가로선

**캡스톤 디자인 회의록**

2020년 4월 21일 토요일

**─**

# **참석자**

유성근, 김동규, 송찬훈, 신현승

**회의 안건**

## 지난 회의 내용

1. 네트워크 설계 채널 위주 간단한 초안 만들기 - 유성근 팀원
2. DB설계 초안(필요한 데이터 목록정도) 만들기 - 유성근 팀원
3. 각자 파트별로 javascript,node.js,ECMAscript 공부하기

## 새 내용

1. DB 및 네트워크 구조 생각해보기

* 다중채널로 구현 or 단일채널+프라이빗데이터로 구현, ca, 오더러 등등

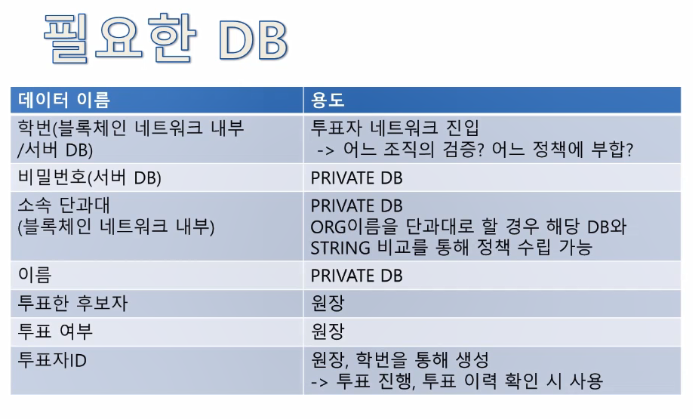
1. 각자 파트별로 javascript,node.js,ECMAscript 공부하기
2. 다음 회의일시 : 4월 25일 (토) 오후 2시

* 네트워크 설계 토의
* DB설계 토의
* IBM evote 따라 해보기? 회의 빈도 조정?

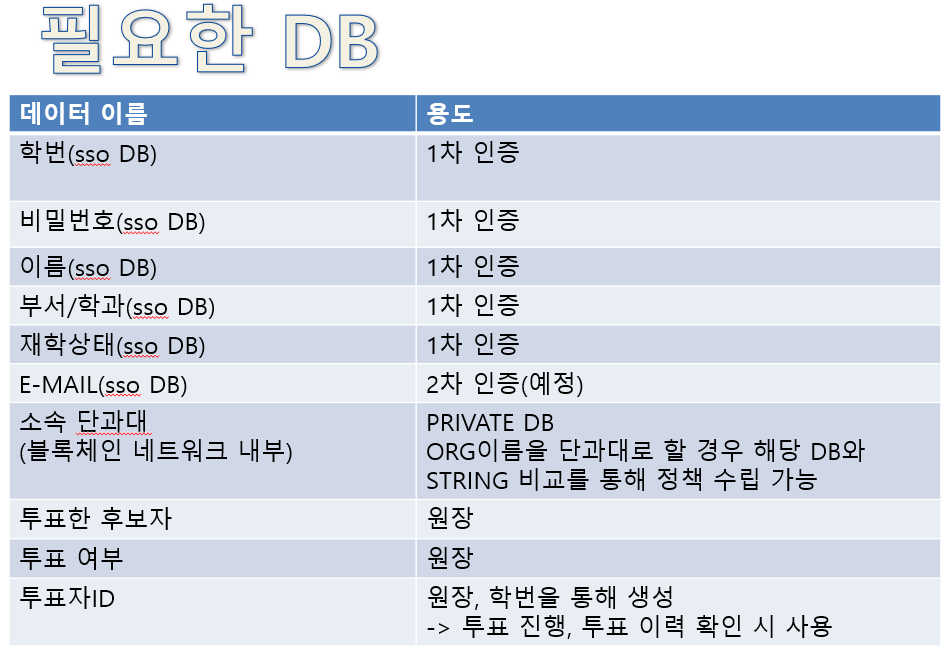
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **구분** | **금주계획** | **완료예정** | **금주실적** | **진척율(%)** | **차주계획** | **완료예정** |
| 네트워크 구조 설계 | 1. 네트워크 설계 간단한 초안  (채널 위주) - 유성근 팀원 | 4.21 | 1.네트워크 설계 토의 | 80% | 1.네트워크 설계 완성 | 4.25 |
| DB 설계 | 1. DB설계 초안   * 유성근 팀원 | 4.21 | 1.DB설계 토의 | 80% | 1.DB설계 완성 | 4.25 |
| 기타 | 1. 프로그래밍언어 공부  ( javascript,node.js,  ECMAscript 등 공부하기) | 미정 |  |  | 1. 프로그래밍언어 공부  ( javascript,node.js,  ECMAscript 등 공부하기) |  |
| 특이사항 |  | | | | | |

# **메모**

* **DB설계**

****

**(↑ 성근팀원 초안) (↓ 현재까지 토의한 내용)**



* + 1차 인증을 할때, SSO와 연동할 계획이었으나 현실적으로 구현이 힘들기 때문에

일단 구현할때는 서버db에 저장(문서에는 향후 SSO연동 한다고 작성).

우리의 서버db는 sso db를 가정한 것이므로 실제 예상되는 sso의 필드를

모방해야함.

* 학번
* 비밀번호(실제로는 sso 연계 db에 들어가있고 sso에는 저장안되지만 넘어가자)
* 신분id ?(교직원인지 학생인지를 구별하기위해 실제SSO에서는 필요하지만 교내 투표를 구현하는 우리 입장에서는 모두 학생을 대상으로만 하기때문에 굳이 안넣어도 될듯)
* 이름
* 부서명(학과)
* 재학상태(재학or휴학 등)
* 전화번호, 이메일

- 이메일, 핸드폰 번호는 2차 인증용도로 사용, 이메일은 따로 받지

않고 학번을 통해 학교이메일을 쓰는 방법도 있음.

- 2차 인증으로 이메일이 구현하기 쉽고 핸드폰은 비용적으로

비싸니까 이메일을 받는 것으로..

(문서상으로는 향후 핸드폰으로 한다고 하자)

* + 소속단과대(단과대별로 나눠서 user만들기로 했으므로)
* 학번도 학과대로 나누어지기 때문에 학번을 이용해 단과대를 구분할

수도 있지만, 이 경우 데이터베이스에 받아야되는것도 너무 많을 것

같고, 전과생의 경우 학번이 바뀌는지 여부도 모르기때문에 학번으로

하지 않고 단과대 이름을 string으로 받아서 org이름과 비교하는게

좋을듯.

* + 투표한 후보자
  + 투표 여부( 1 or 0)

굳이 투표여부를 만들지않아도, 투표를 한 사람이라면 투표자 id가 해당 원장에 저장되어있을텐데 서치했을때 찾아진다면 투표했다고 볼수있지 않을까?

=> 인증만 하고 투표는 안한 경우가 생길수도

=> 투표자 id를 인증을 할때가 아닌 투표를 할때 원장에 등록하는걸로 하면

해결됨

=> 일단 혹시 필요할지 모르니 넣어두는걸로..(나중에 투표율 계산할때 용이하게 쓸수도 있고)

* + 투표자 id

ㄱ. 학번을 통해서 특정한 학생한명의 신원만 구분하는게 아니라, ‘어떤 투표를 하는(총학인지 어떤 단과대인지) 누구인지’를 알수있는 투표자 id를 만들어야하지 않나?

=> 선거별로 채널을 나누어 원장을 따로 저장하면, 다시 id로 나눌 필요가 없음

ㄴ. 투표진행과 투표 이력확인은 투표 종료 이후에는 필요없으므로, 투표자id는 만료시간이 있는 프라이빗데이터로 해서 투표 종료후에는 사라지게 하는것이 좋지 않을까? 1년 후에 또 해당 id를 사용해야 한다고 생각하면, 데이터가 지워지는게 맞는것 같음.

* + 기타 토의 내용

ㄱ. 1차인증할때만 개인정보쓰고 블록체인 네트워크에는 모두 같은

user1이라는 이름으로 접속하는데, 어떻게 개개인의 학번과 연동된 id를

생성할수있을까?

=> user1으로 접속한다고 하더라도, 웹이랑 체인코드의 연동을 통해

사용자가 학번데이터를 들고 들어올 수 있으니까 괜찮을듯....

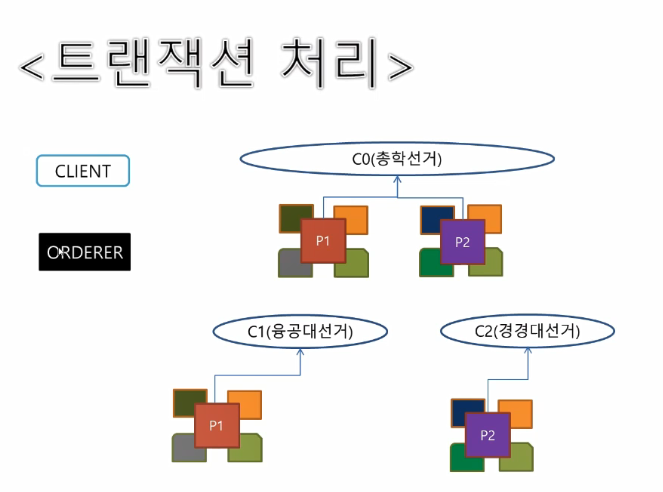
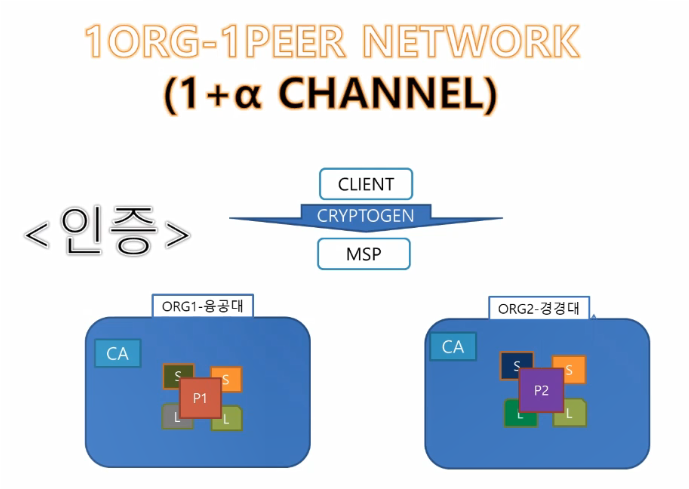
=> 아니면, 이미 투표 자격은 인증 과정에서 입증이 되었으므로 시스템에서

id를 미리 다 만들어놓고, 접속한 순서대로 id를 부여하는 방법도 있음.

그렇게 되면 굳이 학번을 통해 id만들 필요도 없음(조회를 위해 id를 잘

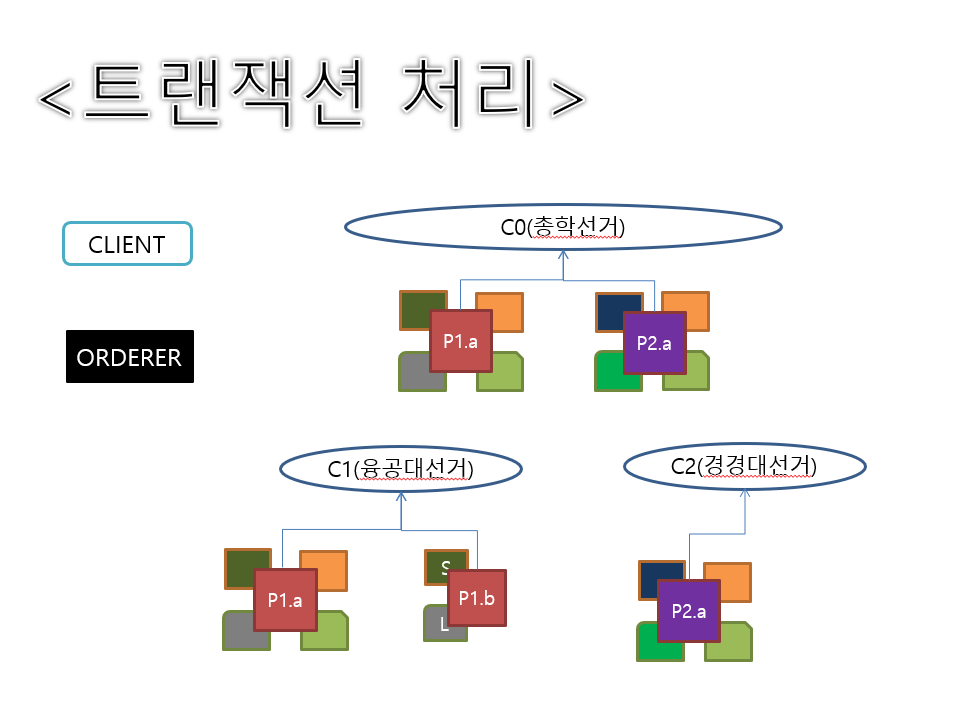
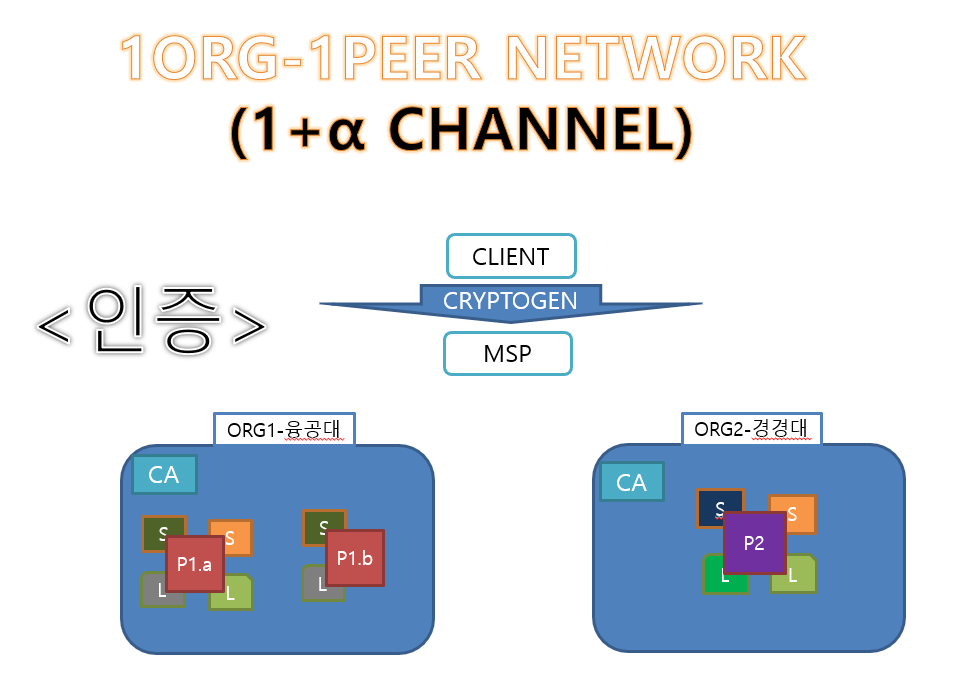
기억하도록 주의를 줄 필요는 있음)

* **네트워크 설계**



(↑ 성근팀원 초안 )

(↓ 현재까지 토의한 내용 )



* + 성근 팀원 의견
    - ca가 아닌 cryptogen으로 키 생성 후, 클라이언트가 접속하면

msp를 통해서 어느 조직으로 들어갈지 정책으로 설정.

단과대 선거는 하나의 피어(단과대)로 이루어진 채널.

총학선거는 모든 단과대를 피어로 가지는 채널.

단과대별 채널과 총학선거채널 등 채널을 다중으로 만들어서 장부를 여러개 만드는 구조.

// 단과대 선거 채널에 피어가 하나뿐인것은 문제가 될 수 있음.

피어가 하나라면 자기 혼자 인돌싱 피어인 동시에 커미팅 피어이므로

검증도 안되고, 원장공유도 안되서 보안적으로 매우 취약.

=> 단과대 안에 학과들로 이루어진 피어 여러개 만들어야

* + 단일 채널 vs 다중 채널
    - 선거별로 채널을 구성하면 만약 선거정보가 수정되거나 단과대가 추가되거나 할때마다 네트워크를 수정하고 채널을 다시 조인하는 일이 너무 어렵지 않을까?
* 선거 특성상 선거가 시작한 이후에 단과대가 추가되거나 하는 일은 없을듯, 단과대 정보가 변경되더라도 시간적 여유가 충분할것.
  + - 채널을 하나로 두고 원장을 모두가 공유하되, 권한에 따라 다른 단과대 선거는 못보게 하는 식으로 구현할 수도 있지 않을까? 프라이빗 데이터가 조직별로 생성되는지 피어별로 생성되는지 잘 모르겠지만 조직별로 생성된다고 한다면 굳이 채널을 나누지 않고 프라이빗 데이터를 통해 채널을 나누는 것과 같은 효과를 얻을 수 있을것 같다.
    - 선거별로 채널을 생성하면 채널이 너무 많아지지 않을까?
* 실제로는 그렇게 많은 선거가 동시에 시행되지 않음. 따라서 채널을 나눈다고 해서 너무 복잡해지는 일은 없을듯
  + - 채널이 한개라면 원장에 프라이빗 데이터로 뭔가를 넣었다는게 해시값으로나마 보임. 채널 나누면 뭔가를 넣었다는 것 조차도 안보임(아예 원장이 다르므로)

따라서 채널나누는게 투표보안의 관점? 투표 익명성의 관점에서는 더 좋을듯

* + - 이 외에도 프라이빗 데이터 사용했을때와 채널 사용했을때의 장단점을 알아봐야

함.

* + 찬훈 팀원 의견
    - fab car 예제 처럼 투표용지를 미리 다 만들어 놓고, 만약 투표를 하게되면 투표용지의 내용을 바꾸는 식으로 구현하는 것도 괜찮을듯.

그렇게 함으로서 얻는 이점은 투표율을 실시간으로 알 수 있고,

중복투표를 이중으로 막는다(투표용지가 없으면 투표를 못하므로)

투표용지의 형식만 조금 바꾸면 의견수렴하는 용지가 되는 등 확장성이 좋다

=> 투표율을 실시간으로 아는거는 학번 아이디 방식으로 해도 큰 속도 차이가 있지는 않을 것 같음. 틀을 만든다는 점에서 오히려 구조 변경 용이성이 없을수도...

초기 네트워크 생성할때 오버헤드가 발생할 수 있고, 투표를 안하는 사람이 있더라도 그 만큼 용량을 차지하게 되는 등 단점이 많을 것으로 예상..초기화하면서 블록을 생성하고, 투표할때 또 블록생성을 생성할 필요가 있을까?

* + 현재까지 정해진 내용
* 투표용지를 미리 만들지 않고, 다중채널(다시 논의)로 구현.

단과대 선거는 학과피어들을 만들어 검증 및 원장 공유

* **기타**
  + 다음회의 시간에 할것

토요일까지 DB설계 및 네트워크 설계 마무리

프라이빗데이터로 구현할지 채널로구현할지, ca와 오더러 어떻게 할지

중간고사 대비 회의 빈도 조정? IBM evote 따라 해보기?