블록체인 기술을 활용한 투표 시스템

201624407 구자윤
201624453 김지우

지도교수 안성용

목 차

제 1 장 과제 배경 및 목적

제 1 절 과제 배경

비트코인의 가치 상승과 이에 관한 이슈는 2017년 처음 언론에 대두된 이후로 꾸준히 국내의 뜨거운 감자였다. 아울러, 비트코인에 활용된 블록체인 기술에 대한 연구와 응용 방안은 국내 학술지와 기업에서 꾸준히 논의되고 있고, 정부에서도 2021년 블록체인 시범사업에 총 194억원을 투입하여, 응용 방안을 모색하고 있다.

보안성이 높고 변조가 어렵다는 특성 때문에 데이터의 무결성 증명이 요구되는 다양한 공공, 민간 사업에 적용되고 있다. 금융업과 물류업 등 보안성과 신뢰성이 중요한 분야에 주로 응용되고 있으며, 더 나아가 지역화폐(Local currency)나 에너지 산업 등 다양한 분야로 그 영역을 확대해 나가고 있다.

제 2 절 과제 목표

전자 투표도 블록체인이 활용될 수 있는 분야 중 하나로, 신뢰성을 담보하는 블록체인 기술의 특성상, 투명한 투표 방식과 집계를 보장할 수 있다. 최근 몇 년간 방송가의 화제였던 시청자 투표를 반영하여 최종 순위를 결정하는 서바이벌 프로그램의 조작 정황이 포착되어, 수사 결과 사실로 드러나 대중들의 공분을 산 적이 있었다. 특정 방송사의 PD가 청탁을 받아 이루어졌으며, 연습생별로 득표율과 순위를 미리 정하고 실제 문자 투표 수치에 일정 숫자를 곱하는 방식을 사용한 것으로 밝혀졌다. 이에 더불어, 2020년 이루어졌던 미 대통령 선거 투표에서도 공화당 재선 후보 도널드 트럼프가 우편 투표 방식의 보안성을 의심하며 선거에 불복하는 해프닝이 있었다. 실제로 죽은 사람이거나 투표 대상자가 아닌데도 투표 편지가 발송되거나, 배송부터 집계까지의 과정에서 상당한 시간이 소요된다는 점에서 조작될 여지가 다분하다는 지적이 있었다. 2016년 미국 대선 2개월 전에는 투표 기계가 신원미상의 해커들로부터 해킹된 사실이 드러나 유권자들의 집계 시스템에 대한 불신을 불러일으킨 사례도 있었다.

두 사건은 개별적인 사건이고, 각각이 다른 분야에서 뜨거운 감자였지만, 두 개의 사건 모두 신뢰성과 보안성이 보장되지 않은 기존 투표 방식의 허점이 주된 화두였다. 기존 전자 투표 시스템 또한 중앙 집중형 방식으로, 데이터 변조 공격에 취약하다는 단점이 있어 집계 과정에서는 오히려 사람이 직접 개표하는 것이 보안성 측면에선 더 낫다는 분석도 많다. 우리는 블록체인을 활용하여 블록체인 기술이 적용된 가상 토큰을 거래하는 방식으로 신뢰성과 보안성이 보장된 상태에서 투표를 진행할 수 있는 Web 기반의 플랫폼을 만들고, 사용자가 집계된 내용을 즉시 확인할 수 있도록 하는 차세대 투표 플랫폼을 구현하고자 한다. 이더리움 블록체인을 이용할 것이며, 더 나아가 안드로이드 환경에서의 모바일 Web-app 또한 제작하여 이용자의 접근성을 높일 계획이다.

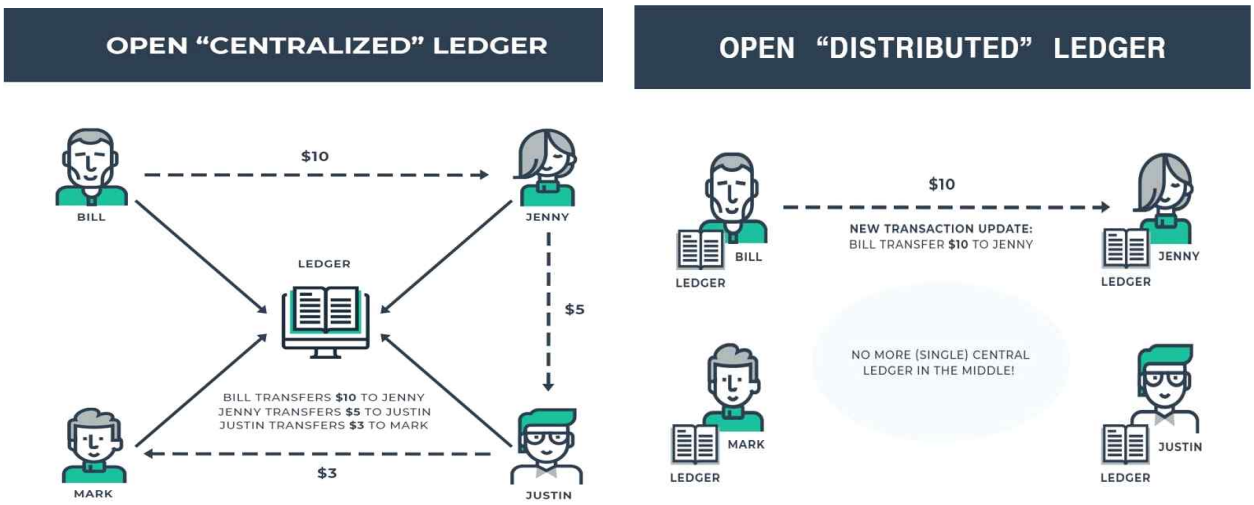


그림 1 중앙 집중형 장부(Centalized Ledger)와 분산형 장부(Distributed Ledger)

제 2 장 요구 사항 분석

제 1 절 보안 요구사항

가) 투표 보안 요구사항

요 구 사 항	설 명
*기밀성(Privacy)	· 시스템에 의해 투표자의 익명성이 보장되어야 한다.
정확성(Accuracy)	· 행해진 투표는 정확하게 집계 결과에 반영되어야 한다.
공정성(Fairness)	· 투표 과정은 공정해야 한다. · 투표에 영향을 주는 요인들은 배제되어야 한다.
합법성(Eligibility)	· 인증된 사용자만이 투표할 수 있다.
이중 투표 방지 (Prevention of double voting)	· 이중 투표는 불가능 하다.
*증명 불가 (Receipt Freeness)	· 투표자는 TTP(The Third Party)에게 자신의 투표를 증명할 수 없다.
검증 가능(Verifiability)	· 시스템이 정확한지 검증할 수 있어야 한다.

강건성(Robustness)	· 변조나 공격에 대해 취약하지 않아야 한다.
건전성(Soundness)	· 부적절한 투표는 집계되지 않아 투표 결과에 영향을 주지 않는다.

표 1 기존의 전자 투표 보안 요구사항

(B.C. Lee, "Analysis of issues for a e-voting introduction," 2005)

제시 및 구현하는 시스템의 경우 2005년에 논의된 기존에 존재했던 전자 투표 모델의 보안 요구사항을 따른다. 개발 과정에서 이러한 요구사항을 고려하며 플랫폼을 고안하고 제작할 것이며, 요구사항이 어떻게 충족되는지에 대해 이후 작성될 보고서들에서 더 서술할 예정이다.

*생성된 이더리움 토큰을 집계할 때 거래 내역이 투명하게 드러나, 투표자를 특정할 수 있게 된다. 기존 방송이나 기업의 SMS 기반 투표 모델를 대체하는 플랫폼처럼 투표자가 특정되어도 큰 문제가 없고, 기존 모델보다 투명성을 증대하는 것이 주 목적이라면 이는 요구사항으로 고려하지 않아도 될 것이다.

*블록체인을 활용하게 되면서 중앙 관리자인 TTP(The Third Party)를 고려하지 않아도 되어, 증명 불가(Receipt Freeness) 요구 사항은 고려되지 않을 것이다.

나) 시스템 보안 요구사항

제시 및 구현하는 시스템의 경우 이더리움 기반의 블록체인을 사용하며 보안 요구사항을 다음과 같이 정의한다.

● 투표권을 의미하는 토큰의 부여 및 전송, 회수 등의 절차는 투명하게 검증될 수 있어야 한다.

● 투표 게시자(관리자)의 권한은 최소화되어야 한다.

● 집계 내용을 표시하는 Web에 대한 부적절한 접근이 토큰의 집계에 영향을 줄 수 없도록 한다.

제 2 절 시스템 요구사항

가) 블록체인 기반 투표/모니터링 시스템
: 블록체인 기반 스마트 컨트랙트를 통해 개인의 투표 내역을 관리한다.

- 스마트 컨트랙트는 블록체인 네트워크에서 작동되는 일종의 프로그램으로, 어떤 목표를 달성하기 위한 요구사항에 맞춰 개발자가 프로그래밍하고, 특정 상황에서 조건이 충족되면 자동으로 수행된다.
- Solidity 언어를 이용하여 투표 방식에 적절한 계약 사항들을 작성하고, 사용자에게 배포한다.
- 사용처에서 비밀 투표가 원칙이라면 사용자를 식별 가능한 개인정보는 단방향 암호화를 통해 암호화 하여 관리한다.

나) Web/Android 기반 투표 플랫폼
: Solidity 언어를 사용하여 이더리움 기반의 투표 시스템 DApp(Decentralized application)을 제작한다.
- 학교, 기업, 공공기관 등 인증된 기관 이용자들이 투표를 개설 가능하도록 한다.
- 자바스크립트, Node.js를 이용하여 web을 개발하며, 블록체인과 연동 가능하도록 Web3.js를 사용한다.
- Web 페이지로 구현한 시스템을 기반으로 안드로이드 어플리케이션을 제작한다.
- (Web/App 공통) 이용자들의 연령과 IT 관련 보유지식에 대한 범위가 다양하므로 간결하고 가독성 높은 UI로 구성한다.

다) 실시간 투표 모니터링 기능
- 특정 투표에 대해 실시간 집계 현황을 모니터링 가능하도록 구현한다.
- 이용자들이 한눈에 알아보기 쉽도록 데이터를 그래프 등으로 시각화한 자료도 포함하여 나타낸다.
- 종료된 투표들에 대한 분석 데이터도 제공한다(ex : 연령대별, 성별, 지역별 투표율).

제 3 장 설계 문서

제 1 절 개발 환경

개발 OS: Windows 10
서버 OS: Ubuntu
개발 언어: Solidity(스마트 컨트랙트 작성), HTML+Javascript, Node.js(Web 개발), Java(안드로이드 개발)

Visual Studio Code
: 웹 개발 환경

- Android Studio
: 안드로이드 개발 환경

- Ganache
: 테스트 목적으로 PC에 설치해서 사용할 수 있는 일종의 간이 블록체인

- EVM(Ethereum Virtual Machine)
: 스마트 컨트랙트 배포 및 실행을 처리하는 이더리움의 일부

- RPC(Remote Procedure Call)
: 별도의 원격제어를 위한 코딩 없이 다른 주소 공간에서 함수나 프로시저를 실행할 수 있게 하는 프로세스간 통신 기술

- Web3.js
: JSON RPC(Remote Procedure Call, 원격 프로시저 호출) 스펙을 구현한 이더리움 자바스크립트 API

제 2 절 적용 기술

가) 블록체인

블록체인은 가상화폐 프로젝트인 비트코인에 적용된 기술로, P2P(Peer-to-Peer) 네트워크를 통해서 관리되는 일종의 분산 데이터베이스이다. 기존의 중앙화된 장부(Centralized ledger)를 탈피하고, 탈중화된 장부(Decentralized ledger)를 목표로 설계된 기술이며, 분산원장 기술(Distributed Ledger Technology)로도 불린다. 거래 정보가 저장된 각 데이터 블록(Block)들이 고리(Chain)구조로 연결되며, 중앙 서버가 아닌 사용자들이 공동으로 기록하고 관리하는 것이 특징이다. 각 데이터 블록의 거래 정보는 해시(Hash) 값으로 변경되어 저장되고, 모든 각각의 블록들은 이전 블록의 거래 정보까지 함께 저장하는 분산형 구조이기 때문에, 데이터 변조에 대한 뛰어난 보안성을 지닌다. 이에 더불어, 다른 블록을 생성해서 추가하는데 일정 시간이 걸리게 하는 개념인 작업증명(Proof-of-Work)가 포함되어 있어 데이터 변조에 많은 노력과 시간이 필요하게 한다. 또한, 모든 거래과정이 즉시 모든 사용자에게 공유되는 신속성과 투명성도 지닌다. 기존 중앙 집중 방식의 전자 장부에서 한 단계 더 나아간 기술로 평가받고 있으며, 블록체인 플랫폼을 활용하게 되면 기존의 안전한 거래에서 필요했던 여러 과정들 생략할 수 있어, 비용 절감 차원에서도 뛰어나다.

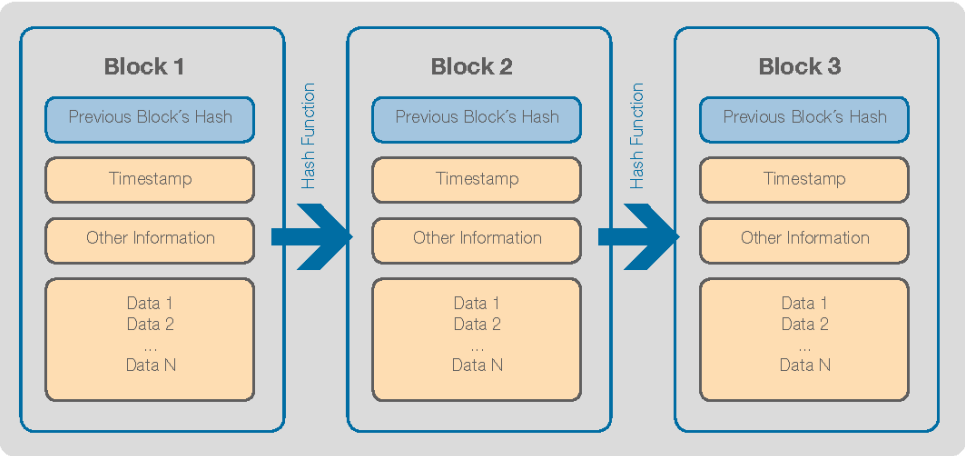


그림 2 블록체인의 구조

나)이더리움

: 이더리움은 블록체인 기술을 여러 분야에 접목할 수 있도록 상향한 기술이다. 비트코인이 블록체인 기술을 최초로 구현한 '1세대 블록체인'이라면 이더리움은 '2세대 블록체인'이라고 불린다. 계산기가 계산 기능에만 충실한 것처럼 비트코인이 결제·송금 기능에 한정돼 있다면 이더리움은 스마트폰처럼 다양한 애플리케이션들을 구동시킬 수 있는 플랫폼에 가깝다. 이더리움은 스마트 컨트랙트(Smart Contract)라는 혁신적인 기술을 블록체인에 접목시키면서 기능적으로 볼 때 비트코인보다 높게 평가받는다. 스마트 컨트랙트는 계약 당사자 간 사전에 합의된 내용을 프로그래밍하여 전자 계약을 체결하고 조건이 충족되면 자동으로 계약이 실행되도록 하는 시스템이다. Solidity라는 자체 개발 언어를 통해 작성되며, 이러한 스마트 컨트랙트를 이용해 개발자는 게임·소셜 네트워크서비스(SNS)·금융 등 다양한 기능이 담긴 디앱(DApp)을 만들 수 있다.

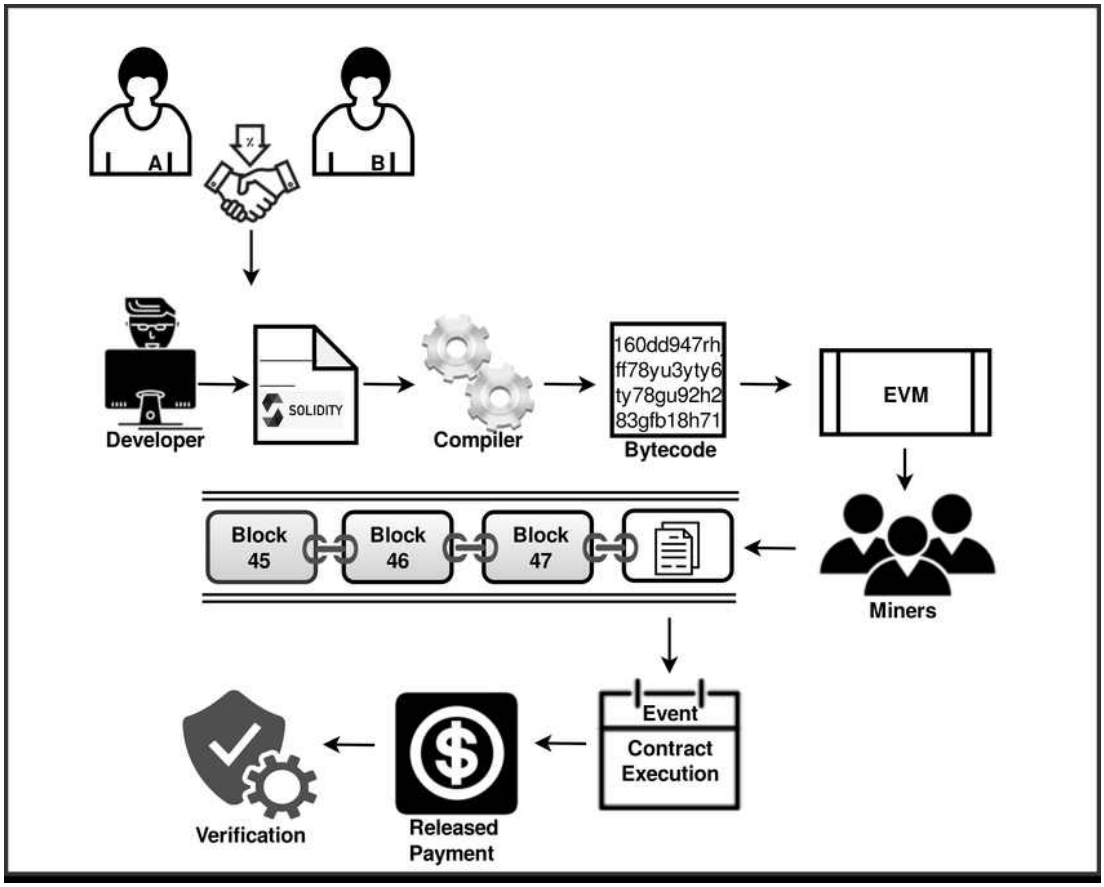
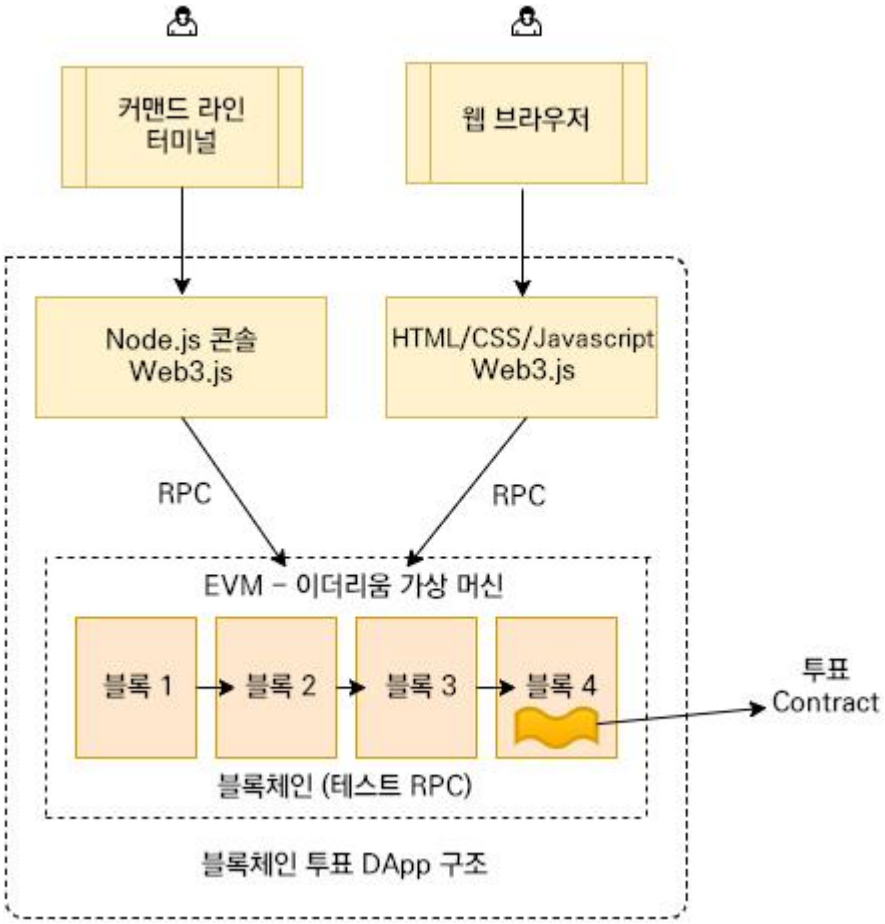


그림 3 이더리움 기반 시스템의 동작 로직

다)디앱(DApp)

: 디앱이란 블록체인을 기반으로 실행되어지는 애플리케이션을 말한다. 여러 블록체인 기술을 기반으로 실행되어 지는데, 이더리움 기반 디앱이라면, 디앱에서 상호작용하는 데이터들이 이더리움 블록체인에 기록되고 호출되는 구조이다.

제 3 절 시스템 구성도



블록체인 가상 테스트 환경 구축 후, Solidity 언어를 활용해 블록체인 트랜잭션으로 온라인 투표가 실행되도록 투표 관련 스마트 컨트랙트를 작성한다. 이후 RPC를 통해 Web3.js를 통해 블록체인과 자바스크립트를 상호작용하게 만들어, 개발한 웹 플랫폼과 연동한다.

제 4 장 개발 일정 및 역할 분담

제 1 절 개발 일정

6월		7월					8월				9월			
3주	4주	1주	2주	3주	4주	5주	1주	2주	3주	4주	1주	2주	3주	4주
개발 언어 및 관련 기술 공부														
	서버 환경 구축													
	블록체인 개발 환경 구축													
			스마트 컨트랙트 작성											
				기본 동작 테스트										
					중간 보고서 준비									
							웹 UI 설계							
								웹 플랫폼 개발						
								RPC를 통한 웹과의 상호작용						
										안드로이드 환경 Web-app 개발				
												문제점 파악 및 오류 수정		
												최종 보고서 준비		

제 2 절 역할 분담

이름	역할 분담
구자윤	- 블록체인 개발 담당 - 블록체인 투표 시스템 개발 및 스마트 컨트랙트 작성
김지우	- 웹/안드로이드 개발 담당 - UI, 플랫폼 설계 및 블록체인과 연동
공통	- 테스트 및 디버깅 - 중간/최종 보고서 작성 - 최종 발표 및 시연 준비