

# 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 보장하는 차세대 전자투표 시스템입니다.

### 1.2 핵심 기술

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

1.3 시스템 특징

- **완전한 익명성:** 누가 어떤 후보에게 투표했는지 절대 알 수 없음
- **검증 가능성:** 유권자가 직접 투표가 올바르게 기록되었는지 확인 가능
- **다양한 투표 방식:** 선거 유형에 맞는 유연한 투표 방식 지원
- **실시간 감사:** 모든 과정이 블록체인에 기록되어 투명한 감사 가능

1.4 지원 투표 방식

본 시스템은 다양한 투표 방식을 지원하여 선거 목적에 맞게 유연하게 운영할 수 있습니다.

투표 방식	설명	활용 예시
1인 1투표 (Single)	전통적인 투표 방식. 1인이 1명의 후보에게 1회만 투표 가능	대통령 선거, 국회의원 선거
복수 투표 (Multi-Limited)	여러 후보에게 투표 가능. 최대 N명, 후보당 최대 M번	이사 선출, 인기투표, 다선호 투표
주기적 리셋 (Periodic Reset)	일정 시간마다 투표권이 리셋됨. 기존 투표는 유효	실시간 인기투표, 데일리 랭킹

**복수 투표 (Multi-Limited) 상세**

설정 예시: 최대 3명 후보 선택, 후보당 최대 2표

✓ 후보 A에 2표, 후보 B에 1표 → 총 3표 ✓

✓ 후보 A에 1표, 후보 B에 1표, 후보 C에 1표 → 총 3표 ✓

✗ 후보 A에 3표 → 후보당 최대 2표 초과 ✗

✗ 후보 A~D에 각 2표 → 최대 후보 수 초과 ✗

**주기적 리셋 (Periodic Reset) 상세**

리셋 주기: 24시간 (매일 자정 기준)

Day 1: 후보 A에 투표 → 기록됨 ✓

Day 1: 재투표 시도 → "이번 기간 이미 투표" ✗

Day 2: 투표권 리셋 → 다시 투표 가능 ✓

Day 2: 후보 B에 투표 → 기록됨 (Day 1 투표도 유효) ✓

※ 이전 투표는 삭제되지 않고 모두 유효합니다

## 2. 주요 기능

### 2.1 유권자 기능

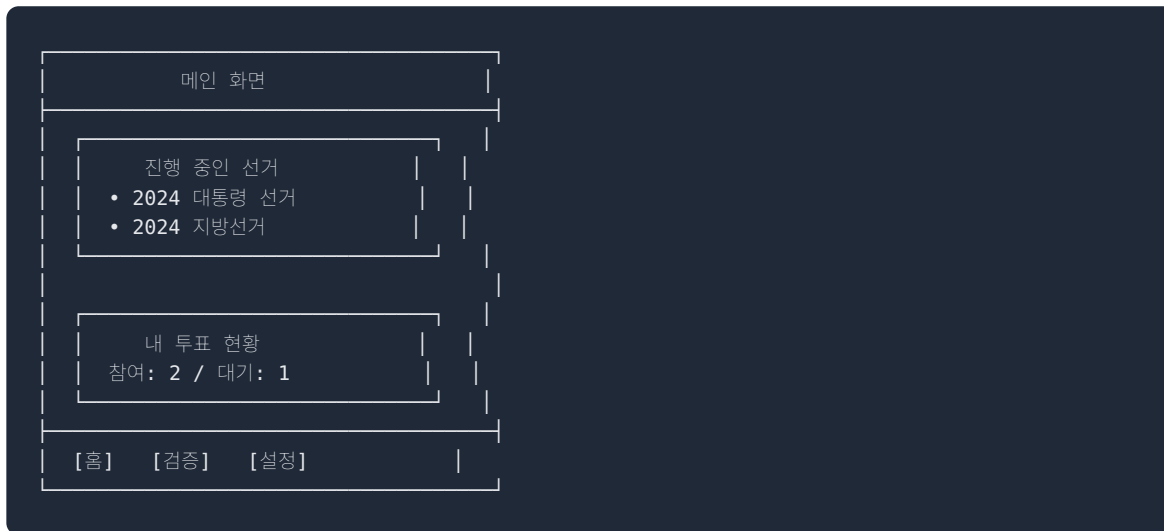
#### 투표하기

- 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

1. App Store에서 "블록체인 투표" 검색
2. "받기" 버튼 클릭
3. Face ID 또는 Touch ID로 설치 확인

#### Android

1. Google Play Store에서 "블록체인 투표" 검색
2. "설치" 버튼 클릭
3. 필요한 권한 허용

### 3.3 초기 설정

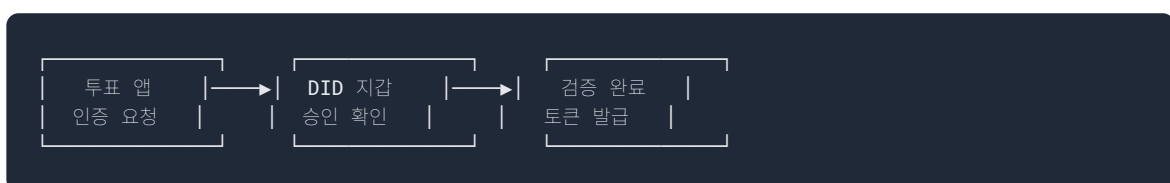
1. 앱 실행
2. 이용약관 동의
3. DID 지갑 연결 (4장 참조)
4. 생체인증 등록 (선택)

## 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

- 인증 요청 확인 후 승인
- 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
투표 방식	선거별 투표 방식 확인 (1인1투표/복수투표/주기적리셋)
네트워크	안정적인 인터넷 연결
배터리	충분한 배터리 잔량 (20% 이상 권장)

### 5.2 투표 절차 (1인 1투표 방식)

#### Step 1: 선거 선택

선거 목록

2024 대통령 선거

기간: 03/09 06:00~18:00

방식: 1인 1투표

상태: 투표 가능

#### Step 2: 후보자 선택

후보자 선택

기호 1번 홍길동 ∞당

기호 2번 김철수 ▲▲당 ✓

기호 3번 이영희 □□당

[확인하기]

Step 3: 투표 확인

투표 확인

선택하신 후보:

기호 2번  
김철수  
▲▲당

▲ 투표 후에는 변경할 수 없습니다

[취소]

[투표하기]

Step 4: 투표 완료

투표 완료

✓

투표가 완료되었습니다

검증 코드: A7F3B2C9D1E4  
(이 코드를 저장해 주세요)

블록체인 TX: 0x7a8b...3c2d

[코드 복사]

[완료]

5.3 복수 투표 방식 (Multi-Limited)

복수 투표 방식은 여러 후보에게 투표할 수 있는 방식입니다.

선거 정보 확인

이사회 이사 선출

투표 방식: 복수 투표

- 최대 3명의 후보 선택 가능
- 후보당 최대 2표까지 중복 가능
- 총 최대 6표

내 투표 현황: 0/6 표 사용

### 후보자 선택 (복수)

후보자 선택 (복수 투표)				
후보 A	김철수	[-] 2 [+]	✓✓	
후보 B	이영희	[-] 1 [+]	✓	
후보 C	박민수	[-] 0 [+]		
후보 D	최지은	[-] 1 [+]	✓	
선택된 후보: 3명 / 최대 3명				
사용한 표: 4표 / 최대 6표				
[확인하기]				

## 5.4 주기적 리셋 투표 방식 (Periodic Reset)

일정 시간마다 투표권이 리셋되어 다시 투표할 수 있는 방식입니다.

### 선거 정보 확인

실시간 인기투표	
투표 방식: 주기적 리셋 (24시간)	
현재 기간: 3일차	
다음 리셋: 6시간 후 (자정)	
오늘 투표 상태: 투표 완료 (내일 다시 투표 가능)	
누적 투표 수: 총 3회 참여	

## 5.5 투표 시 주의사항

### ⚠ 중요 안내 (투표 방식별)

#### 1인 1투표 방식

- 투표는 1인 1회만 가능합니다
- 제출 후 변경이 불가능합니다

#### 복수 투표 방식

- 최대 투표 수 내에서 추가 투표 가능
- 한번 제출한 투표는 변경 불가
- 남은 표를 나중에 사용할 수 있음

#### 주기적 리셋 방식

- 각 기간별로 1회 투표 가능
- 이전 기간 투표는 모두 유효함
- 리셋 시간을 확인하세요

#### 공통 사항

- 검증 코드를 반드시 저장하세요
- 투표 중 앱을 종료하지 마세요

## 6. 투표 검증

### 6.1 검증 유형

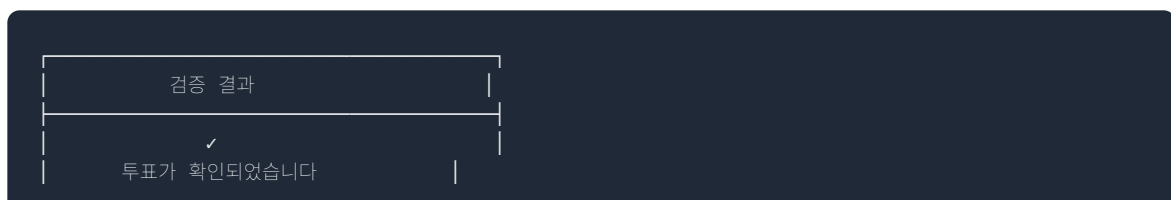
검증 유형	설명	확인 내용
Cast-as-intended	의도대로 투표됨	내 투표가 올바르게 암호화됨
Recorded-as-cast	기록대로 저장됨	암호화된 투표가 블록체인에 기록됨
Tallied-as-recorded	기록대로 집계됨	모든 투표가 정확히 집계됨

### 6.2 검증 방법

#### 내 투표 검증하기

1. 하단 메뉴에서 "검증" 탭 선택
2. 검증 코드 입력
3. "검증하기" 버튼 클릭

#### 검증 결과





선거: 2024 대통령 선거  
상태: 블록체인 확인됨 ✓  
투표 해시: 0x7a8b...  
블록 번호: 12345  
시간: 2024-03-09 09:30:15

## 7. 보안 안내

### 7.1 암호화 보안

투표자 → 투표 선택 → 암호화 → 블록체인 기록  
|  
영지식증명 생성  
(신원 비공개)

- 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, 해당 선거의 투표 방식에 따라 제한이 있을 수 있습니다.

### 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.

### Q7. 복수 투표에서 남은 표를 나중에 사용할 수 있나요?

A: 네, 복수 투표(Multi-Limited) 방식에서는 최대 투표 수 이내라면 여러 번에 나눠 투표할 수 있습니다.

### Q8. 주기적 리셋 투표에서 이전 투표는 어떻게 되나요?

A: 주기적 리셋(Periodic Reset) 방식에서 이전 기간의 투표는 삭제되지 않고 모두 유효합니다.

### Q9. 투표 방식은 누가 정하나요?

A: 투표 방식은 선거 관리자가 선거 생성 시 설정합니다. 유권자는 각 선거의 투표 방식을 선거 상세 화면에서 확인할 수 있습니다.

### Q10. 복수 투표에서 같은 후보에게 여러 번 투표하면 어떻게 되나요?

A: 선거 설정에 따라 다릅니다. "후보당 최대 N표"로 설정된 경우, 해당 제한 내에서 같은 후보에게 여러 표를 줄 수 있습니다.

## 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://vote.kims-ai.com>
- 선거 정보: <https://nec.go.kr>
- 기술 문서: <https://vote.kims-ai.com/docs>

문서 버전: 2.0.0

최종 수정일: 2026년 1월

발행처: 블록체인 투표 시스템 운영팀

본 안내서의 내용은 시스템 업데이트에 따라 변경될 수 있습니다.