<Ethereum 투표 Dapp 개발 - 이경은>

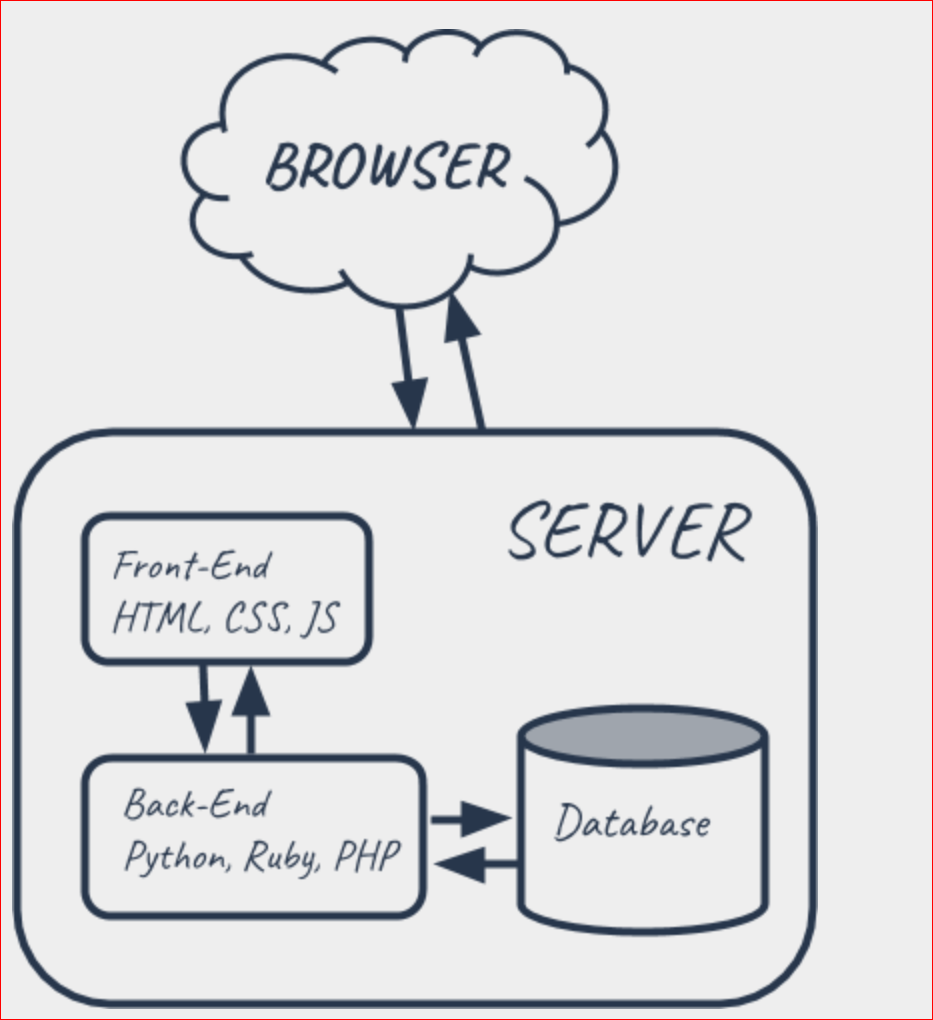
출처

[dappuniversity : the-ultimate-ethereum-dapp-tutorial](http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial)

[https://choi3897.github.io/ethereum/ethereum-dapp-1/#](https://choi3897.github.io/ethereum/ethereum-dapp-1/)

1. 블록체인이란?
   1. 일반적인 web Application

일반적인 Web Application : 우리가 web Application과 상호작용할 때는 웹 브라우저를 이용하여 네트워크를 통해 중앙서버에 연결하게 된다.



어플리케이션의 모든 코드들은 중앙서버에 존재하게 되며, 모든 데이터들 또한 중앙 데이터 베이스에 존재 한다,

우리가 어플리케이션에 트랜잭션을 요청, 전송할 때는 “중앙서버” 통해야만 한다.

중앙서버 형태로, 웹에 투표 어플리케이션을 만들었을 경우, 다음과 같은 문제에 봉착하게 된다.

-데이터베이스 상의 데이터는 조작이 가능하다.

-웹 서버 상의 소스코드는 언제든지 수정될 수 있다.

1-2) 블록체인을 활용한 투표 Application

위의 두가지 문제들 때문에 일반적인 웹에서 돌아가는 중앙집권적인 투표 어플리케이션 대신 투표 앱을 블록체인 상에 배포하여 네트워크에 연결된 누구나 투표에 참여할 수 있게 만들고자 한다. 블록체인 상에 배포된 투표 어플리케이션은 모든 트랜잭션 이력이 기록에 남음과 동시에 데이터 조작이 블가능하며, 소스조차 수정이 불가능하기 때문에 사용자들이 믿고 투표할 수 있는 어플리케이션이 될 것 이다.

블록체인은 네트워크와 데이터베이스가 함께 있는 네트워크 종류라고 할 수 있다.

블록체인은 노드라고 불리는 컴퓨터들의 P2P네트워크이며, 모든 데이터와 코드를 블록체인 상에서 공유한다.

따라서 나의 디바이스가 블록체인에 연결되어 있다면, 나는 곧 블록체인 네트워크 상의 노드인 셈이다. 이렇게 노드가 됨으로써 블록체인 네트워크 상의 모든 컴퓨터 노드들에게 데이터를 전달 할 수 있게 된다. 또한, 노드가 되는 순간부터 나는 블록체인 상의 모든 데이터와 코드들의 사본을 갖게 된다.

블록체인은 중앙 데이터베이스와 달리 모든 트랜잭션 데이터(블록체인 상의 노드들이 서로 공유하고 있다)들이 블록이란 기록들의 묶음에 담기게 된다.

이 블록들은 서로 연결되어 일종의 공공장부(public ledger)를 형성하게 된다. 이 공공 장부는 블록체인 상의 모든 데이터들을 의미하기도 한다. 이 데이터들은 해싱 암호화로 보호되며, 합의 알고리즘으로 검증(vaildation)이 된다.

블록체인 네트워크 상의 노드들에게 분산되어 있는 모든 데이터 사본들은 서로 똑같아야만 한다. 이 때문에 데이터 조작이 힘들어 진다. 전세계에 퍼져 있는 노들들을 조작하는건 사실상 불가능하기 때문이다. 이는 우리가 만들고자 하는 투표 앱에서 상당히 중요한 역할을 한다. 투표자가 투표한 결과가 조작되어서는 안되기 때문이가.

* 1. 일반 유저(투표자)관점의 블록체인 투표 Dapp

일반 유저들이 우리가 만들고자 하는 앱에서 투표를 하기 위해서는 이더리움의 암호화폐 이더(Ether)가 들어있는 지갑주소가 있는 계정이 필요하다.

투표자들은 투표 앱에 접속 후, 투표권을 행사한 뒤, 소정의 트랜잭션 발생 수수료(GAS)를 지불한다.

(블록체인에서 트랜잭션 Read에는 비용이 들지 않지만, 트랜잭션 Write에는 비용이 들기 때문이다.)

투표 트랜잭션이 발생한 즉시, 블록체인 네트워크 상의 일부 노드들이 해당 트랜잭션을 블록에 포함시키며, 트랜잭션을 완료시키게 된다. 이들이 바로 채굴자 이다. 해당 트랜잭션을 완료시킨 채굴자는 투표가 지불했던 수수료(GAS)를 보상으로 받게 된다.

1. 스마트 계약이란?

2-1) 스마트 계약 기본 개념

투표 기능이 있는 어플리케이션 소스코드가 어떤 원리로 블록체인에서 돌아가는 걸까?

이더리움 블록체인은 우리가 짠 코드를 Ethereum Virtual Machine(EVM)으로 실행할 수 있게 구성되어 있다. 이 코드가 스마트 계약이다.

스마트계약은 실제 우리의 ㅇ플리케이션이 돌아가는 모든 비즈니스 로직이라고 할 수 있다. 스마트계약은 블록페인에 데이터를 쓰고 읽는 역할을 하며, 비즈니스 로직들을 실행하는 역할도 할 수 있다. 이는 JS와 유사한 Solidity라고 하는 프로그래밍 언어로 작성된다.

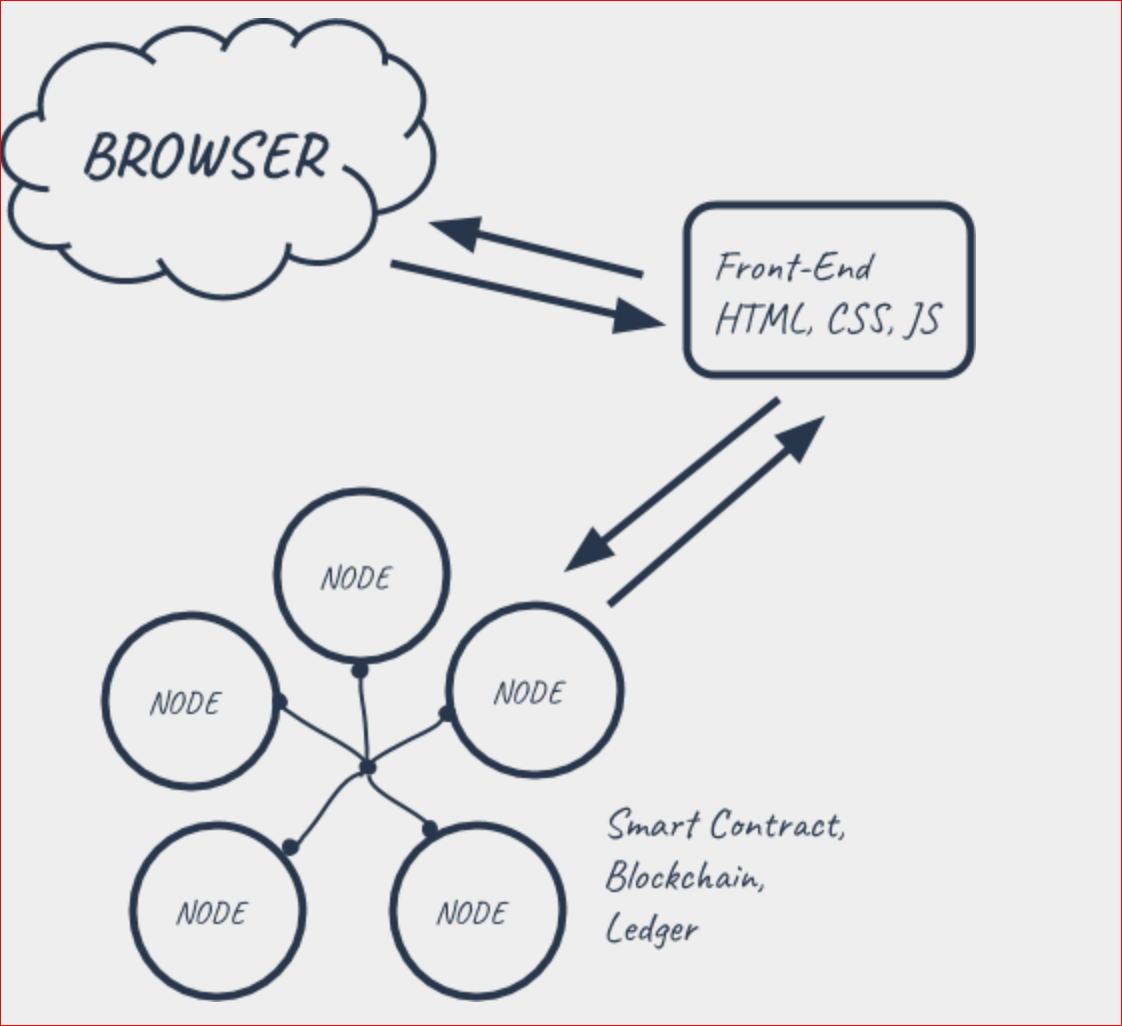
블록체인상의 스마트 계약 함수들은 웹에서의 MIcroService(마이크로 서비스 아키텍처 스타일, 독립적으로 배포 가능한 서비스들의 묶음으로 소프트웨어 애플리케이션을 설계하는 방법)와 유사하다.

공공장부(public ledger)가 블록체인의 데이터 베이스 계층이라면, 스마트 계약들은 실시간으로 data에 트랜잭션을 발생시키는 비즈니스 로직이다.

스마트 계약이라고 불리는 또 다른 이유는, 이들이 계약(covenant)혹은 동의(agreement)기능을 하기 때문이다. 우리 투표 Dapp을 예로 들면, 투표 앱은

1. 나의 투표가 정확하게 카운트 되고
2. 다른 이들의 투표도 한번만 카운트 되며
3. 가장 많은 표를 받은 후보자가 선거에서 승리 할 것

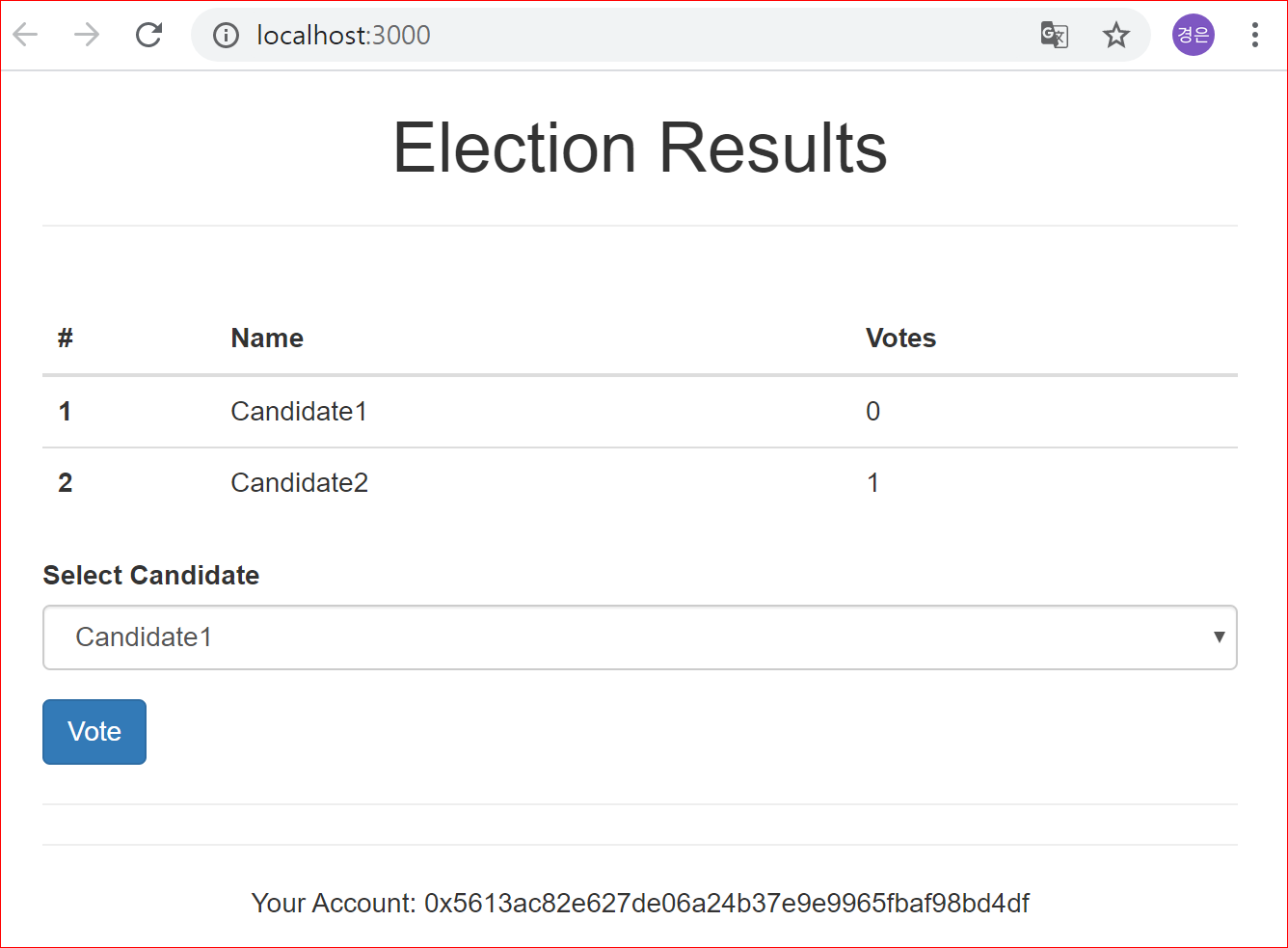
2-2) 투표 Dapp 구조



* 우리는 HTM, CSS,JS로 구성된 전통적인 Front –end- Client 를 작성할 것 이다.

Client는 설치할 Local Ethereum Blockchain에 연결 될 것이다.

* 우리의 투표 Dapp과 관련된 모든 비즈니스 로직들은 solidity로 작성된 ELection이라고 하는 스마트 계약에 작성할 것이다.
* 이 스마트 계약은 우리가 설치한 Local Ethereum blockchain에 배포하여 Accounts들이 투표 할 수 있도록 할 것 이다.



개발 환경 설정

Truffle Frame Work

이더리움 블록체인에서 Dapp을 쉽게 만들게 도와주는 프레임워크다.

Solidity로 스마트 계약을 작성할 수 있는 툴들을 제공헤준다.

또한, Truffle은 우리가 작성한 스마트 계약의 테스트와 블록체인으로의 배포를 도와준다.

뿐만 아니라, 폴더 구조를 미리 만들어 Client – side application 소스코드의 대략적인 아키덱쳐도 미리 잡아 준다.

+FrameWork:애플리케이션 개발에 바탕이 되는 템플릿과 같은 역할을 하는 클래스들과 인터페이스의 집합

Ganache

Local in memory Blockchain 환경이다. Ganache는 10개의 external account 주소에 각각 가상의 100이더가 들어있는 로컬 이더리움 블록체인이다.

Metamask

Metamask extension for Google Chrome

블록체인을 사용하기 위한(블록체인 네트워크에 접속하기 위한)도구 중 하나 이다.

Metamask는 우리의 투표 dapp 개발에 아래와 같은 도움을 준다.