

Functional Document

Liquid Democracy Secure I-Voting through Blockchain Technology

1. Introduction

The Liquid Democracy I-Voting with Blockchain Technology system represents a revolutionary approach to democratic participation, combining the flexibility of delegative democracy with the security and transparency of blockchain technology. This system enables citizens to participate in legislative decision-making through three distinct methods: direct voting, dynamic delegation, and traditional representation, all secured through advanced cryptographic techniques and blockchain infrastructure.

2. Product Goal

Primary Objectives:

- Create a secure, transparent, and accessible digital voting platform
- Enable flexible participation in legislative processes
- Ensure vote integrity through blockchain technology
- Maintain voter privacy using advanced cryptographic techniques
- Provide real-time result tabulation and verification
- Reduce democratic participation barriers

Technical Goals:

- Implement AES-256 encryption in GCM mode for vote security
- Utilize blockchain for immutable vote records
- Integrate AWS KMS for robust key management
- Enable smart contract-based delegation management
- Provide real-time system monitoring and audit capabilities

3. Demography (Users, Location)

User Categories:

1. Citizens (Voters)

- General public eligible to vote
- Age 18 and above
- Verified national identity
- Basic digital literacy

2. Delegates

- Trusted representatives
- Verified credentials
- Domain expertise
- Active participation history

3. Election Officials

- System administrators
- Vote supervisors
- Technical support staff
- Audit personnel

4. System Administrators

- Security specialists
- Network administrators
- Database managers
- Blockchain operators

Location Requirements:

- Internet connectivity
- Compatible devices (mobile/web)
- Secure network access
- Geographic independence

4. Business Processes

1. User Registration and Authentication

- Identity verification through government ID
- Biometric authentication setup
- Blockchain wallet creation
- Digital certificate issuance
- Role assignment and verification

2. Vote Management

- Ballot creation and distribution
- Vote encryption and submission
- Blockchain transaction verification
- Vote confirmation
- Result tabulation

3. Delegation System

- Delegate selection process
- Power transfer verification
- Chain validation
- Delegation history tracking
- Weight calculation

4. Result Processing

- Real-time vote counting
- Delegation chain resolution
- Result verification
- Audit trail generation
- Public result display

5. Features

Feature #1: Secure Authentication

Description: Multi-factor authentication system integrating biometric verification with blockchain-based identity management.

User Stories:

1. "As a voter, I want to securely register using my government ID and biometrics."
2. "As an administrator, I need to verify voter identities and manage user roles."
3. "As a delegate, I want to establish my credentials and domain expertise."

Feature #2: Vote Casting

Description: Secure, encrypted vote submission system with immediate blockchain verification.

User Stories:

1. "As a voter, I want to cast my vote securely from any location."
2. "As a voter, I need immediate confirmation of my vote recording."
3. "As an auditor, I want to verify vote integrity without compromising privacy."

Feature #3: Delegation Management

Description: Dynamic delegation system with transparent power transfer and verification.

User Stories:

1. "As a voter, I want to delegate my vote to trusted experts."
2. "As a delegate, I need to manage multiple delegations efficiently."
3. "As an administrator, I want to monitor delegation chains for security."

6. Authorization Matrix

Role	Vote	Delegate	View Results	Manage Users	System Config	Audit	Smart Contracts
Voter	Yes	Yes	Limited	No	No	No	No
Delegate	Yes	No	Yes	No	No	No	No
Election Official	No	No	Yes	Yes	Limited	Yes	No
System Admin	No	No	Yes	Yes	Yes	Yes	Yes
Auditor	No	No	Yes	No	No	Yes	No
Smart Contract Manager	No	No	Limited	No	Limited	No	Yes

7. Assumptions

1. Technical Infrastructure
 - Reliable internet connectivity
 - Access to compatible devices
 - Sufficient blockchain network capacity
 - Adequate processing power for cryptographic operations
2. User Capabilities
 - Basic digital literacy
 - Access to required identification documents
 - Understanding of delegation concept
 - Ability to maintain secure credentials