Project Structure

The system is a Java implementation of a blockchain-based voting platform with 4 main classes:

1. Voter.java - Handles voter identity with:

- RSA-2048 cryptographic key pair generation for digital signatures

- Unique blockchain address for each voter

- Methods to sign voting data with private keys

- Secure voter verification

2. Vote.java - Represents individual blockchain transactions with:

- SHA-256 hashing for transaction blocks

- Digital signature verification

- Timestamp recording

- Previous block hash linking (creating the chain)

- Immutable vote records

3. Election.java - Manages the election process with:

- Candidate registration and tracking

- Vote casting mechanism with double-vote prevention

- Blockchain verification before tallying results

- Election result calculation

- Unique election hash generation

4. OOP\_Project.java - Main application interface with:

- Interactive menu system for user interaction

- Voter registration workflow

- Secure voting process

- Result display functionality

- Block confirmation simulation

Key Technical Concepts

1. Blockchain Implementation:

- Each vote creates a cryptographically secure transaction block

- Blocks are linked through previous block hashes (chain structure)

- The system maintains an immutable record of all votes

2. Cryptographic Security:

- RSA-2048 public/private key pairs for voter identity

- SHA-256 hashing for transaction integrity

- Digital signatures to verify vote authenticity

- Voter verification through blockchain addresses

3. Double-Vote Prevention:

- The system tracks voter participation by blockchain address

- Each address can only vote once in an election

- Attempts to vote multiple times are rejected

4. Transparency and Verification:

- All votes are publicly verifiable on the blockchain

- Results can only be tallied after blockchain verification

- The entire voting process is transparent while maintaining voter privacy

Demo Workflow

1. Voter Registration:

- Users register with a unique ID and name

- The system generates a random blockchain address

- RSA key pairs are created for digital signatures

- Registration is confirmed with a simulated block confirmation

2. Vote Casting:

- Voters authenticate using their blockchain address

- They select a candidate from the available options

- Their vote is signed cryptographically and added to the blockchain

- A block confirmation simulates network consensus

3. Election Results:

- The system verifies the entire blockchain before tallying votes

- Each vote's signature is verified for authenticity

- Results are displayed with counts for each candidate

- Blockchain status (valid/compromised) is indicated

This project demonstrates core blockchain concepts and cryptographic principles applied to secure electronic voting, making it an excellent educational tool for understanding decentralized applications.