

# 블록체인 응용개발 계획서

0. 제출일: 2025.05.01

1. 과제명: 스마트 계약을 이용한 투표 플랫폼

2. 과제 개발팀

	학번	이름	역할
팀장	2019250051	조근희	투표 등록
팀원	2020810008	김민수	투표 참여
팀원	2020700099	박근하	투표 상태 확인
팀원	2020800029	노승준	투표 결과 안내
팀원	2020700086	허찬욱	결과 검증

3. 개발응용(Target System) 명세

3.1 개발시스템의 목적

현대 민주주의 사회에서 투표는 국민의 의사를 반영하는 가장 기본적인 참여 수단이다. 그러나 기존의 오프라인 및 중앙 집중식 전자 투표 시스템은 보안성, 투명성, 조작 가능성, 투표 과정의 신뢰 부족 등 여러 한계를 갖고 있다. 특히 선거 관리 기관에 의한 중앙 집중적 운영은 특정 주체의 부정행위 가능성이나 시스템 오류에 취약하며, 투표 과정과 결과의 검증이 일반 국민에게는 제한되어 있다는 점에서 신뢰를 저해하는 요소로 작용해 왔다.

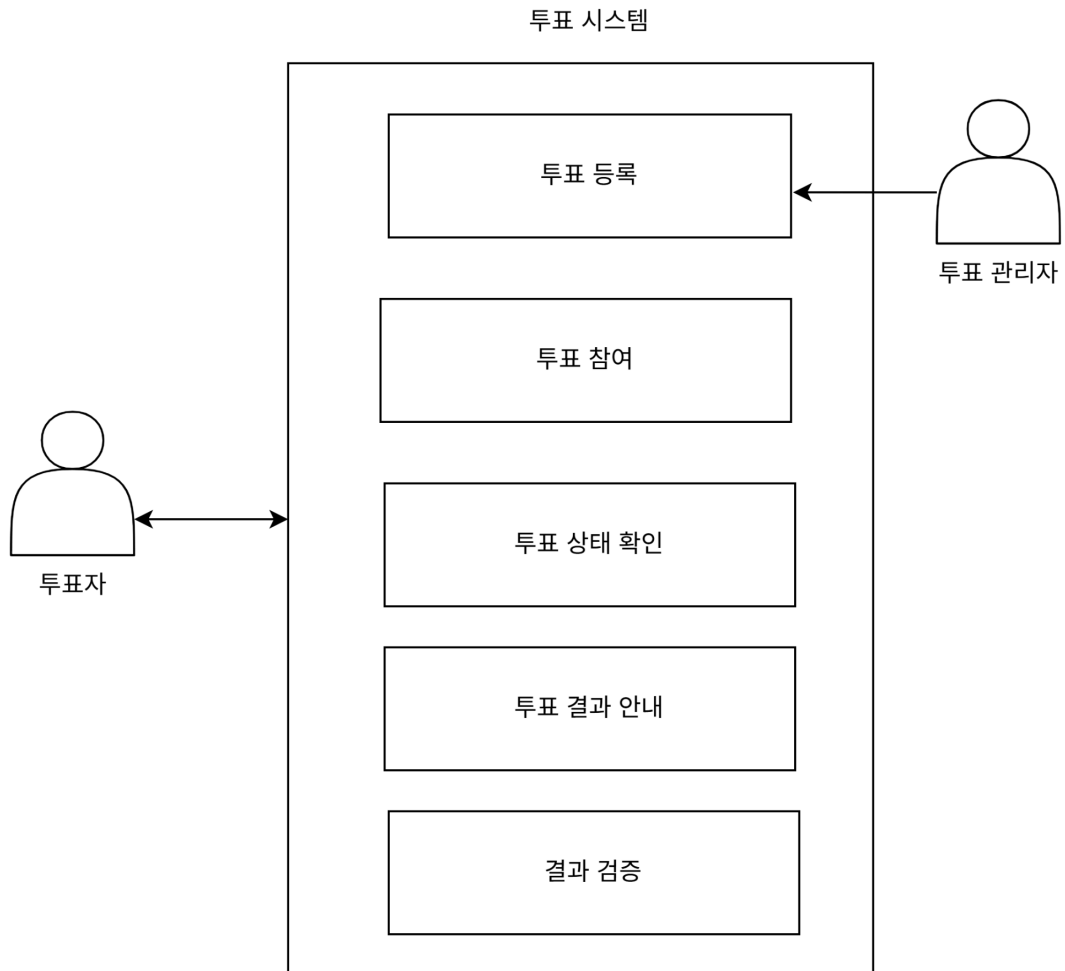
개발하고자 하는 시스템은 이러한 문제를 극복하고자 블록체인 기반의 스마트 계약(Smart Contract)을 활용하여, 투명하고 검증 가능하며, 누구도 결과를 조작할 수 없는 투표 플랫폼을 구축하는 데 목적이 있다. 이 플랫폼은 투표의 생성, 참여, 집계, 공개 전 과정이 자동화된 계약으로 기록되며, 누구나 검증 가능한 상태로 관리된다.

또한, 이 시스템은 개인 정보 보호와 참여의 자유를 보장하면서도 중복 투표나 부정 참여를 방지하는 기능을 갖추고, 다양한 투표 상황(예: 기업의 의사결정, 학교의 학생회 선거, 온라인 커뮤니티 투표 등)에 유연하게 적용될 수 있는 구조를 지향한다. 이를 통해 스마트 계약 기반의 투표 시스템은 기존 투표 시스템이 안고 있던 한계를 극복하고, 신뢰 기반의 새로운 참여 문화를 형성하는 데 기여할 것이다.

### 3.2 개발응용의 예상 사용자 및 사용자가 느끼는 예상 효용

예상 사용자	항목	사용자가 느끼는 예상 효용
공통	정보 보호	블록체인 암호화를 통해 투표자 정보 및 투표 내용의 기밀성 보장
	계약 보호	사전 정의된 스마트 계약 조건에 따라 정확히 이행되며, 결과 조작 불가능
관리자	운영 효율성 향상	투표 생성, 참여, 집계, 결과 공개까지 자동화되어 관리 부담 감소
	비용 절감	인쇄, 인력, 오프라인 시스템 등의 물리적 비용 제거
	신뢰성 확보	투표 내역과 결과가 위변조 불가능한 형태로 블록체인에 기록
참여자	투명성 체감	참여자가 투표 결과의 생성·변경 과정을 실시간으로 검증 가능
	참여 접근성	장소나 시간 제약 없이 모바일/웹을 통한 손쉬운 참여 가능
	프라이버시 보호	개인 식별 정보 비공개 또는 암호화 처리로 익명성 보장
외부 감사자	감사 가능성 확보	블록체인 상의 투표 기록을 통해 제3자의 독립적 감사 가능
	신뢰 기반 검증	공개된 스마트 계약 조건을 기반으로 투표 결과의 무결성 검증 가능

### 3.3 개발응용의 개요도



### 3.4 개발응용의 주요기능

기능	설명
투표 등록	투표 관리자가 투표 주제, 항목, 기간, 참여 조건 등을 스마트 계약으로 등록함
투표 참여	인증된 사용자가 등록된 투표에 참여하며, 1인 1표 원칙 또는 조건 기반 가중치 부여 가능
투표 상태 확인	참여자는 실시간으로 자신이 참여한 투표의 진행 상황(참여율, 마감일 등)을 확인 가능
투표 결과 안내	투표 종료 시점에 스마트 계약에 따라 자동으로 개표되며, 블록체인 상에 결과가 공개됨
결과 검증	제3자가 투표 결과와 스마트 계약의 조건을 블록체인 상에서 직접 검증 가능

### 3.5 개발응용의 범위

개발할 부분	투표 등록, 투표 참여, 투표 상태 확인, 결과 검증, 투표 결과 안내
외부소스 이용	암호화폐 지갑, 암호화폐 송금

### 3.6 개발응용의 예상 요구사항

개발 환경 : Ethereum, React.js, Tailwind CSS, The Graph, ethers.js

프로그래밍 언어 : Solidity, JavaScript

### 3.7 유사시스템의 존재 여부와 기존 유사시스템과의 장단점 비교

비교 항목	K-Voting (중앙화)	Snapshot (탈중앙)	제안 시스템 (스마트 계약 기반)
중앙화 여부	중앙 집중형 (중앙서버 운영)	부분 탈중앙화 (오프체인 + IPFS 저장)	온체인 완전 탈중앙화
검증 가능성	집계 과정 비공개	결과만 공개, 로직은 외부 처리	계약 로직까지 공개 검증 가능
결과 조작 가능성	서버 조작 가능성 존재	스냅샷 시점 조작 가능성 있음	스마트 계약 자동 집행 → 불가능
가스비 부담	없음 (오프체인)	없음 (오프체인 서명 방식)	온체인이므로 있음 → L2 등으로 보완 가능
사용자 프라이버시	KYC 실명 기반	지갑 주소 기반 익명성	선택적 익명성 구현 가능
맞춤형 투표 조건	매우 제한적	주로 토큰 수 기준	조건, 방식, 인증 등 설계 가능
투표 자동화	수동 집계, 서버 처리	오프체인 집계 + 일부 수동 처리	전 과정 스마트 계약 자동화
적용 범위	국내 공공/기관 중심	DAO·Web3 한정	다양한 조직에 맞춤 적용 가능