### CHAPTER 1

### INTRODUCTION

###### 1.1 Background

Elections are the foundation of any democratic system, providing citizens with the right to choose their representatives and influence governance. However, traditional voting systems—whether paper-based or electronic—continue to face significant challenges related to security, transparency, accessibility, and efficiency. Issues such as vote tampering, duplicate voting, human error, and lack of verifiable audit trails have often raised concerns about the credibility and integrity of election outcomes. In many cases, logistical constraints and limited accessibility have also discouraged voter participation, especially among citizens residing in remote or overseas locations.

With the rapid advancement of digital technologies, there is a growing demand for **secure, transparent, and convenient online voting systems**. While online voting offers the potential to simplify the election process and increase participation, it also introduces new challenges related to **data privacy, authentication, and system trustworthiness**. A secure framework is essential to ensure that each vote is cast by a verified voter, counted accurately, and cannot be altered or deleted once submitted.

**Blockchain technology** has emerged as a revolutionary solution to address these challenges. Its decentralized and immutable nature ensures that every transaction—representing a vote—is securely recorded in a distributed ledger that cannot be manipulated. This guarantees **transparency, verifiability, and data integrity**, eliminating the risk of unauthorized modifications. By integrating blockchain with robust authentication mechanisms such as **Voter ID verification** and **OTP-based login**, it becomes possible to design a tamper-proof and trustworthy digital voting platform.

The **TrueVote** project was conceptualized to fulfill this need for a **secure, transparent, and user-friendly online voting system**. It bridges the gap between traditional voting limitations and modern digital security standards. The platform allows voters to register securely, verify their identity, and cast votes from any location, with each vote being permanently stored on the **Ethereum blockchain** as a unique transaction. The system includes dedicated modules for **admins to manage elections, candidates, and voter approvals**, while **voters can participate in elections, track their vote history, and view real-time results**.

Ultimately, **TrueVote** aims to strengthen the democratic process by ensuring that every vote counts and remains immutable. By leveraging blockchain technology and secure web mechanisms, it promotes a **transparent, efficient, and tamper-proof voting environment**, suitable for modern digital governance. The system not only enhances election integrity but also encourages greater voter participation, accessibility, and trust in the electoral process.

**1.2 Introduction**

Elections are a vital component of democratic governance, allowing citizens to express their choices and influence decision-making at various levels of administration. However, traditional voting systems continue to face several challenges such as vote tampering, lack of transparency, logistical inefficiencies, and limited accessibility for remote or disabled voters. Manual vote counting and centralized data handling increase the risk of manipulation, while long queues and restricted polling locations often discourage participation. These issues underline the urgent need for a secure, transparent, and accessible alternative to conventional voting methods.

In recent years, digital technology has transformed numerous aspects of civic and administrative processes, paving the way for electronic voting (e-voting) solutions. However, most existing online voting systems still depend on centralized databases, which remain vulnerable to hacking, unauthorized alterations, and data loss. There is, therefore, a strong need for a system that ensures tamper-proof vote recording, voter authentication, and result verification through a decentralized and transparent framework.

The TrueVote project aims to bridge this gap by developing a blockchain-based online voting platform that ensures integrity, trust, and security in digital elections. The system enables voters to register using their Voter ID, complete authentication through OTP verification, and cast their vote securely via a smart contract deployed on the Ethereum blockchain. Each vote is stored as a unique, immutable blockchain transaction, ensuring that no entity can modify or delete it once recorded. Administrators can create elections, verify voter registrations, manage candidates, and publish results, while voters can view elections, cast votes, and check their voting history — all within a secure and user-friendly interface.

Through this project, we aim to strengthen democratic participation by leveraging blockchain technology to make elections transparent, verifiable, and tamper-proof. The TrueVote system represents a step toward digital democracy, where technology empowers citizens to vote securely and confidently from anywhere, ensuring that every vote is counted and every voice truly matters.

###### 1.3 Problem Statement

The process of conducting elections plays a crucial role in maintaining democracy, yet traditional voting systems continue to face several persistent challenges. Conventional methods, such as paper ballots and electronic voting machines, are often vulnerable to issues like vote tampering, human error, duplicate voting, and lack of verifiable transparency. These problems raise doubts about the credibility and fairness of election outcomes. Additionally, the manual handling of votes and centralized data storage make traditional systems susceptible to manipulation and data breaches.

In many regions, logistical barriers such as long queues, limited polling stations, and inconvenient voting hours discourage voter participation. Remote and overseas voters often find it difficult to access the voting process, leading to reduced voter turnout. Although some online voting platforms have been developed, most rely on centralized databases that can be compromised through cyberattacks or unauthorized access, posing serious risks to election integrity.

Therefore, the main problem addressed by this project is the lack of a secure, transparent, and decentralized voting platform that ensures voter authenticity, prevents vote duplication, and provides publicly verifiable results. The system should allow eligible voters to cast their votes conveniently from any location while guaranteeing data privacy and immutability. The TrueVote project aims to overcome these limitations by developing a blockchain-based voting system that enhances security, transparency, and trust in the electoral process.

###### 1.4 Motivation

In today’s digital era, elections remain one of the most critical components of a democratic society, yet the process of conducting them securely and transparently continues to pose significant challenges. The increasing cases of vote manipulation, data breaches, and lack of verifiable transparency in traditional and electronic voting systems have raised serious concerns about the integrity of election outcomes. Observing these issues in real-world elections motivated the idea of creating a system that could ensure secure, verifiable, and tamper-proof voting through advanced technology.

The motivation behind developing the TrueVote system stems from the vision of transforming the voting process into a more transparent, accessible, and trustworthy activity. Instead of relying on centralized servers or manual vote counting, this system encourages the use of blockchain technology to record votes immutably and verifiably. Blockchain ensures that once a vote is cast, it cannot be altered or deleted, thereby maintaining complete trust in the system. Additionally, it simplifies the voting process for citizens, allowing them to participate securely from anywhere, ensuring accessibility and convenience while maintaining data integrity and voter privacy.

From a technical and educational perspective, the project also serves as an excellent opportunity to apply core concepts of modern web and blockchain development. It involves implementing database management, secure authentication, smart contracts, and encrypted transactions in a real-world context. Building such a system enhances practical skills in both backend and frontend development while also addressing a genuine societal need. The TrueVote project demonstrates how technology can be effectively used to strengthen democratic systems and promote digital trust.

Furthermore, the project is motivated by the need for transparency, fairness, and accountability in the electoral process. Many people lose confidence in elections due to the lack of reliable systems that ensure vote security and public verifiability. By integrating features like voter registration, OTP-based authentication, and blockchain-based vote recording, this system provides a secure and accountable environment for both administrators and voters.

Ultimately, this project is driven by the goal of developing an innovative, user-friendly, and socially beneficial application. The TrueVote system not only aims to enhance election transparency and security but also aspires to bring a positive change in democratic participation. It reflects a collective step toward secure digital governance — promoting electoral integrity, citizen empowerment, and technological advancement in the voting process.

###### 

###### 1.5 Scope

The TrueVote system is designed to function as a comprehensive web-based platform that facilitates secure, transparent, and efficient online voting using blockchain technology. The scope of the project includes voter registration and authentication, election creation and management, candidate registration and approval, OTP-based vote casting, and blockchain transaction recording for verifiable results.

Voters can register on the platform using their Voter ID and complete verification through an OTP sent to their registered email. Once verified, voters can view active or upcoming elections, check candidate details, and cast their vote securely. Each vote is recorded as a unique transaction on the Ethereum blockchain, ensuring that it cannot be altered or deleted after submission. Voters can also view their voting history and check published results once elections are completed.

The admin module oversees the overall system operations, including voter approval, election scheduling, candidate management, and result publication. It also monitors blockchain transaction hashes to verify the authenticity and integrity of recorded votes. However, the system does not include features such as biometric authentication or live election analytics, as its focus is on providing a secure, decentralized, and verifiable voting process rather than real-time monitoring.

In summary, the scope of this project covers the development of a secure and transparent blockchain-based voting system that simplifies election management while maintaining high levels of data integrity and trust. The project emphasizes usability, authenticity, and the promotion of digital democracy through innovative and reliable technology.

### 

### 

### CHAPTER 2

### LITERATURE REVIEW

* 1. **A Secure Electronic Voting System Using Blockchain Technology [Alzahrani, Bulusu, and Shiva (IEEE Access)]**

This research paper introduces a secure and transparent electronic voting system built on blockchain technology. The main goal of the study is to overcome the limitations of traditional voting methods, such as lack of transparency, tampering risks, and dependence on centralized authorities. The system ensures trust, integrity, and verifiability in the voting process through decentralized ledger technology.

The authors emphasize that blockchain can provide a distributed, immutable, and auditable record of votes, making manipulation or unauthorized modification virtually impossible. The system uses cryptographic mechanisms and smart contracts to automate vote recording and result tallying while maintaining voter privacy and system transparency.

**Objectives**

 To design a decentralized and tamper-proof voting system using blockchain.

 To ensure voter anonymity, integrity of votes, and public verifiability.

 To reduce reliance on centralized authorities in managing election data.

 To increase trust and transparency in the election process.

**Methodology**

The general methodology involves:

* **Voter Registration:** Each eligible voter is registered through a secure authentication process, and their identity is verified by an authorized authority. After verification, a unique digital ID is created.
* **Blockchain Setup:** A private or permissioned blockchain network is established, ensuring only authenticated entities (like election commissions or nodes) can participate in consensus and data validation.
* **Smart Contracts:** Smart contracts are used to handle election logic automatically — including candidate information storage, vote casting, and result calculation — ensuring transparency and eliminating manual interference.
* **Vote Casting:** Each voter casts their vote through a blockchain-enabled web interface or application. The vote is encrypted and recorded as a transaction on the blockchain, ensuring it cannot be modified or duplicated.
* **Vote Counting and Verification:** Votes are automatically tallied through the blockchain’s consensus mechanism. The results can be verified by anyone, ensuring auditability and transparency.
* **Security and Privacy:** The system uses public-key cryptography and hashing to secure the voting process. It ensures that while votes are transparent on the blockchain, voter identities remain anonymous.

### ****Key Findings****

The authors conclude that blockchain-based e-voting significantly enhances election security, transparency, and public trust. The system:

* Prevents vote tampering or duplication through immutability.
* Maintains voter anonymity through cryptographic encryption.
* Provides a verifiable and auditable election record.
* Eliminates the need for intermediaries or centralized control.

The study also identifies challenges, such as scalability, voter device security, and network latency, as future research areas. Overall, the proposed system demonstrates that blockchain can revolutionize democratic voting by creating a secure, transparent, and tamper-proof electoral process.

* 1. **Blockchain-Based E-Voting: A Review of Technologies and Implementation Models [P. S. Praveen Kumar et al. (Elsevier)]**

This paper provides a detailed review of various blockchain-based electronic voting systems and the technologies that power them. The authors examine how blockchain can transform traditional voting mechanisms by ensuring transparency, immutability, and decentralization. They analyze multiple implementation models, consensus mechanisms, and cryptographic techniques used in recent research to enhance election integrity and voter trust.

The paper highlights the importance of blockchain’s distributed ledger in eliminating single points of failure and preventing vote tampering. It also discusses how smart contracts can automate different stages of the voting process, such as voter registration, vote casting, and result tabulation, without human intervention.

### ****Objectives****

* To review the existing blockchain-based e-voting systems and their architectures.
* To analyse the role of different blockchain platforms and consensus algorithms in e-22222voting.
* To identify key challenges and limitations in the deployment of blockchain voting 22222systems.
* To propose improvements for achieving scalability, privacy, and usability in digital 33333elections.

### ****Methodology****

The study uses a **comparative review approach**, analysing multiple blockchain-based e-voting prototypes and models proposed in previous literature. The authors evaluate systems based on factors such as technology stack, security mechanisms, transaction handling, and performance.

**1.Blockchain Platforms Reviewed:** The paper reviews blockchain frameworks like **Ethereum, Hyperledger Fabric**, and **EOS**, comparing their suitability for voting applications in terms of speed, cost, and scalability.

**2.Consensus Mechanisms:** The study discusses consensus algorithms such as **Proof of Work (PoW)**, **Proof of Stake (PoS)**, and **Practical Byzantine Fault Tolerance (PBFT),** emphasizing that PBFT and PoS are more efficient and suitable for permissioned election networks.

**3.Security and Cryptography:** The authors highlight the use of **public-key cryptography, hashing**, and **zero-knowledge proofs** to maintain vote secrecy and prevent voter identification or vote manipulation.

**4.Smart Contract Integration:** The paper explains how smart contracts manage and automate voting procedures—verifying voter eligibility, ensuring one vote per person, and performing transparent result aggregation.

**5.Evaluation Criteria:** Each model is assessed for **security, transparency, anonymity, scalability**, and **system efficiency** to identify strengths and areas for improvement.

### ****Key Findings****

The authors conclude that blockchain-based voting systems offer a promising solution to major issues in conventional elections such as fraud, lack of transparency, and centralized control. They observe that:

* Decentralization eliminates the risk of vote tampering.
* Cryptographic techniques preserve voter privacy.
* Smart contracts enhance automation and transparency.
* Public verification builds trust among voters and authorities.

However, the paper also notes limitations in **scalability**, **energy efficiency**, and **user accessibility**. It recommends future research into lightweight consensus protocols and hybrid blockchain architectures to make e-voting more practical and widely adoptable.

Overall, the study provides a strong foundation for developing secure, efficient, and transparent e-voting systems by leveraging blockchain’s core features of decentralization, immutability, and cryptographic trust.

**2.3. Secure Online Voting Using Blockchain with Biometric Integration [Farag, A., Mousa, M., El-Bakry, H.]**

This paper introduces a secure online voting system that integrates **blockchain technology** with **biometric authentication** to ensure election transparency, voter identity verification, and data integrity. The authors aim to address the key challenges in electronic voting systems such as identity fraud, vote duplication, and centralized data control by combining biometric verification with decentralized blockchain-based storage.

The proposed system provides a secure framework that enables voters to authenticate themselves through **fingerprint or facial recognition** before casting their votes. By using blockchain as a distributed ledger, all voting records are stored immutably, ensuring that votes cannot be altered, deleted, or forged

### ****Objectives****

* To develop a secure and transparent online voting model using blockchain technology.
* To integrate biometric authentication for accurate voter verification and fraud prevention.
* To ensure data integrity, privacy, and immutability of votes.
* To enhance the reliability and public trust in electronic voting systems.

### ****Methodology****

The authors design a **multi-layered architecture** combining biometric systems, blockchain infrastructure, and cryptographic protocols to secure every stage of the voting process.

**1.User Registration:** Each voter registers with personal and biometric details (such as fingerprint or facial data), which are verified and stored in an encrypted format within the system.

**2.Biometric Authentication:** Before voting, the user’s biometric input is re-verified to confirm identity, ensuring that only legitimate voters can access the voting interface.

**3.Blockchain Layer:** Once authentication is completed, the voting transaction is recorded on a blockchain ledger. Each vote is represented as a unique encrypted transaction, preventing any modification or duplication.

**4.Encryption and Hashing:** Cryptographic hashing techniques (such as SHA-256) are used to secure the vote data, ensuring that the content of the votes remains confidential and tamper-proof.

**5.Consensus Mechanism:** A permissioned blockchain model is employed, often using **Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA)** for efficient validation without high computational cost.

**6.Vote Counting and Verification:** The counting process is automated through smart contracts, ensuring transparency and accuracy. Results can be audited by verifying blockchain transactions.

### ****Key Findings****

The study concludes that integrating biometric authentication with blockchain significantly enhances the **security, transparency**, and **trustworthiness** of online voting systems. The system ensures that:

* Only registered and authenticated voters can cast a vote.
* Each vote is securely recorded and immutable.
* Voter anonymity is preserved while maintaining verifiability.
* Centralized manipulation or data breaches are effectively prevented.

The authors also highlight challenges such as the **cost of biometric infrastructure, data storage requirements,** and **network scalability,** which need further optimization. Future enhancements may include using lightweight blockchain frameworks and advanced encryption schemes to support large-scale elections.

Overall, the paper demonstrates that combining blockchain and biometrics provides a robust and secure foundation for next-generation electronic voting systems, offering both accountability and convenience in digital democracy.

**2.4 Trustworthy E-Voting Using Blockchain: Challenges and Future Scope [Hossain, M. S. et al. (Springer)]**

Modern democratic systems face significant challenges in maintaining transparency, trust, and security in electronic voting (e-voting) processes. Traditional centralized voting systems are vulnerable to data manipulation, cyberattacks, and lack of public verifiability. Hossain et al. (Springer) propose a blockchain-based e-voting framework to establish a **trustworthy, transparent, and tamper-proof voting system** that enhances voter confidence while ensuring privacy and fairness. The study explores how blockchain’s decentralized architecture, combined with cryptographic techniques, can revolutionize digital voting by eliminating third-party dependency and securing election data.

The paper emphasizes the importance of **immutability, voter anonymity, and public verifiability** in e-voting systems. By recording votes as transactions on a distributed ledger, blockchain ensures that once a vote is cast, it cannot be altered or deleted. This creates an auditable and transparent voting process where all stakeholders can verify the legitimacy of results without compromising voter privacy.

### ****Key Aspects:****

• **Blockchain-Based Architecture:** The proposed system uses a **permissioned blockchain** where registered authorities act as validating nodes. Each vote is treated as a unique transaction stored permanently on the distributed ledger. This decentralization eliminates single points of failure and ensures data integrity throughout the election process.

• **Voter Authentication and Privacy:** Voters are authenticated using unique digital credentials, ensuring that only eligible participants can cast a vote. Cryptographic methods such as public-key encryption and hash functions protect voter identities while maintaining the anonymity of ballots.

• **Smart Contract Automation:** The system leverages **smart contracts** to automatically execute election operations, including vote recording, counting, and result publishing. This automation minimizes human intervention and prevents tampering or vote duplication.

• **Transparency and Verifiability:** Every vote recorded on the blockchain can be publicly verified without revealing voter information. The immutable nature of blockchain ensures that all voting data remains auditable and transparent for independent validation.

• **Security and Data Integrity:** Blockchain’s cryptographic foundations protect against unauthorized modifications and double voting. The consensus mechanism, such as **Proof of Authority (PoA)** or **Practical Byzantine Fault Tolerance (PBFT)**, ensures trust among validating nodes while maintaining high transaction throughput.

• **Challenges Identified:** The study outlines potential limitations, including scalability issues in handling national-level elections, high computational overhead, and the need for comprehensive legal and regulatory frameworks to support blockchain-based voting.

• **Future Scope:** The authors suggest exploring **AI-driven anomaly detection, zero-knowledge proofs,** and **hybrid blockchain models** to enhance system scalability and security. Integration with biometric verification and mobile-based voting interfaces is also recommended for improved accessibility and user trust.

**2.5 Lightweight Blockchain E-Voting for Educational Institutions [Singh, A., Kumar, S. (IJCSNS)]**

Educational institutions require secure, transparent, and easily auditable voting systems for student elections and other organizational decisions. Traditional paper-based or centralized electronic voting systems are prone to manipulation, human errors, and lack transparency. Singh and Kumar (IJCSNS) propose a lightweight blockchain-based e-voting system specifically designed for educational environments, aiming to provide a secure, verifiable, and efficient voting mechanism while minimizing computational and infrastructural overhead.

The paper highlights how blockchain’s decentralized ledger, combined with lightweight cryptographic techniques, can simplify the election process for small-scale environments such as universities and colleges. By recording votes as blockchain transactions, the system ensures immutability, voter privacy, and verifiability, even in resource-constrained settings.

**Key Aspects:**

• **Lightweight Blockchain Architecture:** The system uses a permissioned blockchain with minimal computational requirements, suitable for educational institutions. Voting authorities act as validating nodes, ensuring vote integrity while maintaining low resource consumption.

• **Voter Authentication and Anonymity:** Students are authenticated using unique digital credentials issued by the institution. Cryptographic hashing and encryption protect voter identities, ensuring that votes remain anonymous yet verifiable.

• **Smart Contract-Based Voting:** Smart contracts automatically manage voting operations, including vote submission, validation, counting, and result publication. This reduces manual effort and prevents double voting or manipulation.

• **Transparency and Auditability:** All votes are recorded on the blockchain, allowing administrators and stakeholders to audit the election results without compromising voter anonymity.

• **Security and Integrity:** The system leverages lightweight consensus mechanisms suitable for small-scale deployments, ensuring secure vote recording, tamper-resistance, and protection against unauthorized modifications.

• **Challenges Identified:** The study notes potential limitations such as network latency, adoption resistance among students, and the need for secure digital credential management.

• **Future Scope:** The authors suggest integrating mobile voting interfaces, biometric verification, and scalable consensus algorithms to enhance accessibility, usability, and security. Further research on hybrid lightweight blockchain models could enable broader adoption in larger educational networks.

**2.6 Decentralized E-Voting System Using Ethereum Blockchain [Ali, R., Anwar, Z., & Khan, S. (IEEE Xplore)]**

Ali and colleagues proposed a decentralized Ethereum-based e-voting framework that ensures transparency, immutability, and voter anonymity. The system leverages smart contracts to automate vote casting and tallying, thereby eliminating the need for third-party supervision. Although effective in preventing tampering, the study noted high gas costs and transaction delays, making it less practical for smaller organizations.

**Key Aspects:**

* Smart Contract Automation: Enables automatic vote recording and counting without human interference.
* Decentralized Ledger: Ensures immutability and tamper-proof record storage across multiple nodes.
* Voter Anonymity: Achieved through cryptographic techniques that separate identity from the vote.
* Transparency and Verifiability: Every transaction is traceable on the blockchain, ensuring public auditability.
* Challenges: High transaction fees (gas costs), latency in Ethereum network, and scalability concerns for institutional use.
* Relevance: Highlights the need for lightweight blockchain systems like Singh & Kumar’s, optimized for resource-limited educational environments.

**2.7. Blockchain-Enabled E-Voting [Kshetri, N., & Voas, J. (IEEE Computer)]**

Kshetri and Voas explored the potential of blockchain technology in transforming traditional voting systems by providing a secure, transparent, and tamper-resistant framework. Their study emphasized how decentralized trust mechanisms can address election fraud, vote manipulation, and transparency issues. However, they also discussed practical challenges such as scalability, identity management, and voter accessibility that hinder mass adoption.

**Key Aspects:**

* Decentralized Trust Model: Removes the need for central authorities in vote storage and verification.
* Immutable Ledger: Guarantees that votes cannot be altered once recorded.
* Enhanced Transparency: Publicly verifiable blockchain records increase trust in election outcomes.
* Security Concerns: Addresses risks of tampering and unauthorized access through consensus mechanisms.
* Challenges: Scalability limitations, lack of voter identity verification standards, and usability barriers.
* Relevance: Provides a theoretical foundation for adopting blockchain in voting systems, inspiring lightweight, scalable models like Singh & Kumar’s designed for educational institutions.

**2.8 Fair and Transparent Blockchain E-Voting System [Hardwick, F. S., Akram, R. N., & Markantonakis, K. (IEEE Transactions on Emerging Topics in Computing)]**

Hardwick and colleagues developed a fair and transparent e-voting protocol based on blockchain that emphasizes end-to-end verifiability and auditability. Their design ensures that each vote is recorded immutably while maintaining voter privacy and preventing double voting. The study also explored consensus mechanisms for small-scale deployments and proposed improvements to reduce latency and increase efficiency.

**Key Aspects:**

* End-to-End Verifiability: Voters can verify that their votes are correctly recorded without revealing identities.
* Immutable Blockchain Ledger: Prevents vote alteration and enables public auditing.
* Anti-Double Voting Mechanism: Smart contract logic ensures each voter can vote only once.
* Consensus Efficiency: Evaluates low-latency algorithms suitable for smaller environments.
* Challenges: Balancing transparency with voter privacy and managing blockchain scalability.
* Relevance: Supports the idea of secure, efficient, and auditable voting systems, aligning with Singh & Kumar’s goal of implementing low-resource, lightweight blockchain-based e-voting for academic institutions.

**2.9 Institutional E-Voting Framework Using Private Blockchain [Patel, V., & Shah, K. (IJACSA)]**

Patel and Shah introduced an e-voting framework tailored for academic institutions using a private permissioned blockchain. The system employed hashed student identifiers for voter authentication and institutional nodes for vote validation. It was designed to improve trust, transparency, and accountability in student elections but required technical expertise for setup and maintenance, limiting ease of deployment.

**Key Aspects:**

* Permissioned Blockchain: Restricted validator access to institutional authorities for controlled participation.
* Hashed Voter IDs: Ensured anonymity while allowing verification of vote legitimacy.
* Distributed Validation: Reduced chances of single-point failure or data manipulation.
* Auditability: All voting records were available for transparent verification post-election.
* Challenges: Technical complexity in deployment and dependency on skilled personnel.
* Relevance: Shares the same institutional application domain as Singh & Kumar’s study but emphasizes the need for simpler and more lightweight blockchain designs suited for real-world educational environments.

**2.10 Lightweight Blockchain for Secure and Scalable Voting Systems [Noor, T. H., Zeadally, S., & Alfazi, A. (Elsevier)]**

Noor and colleagues proposed a lightweight blockchain-based voting model designed to enhance scalability, speed, and energy efficiency. The system utilizes a Proof of Authority (PoA) consensus mechanism and efficient cryptographic algorithms to maintain security while minimizing computational cost. The authors also explored mobile and web-based interfaces to improve voter accessibility in local and institutional elections.

**Key Aspects:**

* Lightweight Architecture: Optimized for low-resource environments with minimal hardware requirements.
* Proof of Authority (PoA) Consensus: Ensures fast block confirmation and reduced energy consumption.
* Secure Encryption: Protects voter data and ballot privacy using lightweight cryptographic methods.
* Cross-Platform Support: Enables participation via mobile and web applications.
* Challenges: Balancing performance and decentralization while maintaining security.
* Relevance: Closely aligns with Singh & Kumar’s approach, providing strong evidence that lightweight blockchain models are ideal for educational institutions needing secure yet resource-efficient e-voting solutions.

### 

### CHAPTER 3

### PROPOSED SYSTEM

The proposed TrueVote system is designed to provide a secure, transparent, and user-friendly platform for conducting online elections using advanced blockchain technology.

It aims to eliminate electoral fraud, manipulation, and unauthorized access, ensuring that every vote is cast and recorded accurately while maintaining the integrity of the election process.

Unlike conventional electronic voting systems that rely on centralized servers susceptible to hacking or tampering, TrueVote leverages a decentralized blockchain ledger, making each vote immutable, traceable, and auditable.

Voter authentication is strengthened using a dual verification mechanism consisting of Voter ID validation and OTP (One-Time Password) authentication, ensuring that only eligible participants can cast votes.

The system employs smart contracts to automate the entire voting workflow, including vote recording, vote counting, and result publication, significantly minimizing human errors, intervention, and the possibility of duplicate voting.

Each voter has access to a personal voting history dashboard, enabling them to verify that their vote has been successfully recorded and to review results from past elections.

Administrators are provided with a robust dashboard to manage elections efficiently, including the creation of elections, management of candidates, scheduling of election dates, monitoring of blockchain transactions, and secure publication of results.

TrueVote ensures that all sensitive data, including voter credentials and election details, are encrypted and securely stored in a structured database integrated with the blockchain for redundancy and verification.The system supports role-based access control, allowing separate functionalities for voters and administrators to prevent unauthorized operations and maintain the security and integrity of the platform.

By combining cryptographic security, blockchain immutability, automated smart contract operations, and reliable authentication mechanisms, TrueVote guarantees fair, transparent, and verifiable elections.

The platform is also designed to be scalable, accessible, and adaptable for different election sizes, from small institutional polls to larger organizational or regional elections, without compromising speed or security.

Additional features such as real-time notifications, audit trails, secure session management, and encrypted storage of voter information further enhance trust, convenience, and reliability.

Overall, TrueVote represents a comprehensive solution for digital elections, ensuring transparency, accountability, and confidence among all stakeholders while providing a smooth and intuitive voting experience.

**3.1 Blockchain-Based Vote Recording**

**Each vote is treated as a unique transaction on the blockchain, ensuring immutability and traceability. Votes cannot be altered, deleted, or duplicated, providing full transparency and trustworthiness.**

**3.2 Voter Authentication System**

**Voters must verify their Voter ID and OTP before accessing the system. This prevents unauthorized access and ensures that only eligible voters participate.**

**3.3 Smart Contract Automation**

**Smart contracts automatically execute election operations such as vote submission, tallying, and result declaration. This eliminates human intervention and prevents errors or manipulation.**

**3.4 One Vote Per User Enforcement**

**The system ensures single-vote enforcement, so no voter can vote more than once per election. Smart contracts verify voter eligibility in real time during vote submission.**

**3.5 Election Management**

**Admins can create elections with details such as election code, title, type, constituency, start date, and end date. Election status is updated dynamically as Upcoming, Ongoing, or Completed.**

**3.6 Candidate Management**

**Admins can add candidates with party name, symbol, manifesto, and verification documents. Candidate details are visible to voters to make informed voting decisions.**

**3.7 Transparent Result Publishing**

**Results are published through the blockchain, ensuring that votes are auditable and verifiable by both administrators and voters. Any disputes can be resolved by reviewing transaction records.**

**3.8 Secure Login and Session Management**

**The platform uses OTP-based login, encrypted passwords (bcrypt/PHP password\_hash), and automatic session expiry. This prevents unauthorized access and protects voter accounts.**

**3.9 Voting History Dashboard**

**Voters can track their voting history, submitted votes, and election results.This enhances auditability and trust in the system.**

**3.10 Role-Based Access Control**

**Admins and voters have distinct permissions, preventing unauthorized actions. Only admins can create elections, approve candidates, and monitor blockchain transactions, while voters can cast votes and view results.**

**3.11 Data Integrity and Security**

**Blockchain cryptography ensures that vote data is secure, immutable, and tamper-proof. MySQL database stores voter profiles, election details, and candidate information securely.**

**3.12 User-Friendly Interface**

**The platform is designed to be intuitive and easy to navigate for both technical and non-technical users.**

**Clear interfaces for admin dashboards and voter dashboards improve usability and engagement.**

**3.13 Auditable Blockchain Ledger**

**Every vote has a unique transaction hash, which can be used to verify authenticity without compromising voter privacy. This creates trust and accountability in the election process.**

**3.14 Mobile and Web Compatibility**

**TrueVote supports both desktop and mobile devices, enabling users to participate from anywhere. The responsive design ensures a smooth voting experience across platforms.**

**3.15 Secure Result Backup**

**All election data and results are stored on the blockchain and mirrored in a secure database backup, preventing data loss.**

### CHAPTER 4

### METHODOLOGY

The methodology for the TrueVote project follows a structured and multi-phase approach aimed at developing a secure, transparent, and decentralized online voting system using blockchain technology. It integrates PHP-based web development for the application layer, MySQL for efficient data management, and Ethereum smart contracts for blockchain integration. The goal is to ensure that each vote remains authentic, immutable, and verifiable while maintaining user privacy and the overall integrity of the election process.

This approach is designed to streamline the entire election workflow—from voter registration to result declaration—while ensuring data accuracy, user trust, and system scalability. The methodology progresses through several stages, including voter registration, authentication, election setup, blockchain-based vote casting, and result verification. Each component is carefully coordinated to maintain a tamper-proof and verifiable voting experience. Overall, this methodology ensures that both voters and administrators interact within a secure, transparent, and user-friendly digital environment that upholds democratic principles and fosters trust in digital voting.

**4.1 Data Collection and User Registration**

The first phase of the TrueVote system involves collecting essential voter and election-related data. During registration, voters provide basic information such as their name, email, Voter ID, and password. Administrators then verify and approve these registrations after validating the Voter ID details to ensure authenticity. Meanwhile, candidate and election information—such as the election title, code, type, and constituency—are entered by the admin through dedicated web forms.

All the collected data is stored in relational MySQL tables such as voters, elections, candidates, and votes, which are linked using foreign key relationships to maintain referential integrity. Data validation mechanisms prevent duplicate or invalid registrations, while sensitive information such as passwords remains encrypted to ensure voter privacy and data protection.

**4.2 Preprocessing and Authentication**

Before the voting phase begins, the system undergoes preprocessing and authentication to ensure that only eligible voters are allowed to participate. Each user must verify their identity through an email-based OTP system, which prevents impersonation and unauthorized access. During this phase, session validation mechanisms are also enforced to restrict voters to a single active session, thereby preventing multiple logins from different devices.

Additionally, an eligibility check is performed to ensure that voters can participate only in the elections for which they are registered and that are currently active. This preprocessing phase guarantees the accuracy and authenticity of voter and election data before any interaction with the blockchain layer takes place.

**4.3 Blockchain Integration and Vote Casting**

The core of the TrueVote system lies in its integration with blockchain technology, which ensures transparency, immutability, and accountability. Once a voter’s identity is successfully verified through the OTP process, they are permitted to cast their vote via the web interface. The selected candidate’s ID, along with the voter’s unique details, is transmitted to a smart contract deployed on the Ethereum blockchain.

The smart contract validates whether the voter has already voted in that particular election, ensuring the “one person, one vote” principle. Each submitted vote is stored as a unique blockchain transaction, identified by a distinct transaction hash. This hash makes every vote publicly verifiable and immutable, guaranteeing that no one can alter or delete recorded votes. Through this mechanism, the TrueVote system eliminates the possibility of vote manipulation or tampering, thereby ensuring complete transparency.

**4.4 Smart Contract Logic and Result Computation**

Smart contracts, written in Solidity, manage the backend logic for recording and counting votes. Once a transaction is confirmed on the blockchain, the corresponding candidate’s vote tally is automatically updated. These smart contracts also contain access control features that allow only administrators to create or close elections, ensuring that sensitive operations are restricted to authorized personnel.

At the conclusion of an election, the results are computed automatically on the blockchain and displayed on both the admin and voter dashboards. This automation removes the need for manual vote counting, significantly reducing the chances of human error and enhancing public trust in the election process through transparent result computation.

**4.5 Security Measures and Data Protection**

Security plays a crucial role at every stage of the TrueVote system. User passwords are encrypted using PHP’s password\_hash() function before being stored in the database, ensuring that sensitive credentials remain protected. Session management is implemented to prevent simultaneous multiple logins by a single user, and blockchain data remains unalterable once recorded, guaranteeing complete immutability.

Additionally, regular database backups and strict server-side validations are performed to safeguard against data corruption and unauthorized access. Administrative permissions are also restricted to ensure that only verified users can perform critical operations such as approving candidates or publishing results. These combined security measures maintain the integrity and reliability of both the centralized and decentralized components of the system.

**4.6 System Workflow and Role Interaction**

The overall workflow of the TrueVote platform integrates three primary modules: Admin, Voter, and Blockchain Layer. The administrator is responsible for creating and managing elections, verifying voter and candidate information, and publishing results. The voter, on the other hand, registers on the platform, verifies their identity through an OTP, views available elections, casts their vote via blockchain, and later checks the published results.

Meanwhile, the blockchain layer executes smart contract functions, validates transactions, and immutably stores vote hashes. This modular interaction ensures seamless coordination between all system components, maintaining a transparent and efficient election lifecycle from registration to result verification.

**4.7 User Interface and Dashboard Integration**

The user interface of TrueVote is designed using HTML, CSS, JavaScript, and Bootstrap, providing an intuitive and responsive experience for both voters and administrators. The voter dashboard displays relevant election details, candidate profiles, and a record of voting history, including blockchain transaction hashes for transparency. The administrator dashboard offers comprehensive control over voter management, candidate verification, election scheduling, and the publication of results.

Through its interactive design and responsive layout, the interface ensures accessibility across different devices. Additionally, real-time notifications and feedback messages keep users informed about important election updates, verification statuses, and results, contributing to an engaging and transparent digital voting experience.

### CHAPTER 5

### SYSTEM ARCHITECTURE

****

**FIGURE 5.1. *System Architecture***

The system architecture of the TrueVote project represents the interaction between key system components — namely the Admin, Voters, the TrueVote Web Application, and the Database integrated with the Blockchain Network.

It defines the logical structure and data flow among these entities to ensure secure, transparent, and tamper-proof election management — from voter registration to result publication.

The architecture adopts a three-tier design — User Interface Layer, Application Layer, and Database Layer with Blockchain Integration — each playing a vital role in maintaining efficiency, scalability, and security.

**5.1 User Interface Layer**

* This layer provides a user-friendly interface for both Admin and Voters.
* Voters can register, verify OTP, log in, view elections, and cast votes securely through interactive web forms.
* Admins can manage elections, add candidates, verify voters, and publish results.
* The system ensures smooth navigation with role-based access control, preventing unauthorized access to admin or voting features.
* Designed using HTML, CSS, JavaScript, and PHP, the interface ensures responsiveness across mobile and desktop devices.

**5.2** **Application Layer**

* The Application Layer serves as the core processing unit that manages all logical operations and interactions between the UI and the backend database.
* It handles:
* Authentication & OTP verification
* Election and candidate management
* Blockchain transaction initiation for vote recording
* Vote counting and result retrieval through smart contracts
* When a voter logs in, the system authenticates credentials and ensures that the user is authorized

for a specific election.

* Key modules in this layer include:
* Voter Management: Registers and verifies voters.
* Election Management: Admin can create, update, or close elections.
* Blockchain Handler: Connects to the Ethereum smart contract for vote transactions.
* Result Module: Fetches and displays vote counts from blockchain data.
* This layer ensures smooth, real-time communication between the web application, the database and the blockchain network.

**5.3 Database Layer**

* The Database Layer stores and manages all critical system information using MySQL.
* It includes structured tables such as:
* Admin – Stores admin credentials and privileges.
* Voter – Holds voter details, verification status, and login credentials.
* Election – Contains election metadata and schedule.
* Candidate – Stores candidate details and linked election IDs.
* Vote – Records voting activities and status flags.
* OTPlog – Logs OTP generation and verification attempts.
* BlockchainRecords – Maintains transaction hashes and timestamps for transparency.
* The database ensures referential integrity, encryption of sensitive data, and high availability through efficient indexing and query optimization.

**5.4 Admin Module**

* The Admin acts as the supervisory authority of the TrueVote system.
* Responsibilities include:
* Verifying and approving voter registrations.
* Creating and managing elections and candidates.
* Monitoring voting progress and blockchain transaction logs.
* Publishing verified results after election closure.
* Admins have exclusive access to analytical reports, system logs, and error monitoring tools to ensure fair and transparent elections.

**5.5 Voter Module**

* The Voter is the primary user interacting with the TrueVote platform.
* Functionalities include:
* Registration & OTP verification to confirm identity.
* Viewing active elections and candidate lists.
* Casting votes securely — each vote triggers a blockchain transaction recorded on the Ethereum ledger.
* Viewing voting history and blockchain transaction hashes for verification.
* Each voter is restricted to casting one vote per election, enforced through smart contract validation.

**5.6 Data Flow and Communication**

* The architecture ensures bidirectional communication between the web system, database, and blockchain:
* When a voter registers, details are stored in the database and verified via OTP.
* During voting, the system interacts with the blockchain smart contract to record

the vote transaction.

* The transaction hash is then stored in the database for future reference.
* Admins retrieve summarized election data and results directly from both the database

and blockchain records.

* This seamless data flow maintains synchronization and transparency across all layers.

**5.7 Security and Access Control**

* Role-based authentication ensures only authorized users perform sensitive operations.
* Data encryption protects stored voter credentials and transaction details.
* Blockchain immutability prevents tampering or double voting.
* Session management ensures single-login enforcement and automatic logout on inactivity.
* Regular backups and audit trails enhance reliability and accountability.

### 

### 

### CHAPTER 6

### MODULES

TrueVote – Blockchain-Based Secure E-Voting System is designed with multiple functional modules to provide a transparent, tamper-proof, and user-friendly digital voting experience. Each module serves a unique role in ensuring smooth election operations, secure data management, and a seamless experience for both administrators and voters. The system follows a role-based design where modules are specifically tailored for Admins, Voters, and System Administrators (Super Admins) to ensure efficiency, security, and accountability throughout the electoral process. The following sections describe each major module of the TrueVote system in detail.

**6.1 Admin Modules**

**6.1.1 Admin Dashboard**

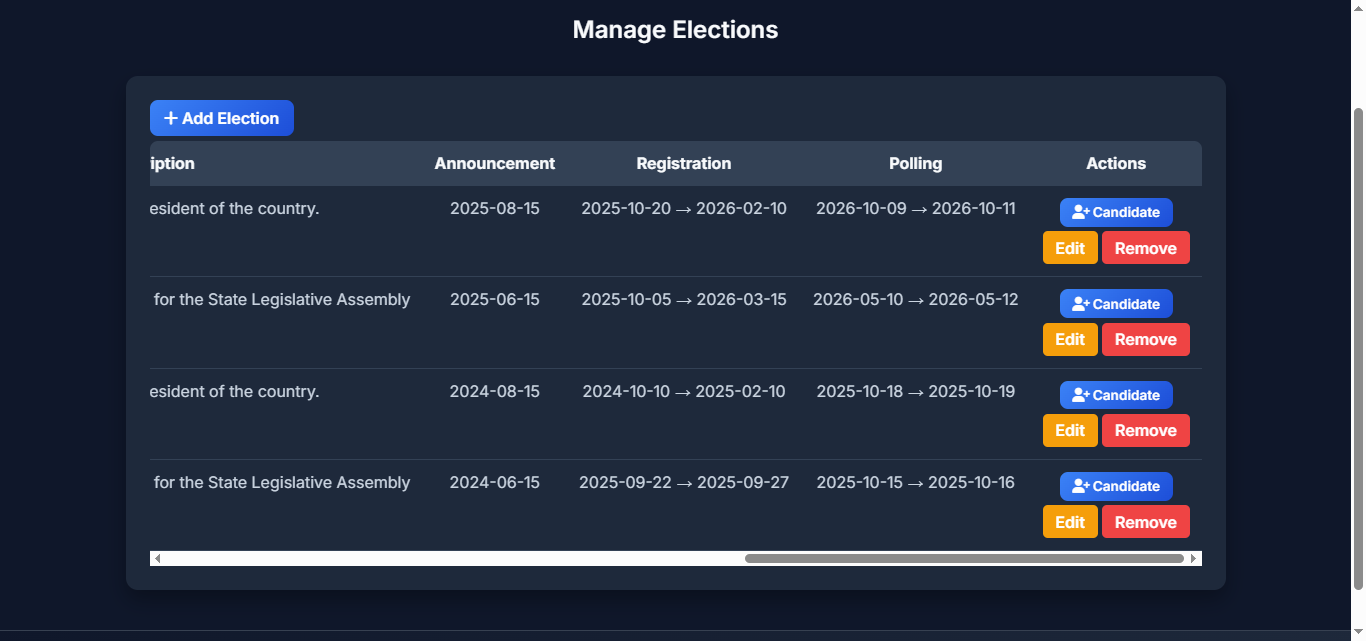
The Admin Dashboard serves as the central control hub of the TrueVote system, allowing administrators to monitor and manage all election activities in real time. It displays vital statistics such as Total Elections, Approved Voters, Active Elections, and Published Results. The dashboard also offers quick access to manage voters, candidates, and election records while monitoring blockchain status for transaction integrity. This centralized view helps administrators oversee the election lifecycle and ensure transparency and smooth operations.



***FIGURE 6.1 Admin Dashboard***

**6.1.2 Election Management**

The Election Management module enables administrators to create, configure, and manage elections. Admins can specify election names, types (general, by-election, local body), schedule start and end times, and assign candidates. Once elections are created, the system automatically generates a secure blockchain-based record for vote tracking. The module also provides options to view ongoing and completed elections, ensuring full control and traceability of all electoral activities.



***FIGURE 6.2 Election management***

**6.1.3 Candidate Management**

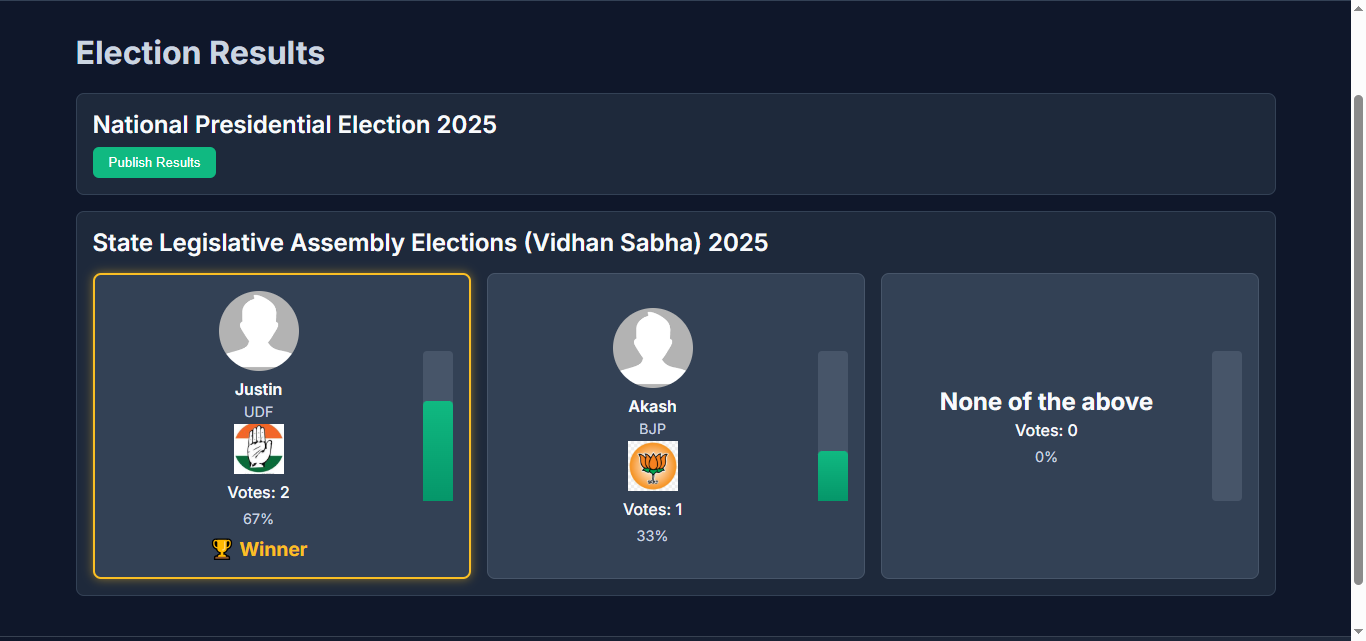
The Candidate Management Module allows the administrator to efficiently add, verify, edit, and remove candidates contesting in elections. Each record includes details such as candidate name, party symbol, photo, age, and constituency. Before publishing, the admin verifies candidate details to ensure authenticity and prevent duplicate or invalid entries. Once approved, candidate information is securely stored on the blockchain, ensuring immutability and transparency. The module also supports updates in case of by-elections and provides an organized interface to view or search candidate details by election type. Role-based access control ensures that only authorized administrators can make changes. By maintaining accurate and verified candidate records, this module ensures fairness, credibility, and trust in the digital election process.

****

***FIGURE 6.3 Candidate Management***

**6.1.4 Result Declaration**

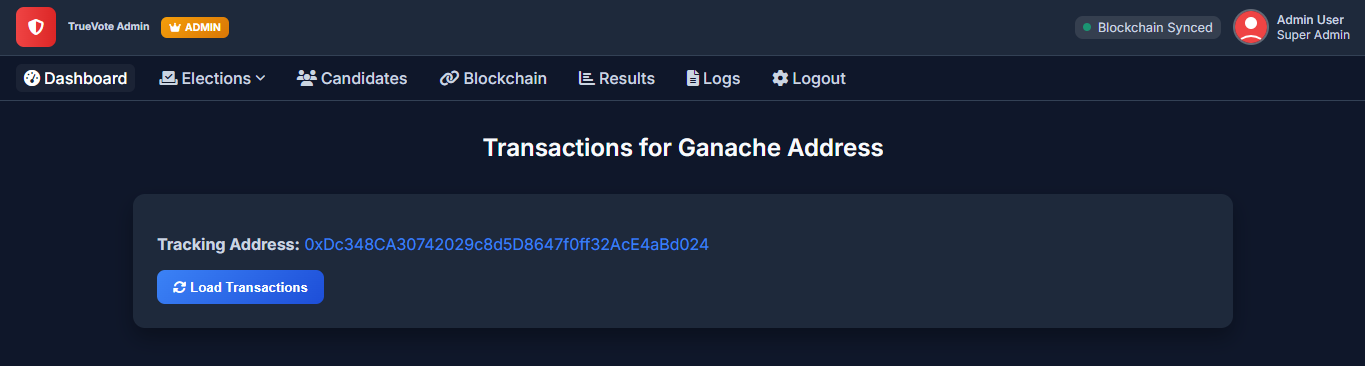
The Result Declaration Module is responsible for processing, verifying, and displaying election outcomes once the voting phase concludes. It retrieves vote data directly from the blockchain ledger, ensuring complete transparency and immutability of results. The module automatically aggregates votes, calculates percentages, and identifies the winning candidate based on the highest vote count. Real-time visual representations such as bar and pie charts enhance result clarity for administrators and the public. Additionally, the admin can publish, revoke, or archive election results and generate downloadable reports for official documentation. This automated, tamper-proof process eliminates human counting errors, enhances trust in the system, and ensures that results are fair, accurate, and verifiable through the blockchain audit trail.

****

***FIGURE 6.4 Result Declaration***

**6.1.5 Blockchain Monitoring**

The Blockchain Monitoring Module gives super administrators real-time insights into all TrueVote blockchain operations. It tracks new blocks, verifying hashes, timestamps, and transaction validity to ensure integrity and immutability. All transactions, including votes and candidate registrations, are logged while preserving voter anonymity. The system prevents duplicates and tampering, monitors node synchronization, and confirms transactions, enhancing reliability. This module ensures that every recorded vote remains secure, transparent, and permanently verifiable on the blockchain.

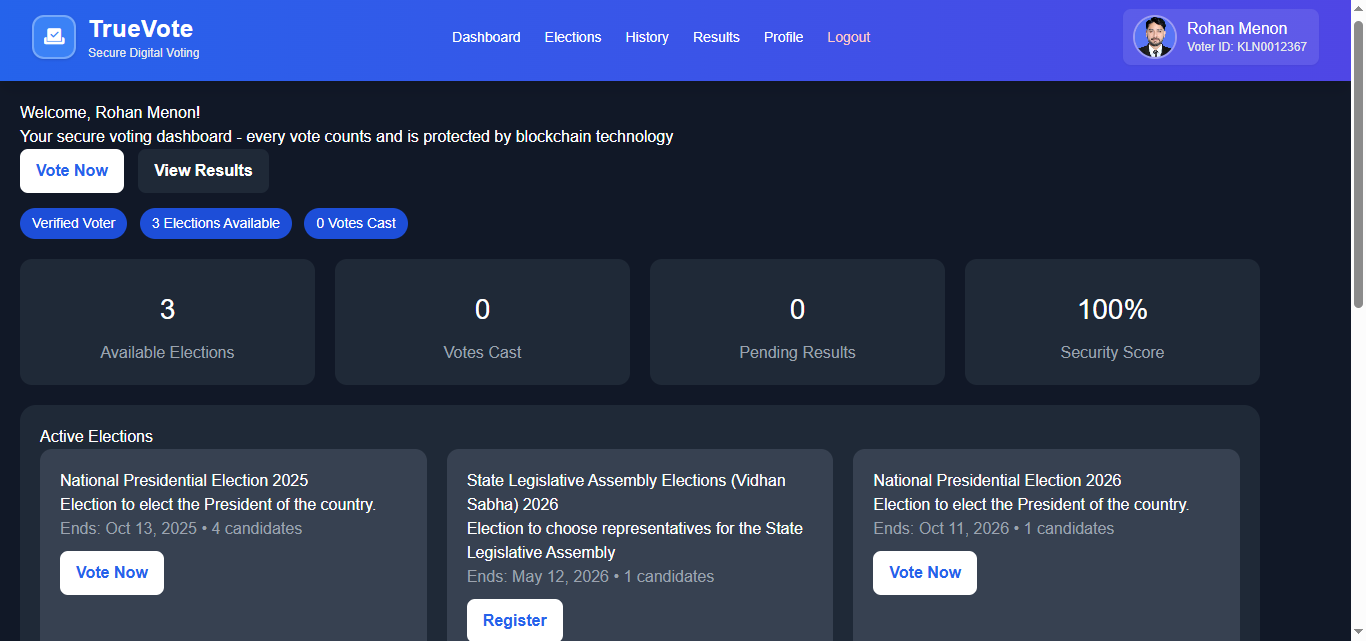


***FIGURE 6.5 Blockchain Monitoring***

**6.2 Voter Modules**

**6.2.1 Voter Dashboard**

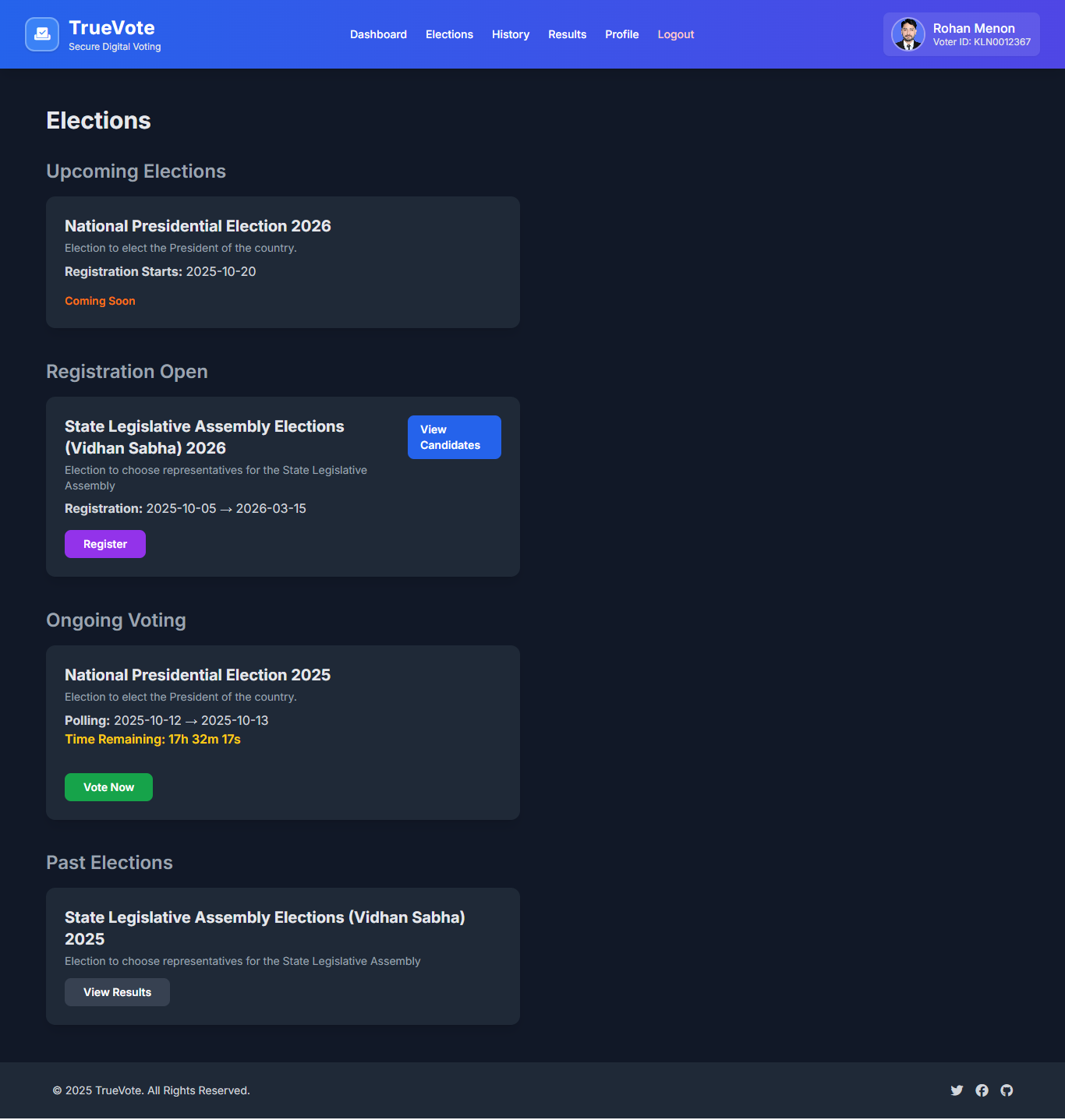
The Voter Dashboard serves as the primary interface for registered users, providing a centralized platform to manage all voting-related activities within the TrueVote system. It presents key election details such as Ongoing, Upcoming, and Past Elections, allowing voters to stay informed and participate actively. Each election listing includes candidate profiles, party symbols, and relevant timelines for easy reference. The dashboard also integrates blockchain verification indicators to assure users of data integrity and transparency. Voters receive real-time notifications, alerts, and reminders regarding election schedules, deadlines, and result announcements. Additionally, the interface offers quick access to voting guidelines, personal profile details, and status updates, ensuring a smooth and user-friendly voting experience that promotes trust, accessibility, and active civic participation in the digital election process.



***FIGURE 6.6 Voter Dashboard***

**6.2.2 Election Page**

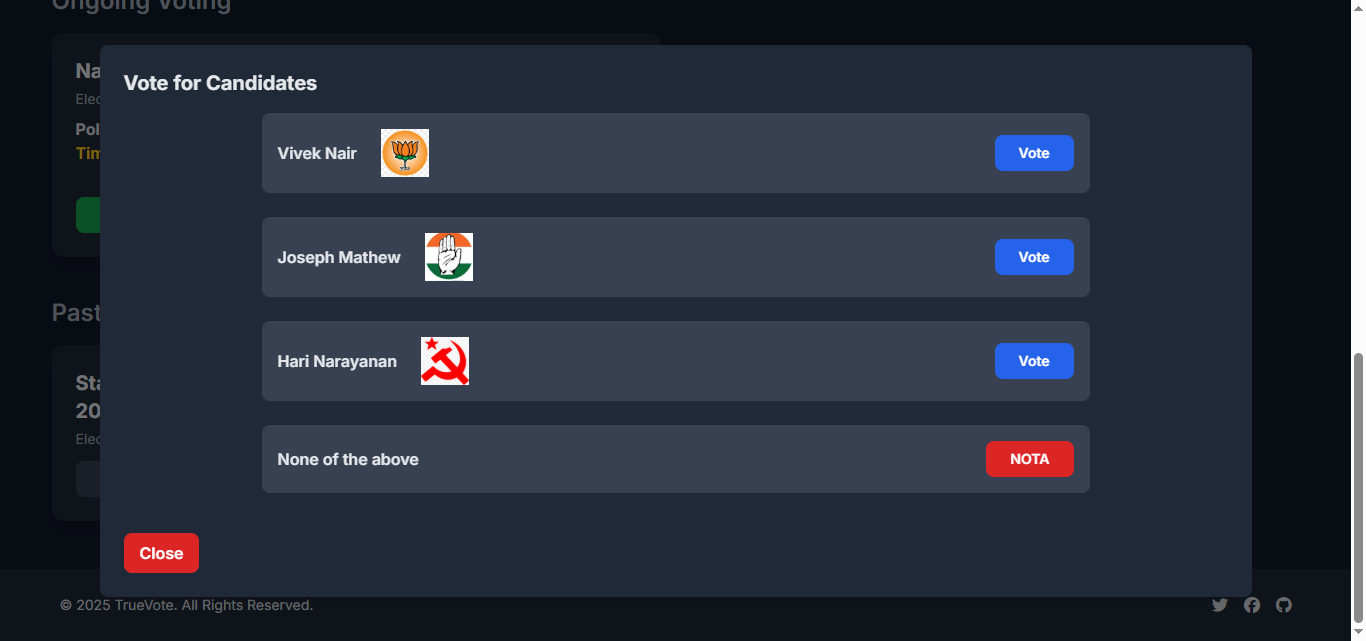
The Elections Page module is a vital component of the TrueVote system, offering structured, time-based access to all elections. It allows voters to navigate seamlessly by categorizing elections into Upcoming, Registration Open, Ongoing, and Past statuses. This organization ensures that users can easily identify which elections they are eligible to participate in, track upcoming events, and review past results. By providing clear timelines and status updates, the module enhances transparency and accountability within the electoral process. It also supports efficient management of the electoral lifecycle, from voter registration and active participation to post-election analysis and archival of results.



***FIGURE 6.7 Election page***

**6.2.3 Voting Page**

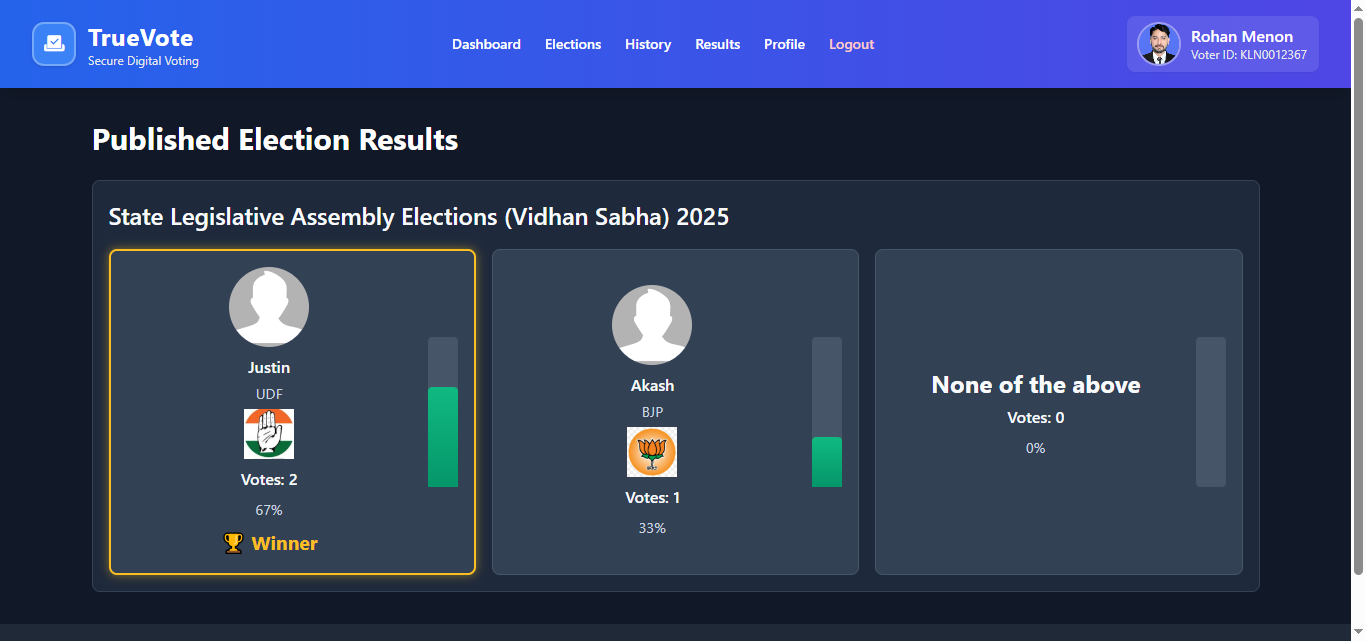
The Voting Page serves as the core interface of the TrueVote system, enabling voters to cast their votes securely and effortlessly. Each authenticated voter is presented with a verified list of candidates, complete with names, party symbols, and a NOTA (None of the Above) option. Before allowing submission, the system verifies voter eligibility and ensures that each user votes only once. Upon confirmation, the vote is instantly encrypted and recorded as an immutable blockchain transaction, guaranteeing transparency and tamper-proof storage. This process upholds fairness, data integrity, and voter anonymity, ensuring that every ballot cast is secure, verifiable, and permanently stored on the blockchain ledger.



***FIGURE 6.8 Voting page***

**6.2.4 Result Page**

The Results View module allows voters to access published election outcomes in a clear and transparent manner. Results are presented through visual charts and candidate cards, showing total votes, vote percentages, and the declared winner. Each voter can verify that their vote was securely recorded and counted using blockchain references, ensuring integrity and trust in the digital voting process. By combining intuitive visualizations with blockchain-backed verification, the module not only simplifies result interpretation but also reinforces confidence in the system. It serves as a key tool for transparency, accountability, and voter assurance within the TrueVote platform.



***FIGURE 6.9 Result page***

### 

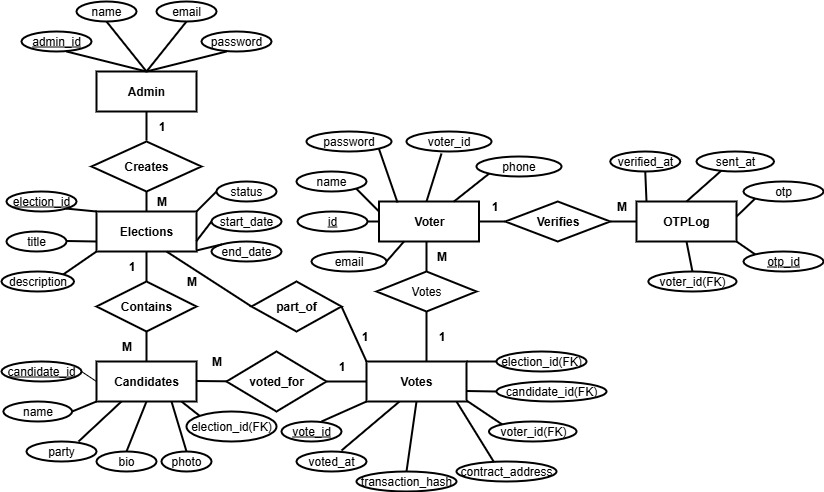
### 

### CHAPTER 7

### DIAGRAMS

**7.1 Entity Relationship (ER) Diagram**

The ER Diagram of the TrueVote system illustrates the relationships between key entities such as Admin, Voter, Election, Candidate, Vote, and OTPLog. Admin manages elections and candidates, while Voters register, verify identity using OTP, and cast votes securely. The Election entity holds details like title, description, and duration, and each election includes multiple candidates. The Vote entity links voters, candidates, and elections, storing information such as transaction hash and timestamp for blockchain verification. The OTPLog entity records OTP verification details to ensure secure authentication. Overall, the diagram shows how all components interact to ensure transparent, verifiable, and tamper-proof digital voting.



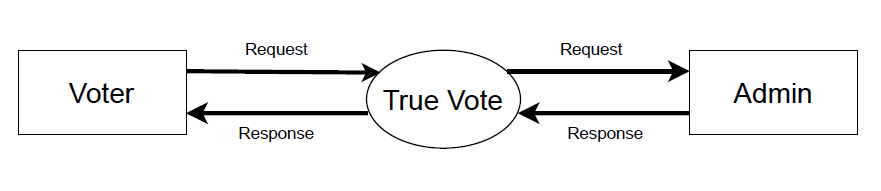
**FIGURE 7.1 *ER diagram***

**7.2 Data Flow Diagram (DFD)**

The Data Flow Diagram (DFD) of the TrueVote system represents how data flows between different components of the digital voting platform. It illustrates the exchange of information between voters, admins, and the blockchain-based system. The Admin manages elections and candidates, while Voters interact with the system through processes like registration, OTP verification, and casting votes. The system validates inputs, records votes securely on the blockchain, and stores related data such as election details, voter credentials, and transaction logs. Overall, the DFD provides a clear overview of how secure and transparent data processing occurs in TrueVote.

**7.2.1 LEVEL 0 DFD**

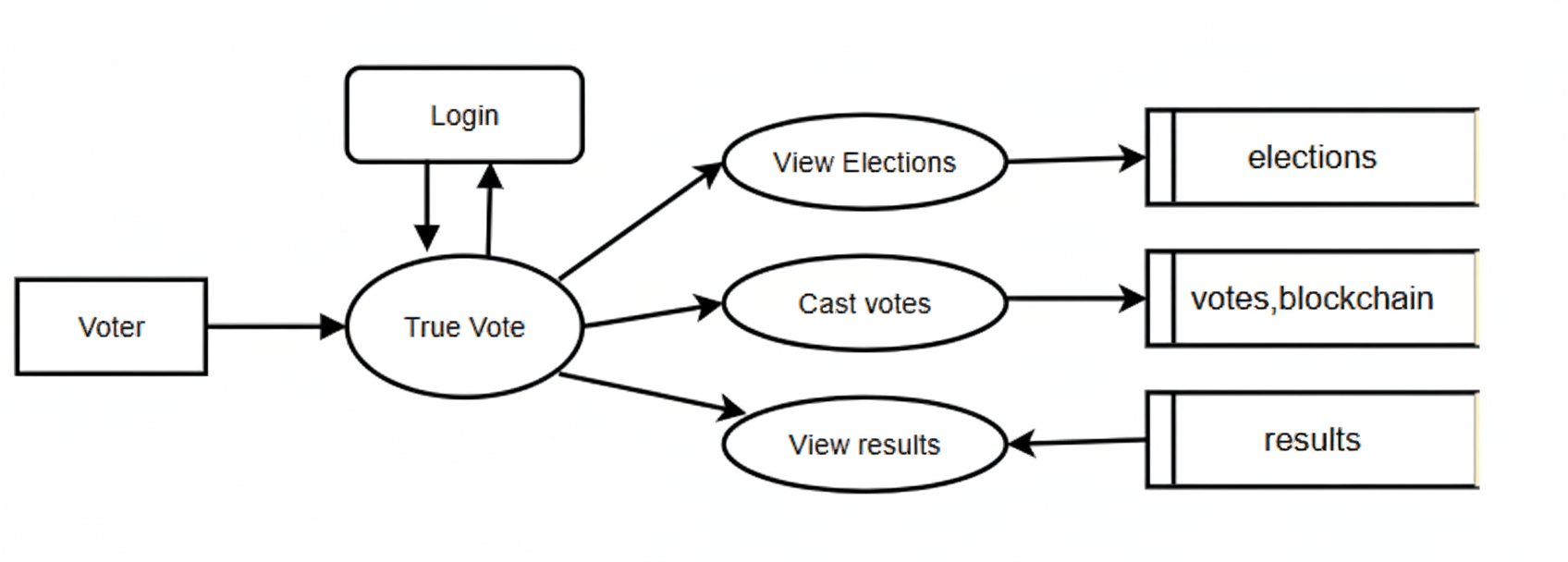
A Level 0 Data Flow Diagram, also known as a context diagram, provides an overall view of the TrueVote system as a single process. It shows how the system interacts with external entities such as Voters and Admins by representing the flow of requests and responses between them. Voters send requests for registration, authentication, and voting, while Admins manage elections and candidate data. The system processes these requests and provides responses accordingly. In simple terms, this diagram defines the boundaries of TrueVote and its relationship with the external environment.



**FIGURE 7.2 *DFD Level 0***

**7.2.2 LEVEL 1 DFD VOTER**

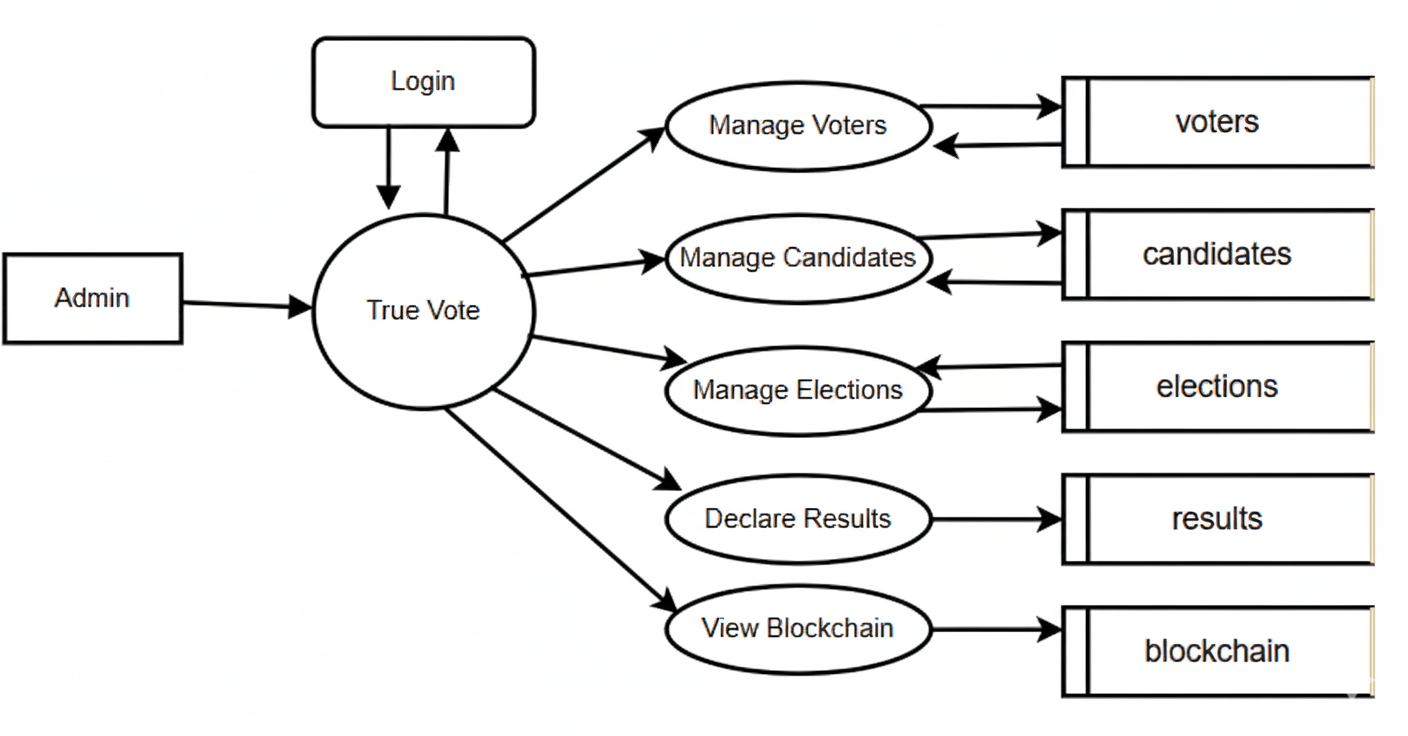
A Level 1 Data Flow Diagram (DFD) for voter provides a detailed breakdown of the main processes that occur within the system and shows how data flows between the voter, the system’s internal components, and the data stores. It expands on the Level 0 DFD by illustrating the internal functions that handle specific voter actions.



**FIGURE 7.3 *DFD Level 1 Voter***

**7.2.3 LEVEL 1 DFD ADMIN**

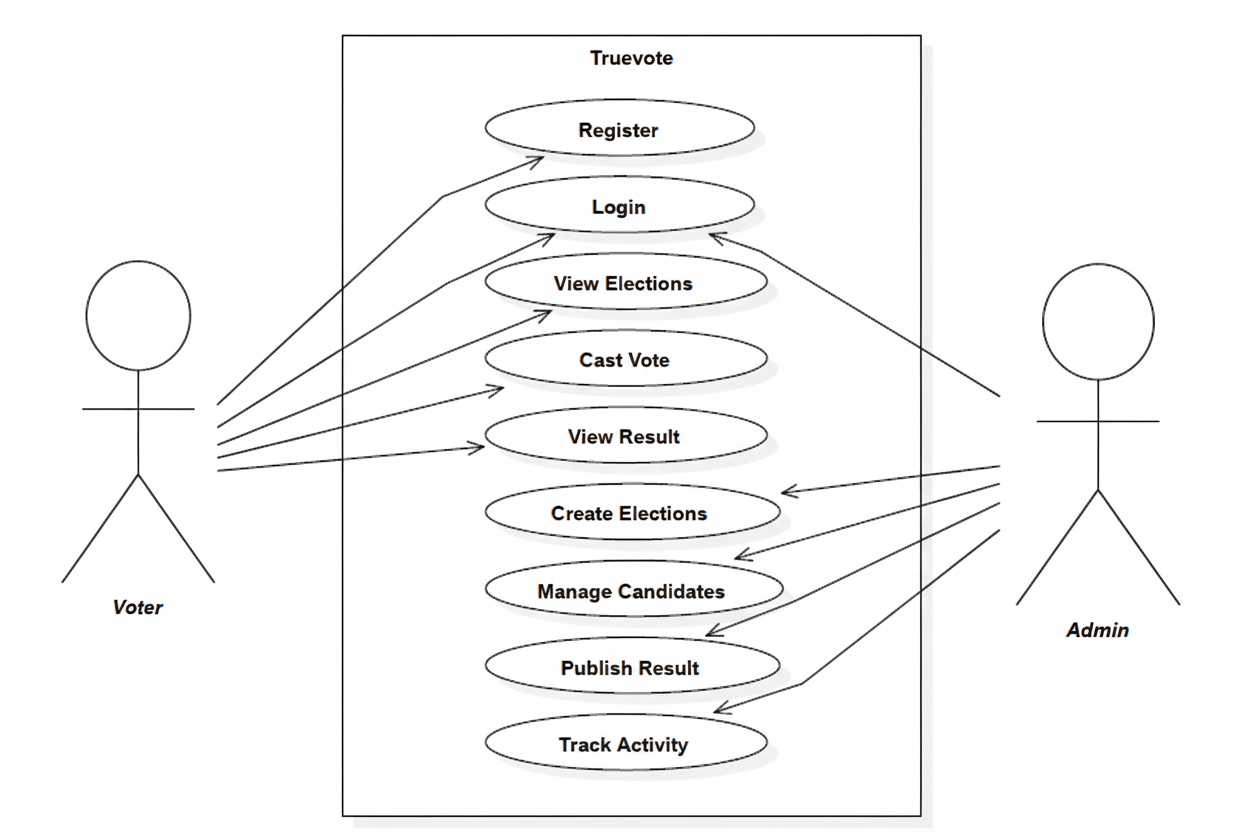
The Level 1 Data Flow Diagram (DFD) for Admin illustrates how the administrator interacts with different internal processes of the system to ensure smooth management, monitoring, and control. It breaks down the main activities the admin performs and shows how data moves between the admin, system modules, and data stores. Thus, the Level 1 DFD for the admin clearly represents how the administrator interacts with multiple processes and databases to maintain order, security, and efficiency across the entire system.



**FIGURE 7.4 *DFD Level 1 Admin***

**7.3 USECASE DIAGRAM**

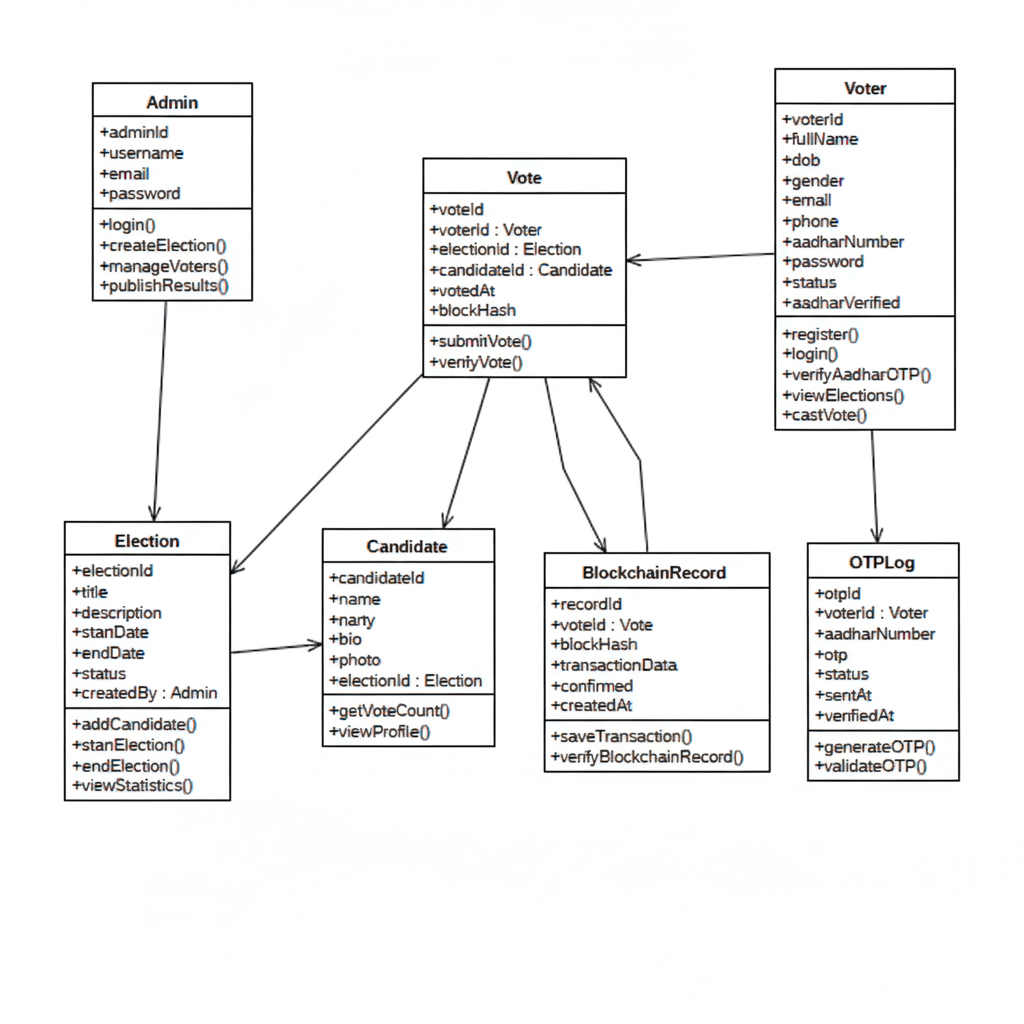
A Use Case Diagram visually represents the interactions between users and a system, showing how external actors communicate with the system’s main functions. It illustrates the relationships between different roles and the actions they can perform, providing a clear picture of the system’s functional scope. The diagram helps to identify who will use the system and what operations they will carry out, making it easier to understand user requirements and system behaviour. Each actor represents a specific type of user or external entity, while each use case describes a goal that the actor wants to achieve through the system.



**FIGURE 7.5 *Use Case Diagram***

**7.4 CLASS DIAGRAM**

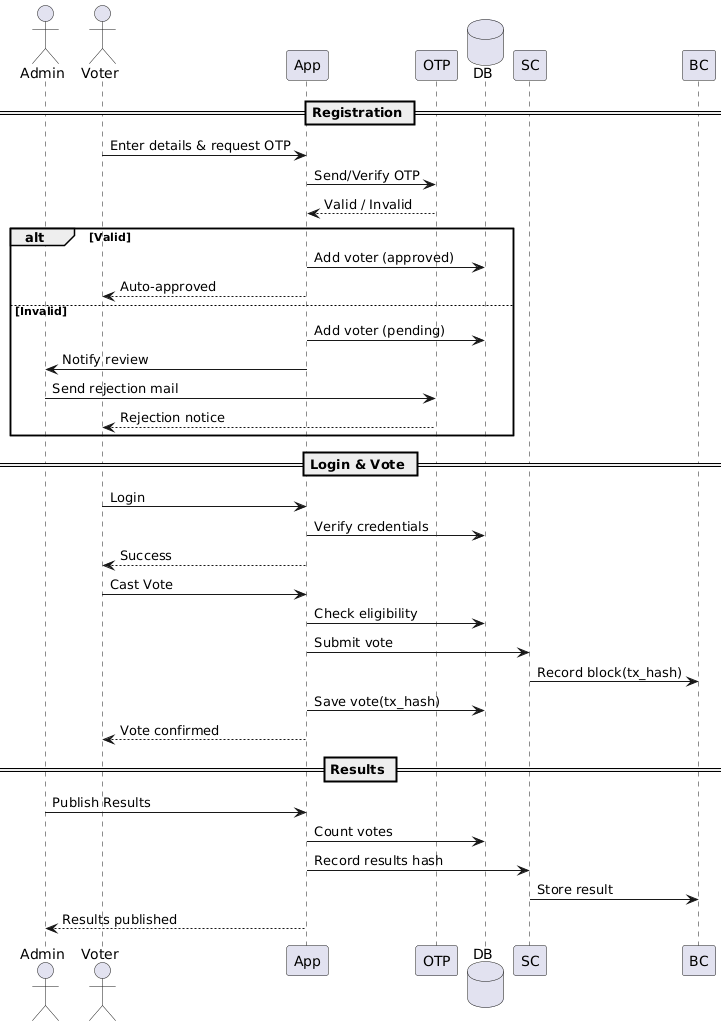
A Class Diagram provides a detailed structural view of a system by illustrating its classes, attributes, methods, and the relationships between them. It serves as a blueprint for the system’s object-oriented design, showing how different entities interact and depend on one another. In a class diagram, each class represents a real-world concept or component within the system, containing its properties and behaviours. The diagram also depicts various relationships such as inheritance, association, aggregation, and composition, which define how classes collaborate to perform system functions.



**FIGURE 7.6 *Class Diagram***

**7.5 SEQUENCE DIAGRAM**

A Sequence Diagram is a type of diagram that illustrates how actors and components interact with each other in a particular sequence over time. It visually represents the flow of messages or interactions between different components or actors in the system to accomplish a specific function or process. In the TrueVote project, the sequence diagram shows how the Admin, Voter, App, Database, and Blockchain components communicate during activities like registration, login, voting, and result publication, highlighting the order and timing of each interaction.



**FIGURE 7.7 *Sequence Diagram***

**CHAPTER 8**

**TESTING**

**8.1 Overview**

Testing is a crucial phase in the development of the TrueVote – Blockchain-Based Voting System, ensuring that every component functions as intended, meets security and usability standards, and maintains system integrity. Since the project deals with sensitive election data and blockchain operations, thorough testing was conducted to verify accuracy, transparency, and performance. This phase helped detect and resolve potential bugs, confirm that all modules interacted properly, and ensure the system operated seamlessly under real-world conditions. The testing process validated both the technical and functional aspects of the application, guaranteeing that TrueVote is reliable, secure, and ready for deployment in actual election environments.

**8.2 Objectives of Testing**

The main objective of testing the TrueVote system was to ensure accuracy, security, and performance across all modules. Specific goals included verifying that the voting, candidate management, voter authentication, and result declaration modules worked according to specified requirements. Testing also aimed to ensure immutability of blockchain transactions, prevention of duplicate votes, and secure data handling during user interactions. Additionally, response time, system scalability, and user accessibility were evaluated. Overall, the goal was to confirm that TrueVote delivered a smooth, transparent, and tamper-proof digital voting experience.

**8.3 Types of Testing Conducted**

Multiple testing methods were applied to ensure the robustness and reliability of the TrueVote system. These included:

* Unit Testing: Verification of individual modules such as login, candidate registration, and vote casting.
* Integration Testing: Ensured seamless interaction among modules like voter authentication, blockchain transaction handling, and result computation.
* System Testing: Evaluated the complete workflow of the voting process from registration to result declaration.
* User Acceptance Testing (UAT): Ensured the system met the expectations of both voters and administrators.
* Performance and Security Testing: Tested response times, transaction speed, and protection against unauthorized access or tampering.

**8.4 Unit Testing**

Unit testing was the first phase, focused on checking the correctness of individual modules. Core functions such as voter registration, OTP verification, vote submission, and admin login were tested with sample data. Each function was validated for correct input handling, output generation, and exception management. For example, during testing, the system was verified to reject multiple votes from the same user and to properly encrypt each transaction before adding it to the blockchain. All minor bugs detected during this phase were corrected immediately to ensure stability in later testing stages.

**8.5 Integration Testing**

Integration testing ensured that different modules worked harmoniously together. The interaction between the frontend, backend, and blockchain network was tested to confirm smooth communication. For example, when a vote was cast, the system verified voter eligibility, recorded the vote on the blockchain, and updated the total vote count in real time. The testing ensured that the blockchain ledger accurately reflected all valid transactions without duplication or loss. Integration testing also validated the synchronization between the admin’s control panel and voter-side operations, confirming overall system coherence.

**8.6 System Testing**

System testing involved evaluating the entire TrueVote system as a whole. It verified the complete workflow, including voter authentication, candidate management, vote casting, and result display. The admin’s ability to monitor elections, manage candidates, and publish results was thoroughly checked. Realistic test data was used to simulate a full election cycle. The testing confirmed that the system maintained transparency, immutability, and accuracy throughout the process. Additionally, error handling, transaction logs, and blockchain audit trails were validated to ensure that the system operated reliably under all conditions.

**8.7 User Acceptance Testing (UAT)**

User Acceptance Testing was conducted with selected participants representing both voters and administrators. The users performed all major operations — such as logging in, viewing candidates, casting votes, and checking results. The testing confirmed that users could easily navigate the system and complete voting without confusion. Feedback was collected regarding clarity, response speed, and design. Based on this input, minor improvements were made to enhance usability. The test users reported that the process felt secure, simple, and trustworthy, confirming the system’s readiness for real-world deployment.

**8.8 Performance and Security Testing**

Performance and security testing were critical due to the sensitive nature of voting data. The system was tested under high loads to ensure it could handle multiple concurrent voters without lag or downtime. Response times for operations like voter authentication, blockchain transaction confirmation, and result updates remained within acceptable limits. Security testing involved checking for vulnerabilities such as SQL injection, unauthorized access, and data tampering. Encryption, hash verification, and blockchain integrity checks were validated to ensure that every vote remained immutable and private.

**8.9 Result Analysis**

The testing phase confirmed that the TrueVote system met all functional and non-functional requirements. All critical modules, including voter authentication, blockchain integration, and result declaration, performed accurately and consistently. Integration between the web interface, database, and blockchain was seamless, with no data loss or transaction errors. User feedback indicated high satisfaction with usability and system transparency. Performance analysis showed strong reliability even under simulated high voter traffic. Overall, the results demonstrated that TrueVote is secure, efficient, transparent, and ready for real-world election implementation.

### 

### 

### CHAPTER 9

### ADVANTAGES & DISADVANTAGES

**9.1 Advantages**

* **Enhanced Security:** TrueVote leverages blockchain technology to ensure that every vote is securely recorded and tamper-proof, eliminating risks of data manipulation or unauthorized access.
* **Transparency and Trust:** Since all voting transactions are stored on a public, immutable ledger, the system promotes complete transparency and builds voter confidence in the election process.
* **Elimination of Electoral Fraud:** The decentralized nature of blockchain prevents vote duplication, fake registrations, and result tampering, ensuring fair and verifiable elections.
* **Efficient Vote Counting:** Votes are automatically recorded and verified through smart contracts, enabling instant and accurate result generation without manual intervention.
* **User-Friendly Participation:** The platform offers a simple and intuitive interface where voters can securely register, verify via OTP, and cast their votes easily using any device with internet access.

**9.2 Disadvantages**

* **Dependence on Internet Connectivity:** As the system operates online, stable internet access is required. Poor connectivity may delay vote submission or transaction confirmation.
* **Blockchain Transaction Costs:** Deploying and executing smart contracts on blockchain networks may involve gas fees, which could increase operational costs during large-scale elections.
* **Technical Literacy Requirement:** Some voters may find it difficult to understand blockchain-based processes or online voting steps, especially those unfamiliar with digital systems.
* **Scalability Limitations:** Handling a massive number of simultaneous blockchain transactions during national elections could strain system performance and slow down processing times.
* **Data Privacy Concerns:** Although blockchain ensures transparency, storing voter-related data must comply with privacy standards to prevent misuse or unintended exposure of personal information.

### 

### 

### CHAPTER 10

### RESULT

### 

The TrueVote system was successfully conceptualized, designed, and implemented to provide a secure, transparent, and efficient digital voting platform. This system bridges the gap between traditional voting methods and emerging digital solutions by leveraging the power of blockchain technology and smart contracts to ensure that elections are conducted with the highest levels of trust and integrity. TrueVote brings together voters, administrators, and election authorities in a unified blockchain-based environment, ensuring complete end-to-end election management. From voter registration and verification to vote casting and result publication, each process is executed with accuracy, security, and transparency.

The system’s blockchain backbone plays a pivotal role in maintaining electoral integrity. Each vote is stored as a unique and immutable transaction on the blockchain, ensuring that it cannot be altered, deleted, or duplicated. This eliminates possibilities of vote tampering, unauthorized manipulation, or data breaches, which are common in centralized systems. The integration of OTP-based voter authentication ensures that only verified users can participate, maintaining the authenticity of each ballot. The design focuses equally on simplicity and reliability—allowing even non-technical users to participate in elections easily and confidently.

During the testing and evaluation phases, TrueVote exhibited outstanding performance in terms of both functionality and security. The system enabled voters to register and cast their votes seamlessly through an intuitive interface. Each registered voter could authenticate their identity using OTP verification before proceeding to vote, thereby ensuring that every vote cast was genuine. Administrators were equipped with a dedicated management dashboard to create elections, manage voter lists, and monitor progress in real time. The role-based access control mechanism ensured that different user roles—such as voters, administrators, and election officers—had restricted and clearly defined privileges, reducing the risk of unauthorized access or system abuse.

TrueVote also provided real-time visualization of election results, allowing instant access to aggregated data while preserving voter anonymity. This feature gave election authorities immediate insights into turnout statistics, region-wise participation, and performance analysis without compromising the confidentiality of individual votes. The integration of smart contracts automated vote validation and result generation, reducing manual intervention and human error while ensuring fairness and transparency.

Performance testing further validated the system’s scalability and stability. The platform could handle multiple concurrent users voting simultaneously without delays or crashes. Transactions on the blockchain were executed efficiently, and data synchronization occurred accurately between the database and blockchain ledger. The inclusion of encrypted authentication, secure connections, and blockchain verification strengthened the system’s resistance to cyberattacks and data breaches. Even under stress conditions, the system maintained consistent performance, confirming its readiness for larger-scale deployment in national or institutional elections.

User feedback played an important role in assessing the system’s usability and acceptance. Voters appreciated the platform’s ease of use, intuitive design, and smooth voting experience, highlighting how it removed many of the difficulties associated with traditional voting methods such as long queues, manual errors, and delayed counting. Administrators valued the automation, real-time monitoring, and data reliability provided by the dashboard, noting significant improvements in efficiency and accountability compared to conventional systems.

Overall, the TrueVote system successfully demonstrated that blockchain technology can serve as a practical and secure foundation for digital elections. It addressed major issues such as electoral fraud, lack of transparency, vote duplication, and inefficient counting. By providing tamper-proof and verifiable voting records, TrueVote reinforces trust among voters and ensures that every vote truly counts. The project establishes that decentralized systems can effectively enhance the credibility and fairness of elections in modern democracies.

### 

### 

### CHAPTER 11

### CONCLUSION & FUTURE SCOPE

**11.1 Conclusion**

The TrueVote project marks a major step forward in modernizing and securing the electoral process through blockchain technology. Traditional voting systems often face challenges such as vote tampering, unauthorized access, and lack of transparency. TrueVote addresses these limitations by leveraging blockchain’s decentralized and immutable nature, ensuring that each vote cast is permanently recorded and cannot be altered or deleted. Every transaction is cryptographically verified and stored on a distributed ledger, guaranteeing the integrity and authenticity of election data. This decentralized approach eliminates single points of failure and builds voter confidence in the credibility of results.

The system integrates several core modules such as voter registration, OTP-based authentication, candidate management, voting interface, result declaration, and blockchain monitoring, each designed to enhance transparency and reliability. Through its intuitive interface, TrueVote allows voters to securely authenticate themselves and cast their votes with a single click, while administrators can monitor blockchain transactions and verify results in real time. The use of smart contracts automates the result-counting process, eliminating manual intervention and ensuring fairness.

TrueVote not only provides security but also promotes inclusivity and accessibility. It empowers citizens to participate in elections digitally, breaking geographical barriers and reducing human dependency in election management. The transparency offered by blockchain technology builds trust among voters, administrators, and government authorities, ensuring that every vote is verifiable, confidential, and tamper-proof. The project also demonstrates how emerging technologies like blockchain can be effectively applied in civic systems to enhance governance, accountability, and efficiency.

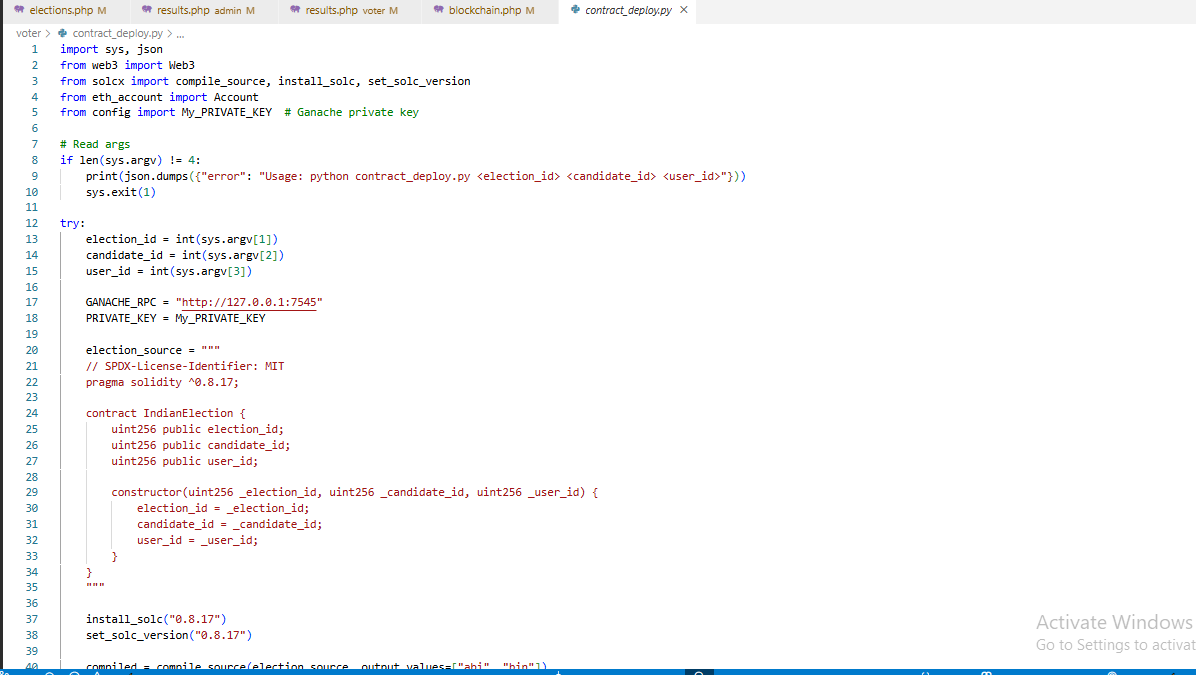
By successfully combining the principles of decentralization, cryptographic security, and automation, TrueVote lays a strong foundation for a new era of digital democracy. The project’s success validates the feasibility of implementing blockchain-based voting systems in real-world scenarios, providing a scalable, transparent, and corruption-resistant solution. Overall, TrueVote stands as a powerful example of how technology can reinforce public trust and integrity in the democratic process.

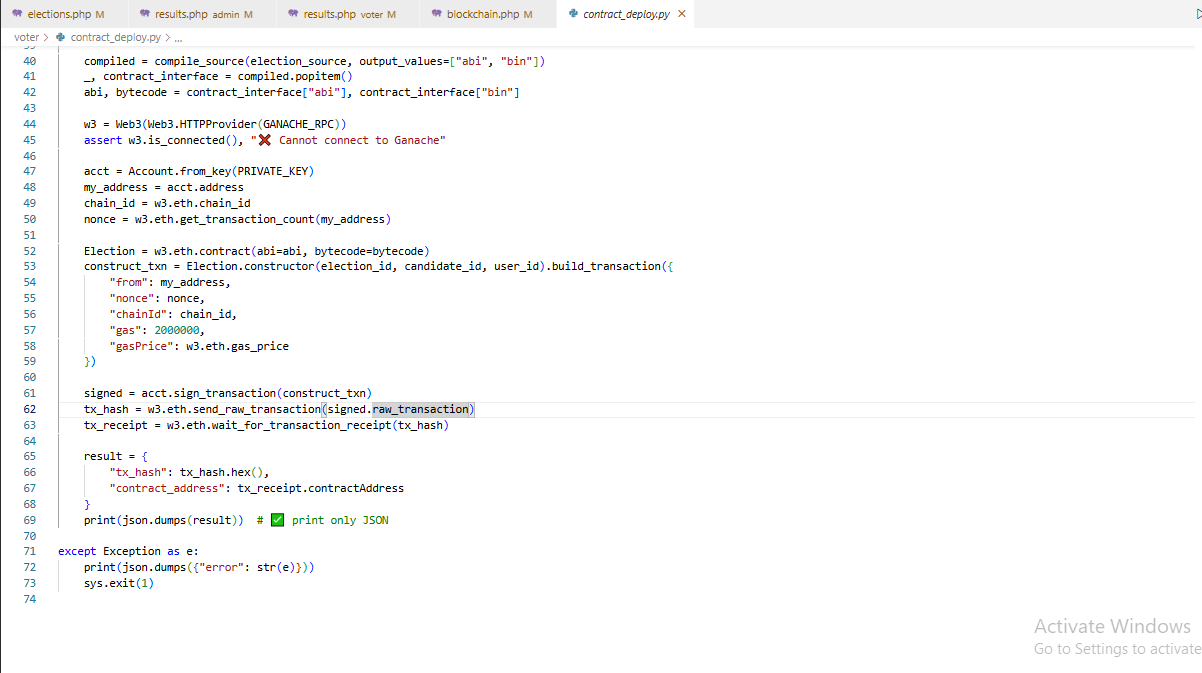
**11.2 Future Scope**

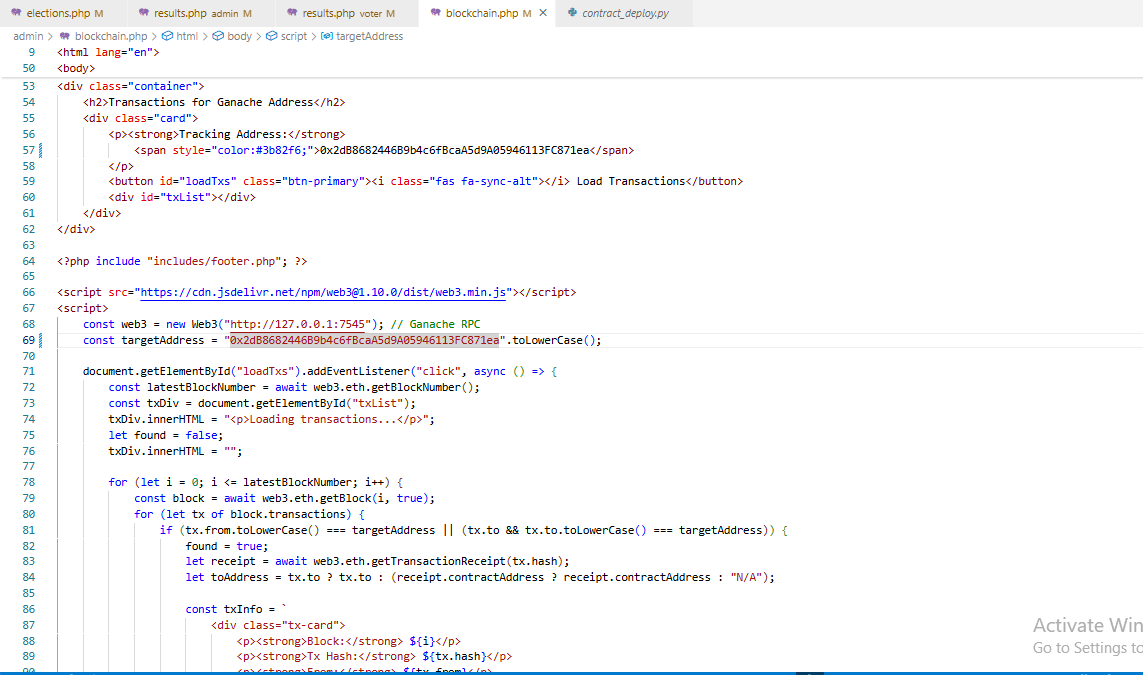
The future potential of TrueVote is vast, offering many opportunities to enhance scalability, accessibility, and voter trust. Future versions can integrate biometric authentication such as fingerprint and facial recognition to strengthen voter verification and prevent impersonation or multiple voting. A mobile-based version can further improve accessibility, enabling citizens to securely vote from anywhere, especially in rural areas. Integration with government ID databases like Aadhaar or national voter registries would ensure authenticity, while AI-driven analytics dashboards could provide real-time insights on voter turnout and participation trends without compromising privacy.

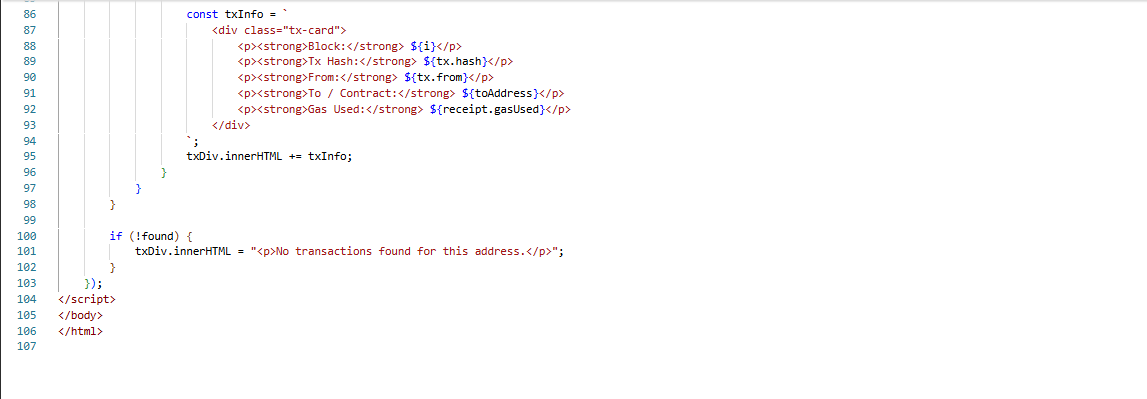
To further improve security and transparency, TrueVote can adopt decentralized storage networks like IPFS, AI-based fraud detection, and certified smart contract audits. Multilingual interfaces and accessibility features such as text-to-speech options will make the system more inclusive. Deploying TrueVote as a consortium blockchain managed by multiple election authorities will ensure fairness and decentralization. With cloud scalability, legal compliance, and robust infrastructure, TrueVote can evolve into a trusted digital voting solution for large-scale political, institutional, and organizational elections—upholding security, transparency, and fairness in every vote cast.

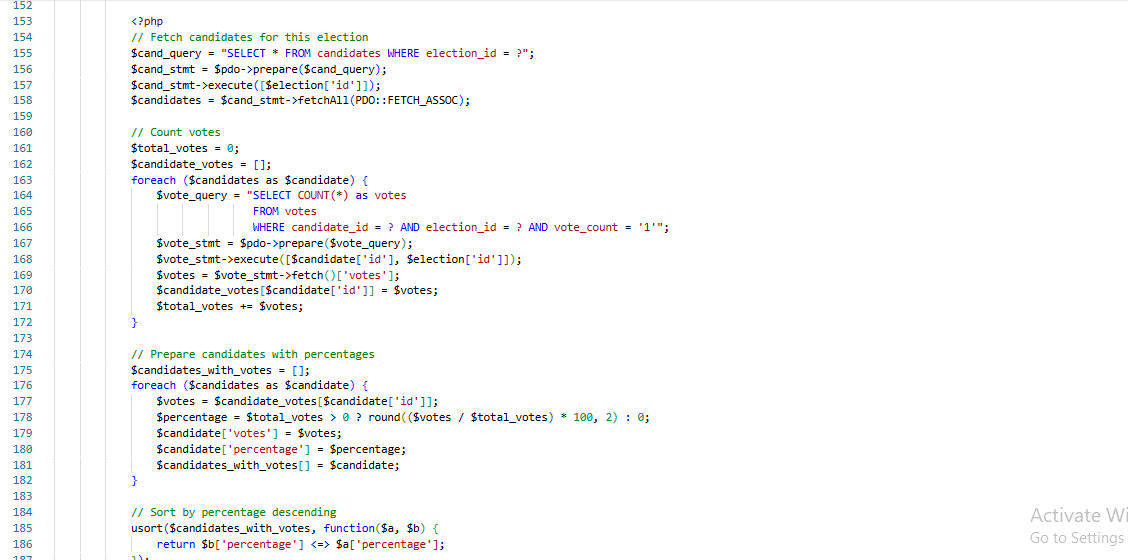
**APPENDICES**

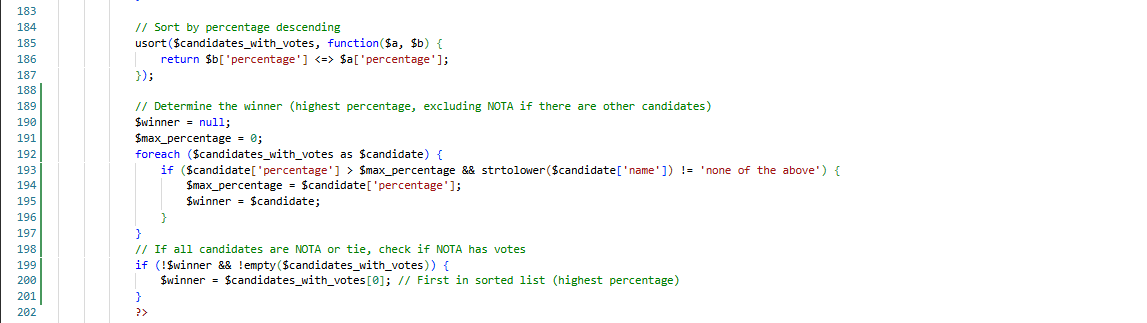












**REFERENCES**

**[1].** **Ali, R., Anwar, Z., & Khan, S.** (2020): Decentralized E-Voting System Using Ethereum Blockchain. [Source: IEEE Xplore]

**[2]**. **Kshetri, N., & Voas, J.** (2020): Blockchain-Enabled E-Voting. [Source: IEEE Computer]

**[3].** **Hardwick, F. S., Akram, R. N., & Markantonakis, K.** (2020): Fair and Transparent Blockchain E-Voting System. [Source: IEEE Transactions on Emerging Topics in Computing]

**[4].** **Patel, V., & Shah, K.** (2021): Institutional E-Voting Framework Using Private Blockchain. [Source: International Journal of Advanced Computer Science and Applications (IJACSA)]

**[5].** **Noor, T. H., Zeadally, S., & Alfazi, A.** (2023): Lightweight Blockchain for Secure and Scalable Voting Systems. [Source: Future Generation Computer Systems, Elsevier]

**[6].** **Russo, A., Fernández Anta, A., González Vasco, M. I., & Romano, S. P.** (2021): Chirotonia: A Scalable and Secure E-Voting Framework Based on Blockchains and Linkable Ring Signatures. [Source: arXiv preprint]

**[7].** **Onur, C., & Yurdakul, A.** (2022): ElectAnon: A Blockchain-Based, Anonymous, Robust, and Scalable Ranked-Choice Voting Protocol. [Source: arXiv preprint]

**[8].** **Stančíková, I., & Homoliak, I.** (2022): SBvote: Scalable Self-Tallying Blockchain-Based Voting. [Source: arXiv preprint]

**[9].** **Kiashemshaki, K., Chukwuani, E. N., Jalili Torkamani, M., & Mahmoudi, N.** (2025): Secure and Scalable Blockchain Voting: A Comparative Framework and the Role of Large Language Models. [Source: arXiv preprint]

**[10].** **Anonymous.** (2025): Leveraging Blockchain for Robust and Transparent E-Voting Systems. [Source: ScienceDirect – Journal Article]

**[11].** **Anonymous.** (2024): Blockchain-Based E-Voting Systems: A Systematic Literature Review. [Source: SSRN – Peer-Reviewed Survey]

**[12].** **Anonymous.** (2024): Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges. [Source: SpringerLink – Journal Article]

**[13].** **Anonymous.** (2024): E-Voting System Using Cloud-Based Hybrid Blockchain Technology. [Source: ScienceDirect – Journal Article]

**[14].** **Anonymous.** (2024): Blockchain-Based Electronic Voting Systems: A Case Study in Morocco. [Source: ScienceDirect – Journal Article]

**[15].** **Anonymous.** (2024): Enhancing Security and Transparency in Online Voting Through Blockchain Decentralization. [Source: Springer – Journal Article]

**[16].** **Alzahrani, A., Bulusu, N., & Shiva, S.** (2021): A Secure Electronic Voting System Using Blockchain Technology. [Source: IEEE Access]

**[17].** **Praveen Kumar, P. S., et al.** (2022): Blockchain-Based E-Voting: A Review of Technologies and Implementation Models. [Source: Elsevier]

**[18].** **Farag, A., Mousa, M., & El-Bakry, H.** (2023): Secure Online Voting Using Blockchain with Biometric Integration.

**[19].** **Hossain, M. S., et al.** (2024): Trustworthy E-Voting Using Blockchain: Challenges and Future Scope. [Source: Springer]

**[20].** **Singh, A., & Kumar, S.** (2025): Lightweight Blockchain E-Voting System for Educational I nstitutions. [Source: IJCSNS]