CSDL7022: BLOCKCHAIN

ASSIGNMENT NO: 1 (GROUP NO: 5)

CASE STUDY ON

BLOCKCHAIN AND CONTRACT BASED VOTING APPLICATION

Sarvesh Tikekar (64)
Nathan Pimenta (48)

Presesntation Date: 18th August 2025

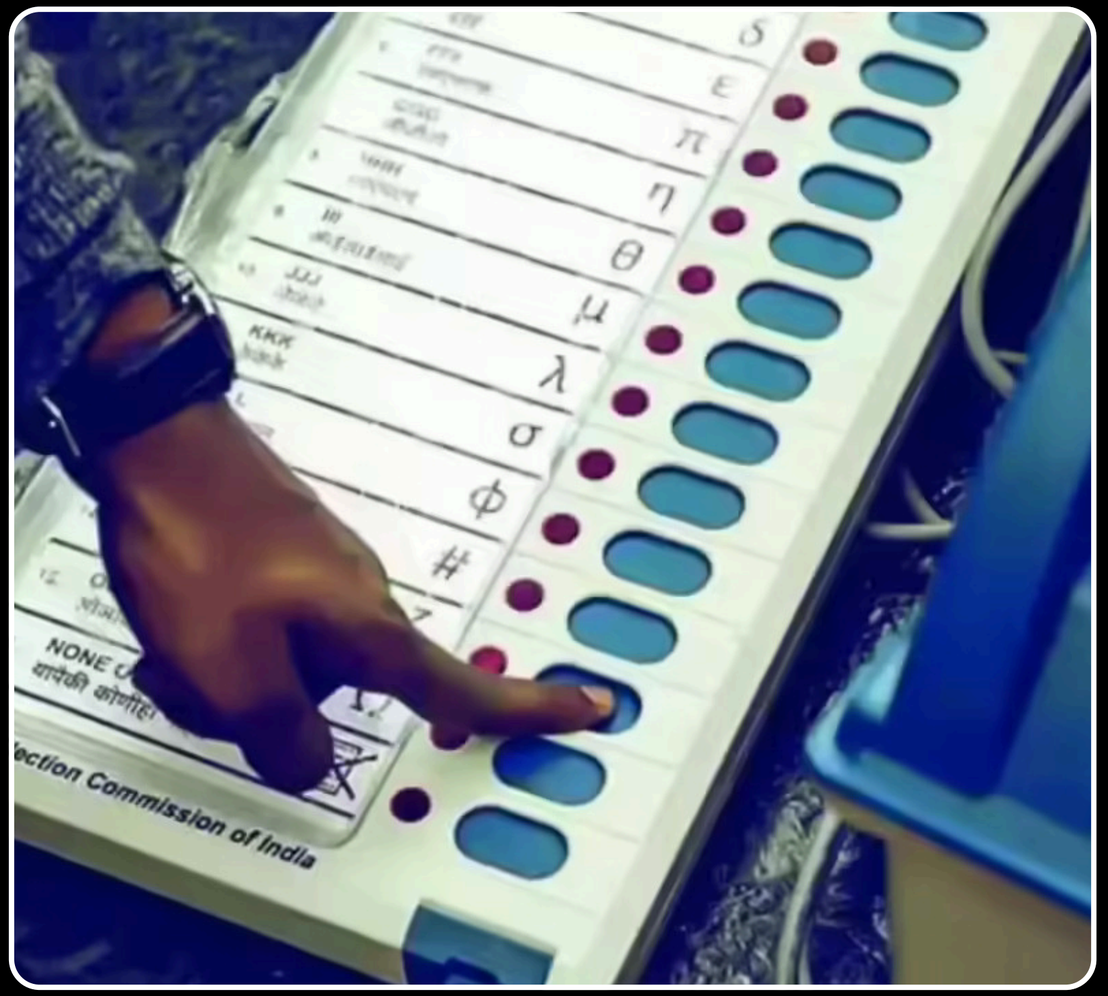
PROBLEM STATEMENT

Traditional voting systems, whether **paper-based or electronic**, often face challenges such as

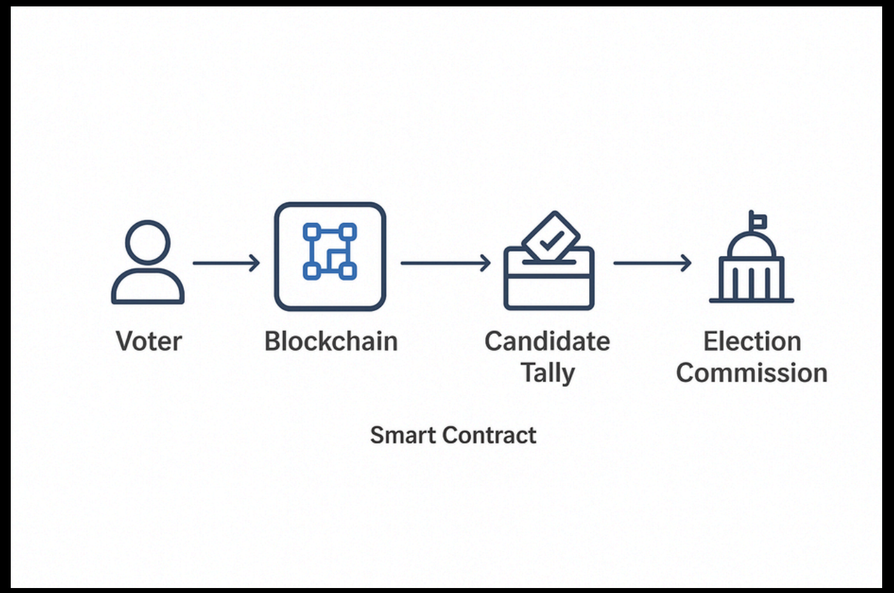
a. Tampering of Votes
b. Lack of transparency
c. Delayed results
d. Vulnerability to centralized control.

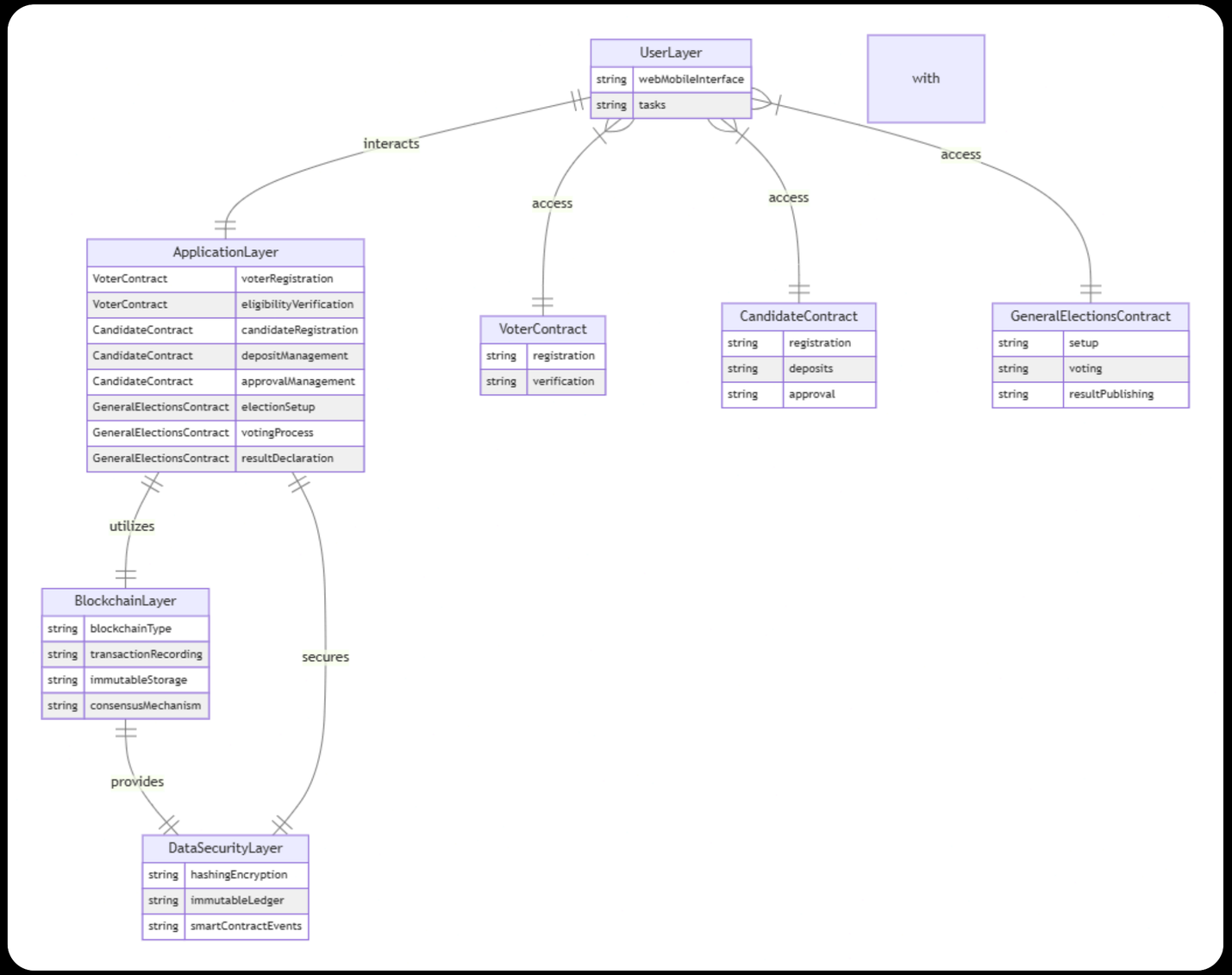
The above listed issues undermine public trust in elections and can lead to disputes, creating the need for a secure, transparent, and tamper-proof voting system that ensures vote integrity, real-time verifiability, voter privacy, and resistance to manipulation.

A blockchain and smart contract-based solution can achieve this through decentralized vote recording, cryptographic verification, and automated result tallying, ensuring trust and efficiency.



SYSTEM ARCHITECTURE AND UML DIAGRAM





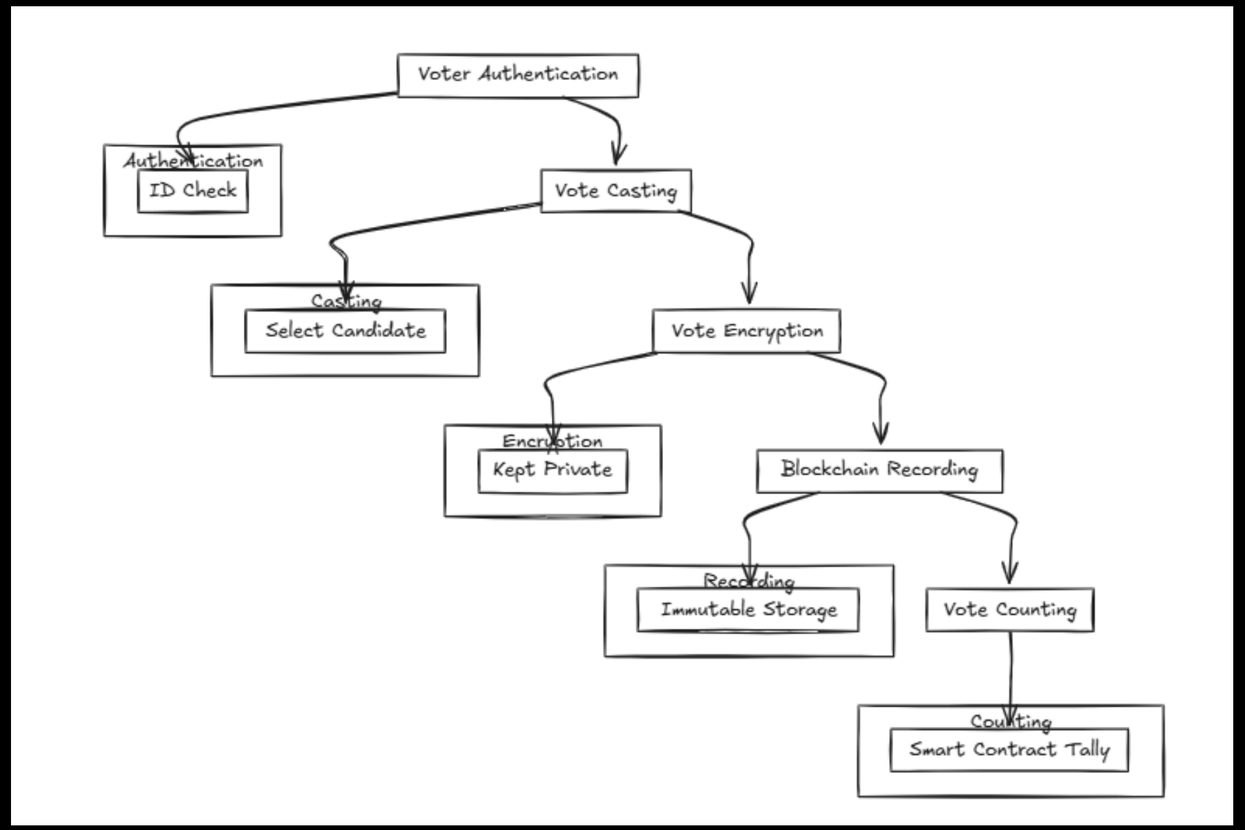
DESIGN CONSIDERATION

- Security & Integrity: Cryptography prevents tampering
- Transparency: Votes visible on blockchain (anonymous)
- Scalability: Handle millions of voters
- Anonymity & Privacy: Protect voter identity
- Accessibility: Simple, user-friendly interface

SMART CONTRACTS IN VOTING

- Automates voting rules (eligibility, one vote per person)
- Immutable execution (rules can’t be altered)
- Validates and rejects duplicate/invalid votes
- Transparent tallying of votes
- Removes intermediaries (trustless system)

PROCESS OF VOTING



ENTITIES IN THE ELECTION PROCESS

Voter Entity in Election

- An eligible citizen who must register their details within a specific time window. Their registration requires verification by their local Election Officer. Once approved, they can cast a single vote during the election period.

- To be eligible to vote in the election, an individual must:

1. Register their details within the designated time frame.
2. Be successfully verified and approved by the Election Officer of their constituency.

Candidate Entity in the Election

- An individual running for office who must register with their details, party, and a security deposit during a set period and they must also be verified by their constituency's Election Officer. Here only **verified candidates** can contest and receive votes.

- To be eligible to contest for election, an individual must:

1. Register with their personal details, party affiliation, and a security deposit within the designated time frame.
2. Be successfully verified and approved by the Election Officer of their constituency.
3. Only after meeting both criteria is a candidate officially allowed to contest and receive votes.

Election Commission (EC) in Election

- Election Commissioner (EC): The highest authority. Appoints Election Officers and holds emergency system-wide powers.
- Election Officers (EO): Appointed by the EC to manage a single constituency. They verify local voters and candidates and initiate the vote count for their area.

BENEFITS OF A BLOCKCHAIN BASED APPROACH FOR A VOTING SYSTEM

- **Transparency**: Every step, starting from registration to the final vote, is recorded on an immutable ledger and creates a public and verifiable audit trail, proving the **process was followed correctly without compromising voter secrecy.**
- **Security**: Sensitive identities are protected using cryptographic hashes instead of being stored directly. Smart contracts enforce strict access controls, preventing unauthorized actions and tampering.
- **Automation & Accuracy**: The vote tallying process is automated, eliminating human error from manual counting and enabling the rapid and precise delivery of results.
- **Audibility**: The entire election lifecycle is permanently logged on the blockchain, providing a clear and chronological record of all significant actions for complete and trustworthy auditing.

LIMITATIONS OF A BLOCKCHAIN BASED APPROACH FOR A VOTING SYSTEM

- **Scalability**: Storing large lists of voters and candidates directly on-chain is inefficient. As participant numbers grow, transaction fees would become prohibitively expensive, making the system unworkable for large-scale elections.
- **Cost**: Every action, from registration to voting, requires a transaction fee in the form of **("gas"),** hence in a major election, the total cost could become a significant financial barrier for both the administration and the public.
- **User Experience (UX)**: Requiring the general public to manage cryptographic wallets and private keys is a major technical hurdle that could lower participation and lead to lost voting rights if keys are misplaced.
- **Centralization of Power**: While voting is decentralized, administrative control is concentrated in the single Election Commissioner role. If this account were compromised, it would become a single point of failure, jeopardizing the entire election's integrity.

THANK YOU

GitHub Link