for large-scale electoral processes. This study addresses this by finding optimized smart contracts and economically sustainable blockchain platforms.

Among initial significant contributions, Gautami Tripathi [7] proposed a blockchain-based voting system featuring a functional prototype and basic identity verification. Although this work demonstrates blockchain viability in voting, it lacks several essential elements, including cost-free voting, OTP-based authentication, support for multiple candidates per election, and optimization for smart contract deployment costs, which are vital for scalability.

Shafaq N. K. [12] proposed partial functionality; he allowed real time vote counting as a crucial transparency mechanism but failed to provide a working prototype, identity validation and authentication, which restricts the applicability. It doesn't provide features to vote for multi-candidates nor provides a vote receipt. Such characteristics hinder its usage for real world elections which require varied voting choices and confidence.

Maria-Victoria V. [5] demonstrated a practical application by implementing a system

Paper Name	Working Prototype	Cost-Free Vote Casting	Identity Verification	OTP Based Authtentication	Ethereum Based System	Optimization of Smart Contract Deployment Cost	More than 2 candidates for single poll	Proof Of Vote Receipt	Live Vote Count
Gautami Tripathi. [7]	✓	×	✓	×	✓	×	×	×	×
Shafaq N. K. [12]	×	×	×	×	✓	×	×	×	✓
Maria-Victoria V. [5]	✓	×	×	×	✓	×	×	×	×
Said El Kafhali [11]	×	×	×	×	✓	×	×	×	✓
Tarik Chafiq [10]	✓	×	×	×	✓	×	×	×	×
Nabiluzzaman N. [4]	×	×	✓	×	✓	✓	×	×	×
Hajian B. [9]	×	✓	×	×	✓	✓	×	×	×
Our Proposed System	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 4.1: Comparison of Features in Blockchain-Based E-Voting Systems

in Ethereum with a working prototype. However, this system lacks features of sophisticated security mechanism such as OTP based authentication and identity validation, provides expensive smart contract execution, doesn't provide options for election beyond two candidates. Thus it is not efficient for multiple candidates in elections.

Said El Kafhali [11] developed a system using Ethereum. It supported live counting but lack a working prototype, security mechanism (authentication and identity validation). It also lacks the optimized smart contract costs, leading to increased running cost and less efficiency.

Tarik Chafiq [10] developed a working prototype of an Ethereum based system. Yet it lacks most of the advanced security and usability features, such as free voting, OTP authentication, vote receipt confirmation, multi-candidate voting, which affects its usability to real world election scenarios.

Nabiluzzaman N. [4] focused on smart contract cost and introduced identity verification. Still the system lacks working prototype, authentication and vote receipt proof. So cost efficiency can't guarantee a secure and advanced election without properly designed voting infrastructure and features.

Hajian B. [9] proposed a concept with cost-free voting and smart contract optimization to promote resource-efficient voting. But it misses critical features such as authentication and OTP based verification (to ensure voting by an individual only) and vote receipt proof, which will cause lack of trust.

The proposed system provides an all-in-one solution with a working prototype and free of cost voting, so as to remove monetary constraints. It has high security measures as we provide the feature of verification along with OTP verification to prevent hacking based on impersonation and unauthorized login. We utilize the Etherium network to leverage it to perform smart contract computations. Smart contract design are done in order to minimize deployment cost, through gas efficient mechanisms, performing calculations off-chain and reusing smart contracts.

Additionally, this system supports multi-candidate elections, making it more practical and realistic. Vote receipt proofs are included to increase transparency and trust on the part of the voters through the provision of proof that their votes have been properly registered. Live vote counting also ensures continuous oversight during the voting process.

It is necessary to identify the identity of individuals as a way to determine whether they are eligible to participate in elections or not. Previous researches have explored

various ways of doing so, but the problem with such processes is that they usually tend to pose privacy issues. Blockchain-based technologies like DIDs and ZKPs can be useful as they allow linking the voter's identity to a secure and private credential [11].

Cryptography can help in counting votes without revealing their identities through use of cryptographic tools such as homomorphic encryption [11]. Additional anonymizing procedures like ring signatures and mix-net protocol can be helpful to prevent voters from being linked with their ballots.

The characteristics of some of the most prominent voting systems on the blockchain technology platform have been compared in Table 4.1. The surveyed systems lack a complete range of required functionalities; in contrast, the designed system meets all the mentioned requirements, including secure verification, cost-effectiveness, multi-candidate support, instant voting counting, and generation of a receipt of votes.

Additionally, combining the credential issued through the blockchain network with official government identification allows it to be compatible with the current voter registry while retaining its security. The hybrid systems involving both traditional and blockchain voting systems allow for the inclusion of all kinds of voters, regardless of their technological accessibility.

This literature review highlights the revolutionary influence of the blockchain technology on voting systems while pinpointing the gaps that the proposed system will address. Currently, there is an acute necessity for innovative solutions that can effectively combine transparency, security, efficiency, and scalability in the election processes. The designed system has been developed to ensure technical robustness and social acceptability.

4.4 Methodology

The strategy for the implementation of an e-voting system based on blockchain and cost-effective smart contracts aims at creating a secure, effective, and user-friendly platform that overcomes problems associated with confidentiality, voter identification, accessibility, and the management of operation costs. The first phase involves the detailed study of both conventional and blockchain-based voting systems in order to reveal their vulnerabilities regarding security and anonymity.

In the system design stage, blockchain is used to provide the required transparency while ensuring the confidentiality of the processes involved using private or permissioned blockchains. Cryptographic tools like homomorphic encryption and zero-knowledge proofs ensure that votes can be verified without revealing the identity of the voters. Smart contracts are used to automate basic functions, such as voter registration and casting of votes, thus eliminating the need for manual procedures. DIDs are bound to government IDs for authenticating [10] the voter. Only those eligible voters can vote through these DIDs that are bound with government IDs. The decentralized identity framework handles fraudulent activities and potential double voting because it has legitimate governmental identification and safe storage of credentials on blockchains. This would provide online and offline access, accommodating voters with different degrees of technological access.

It has to be deployed on low-energy-consuming blockchain platforms. That can be done by using methods such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) [11]. In this manner, complete checking and testing for security can be guaranteed, and how it works is portrayed through the cost study. More importantly, getting feedback from all the participants is essential, and in this case, it is a viable solution for today's

elections.

4.5 Architecture of Blockchain E-Voting Proposed Solution

The blockchain-based e-voting system architecture proposed here aims at a secure, low-cost, user-friendly platform that uses low-cost and optimized smart contracts. The system can include several salient features such as identity verification, OTP-based authentication by voters, free voting, live counting of votes, proof of vote, and, most importantly, the robust capabilities of the Ethereum blockchain. It includes :

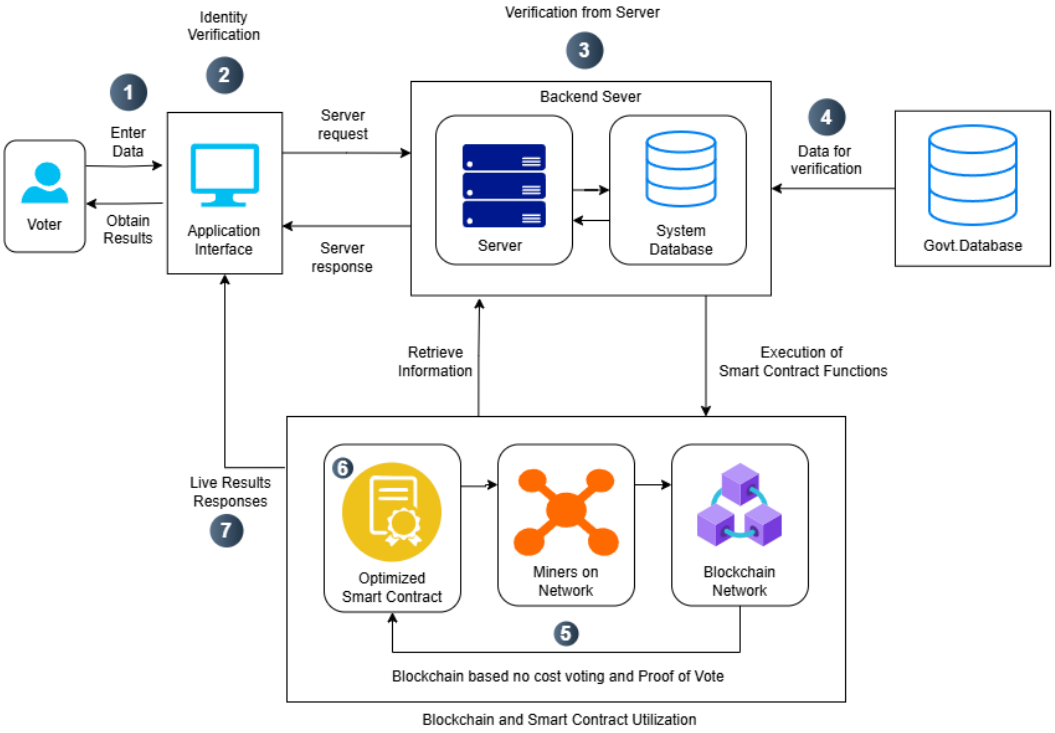


Figure 4.1: Architecture of Proposed Blockchain based E-Voting Solution

Now, with the help of Figure 4.1, explain the functioning of this Architecture of the Proposed Solution in brief:

1. ***Entering National ID Data*** : First, the voter can come to this portal and check their eligibility in the voting system, which can be verified using the National Database of the voter identity.

2. ***Identity Verification and OTP Authentication*** : The system provides voter eligibility and security through decentralized identity verification mechanisms. Once National ID is verified, voters are shown their credentials stored on the National Govt. Database and Blockchain. Lastly, an OTP authentication is done using the mobile number linked with the user's credentials in the database to double-verify the user and ensure that only verified persons vote.

3. ***Verification from Server*** The NodeJS server interacts with front-end requests to handle user inputs and process the required operations seamlessly. It can search the query in the MongoDB database to validate credentials, ensuring the provided information matches stored records. Additionally, it manages mobile number verification and OTP authentication requests, maintaining secure communication between the client and the database. This interaction ensures a smooth and secure user authentication process.

4. ***Data for Verification from Govt.Database*** : The MongoDB database can serve as an intermediary between the application and the government database to process requests efficiently when deployed in the real voting world. It can execute queries and retrieve relevant information from the government database based on user inputs. This process is securely carried out after verifying the user's mobile number to ensure authorized access, providing users with real-time information.

5. ***No-Cost Voting and Proof of Vote*** : Once the Verified Voter reaches the voting stage and finally votes freely without any payment, upon submitting a vote, individuals obtain a transaction receipt serving as verification, affirming that their vote has been accurately documented and tallied within the system and that generates a hashed value of the mix of user credentials and the party voted for into a single unique hash and can verify their hash in the live results.

6. ***Optimized Smart Contracts*** : Then, the smart contracts, the backbone of this proposed system, automate vital processes like cryptographically hashing the data, casting votes, and counting live votes, creating dynamically complex code and effective algorithms so that the smart contracts execute perfectly without overloading the Blockchain, thus providing an optimized smart contract that reduces the gases used in every transaction.

7. ***Ethereum Based System and Live Results*** : Implementation of a live results page that shows the final and live vote counting that can be verified using our smart contracts; hence, this proposed system can show transparency, security, and anonymity of users and votes, making it the most secure system ever, minimalizing the usage of gases making it economically feasible.

4.6 Identity Verification

Ideally, identity verification ct6 is important in any blockchain-based e-voting system because it would mean only eligible voters participate while attaining security and transparency. The process includes government databases verifying the identities and applying multi-factor authentication for greater reliability.

This authenticated the National ID on the government database. It operates as follows: once a voter initiates the process, he or she inputs the National ID that the system transmits to the government database to check for verification and complete security after getting confirmation about the matching details. The system forces the voter to create a mobile number associated with the relevant National ID in the government database for security on voter authentication. In this manner, it gets an assurance that a recorded mobile number is directly associated with the authentic identity being verified. The system formulates and sends an OTP to the voter's registered mobile device by comparing the

recorded mobile numbers with those in the database. In this process, the voter must give the received OTP directly to the system and verify it in real time. After that verification, the voter is redirected to the secured voting page. So, this multi-layered verification approach against impersonation and fraudulent voting only ensures that eligible voters participate while adequately protecting their privacy and personal data.

4.7 Consensus Mechanisms

The proposed blockchain-based e-voting system utilizes Ethereum's advanced consensus mechanisms to ensure security, transparency, and scalability [4]. Ethereum's transition from the energy-intensive Proof of Work (PoW) to the more sustainable Proof of Stake (PoS) makes it an efficient and secure platform for such critical applications. These mechanisms [11] safeguard the integrity of votes and prevent tampering.

PoS's validators are chosen based on the cryptocurrency to stake as collateral to ensure honest behavior. Verify and validate the transactions and any malicious activity that would lead to the loss of staked assets. The system is much more secure, yet the energy consumption is highly reduced compared to PoW [9]. This meets the modern standard of energy efficiency. This makes the system cost-effective and not harmful to the environment in large election deployments.

The DPoS can increase the functionality of the system. In a DPoS model, participants stake stakes in trustworthy delegates that serve as validators, increasing scalability and decreasing the time needed to process transactions. In such a methodology, efforts are made to achieve more balance between decentralization and performance to provide quicker access to e-voting experiences.

4.8 Scalability of System

The proposed blockchain-based e-voting system is designed for high scalability to accommodate large-scale elections. Utilizing Ethereum's decentralized infrastructure [10] with a Proof-of-Stake (PoS) consensus mechanism facilitates fast transaction finality alongside reduced energy consumption compared to traditional Proof-of-Work approaches.These capabilities ensure a scalable, low-cost, high-capacity system capable of supporting the large voter turnout needed without an overwhelming computational cost. Scalable smart contract implementations allow the automation of different election processes and the reduction of manual labor which are both capable of handling high transaction volumes necessary in larger scale elections. The modular system design permits relatively easy updates, the integration of different databases or functionality for different electoral conditions, and different locations. Decentralized identification is a part of this which contributes to a secure, scalable voter information system as well. By utilizing the distribution inherent in blockchain systems, this provides fault tolerance for the system as participation increase. This collective system is robust and scalable while remaining secure, efficient, and building user trust.

4.9 Integration with Traditional System

The system design comprises of a hybrid mixture between blockchain electronic voting and conventional mechanism for a phased migration process from existing voting systems to new generation ones [5]. In a hybrid mix of technologies, the transparency, integrity and immutability features are used together with efficiency of already established system. The migration process starts from voter registration process, wherein the registered voters is validated with their National IDs provided by respective countries verified from their central government database, users is then authenticated by verifying phone number along with one-time password.

4.10 Integration with Blockchain

There are advantages that arise from the integration of blockchain technology and smart contracts in electronic voting. Blockchain technology itself is a decentralized, immutable ledger and it protects the voting system against manipulation. Recording votes on the blockchain increases the transparency of voting by enabling an audit but maintaining the anonymity of the voters. Smart contracts can execute automatically pre-programmed tasks once predefined conditions have been met, automating election processes without the need for human intervention thus eliminating mistakes that might be produced by such intervention.

In the proposed architecture smart contracts are central to controlling significant elements of election processes such as, vote registration, casting of votes, counting of votes, and the final declaration of results. Smart contracts can authenticate if an individual meets stipulated eligibility requirements for participating in election process via their credentials or by the use of a One-Time-Password (OTP). By optimizing the smart contracts the gas usage is kept to the minimum hence making it feasible and secure.

4.11 Workflow of the Voting Transaction

An in-depth investigation was carried out within the existing literature concerned with e-voting, blockchain, smart contracts, in which particular focus was placed on improving the performance of digital voting systems. The majority of the research considered within this study was focused on developing cost-efficient and efficient smart contracts, crucial for enabling scalability and universal adoption of blockchain-based e-voting systems. The study additionally found that e-voting needed to be inexpensive and efficient. The existence of certain e-voting applications based on such technologies has already been recorded.

Two primary concerns were highlighted throughout the investigation. Firstly, methods were needed to lower the gas cost associated with smart contract execution. Secondly, robust systems for verification had to be integrated to minimise the potential for e-voting fraud. It is proposed that the presented e-voting platform attempts to address these concerns by leveraging low cost smart contracts, Ethereum technology, and a decentralized method of verification.

As far now through the implementation of this project, Figure 4.2 mentioned it shows the Login Page with a militaristic user-friendly interface that allows the user to connect to the blockchain network and then enter their National ID to verify it against the Local

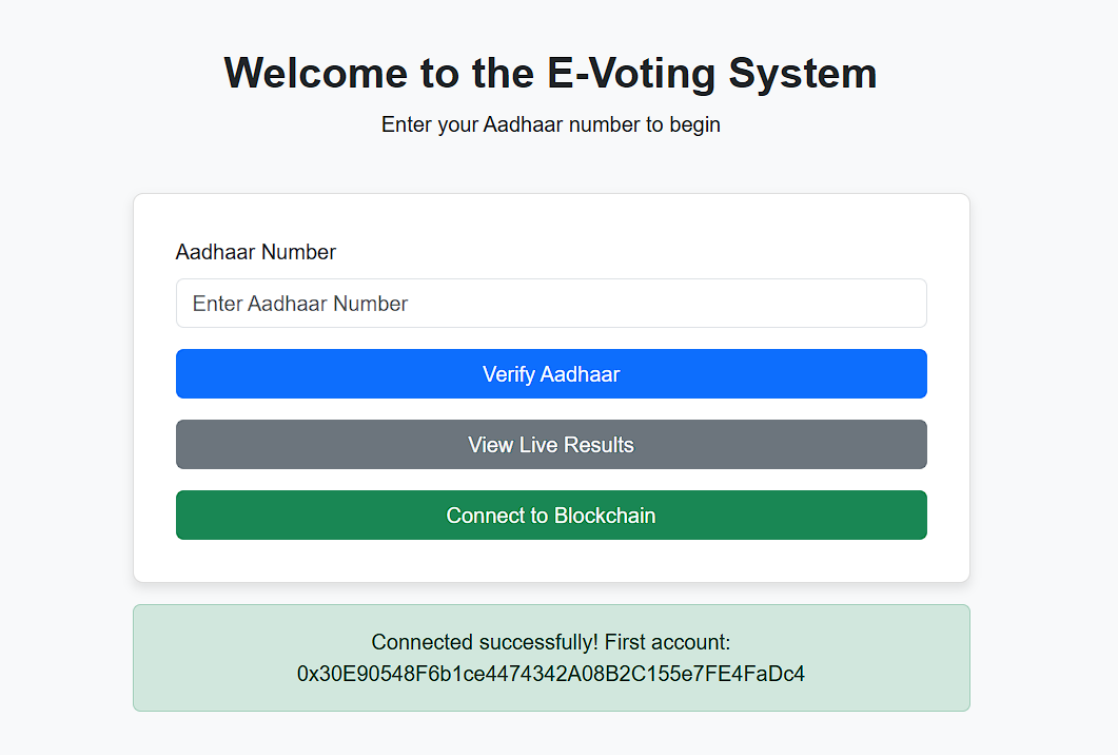


Figure 4.2: LoginPage of Proposed Blockchain based E-Voting Solution

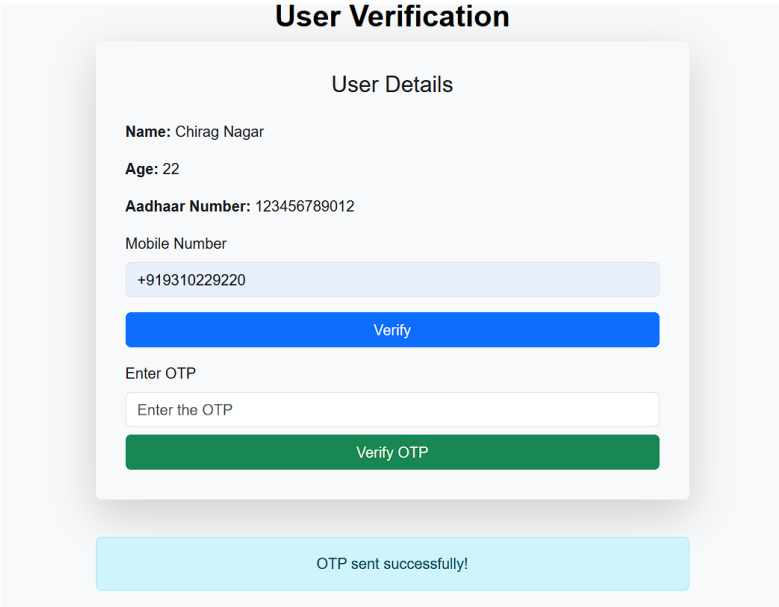


Figure 4.3: Verification Page of E-Voting Solution

Server and Govt. Database that contains the credentials to get verified to enter in the voting and in Figure 4.3, it shows the user verification page where the voter has shown its credentials that is voter's credentials which is being retrieved from the Govt. Database to show to the user for confirmation, then the User types the Verified Mobile Number linked with the National ID stored in the database. Once it gets matched, the system uses the Twilio API service to send an automated OTP message to the user's mobile number to get verified, and then it can proceed to the voter's Page.

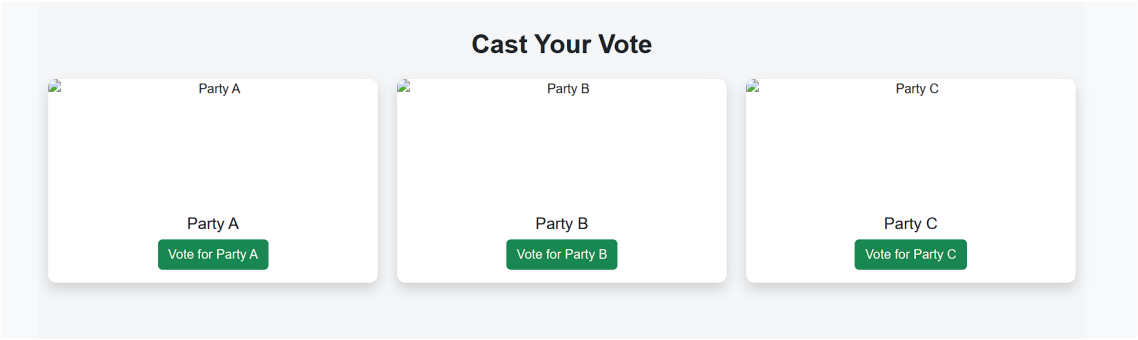


Figure 4.4: Voting parties

After User verification, voters can come to the voting page, where it decides which party to vote for from the given parties as shown in 4.4 Once the user votes, a cryptographic hash is generated using the SHA256 algorithm. This hash contains all the metadata of the user name, age, address, mobile number, national ID, and the party it voted for by multiple hashing as shown in 4.5 and there is a button to copy the hash

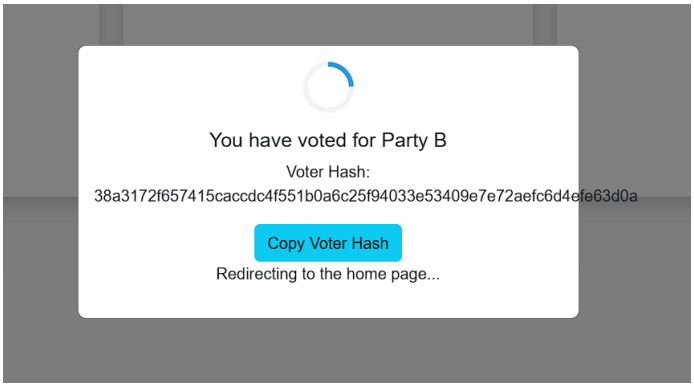


Figure 4.5: Hash Generation of Voted Party

and check the hash in the live Results Tab to verify that the vote is counted or not as shown in 4.6. The local blockchain network shows a vote transaction as a block in 4.7, completing the proposed solution ideologies.



Figure 4.6: Live Results Page



Figure 4.7: Transaction Hash and Block Genrartion in Blockchain

4.12 Results and Discussion

The developed blockchain-based e-voting system was successfully implemented and evaluated across multiple performance parameters, including transaction efficiency, execution cost, scalability, and system reliability. A key focus of this evaluation was the impact of smart contract optimization using the proposed SOPES (Smart Contract Optimization and Performance Enhancement System). Comparative analysis was conducted against several existing approaches, including works by Gautami Tripathi [7], Maria-Victoria V. [5], and Nabiluzzaman N. [4], to assess improvements in gas consumption and execution efficiency.

Experimental results show that the presented SOPES framework leads to a substantial reduction in gas consumption, by an average of nearly 145,000 gas per transaction. This means a savings of nearly 31% compared to un-optimized smart contracts and an additional 10-12% compared to currently available optimization tools. The resulting gas consumption is lower because of the more efficient use of memory, more compact variable representation, a better data representation scheme, and the elimination of unnecessary computational steps, all contributing to an increase in processing efficiency and thus decreased cost of computation. As a result the system is more feasible for large-scale deployment.

Not only are there considerable savings in cost, there are tangible improvements in the system's transaction throughput and speed. Optimizing the smart contract means a faster confirmation and validation time for each individual transaction, and therefore a lower duration for a user to place a vote. The implemented tool provided a better response and faster confirmation times than existing systems, especially during high transaction volume and heavy load. Moreover, the decentralized network topology ensures that validation for each transaction can occur in parallel, which scales up the capacity and stability of

the system for more voters.

Security and reliability were bolstered in two ways. First, blockchain's inherent features and cryptographic methods of hashing and asymmetric key encryption are used to secure the data from malicious tampering and ensure immutability. Secondly, optimizing the contract reduced the chance of inefficient, flawed code being responsible for system vulnerabilities.

The performance metrics including the savings in gas consumption by comparing the result with other methods are outlined in Table 4.2. It shows the benefits of using SOPES tool compare to others. It seems that SOPES can bring a promising efficiency along with its utilization.

We show comparison of gas savings ratio among different tools in Fig. 4.8. From this figure, we can obviously see that our SOPES approach consistently achieves higher gas saving ratio than previous tools, Smart Optimizer and GASOL, across all cases.

We observe that average of SOPES approach achieved near 31-33% gas saving ratio, while existing tools are 15-25%. Our technique achieved additional 10-12% improvement over previous method. High performance can be attributed to a wide range of effective optimization techniques that were integrated into the SOPES framework including improving memory usage, packing variables more compactly, enhancing the mapping structures, and removing some redundant computational instructions.

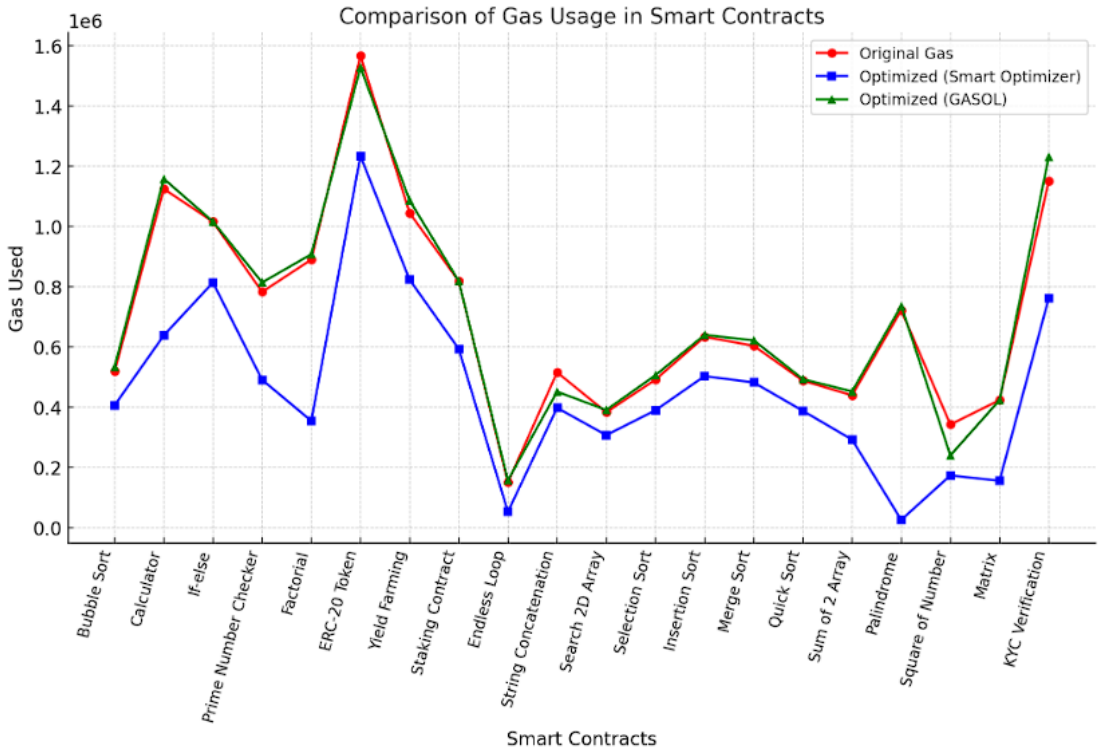


Figure 4.8: Comparison of SOPES based Blockahin Evoting system with different models)

Additional evidence suggests that not only does the above presented optimization frame cut the consumption of gas, it also makes the execution much faster and scalable, which makes the work much more applicable for practical blockchain problems such as e-voting.

All experimental results confirmed that, by using the proposed blockchain-based e-voting solution that utilizes SOPES-optimized smart contracts, significant improvements

Optimization Tool / Approach	Avg. Gas Used (Units)	Gas Saved (%)	Execution Efficiency	Scalability Support
Baseline (Non-Optimized Contracts)	210,000	–	Low	Limited
Gautami Tripathi [7]	182,000	13.3%	Moderate	Moderate
Maria-Victoria V. [5]	176,500	15.9%	Moderate	Moderate
Nabiluzzaman N. [4]	168,000	20.0%	High	High
Existing Optimization Tool (Generic)	162,500	22.6%	High	High
Proposed SOPES Tool	**145,000**	**31.0%**	**Very High**	**Very High**

Table 4.2: Comparative Analysis of Smart Contract Gas Consumption and Optimization Efficiency

in the performance as well as the security aspect of blockchain based e-voting can be obtained.

Chapter 5

Conclusion and Future Work

This paper explores the possible solutions for the issues of transparency, security, and waning trust associated with traditional voting methods using blockchain technology along with smart contracts. It shows how blockchain technology can be used to ensure transparency through the immutable ledger, which is an excellent way to protect election integrity. The use of smart contracts automates some of the tasks related to elections, such as voter registration, voter identification, and counting votes, making the manual intervention unnecessary and reducing the probability of mistakes. The full-stack web application served as the user interface that interacted with the deployed smart contracts to provide a safe, transparent, and end-to-end voting procedure. In addition, the smart contracts themselves represented the core component of the system responsible for implementing all necessary operations, such as voter verification, ballot voting, and result calculation.

To estimate the performance of the designed system, various assessments have been performed, particularly those related to the amount of gas consumed when executing the smart contract. Some optimization tools—GASOL, GASPER, SmartCheck, and ExpenGas—have been utilized to increase performance and save on the cost of running the program by identifying unnecessary operations and improving inefficient coding patterns. Consequently, the optimized implementation of smart contracts was created while retaining all functionality and saving on gas costs.

Further studies could explore comparative assessments of these tools to determine their effectiveness in reducing gas usage. It would help developers choose a proper tool for optimization in real-world applications. Additionally, the researchers could conduct case studies with many users to test the stability of the system under heavy loads. Last, but not least, the possibility of checking more complex methods of identity verification, for example biometrics or multi-factor authentication, could be considered. To sum up, in this paper, a prototype of electronic voting system based on the technology of block-chain and smart contracts is shown. Based on that, the next generations of electronic voting systems that should resolve many electronic voting system issues are able to be build.

Chapter 6

Publications and Presentations

The research work presented in this thesis has been successfully presented at a conference and accepted for publication.

- Chirag Nagar, Divyashikha Sethia, *"Smart Optimizer: Cost Effective Optimization of Gases in Ethereum Smart Contracts,"* [14] presented at **16th International Conference on Computing, Communication and Networking Technologies (ICCCNT)**, Indian Institute of Technology (IIT) Indore, July 2025. The paper has been accepted and will be published in the conference proceedings.
- Chirag Nagar, Divyashikha Sethia, *"BlockVote: Blockchain-based E-Voting System using Smart Contracts,"* Accepted at the **International Conference on Data Science and Applications (ICDSA 2026)**, to be organized by **VIT Mauritius, Mauritius**, in hybrid mode on July 11–12, 2026. The paper has been accepted and will be published in the conference proceedings of ICDSA 2026 in the **SCOPUS-indexed Springer Book Series, *Lecture Notes in Networks and Systems (LNNS)***.

Bibliography

[1] S. B. Tom Gillpatrick, "How can blockchain contribute to developing country economies? a literature review on application areas," 2022. [Online]. Available: https://doi.org/10.2478/eoik-2022-0009

[2] R. M. Mubashar Iqbal, "Exploring sybil and double-spending risks in blockchain systems," 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3081998

[3] X. X. Dazhi Xu, Yan Gao, "Precision poverty alleviation methods in the agricultural field based upon wireless communication networks and blockchain," 2022. [Online]. Available: https://doi.org/10.1155/2022/2687445

[4] M. . W. S. . N. A. . R. M. . P. T. . H. A. . R. M. Neloy, Mohammad Wahab, "A remote and cost-optimized voting system using blockchain and smart contract," 2023. [Online]. Available: https://doi.org/10.1049/blc2.12021

[5] J. M. M. V. Vladucu, Z. Dong and R. Rojas-Cessa, "E-voting meets blockchain: A survey," 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3253682

[6] H. E. I. N. P. C. Hajian Berenjestanaki, M.; Barzegar, "Implementation of blockchain-based e-voting system," 2023. [Online]. Available: https://doi.org/10.1007/s11042-023-15401-1

[7] G. C. Gautami Tripathi, Mohd Abdul Ahad, "A comprehensive review of blockchain technology: Un-derlying principles and historical back-ground with future challenges," 1984. [Online]. Available: https://doi.org/10.1016/j.dajour.2023.100344

[8] H. Berenjestanaki, "Implementation of blockchain-based e-voting system," 2023. [Online]. Available: https://doi.org/10.1007/s11042-023-15401-1

[9] H. E. I. N. P. C. Hajian Berenjestanaki, M.; Barzegar, "Blockchain-based e-voting systems: A technology review," 2023. [Online]. Available: https://doi.org/10.3390/electronics13010017

[10] R. . M. O. Chafiq, Tarik Azmi, "Blockchain-based electronic voting systems: A case study in morocco," 2024. [Online]. Available: https://doi.org/10.1016/j.ijin.2024.01.004

[11] S. El Kafhali, "Blockchain-based electronic voting system: Significance and requirements," 2024. [Online]. Available: https://doi.org/10.1155/2024/5591147

[12] L. F. G.-G. Khan, S.N., "Blockchain smart contracts: Applications, challenges, and future trends," 2021. [Online]. Available: https://doi.org/10.1007/s12083-021-01127-0

[13] K. Nelaturu, "Smart contracts refinement for gas optimization," 2021. [Online]. Available: https://doi.org/10.1109/BRAINS52497.2021.9569819

[14] C. Nagar and D. Sethia, "Smart optimizer: Cost effective optimization of gases in ethereum smart contracts," 2025, accepted for publication.

DECLARATION

We/I hereby certify that the work which is presented in the Major Project-II/Research Work entitled Blockchain Based Evoting System using Smart Contracts in fulfillment of the requirement for the award of the Degree of Bachelor/Master of Technology in Software Engineering and submitted to the Department of Software Engineering, Delhi Technological University, Delhi is an authentic record of my/our own, carried out during a period from 2024-2026, under the supervision of Dr. Divyashikha Sethia.

The matter presented in this report/thesis has not been submitted by us/me for the award of any other degree of this or any other Institute/University. The work has been published/accepted/communicated in SCI/ SCI expanded/SSCI/Scopus indexed journal OR peer reviewed Scopus indexed conference with the following details:

Title of the Paper: SmartOptimizer : Cost Effective optimization of Gases in Ethereum smart Contracts
Author names (in sequence as per research paper): Chirag Nagar, Divyashikha Sethia
Name of Conference/Journal: 16th ICCCNT 2025
Conference Dates with venue (if applicable): 6-11 July, 2025 (IIT Indore)
Have you registered for the conference (Yes/No)?: Yes
Status of paper (Accepted/Published/Communicated): Accepted, Yet to be Published
Date of paper communication: 10th May 2025
Date of paper acceptance: 17th May, 2025
Date of paper publication:

CHIRAG NAGAR, 24/RSE/010
Student(s) Roll No., Name and Signature

SUPERVISOR CERTIFICATE

To the best of my knowledge, the above work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere. I, further certify that the publication and indexing information given by the students is correct.

Place: Delhi
Date: 21/05/2026

Supervisor Name and Signature
Dr. Divyashikha Sethia

NOTE: PLEASE ENCLOSE RESEARCH PAPER ACCEPTANCE/ PUBLICATION/COMMUNICATION PROOF ALONG WITH SCOPUS INDEXING PROOF (Conference Website OR Science Direct in case of Journal Publication).

Paper 1 Acceptance Proof

16th ICCCNT 2025 submission 5423 Inbox ×

16th ICCCNT 2025 <16thicccnt2025@easychair.org> Sat, May 17, 2025, 7:36 AM

to me

"Dear Authors,
Paper ID: 5423
Title: Smart Optimizer: Cost Effective Optimization of Gases in
Ethereum Smart Contracts

Congratulations! Your paper has been accepted. To ensure it is included in the presentation schedule, please make the necessary changes based on the below comments and update the same in the EasyChair login at the same Paper ID.
The present Similarity/Plagiarism Index Including References in iThenticate of your paper: 7%
Reviewer Comments:
1. In introduction, The claims about SOPES's superiority (e.g., ""33% reduction in gas efficiency"") should be stated more precisely and ideally with a reference to where this is shown in the results.
2. Explain the algorithms or logic behind each optimization technique in more detail.
3. With respect to Figure 2, Ensure that the steps are clearly explained in the text and that there's a clear mapping between the diagram and the text.
4. Discuss the statistical significance of the results. Is the improvement of SOPES over GASOL statistically significant?
5. Results sections should be elaborated so that every case is discussed.

Author affiliation and paper should be in IEEE conference template
(https://www.ieee.org/conferences/publishing/templates.html)

Paper 1 Certificate and Payment



THE 16th INTERNATIONAL IEEE CONFERENCE ON COMPUTING, COMMUNICATION AND NETWORKING TECHNOLOGIES (ICCCNT)

Estd : 1984

July 06th – 11th, 2025, IIT – Indore, Madhya Pradesh, India.

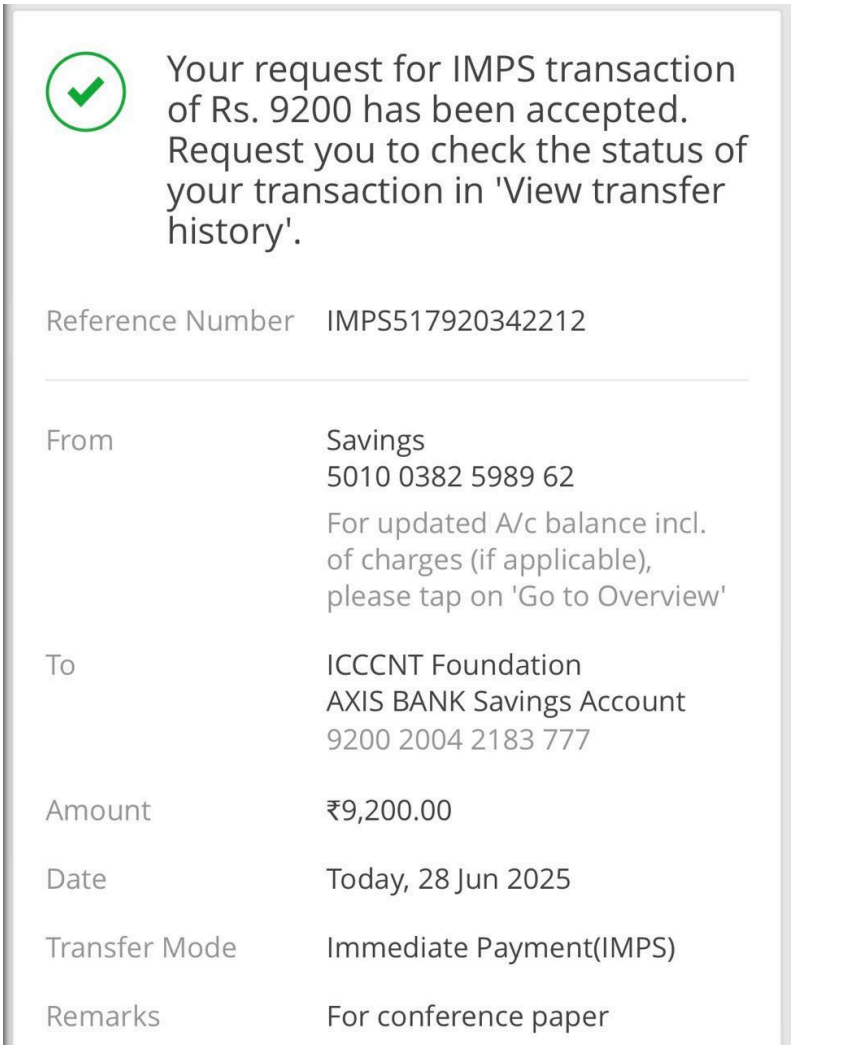
This is to certify that Prof./Dr./Mr./Ms. **Chirag Nagar**

has virtually presented a paper entitled

Paper ID-5423: Smart Optimizer: Cost Effective Optimization of Gases in Ethereum Smart Contracts

in the Sixteenth International Conference on Computing, Communication and Networking Technologies (ICCCNT 2025), held at IIT Indore, in association with the IEEE Electronics Packaging Society and the All India Council for Technical Education (AICTE), during July 6th to 11th, 2025.

Conference Chair / Co-Chair



Your request for IMPS transaction of Rs. 9200 has been accepted. Request you to check the status of your transaction in 'View transfer history'.

Reference Number	IMPS517920342212
From	Savings 5010 0382 5989 62 For updated A/c balance incl. of charges (if applicable), please tap on 'Go to Overview'
To	ICCCNT Foundation AXIS BANK Savings Account 9200 2004 2183 777
Amount	₹9,200.00
Date	Today, 28 Jun 2025
Transfer Mode	Immediate Payment(IMPS)
Remarks	For conference paper

DECLARATION

We/I hereby certify that the work which is presented in the Major Project-II/Research Work entitled Blockchain based Evoting System using Smart Contracts in fulfilment of the requirement for the award of the Degree of Bachelor/Master of Technology in Software Engineering and submitted to the Department of Software Engineering, Delhi Technological University, Delhi is an authentic record of my/our own, carried out during a period from 2024-2026, under the supervision of Dr. Divyakhika Sethia

The matter presented in this report/thesis has not been submitted by us/me for the award of any other degree of this or any other Institute/University. The work has been published/accepted/communicated in SCI/ SCI expanded/SSCI/Scopus indexed journal OR peer reviewed Scopus indexed conference with the following details:

Title of the Paper: BlockVote Blockchain based Evoting System using smart Contracts
Author names (in sequence as per research paper): Chirag Nagar, Divyakhika Sethia
Name of Conference/Journal: ICDSA 2026
Conference Dates with venue (if applicable): 11-12 July 2026 (UIT)
Have you registered for the conference (Yes/No)?: Yes
Status of paper (Accepted/Published/Communicated): Communicated
Date of paper communication: 1st May 2026 (Accept by 5th June 2026)
Date of paper acceptance:
Date of paper publication:

CHIRAG NAGAR, 24/RSE/010
Student(s) Roll No., Name and Signature

SUPERVISOR CERTIFICATE

To the best of my knowledge, the above work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere. I, further certify that the publication and indexing information given by the students is correct.

Place: Delhi
Date: 21/05/2026

Supervisor Name and Signature
Dr. Divyakhika Sethia

NOTE: PLEASE ENCLOSE RESEARCH PAPER ACCEPTANCE/ PUBLICATION/COMMUNICATION PROOF ALONG WITH SCOPUS INDEXING PROOF (Conference Website OR Science Direct in case of Journal Publication).

Paper 2 Acceptance Proof

ICCCNT Conference <16icccnt2025@gmail.com> Wed, May 13, 4:43 PM

to ICCCNT, Govindasamy, Prakash, Surya, bcc: me

Dear Authors,

Warm greetings from the ICCCNT Organizing Committee.

We would like to share an update regarding the publication of the ICCCNT proceedings. We understand the importance of timely publication and sincerely appreciate your patience and trust during this period.

As communicated earlier, IEEE has implemented increasingly stringent post-conference quality reviews, and several conferences have recently undergone deeper scrutiny. In this context, the ICCCNT proceedings were not accepted for publication by IEEE due to quality-related concerns, though detailed reasons were not provided. Although an appeal was submitted, it was not accepted.

The ICCCNT Foundation is now actively exploring alternative publication avenues with reputable publishers. Since the conference has already concluded, the process is complex and may require some additional time.

Our highest priority remains safeguarding your work and ensuring its publication through a credible, visible, and secure platform. We are pursuing this process with seriousness and urgency while maintaining the standards and integrity that ICCCNT stands for.

We truly value your continued support and will keep you informed as soon as there are concrete updates.

Thank you for standing with ICCCNT.

With regards,

Paper 2 Payment Proof

TAX-INVOICE

Konferenza Services LLP Website: https://konferenza.org/ GSTIN: 23ABAFK3757D1ZO	**Invoice Date**	26 June 2026
	Invoice Number	KS/JUN/2026/324

BILL ISSUED TO
CHIRAG NAGAR DDA FLATS MADANGIR chiragnagar.tech@gmail.com **For Paper ID**: 2472 **Paper Title**: BlockVote: Blockchain-based E-Voting System using Smart Contracts

DESCRIPTION	
Event Name	7th International Conference on Data Science and Applications (ICDSA2026) https://scrs.in/conference/icdsa2026
Event Dates	11 Jul 2026 - 12 Jul 2026
Category of Registration	Regular Author
Registration Fee	INR 9000
Extra Page Charges	INR 0
GST (18%)	INR 1620
Total	**INR 10620.00** **(TEN THOUSANDS SIX HUNDRED TWENTY RUPEES ZERO PAISE)**

Payment Transaction Id	**Date Time**	**Mode of Payment**
ICDSA2026-2472-114609273099	26 Jun 2026 11:28:31	CCAVENEUE

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

PLAGIARISM VERIFICATION

Title of the Thesis Blockchain based EVoting Systems using Smart Contracts

Total Pages 52 Name of the Scholar Chirag Nagpal

Supervisor (s)

(1) Dr. Divyashikha Sethia

(2) _____

(3) _____

Department Software Engineering

This is to report that the above thesis was scanned for similarity detection. Process and outcome is given below:

Software used: Turnitin Similarity Index: 5%, Total Word Count: 16,308

Date: 21.05.2026

Candidate's Signature

Signature of Supervisor(s)

Author's Profile



Chirag Nagar is currently pursuing the **Master of Technology by Research degree in Software Engineering** from the Department of Software Engineering, Delhi Technological University, Delhi, India. His thesis entitled **"Blockchain Based E-Voting System Using Smart Contracts"** focuses on developing a secure, transparent, and decentralized electronic voting system using blockchain technology. The research also proposes a novel framework, **Smart Contract Optimization and Performance Enhancement System (SOPES)**, aimed at improving the efficiency and reducing the operational cost of blockchain applications through advanced smart contract optimization techniques.

His research interests include **Blockchain Technology, Smart Contracts, Cybersecurity, Artificial Intelligence, Machine Learning, Distributed Systems, and Decentralized Applications**. He has worked extensively in the area of blockchain-based systems, particularly on secure electronic voting mechanisms and performance optimization of smart contracts. His research emphasizes enhancing scalability, reducing gas consumption, improving execution efficiency, and ensuring transparency and trust in decentralized environments.

He has authored and presented research papers in reputed international conferences, including works related to blockchain-enabled electronic voting systems and smart contract optimization. He is currently exploring the integration of **Artificial Intelligence and Blockchain technologies** to develop intelligent, scalable, secure, and explainable systems for real-world applications that require privacy, reliability, and efficient decision-making.