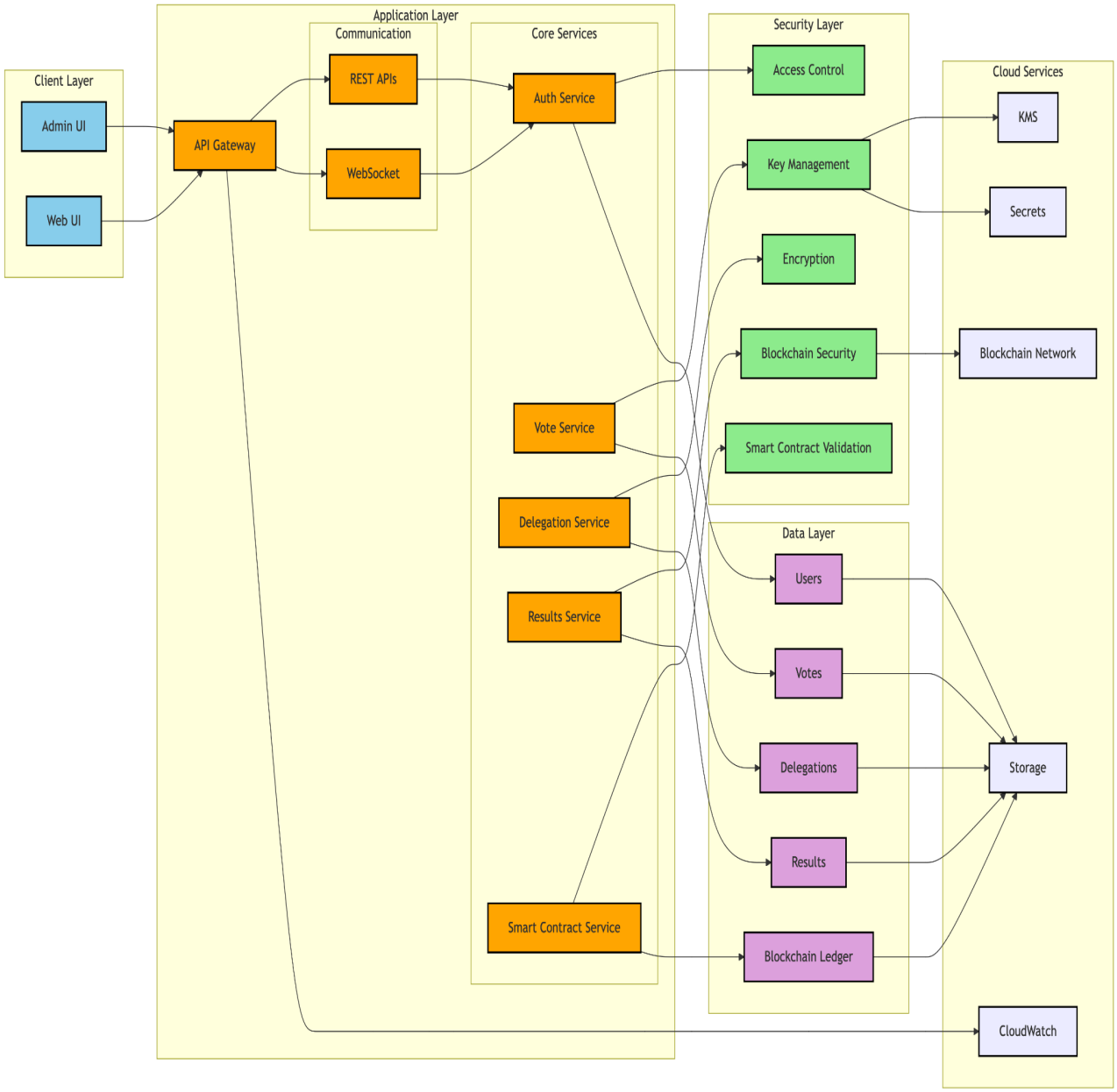
Architecture Document

Liquid Democracy Secure I-Voting through Blockchain Technology



1. **Client Layer**

   The frontend interface layer that users interact with directly:

   Admin UI

   - Management dashboard for system administrators
   - Election configuration and monitoring tools
   - User management interface
   - System analytics and reporting
   - Security audit controls

   Web UI

   - Voter registration and authentication portal
   - Vote casting interface
   - Delegation management system
   - Real-time result visualization
   - Personal voting history tracking

2. **Application Layer**

   API Gateway

   - Central entry point for all client requests
   - Request routing and load balancing
   - API version management
   - Rate limiting and throttling
   - Request/response transformation

   Communication

   - REST APIs:
     - Stateless communication protocol
     - Vote submission endpoints
     - User management APIs
     - Result retrieval services
   - WebSocket:
     - Real-time updates for vote counts
     - Live delegation changes
     - Instant result broadcasting
     - System status notifications

   Core Services

   - Auth Service:
     - User authentication and authorization
     - Session management

        - Token validation
        - Access control enforcement
    - Vote Service:
        - Vote encryption and submission
        - Vote verification
        - Anti-double voting checks
        - Vote receipt generation
    - Delegation Service:
        - Delegation chain management
        - Weight calculation
        - Cycle detection
        - Revocation handling
    - Results Service:
        - Real-time vote tallying
        - Result verification
        - Statistical analysis
        - Report generation
    - Smart Contract Service:
        - Contract deployment
        - Transaction management
        - Gas optimization
        - Event handling

3. **Security Layer**

    Access Control

    - Role-based access management
    - Multi-factor authentication
    - Session management
    - IP-based restrictions

    Key Management

    - AWS KMS integration
    - Key generation and rotation
    - Secure key storage
    - Access logging

    Encryption

    - AES-256 with GCM mode
    - End-to-end encryption
    - Zero-knowledge proofs
    - Homomorphic encryption

    Blockchain Security

    - Smart contract validation
    - Consensus mechanisms
    - Merkle tree verification

- Transaction signing

Smart Contract Validation

- Code verification
- Security audit
- Gas optimization
- Vulnerability checking

4. **Data Layer**

Users

- Voter profiles
- Authentication data
- Access permissions
- Activity logs

Votes

- Encrypted ballots
- Vote metadata
- Timestamp records
- Verification proofs

Delegations

- Delegation relationships
- Weight distributions
- Historical records
- Chain validations

Results

- Vote tallies
- Statistical data
- Audit trails
- Performance metrics

Blockchain Ledger

- Distributed ledger
- Smart contracts
- Transaction history
- Block metadata

5. **Cloud Services**

KMS (Key Management Service)

- Key generation
- Key storage
- Encryption operations
- Access control

Secrets

- Credential management
- Certificate storage
- API keys
- Configuration data

CloudWatch

- Performance monitoring
- Error tracking
- Resource utilization
- Security alerts

Storage

- Vote backups
- System logs
- Audit records
- Configuration files

Blockchain Network

- Validator nodes
- Consensus participants
- Network orchestration
- State synchronization