**중간 보고서**

**( KBK\_election )**

**블록체인 기반 분산 선거 시스템 개발**

**정보컴퓨터공학부**

**201024408 권성욱**

**201224438 김주수**

**201424574 박문수**

1. **요구조건및제약 사항분석 (수정사항)**
2. 요구조건

* 프로젝트 진행 시 필요한 요건들을 정의한다.

1. 주요 기능

|  |  |
| --- | --- |
| 후보 등록 | 선거 관리 노드의 인증을 받고 후보자로서 주소를 등록한다. |
| 신원 확인 | 유권자가 투표권을 받기 위해서 선거 관리 노드에게 신원을 확인받는다. |
| 투표 | 비트코인의 거래 기능을 이용해서 투표를 진행한다. |
| 개표 | 각 후보자의 득표수를 계산한다. |
| 실시간 득표 현황 | 득표 상황을 일정 시간마다 개표하여 시각화 서비스를 제공한다. |
| 채굴 기능 | 선거 관리 노드 -> 유권자 트랜잭션 과 유권자 -> 후보자 트랜잭션을 채굴해서 블록을 만들고 블록체인을 형성 |

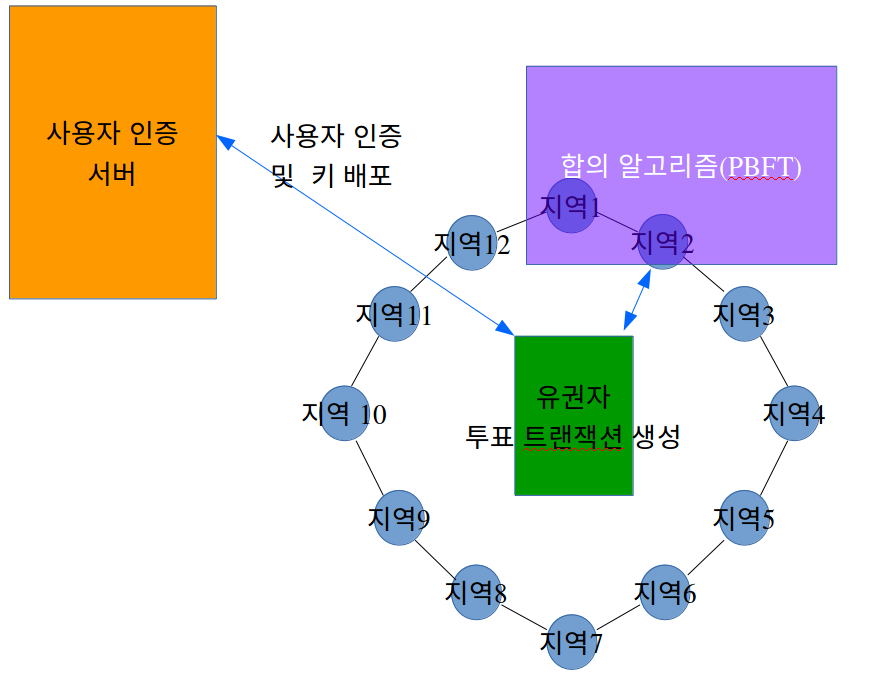
1. 기능 구상

|  |  |
| --- | --- |
| 후보 등록 | 후보자 노드의 지갑에서 투표권을 받을 주소를 생성하고 DB에 저장해서 트랜잭션 생성 시에 DB에 저장된 주소로만 트랜잭션을 생성하도록 설정한다. |
| 신원 확인  투표권 획득 | 신원 확인하기 위해 신상정보DB를 통해 체크한다. 주민번호와 이름의 정보로 신원정보를 확인한다. ( 옵션 : 얼굴, 신분증 또는 지문인식 )  신원이 확인된 유권자에게 선거 관리 노드는 투표권을 하나 전송하는 트랜잭션을 생성한다. |
| 투표 | 신원확인을 마친 유권자는 투표권을 받게 되고 후보 등록 기능을 통해 저장되어 있는 후보자들 주소 중 자신이 원하는 주소로 투표권을 보내는 트랜잭션을 생성한다. |
| 개표 | 선거 관리 노드는 등록되어 있는 각 후보자의 주소를 이용해서 블록체인을 훑어보며 획득한 투표권의 총합을 계산한다. |
| 실시간 득표 현황 | 중간 중간 개표 기능을 사용하여 현재까지 득표 현황을 웹으로 확인 가능하도록 한다. |
| 채굴 기능 | 기존의 비트코인의 높은 난이도를 낮추되 어느 정도의 보안을 유지할 수 있도록 난이도를 조정해서 블록의 생성속도를 높이고 빠른 개표가 가능하도록 한다.  투표권을 채굴하는 것이기 때문에 채굴의 보상은 없다, 따라서 지갑이 필요하지 않음 |

**2. 설계 상세화 및 변경 내용**

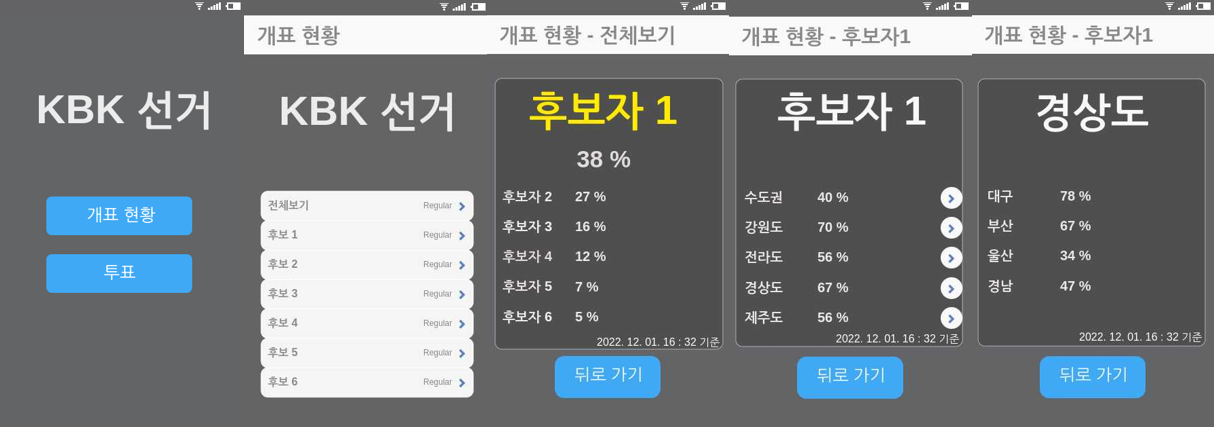
**2.1 시스템 설계도**

**a. 내부 설계 예상도**

****

**b. 외부 설계 예상도(Mocup)**

****

****

**2.2 변경 내용**

**(1) 합의 알고리즘 : pow → PBFT**

**신뢰된 마이너만 블록 생성에 참여하기 위한 대안책.**

**인증서버로 구현가능할 시 기존의 pow 알고리즘을 유지할 계**

**(2) 사용자 인증 서버 : 유권자 인증을 위한 초기 진입시 사용자 인증 서버 구현 예정**

**향후 선거관리자 노드(지역1,2,3,,)에 대한 인증 여부도 구체화할 예정**

**3. 갱신된 과제 추진 계획**

|  |  |  |  |
| --- | --- | --- | --- |
| **추진내용** | **추진일정** | | |
| **7월** | **8월** | **9월** |
| 노드 개발 |  |  |  |
| 블록 체인, P2P 서버 |  |  |  |
| 유권자 인증, 후보자 등록 서버 개발 |  |  |  |
| 웹 개발 |  |  |  |
| 테스트 및 디버깅 |  |  |  |

**4. 구성원별 진척도**

**4.1 역할 분담 변경**

|  |  |
| --- | --- |
|  | 담당 |
| 권성욱 | 개발환경 구축 및 블록체인 생성 |
| 김주수 | 트랜잭션 생성 및 지갑 개발 |
| 박문수 | 웹 개발 및 신분 확인 시스템 개발 |

**4.2 현황**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 종료(done) | 진행(ing) | 예정(will) | 비고 |
| 권성욱 | - 팀원 전원 개발 환경 구축  - MSFC 환경에서 블록(genesis) 생성 | - Genesis 블록 내용 채우기  - miner.h 내용 현재 프로젝트에 추가 하기 | - 1000개 이상의 블록체인 생성 및 블록 해시값 검색 |  |
| 김주수 | -지갑에서 특정 주소로 트랜잭션 생성  - 본인 인증 확인 | - 지갑에 유효한 코인 셋 생성 | -특정 주소를 사용하여 사용 가능한 코인 총 합 계산 | -지갑에 유효한 코인 셋 생성 부분의 필요성 고려 |
| 박문수 |  | -웹 개발 |  |  |

**5. 과제 수행 내용 및 중간 결과**

5.1 개발 현황 (4.2 참고)

5.2 개별 과제 수행 및 중간 결과

1. 권성욱

- MSVC 환경 구축을 위한 필수 라이브러리[ boost, libevent, barkeryDB 기타라이브러리] 설치 이후 프로젝트 생성함

- block.h 내부에 있는 block 생성자를 이용하여 간단한 mian 작성 이후 전체 프로젝트 컴파일 진행

- 그 후 트러블슈팅하며 window 환경에 맞는 코드로 수정해나가기 시작함.(ssize\_t문제, std::max &&std::min 컴파일 오류 등)

- 결과물 : window상 블록생성 가능한 프로젝트(Visual studio)

1. 김주수

4.1Wallet,Transaction 부분 개요

* 마스터 노드

|  |  |
| --- | --- |
| 투표권 획득 | Genesis블록 생성으로 총 발행할 투표권 획득 |
| 트랜잭션 생성 | 인증에 성공한 유권자 노드에게 투표권 전송 트랜잭션 생성 |
| 개표 기능 | 개표를 위한 각 후보자 별 투표권 획득 총합 계산 |

* 후보자 노드

|  |  |
| --- | --- |
| 투표 현황 확인 | 현재까지 주소로 받은 투표권 총량 확인 |
| 트랜잭션 제한 | 이 지갑으로 트랜잭션을 생성하는 것은 불가능 |

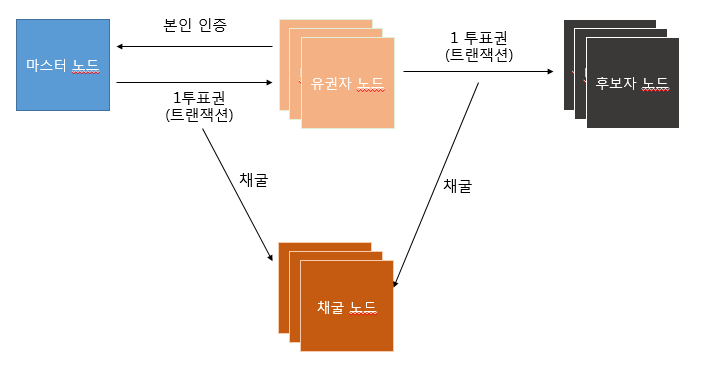
* 유권자 노드

|  |  |
| --- | --- |
| 본인 인증 | 마스터 노드에게 투표권을 얻기 위한 본인 인증 |
| 주소 생성 | 마스터 노드에게 투표권을 얻을 주소 생성 |
| 트랜잭션 생성 | 후보자 노드에게 투표권 전송 트랜잭션 생성(1회로 제한) |

* 채굴 노드

|  |  |
| --- | --- |
| 채굴 | 채굴의 보상이 없으므로 따로 지갑이 필요하지 않다 |

4.2 동작 개요

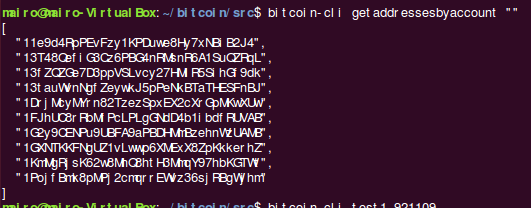


4.3 진행 상황

기본적으로 Bitcoin core의 오픈소스를 사용하며 Wallet의 rpcwallet.cpp을 수정, 원하는 기능을 수행하는 명령어와 함수를 추가하여 동작한다.

* Test1: 유권자가 지갑 소프트웨어를 받고 마스터 노드에게 투표권을 받기 위해 지갑 주소를 생성하고 인증을 받는다

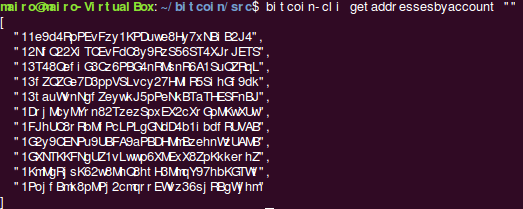
테스트: Bitcoin core의 rpc명령어를 추가해서 실행, DB부분 연동 기능은 아직 미구현이므로 정해진 문자열을 입력해서 일치하는 지로 성공여부 판단



동작 실행 전 지갑의 비트코인 주소들



테스트 실행(성공)



테스트 실행 후 비트코인 주소

인증에 성공하고 12N으로 시작하는 새로운 주소 생성 확인

인증에 성공하면 새로운 주소(투표권을 받기 위한)를 생성하고 마스터 노드에게 투표권을 받을 준비를 한다.

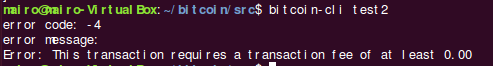


Test1 실패

인증에 실패하면 에러 메시지를 띄우고, 새로운 주소는 생성하지 않는다.

* Test2: 트랜잭션을 생성, 전파하는 명령어 받는 사람(후보자)의 주소와 코인 값(1투표권)은 고정으로 정해놓고 실험하였다.

테스트: bitcoin core의 rpc명령어를 추가해서 실행 받는 사람의 주소는 유효한 값을 임의로 하나 고정, 보내는 코인 값은 1\*CENT로 고정하고 Transaction을 생성했다.



Test2 실행 확인



Test2 실행 확인

입력된 파라미터 값들의 이상이 있는지 확인을 하는 과정(유효한 비트코인 주소인가?, 전송하려는 값이 유효한가?)을 거치고 나면 트랜잭션을 만드는 sendMoney함수를 실행한다. 하지만 실행하는 환경의 wallet에는 사용 가능한 코인 셋이 없기 때문에 중간에 트랜잭션 생성에 실패하며, 결과적으로 error를 반환했다.

Receiver와 Coin은 고정시킨 값으로 정상적으로 나오지만 트랜잭션 생성 결과 부분은 실패하여 실제 트랜잭션은 아무런 정보가 입력되지 않았고 생성 실패의 이유는 자금이 충분하지 않다고 나온다.

따라서 인증을 받고 지갑으로 코인을 넣는 과정이 필요하며, 코인을 직접 생성하는 함수를 만들어서 실험을 해보려 하였으나 트랜잭션 생성부분의 유효성 검사부분에서 막혀 생성에 실패한다. 마스터 노드가 Genesis블록을 생성하면서 받게 되는 보상을 투표권의 총량으로 하여 유효한 투표권을 생성하고 그것을 유권자 노드에게 전달하는 방식을 고려해야 한다..

4.4 추가해야 하는 기능, 명령어

* 지갑 주소를 파라미터로 받아사용가능한 코인(투표권)의 수량 확인 -> 개표, 투표현황에 사용
* 위의 기능들이 안정화 되고 기본적인 투표의 진행이 가능하게 된다면 트랜잭션에 유권자의 정보(사는 지역, 나이, 성별)등을 추가하는 방법을 고려
* 후보자 노드의 지갑은 트랜잭션의 생성은 불가능한 Watch-only지갑 주소를 사용가능한지 검토
* 지갑에서 바로 사용할 수 있는 유효한 코인의 생성방법