

# 블록체인 모바일 투표 시스템

## 사용 안내서

### 목차

- 시스템 소개
- 주요 기능
- 앱 설치 및 설정
- 인증 방법
- 투표 방법
- 투표 검증
- 보안 안내
- FAQ
- 문의처

## 1. 시스템 소개

### 1.1 개요

블록체인 모바일 투표 시스템은 최첨단 암호학 기술을 활용하여 투표의 무결성과 익명성을 **수학적으로 보장**하는 차세대 전자투표 시스템입니다.

### 1.2 핵심 기술

기술	설명
<b>블록체인 (Hyperledger Fabric)</b>	모든 투표 기록을 변조 불가능하게 저장
<b>동형암호 (CGS)</b>	투표 내용을 암호화한 상태로 집계
<b>영지식증명 (ZKP)</b>	신원 노출 없이 투표 자격 증명
<b>분산신원증명 (DID)</b>	탈중앙화된 본인 인증
<b>생체인증 (FIDO2)</b>	지문/얼굴 인식 보안

### 1.3 시스템 특징

- 완전한 익명성:** 누가 어떤 후보에게 투표했는지 절대 알 수 없음
- 검증 가능성:** 유권자가 직접 투표가 올바르게 기록되었는지 확인 가능
- 중복투표 방지:** 암호학적 기법으로 1인 1표 보장
- 실시간 감사:** 모든 과정이 블록체인에 기록되어 투명한 감사 가능

## 2. 주요 기능

### 2.1 유권자 기능

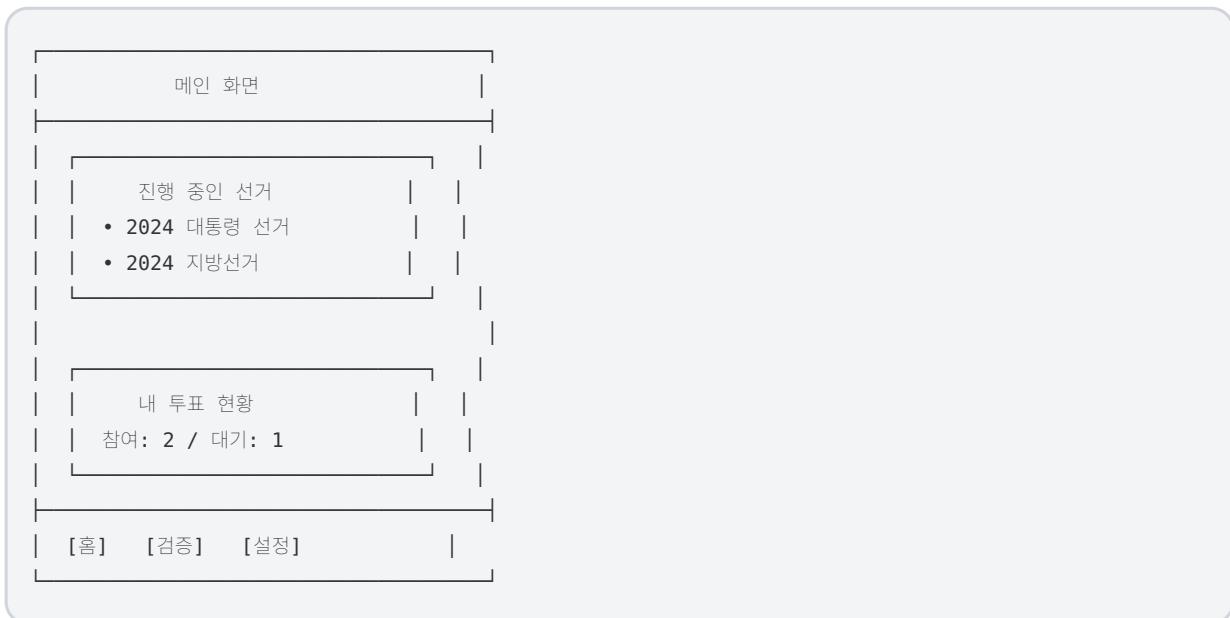
#### 투표하기

- 진행 중인 선거 목록 확인
- 후보자 정보 조회
- 암호화된 투표 제출
- 투표 영수증 발급

#### 검증하기

- 내 투표가 올바르게 기록되었는지 확인
- 블록체인 트랜잭션 조회
- 영수증 코드로 투표 검증

### 2.2 화면 구성



## 3. 앱 설치 및 설정

### 3.1 시스템 요구사항

구분	요구사항
iOS	iOS 14.0 이상
Android	Android 10.0 이상
저장공간	최소 100MB
네트워크	인터넷 연결 필수

### 3.2 설치 방법

#### iOS 설치

- App Store에서 "블록체인 투표" 검색
- "받기" 버튼 클릭
- Face ID 또는 Touch ID로 설치 확인

#### Android 설치

- Google Play Store에서 "블록체인 투표" 검색
- "설치" 버튼 클릭
- 필요한 권한 허용

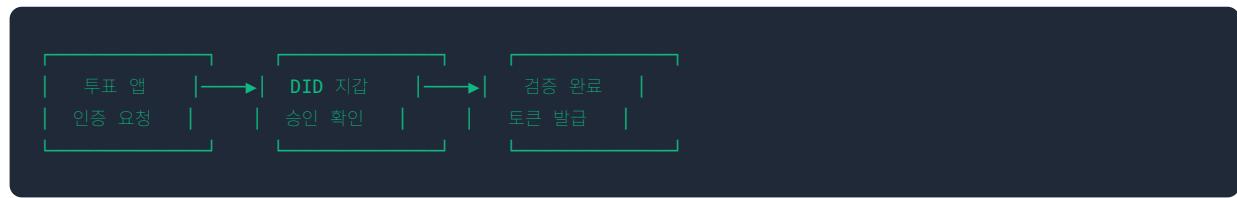
### 3.3 초기 설정

- 앱 실행
- 이용약관 동의
- DID 지갑 연결 (4장 참조)
- 생체인증 등록 (선택)

## 4. 인증 방법

## 4.1 DID 인증

DID(분산신원증명)는 정부나 기업이 아닌 개인이 직접 관리하는 디지털 신원증명입니다.



### 인증 절차

- 1 "DID로 로그인" 버튼 클릭
- 2 DID 지갑 앱 자동 실행
- 3 인증 요청 확인 후 승인
- 4 투표 앱으로 자동 복귀

## 4.2 생체인증 설정

빠른 재로그인을 위해 생체인증을 등록할 수 있습니다.

- 설정 > 보안 > 생체인증
- "생체인증 등록" 선택
- 지문 또는 얼굴 등록

## 5. 투표 방법

### 5.1 투표 전 확인사항

확인사항	설명
투표 기간	선거 기간 내인지 확인
네트워크	안정적인 인터넷 연결
배터리	충분한 배터리 잔량 ( <b>20%</b> 이상 권장)
시간	투표 완료까지 약 <b>3-5분</b> 소요

### 5.2 투표 절차

## 1 선거 선택

선거 목록
2024 대통령 선거
기간: 03/09 06:00~18:00
상태: 투표 가능

## 2 후보자 선택

후보자 선택
기호 1번 홍길동 ☺당
기호 2번 김철수 △△당 ✓
기호 3번 이영희 □□당
[확인하기]

### 3 투표 확인

투표 확인

선택하신 후보:

기호 2번 김철수  
△△당

⚠️ 투표 후에는 변경할 수 없습니다

【취소】      【투표하기】

### 4 투표 완료

투표 완료

✓  
투표가 완료되었습니다

검증 코드: A7F3B2C9D1E4  
(이 코드를 저장해 주세요)

블록체인 TX: 0x7a8b...3c2d

【코드 복사】      【완료】

#### ⚠️ 중요 안내

- 투표는 1인 1회만 가능합니다
- 제출 후 변경이 불가능합니다
- 검증 코드를 반드시 저장하세요
- 투표 중 앱을 종료하지 마세요

## 6. 투표 검증

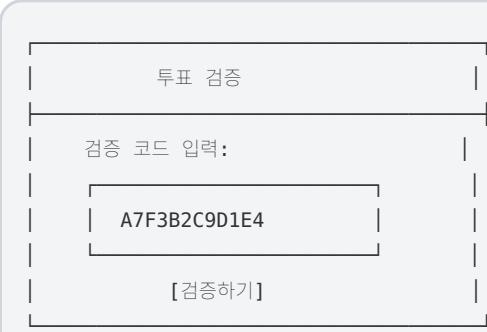
### 6.1 검증 유형

검증 유형	설명	확인 내용
Cast-as-intended	의도대로 투표됨	내 투표가 올바르게 암호화됨
Recorded-as-cast	기록대로 저장됨	암호화된 투표가 블록체인에 기록됨
Tallied-as-recorded	기록대로 집계됨	모든 투표가 정확히 집계됨

### 6.2 검증 방법

#### 내 투표 검증하기

- 하단 메뉴에서 "검증" 탭 선택
- 검증 코드 입력
- "검증하기" 버튼 클릭



#### ✓ 검증 성공 결과

- 선거: 2024 대통령 선거
- 상태: 블록체인 확인됨 ✓
- 투표 해시: 0x7a8b...
- 블록 번호: 12345

## 7. 보안 안내

## 7.1 암호화 보안



- 암호화:** 모든 투표는 CGS 동형암호로 암호화
- 익명성:** 영지식증명으로 신원 노출 없이 자격 증명
- 무결성:** 블록체인에 기록되어 위변조 불가

## 7.2 개인정보 보호

항목	보호 방법
투표 내용	동형암호화 (복호화 키 분산 보관)
투표자 신원	영지식증명 (신원 연결 불가)
인증 정보	DID (분산 저장, 본인만 접근)
통신 데이터	TLS 1.3 암호화

## 7.3 보안 권장사항

### 안전한 투표를 위한 권장사항

- 공식 앱스토어에서만 앱 다운로드
- 앱을 항상 최신 버전으로 유지
- 공공 Wi-Fi 대신 모바일 데이터 사용 권장
- 검증 코드는 안전한 곳에 보관
- 타인에게 DID 인증 요청 절대 승인 금지

## 8. FAQ

### **Q1. 투표 중 앱이 종료되면 어떻게 되나요?**

**A:** 투표 제출 전이라면 처음부터 다시 진행해야 합니다. 제출이 완료된 경우 검증 코드로 투표 상태를 확인할 수 있습니다.

### **Q2. 투표 후 선택을 변경할 수 있나요?**

**A:** 아니요, 제출된 투표는 블록체인에 기록되어 변경이 불가능합니다. 이는 투표의 무결성을 보장하기 위함입니다.

### **Q3. 검증 코드를 분실했습니다.**

**A:** 보안상의 이유로 검증 코드를 재발급할 수 없습니다. 다만, 투표 자체는 정상적으로 기록되어 있습니다.

### **Q4. 다른 기기에서 투표할 수 있나요?**

**A:** DID 인증을 통해 다른 기기에서도 투표할 수 있습니다. 단, 이미 투표한 선거에는 재투표할 수 없습니다.

### **Q5. 투표 결과는 언제 확인할 수 있나요?**

**A:** 선거 종료 후 집계가 완료되면 앱과 공식 웹사이트에서 결과를 확인할 수 있습니다.

### **Q6. 내 투표가 누구에게 갔는지 누가 알 수 있나요?**

**A:** 아니요, 절대 알 수 없습니다. 동형암호화와 영지식증명 기술로 투표 내용과 투표자 연결이 수학적으로 불가능합니다.

## **9. 문의처**

**고객센터**

연락처	정보
전화	1588-0000 (평일 09:00-18:00)
이메일	support@voting.example.com
카카오톡	@블록체인투표

## 긴급 문의 (선거일)

- 전화: **1588-0001** (24시간)
- 현장 지원: 각 투표소 담당자

## 관련 웹사이트

- 공식 홈페이지: <https://voting.example.com>
- 선거 정보: <https://nec.go.kr>
- 기술 문서: <https://docs.voting.example.com>

문서 버전: 1.0.0 | 최종 수정일: 2024년 3월

발행처: 블록체인 투표 시스템 운영팀

본 안내서의 내용은 시스템 업데이트에 따라 변경될 수 있습니다.