VoteChain – A Blockchain-Backed Local-Network Voting System

Secure • Transparent • Tamper-Resistant

Presented by:

Manroop Singh 11022210002

Kevin Dhankhar 11022210014

Mokksh Kapur 11022210034

Vaibhav Sheoran 11022210044

SRM University, Sonipat

Introduction

Digital voting systems have emerged as a transformative solution to increase accessibility, reduce manual errors, and streamline electoral processes. However, traditional centralised systems face significant challenges in maintaining trust and transparency.

VoteChain addresses these concerns by combining blockchain technology with an intuitive user experience, specifically designed for small-scale and local elections such as classroom votes, departmental decisions, and organisational ballots.

Our system prioritises security, transparency, and ease of use without compromising on integrity.

Problem Statement

Centralised Vulnerability

Centralised e-voting systems present single points of failure, making them susceptible to tampering, hacking, and unauthorised access.

Lack of Auditability

Most systems offer no transparent audit trail, making it impossible to verify the integrity of votes after they've been cast.

No Immutable Records

Without permanent, tamper-proof records, vote manipulation can go undetected, eroding trust in electoral outcomes.

Insufficient Role Separation

Limited role-based access control increases the risk of misuse by administrators and unauthorised parties.

These challenges necessitate a **secure, lightweight, and transparent solution** that can restore confidence in digital voting systems whilst remaining accessible for smaller organisations.

Proposed Solution: VoteChain

VoteChain introduces a purpose-built voting platform that leverages blockchain technology to ensure every vote is recorded immutably and transparently. Our solution balances technical sophistication with user-friendly design.

Lightweight Blockchain

Votes are stored in an immutable distributed ledger, preventing any retrospective alterations or tampering.

Secure Authentication

Voters authenticate using unique voter IDs with JWT-based tokens, ensuring only authorised individuals can participate.

Admin Control

Administrators manage the candidate list, control election timing (start/stop), and oversee the complete election lifecycle.

One-Vote Enforcement

The system automatically prevents double-voting, with each voter permitted exactly one ballot per election.

Web-Based Interface

A clean, intuitive web interface ensures accessibility for users of all technical backgrounds.

FastAPI Backend

Robust REST API architecture handles all operations securely and efficiently, ensuring reliable performance.

System Architecture

VoteChain employs a modular, layered architecture designed for clarity, security, and maintainability. Each component fulfils a distinct role whilst working seamlessly with the others.

01

Frontend Layer

HTML, CSS, and JavaScript provide an accessible web-based interface for voters and administrators.

02

REST API Layer

FastAPI handles all interactions between the frontend and backend, enforcing authentication and authorisation.

03

Database Layer

SQLite manages voter registrations, candidate information, and election metadata with efficient querying.

04

Blockchain Layer

A custom blockchain implementation ensures tamper-proof vote storage with cryptographic validation.

05

Authentication Layer

JWT tokens secure both admin and voter sessions, with role-based access control enforced throughout.

Core Modules

Authentication Module

JWT-based login system supporting dual roles: administrators and voters. Ensures secure session management and token validation.

Admin Module

Comprehensive control panel for managing candidates, initiating and concluding elections, and viewing real-time results with detailed analytics.

Voter Module

Intuitive interface allowing voters to browse candidates, cast their ballot securely, and check election results once voting concludes.

Election Lifecycle

Manages three distinct states: **NOT STARTED → ONGOING → ENDED**. Enforces strict state transitions to maintain election integrity.

Blockchain Module

Handles transaction creation, block mining, cryptographic hashing (SHA-256), and continuous chain validation to detect tampering.

Blockchain Workflow

Every vote in VoteChain follows a rigorous cryptographic process ensuring integrity and transparency:

1

Transaction Creation

Each vote is converted into a transaction containing voter hash and candidate selection.

2

Pending Pool

Transactions are temporarily stored in a pending pool awaiting block creation.

3

Block Mining

Transactions are mined into a new block containing index, timestamp, and cryptographic hash.

4

Chain Validation

SHA-256 hashing links each block to its predecessor, creating an immutable chain.

Each block contains: **index**, **timestamp**, **transactions**, **current hash**, and **previous block hash**. This structure ensures that any tampering attempt is immediately detectable through hash verification.

Implementation Details

Backend Framework

FastAPI powers the REST API with SQLAlchemy for database operations, providing high-performance asynchronous request handling.

Frontend Stack

Clean HTML5, modern CSS3, and vanilla JavaScript deliver a responsive interface without framework overhead.

Data Storage

SQLite provides lightweight, reliable storage for voters, candidates, and election metadata with zero configuration.

Security Layer

JWT authentication, SHA-256 hashing, and strict role-based access control protect every transaction and user session.

Development Scripts

Utility scripts generate test data, reset blockchain state, and automate deployment tasks for rapid development.

Testing Suite

Comprehensive unit tests and full voting flow validation ensure system reliability and catch edge cases.

Results & Security Analysis

Demonstrated Results

Seamless Voting Flow

Complete end-to-end voting process verified across multiple test scenarios with zero errors.

Vote Enforcement

One-vote-per-voter constraint successfully prevents duplicate ballots and maintains election integrity.

Blockchain Accuracy

All votes correctly recorded in immutable blocks with proper hash linkage and timestamp validation.

Security Features

Role-Based Access Control

Clear separation between admin and voter privileges prevents unauthorised access to sensitive functions.

Immutable Storage

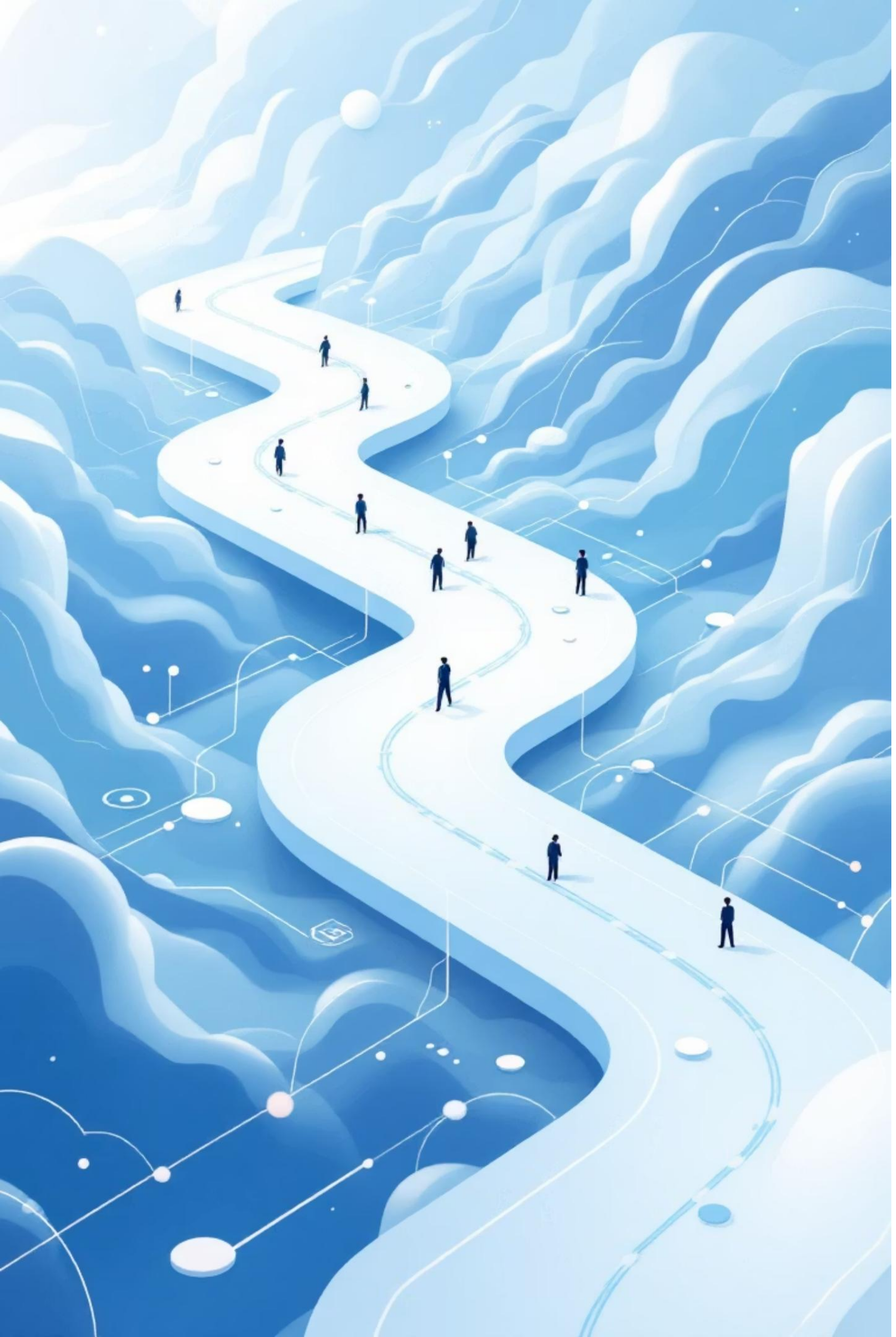
Blockchain ensures votes cannot be altered or deleted after recording, providing permanent audit trail.

Voter Anonymity

Cryptographic hashing preserves voter privacy whilst maintaining vote verifiability and system transparency.

Tamper Detection

Continuous chain validation immediately identifies any attempts to modify historical voting records.



Conclusion & Future Work

VoteChain successfully demonstrates that blockchain technology can enhance voting security and transparency for small-scale elections without sacrificing usability.

Our prototype proves the viability of combining lightweight blockchain with intuitive design for local voting scenarios. The system provides verifiable, tamper-resistant records whilst remaining accessible to non-technical users.

Future Development Roadmap

1. ### Distributed Nodes

   Implement multi-node blockchain architecture for true decentralisation and enhanced resilience.

2. ### Enhanced Security

   Add HTTPS encryption, multi-factor authentication, and encrypted voter ID storage.

3. ### Mobile Platform

   Develop native iOS and Android applications for increased accessibility and convenience.

4. ### Zero-Knowledge Proofs

   Integrate advanced cryptographic techniques to provide mathematical anonymity guarantees.