BADID 멘토링 결과 보고서

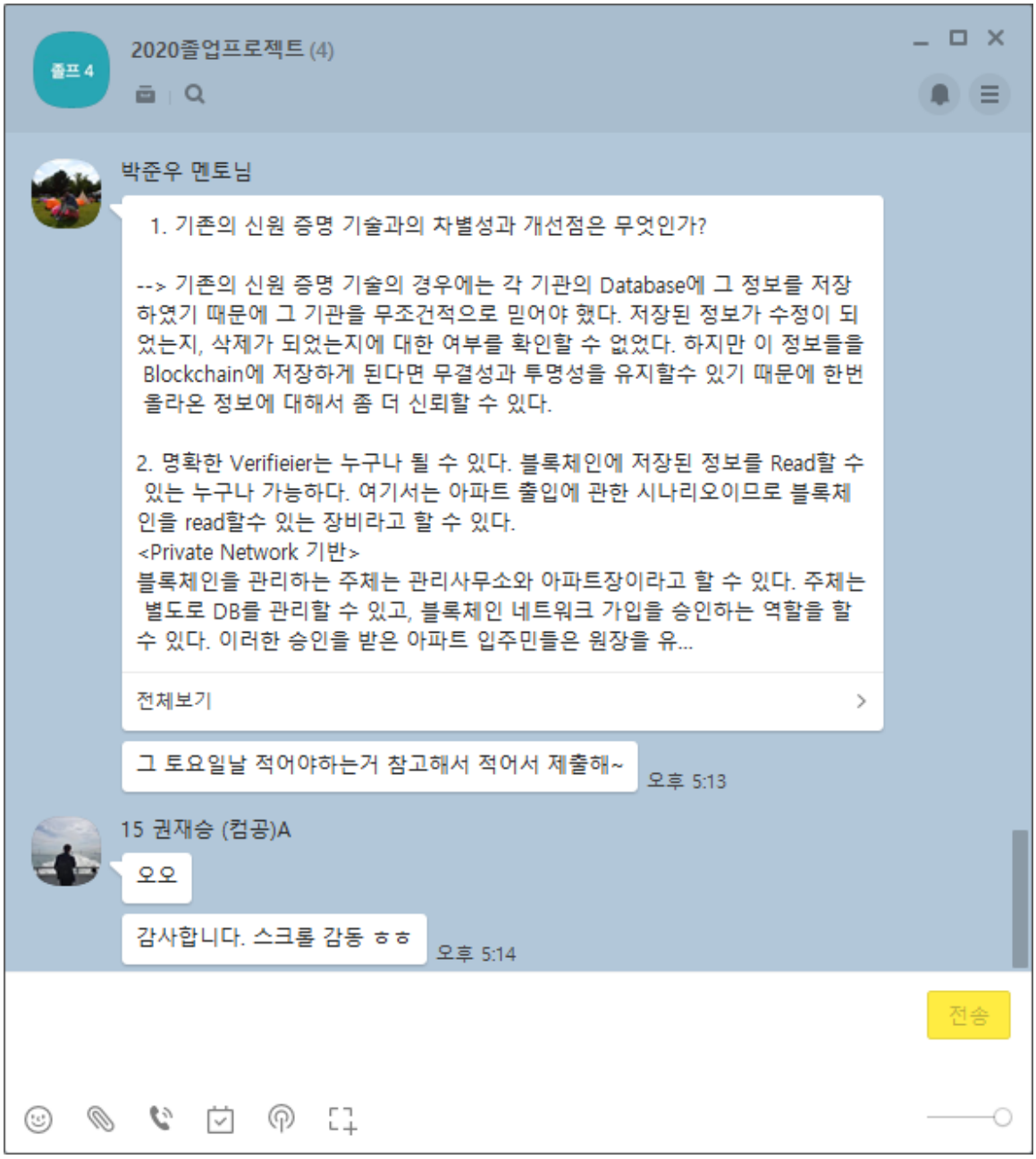
주제 : 블록체인 기반 자기주권형 분산 신원 증명 연구(아파트 출입)

- **멘토링 방법** : 카카오톡
- **멘토링 날짜** : 2020.05.21. 17:00

참가 인원

- **산업체 멘토** : 박준우 멘토
- **참여 학생** : 권재승, 조성락, 오하늘

멘토링 사진



현재 문제점

- 기존 신원 증명 기술과의 차별성과 개선점이 무엇인지 명확하지 않다.
- 블록체인 자체가 기존의 중앙 DB 기반의 사용자 인식하고 어떤 점이 달라서 차별점이 있는지 명확하지 않다.
- 검증자(Verifier)가 누구인지 명확하지 않다.
    - 가장 중요한 신뢰성 문제 : 블록체인 중앙 DB서버로 승인시켜주는 피어가 불분명하다.

- 실제 기관이나 사용자들이 합의 알고리즘을 통해 운영하는 것의 명확하지 않다. 서버 자체를 개인적인 아파트 가입자가 직접 운영하지 않을 가능성이 높은데, 실제로 어떻게 운영하여 문제를 해결할 수 있을지 의문이 든다.

멘토 피드백

Q. 기존의 신원 증명 기술과의 차별성과 개선점은 무엇인가?

A. 기존의 신원 증명 기술의 경우에는 각 기관의 데이터베이스에 그 정보를 저장하였기 때문에 그 기관을 무조건적으로 믿어야 했다. 저장된 정보가 수정이 되었는지, 삭제가 되었는지에 대한 여부를 확인할 수 없었다. 하지만 이 정보들을 블록체인에 저장하게 된다면 무결성과 투명성을 유지할 수 있기 때문에 한번 올라온 정보에 대해서 좀 더 신뢰할 수 있다.

Q. 명확한 검증자(Verifier)가 누구인가?

A. 명확한 검증자(Verifier)는 누구나 될 수 있다. 블록체인에 저장된 정보를 읽을 수 있는 누구나 가능하다. 여기서는 아파트 출입에 관한 시나리오이므로 블록체인을 읽을 수 있는 장비라고 할 수 있다.
프라이빗 네트워크에서 블록체인을 관리하는 주체는 관리사무소와에서 아파트장이라고 할 수 있다. 주체는 별도로 DB를 관리할 수 있고, 블록체인 네트워크 가입을 승인하는 역할을 할 수 있다. 이러한 승인을 받은 아파트 입주민들은 원장을 유지하는 피어(Peer) 역할을 할 수 있다. 이처럼 아파트 입주민들이 직접적으로 피어(Peer)역할을 하여 원장을 유지할 수 있고, 혹은 제 3자에 맡겨 신뢰성 향상을 위한 원장 유지하는 역할을 맡길 수 있다.
이 후 관리소에서는 각각의 입주민에 대한 출입증을 만들어 입주민들에게 발급하고, 검증할 수 있는 정보를 블록체인에 업로드한다. 그 정보는 모든 피어(Peer)들이 나누어 가지며, 검증자(Verifier: 입주민들을 검증할 수 있는 하드웨어 혹은 출입문)는 입주민이 출입증을 제시할 때마다 블록체인에 있는 정보를 읽어와 저장된 값이 일치하는지 여부를 파악한다. 추후 출입 통제를 위해 신원증을 발급했던 시기 및 사용자를 가명으로 블록체인에 저장하여 출입통제 관리를 할 수 있으며, 방문자의 경우에는 출입증을 발급받은 입주민들이 일회용 출입증을 생성하여 블록체인에 저장함으로써 방문자에 대한 관리, 그리고 어떠한 입주민이 그 방문증을 생성해주었는지에 대한 정보도 관리할 수 있어 효율적인 시스템을 만들 수 있다.

앞으로 계획

1. 실제 운영을 담당하는 부분을 아파트 관리 사무소가 할 수 있도록 변경
2. 검증자(Verifier) 아파트장으로 구체화
3. 최종발표에 기존 신원 증명 기술과의 차별성과 개선점이 무엇인지 구체적 설명 추가

깃헙 주소

- https://github.com/wotmd/Project_BADID

유튜브 링크

- https://youtu.be/75Uy5lJU9bA