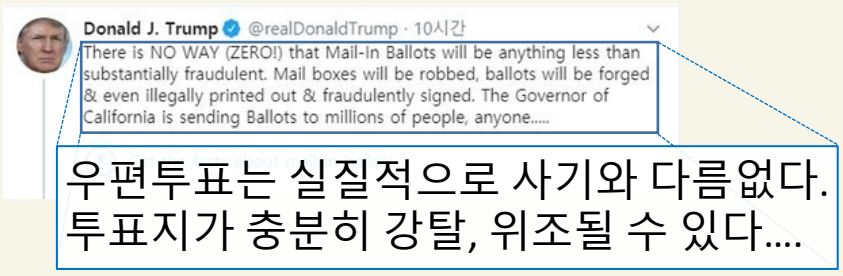
온라인 투표시스템을 위한 블록체인 연구

개발 동기

- 프로듀스 101 투표결과 조작 사건

엠넷, '프로듀스101 순위 조작 PD 징역 2년 확정 - 한겨레 2021.3.11

- 미국 대선 조작 의혹 (트럼프 트윗)

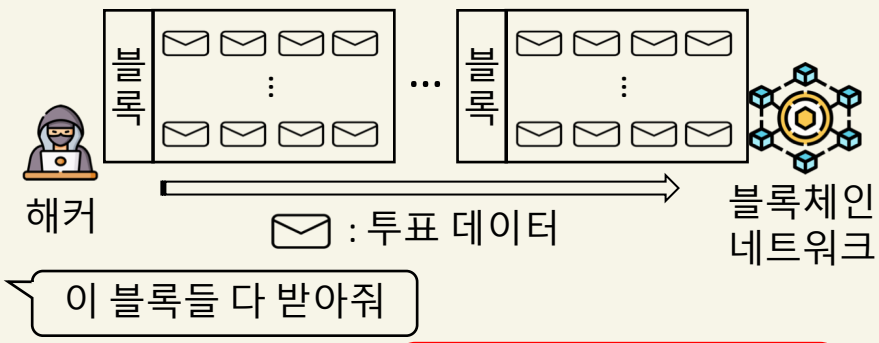


개발 목표

- 대통령 선거에 사용될 수 있는 블록체인에 대한 연구
  - **빠른 속도 (초당 1400건)**
    - 투표 인원: 4500만명
    - 투표 시간: 9시간
  - **불가능한 결과 조작**

기존 블록체인의 속도 문제

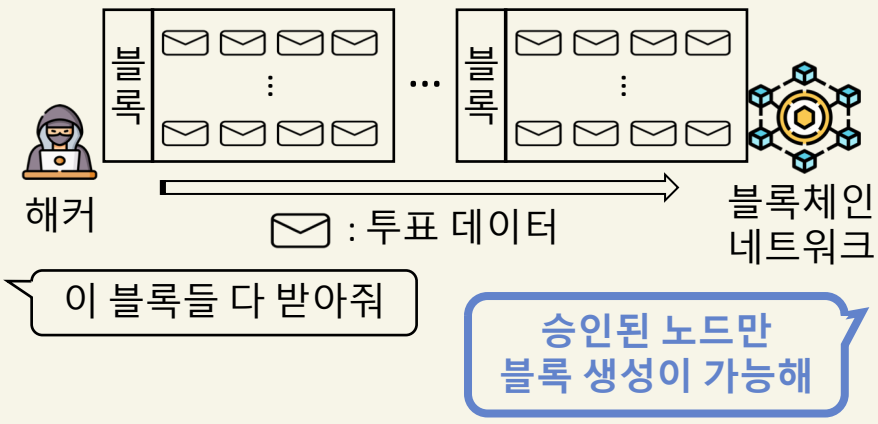
- 기존 블록체인의 속도
  - 비트코인: 초당 **약 7건**
  - 이더리움: 초당 **약 20건**
- 느린 속도의 원인
  - Proof of Work(PoW) : 블록 생성 제휴 시간으로 조작 방지 (비트코인의 제휴시간: 10분)



→ PoW의 제휴시간으로 인해 느림

제안하는 블록체인

- 속도 향상 방법
  - PoW 대신 승인 받은 노드만 블록을 생성하도록 함



→ 제휴시간 없이 조작 방지 (속도 저하 원인 제거)

- 합의 알고리즘
  - **블록 생성**: 이전 블록의 해시 값으로 승인된 노드 중 블록 생성 노드 선정
  - **검증**: 노드들은 생성된 블록을 검증하여, 조작되었다면 네트워크에 블록 재생성을 요청함
  - **결과 집계**: 네트워크가 가진 투표 결과 중 다수를 최종 결과로 집계함

증명 (결과의 조작 불가)

- 이론적 증명
  - 정직한 노드들은 조작되지 않은 블록이 생성될 때까지 블록 재생성을 요청함
  - 그로 인해, 정직한 노드들은 조작되지 않은 결과를 가짐
  - 그 결과, 정직한 노드가 50% 이상이라면 다수결에 의해 집계 결과는 조작되지 않음
- 실험적 증명
  - 실험 #1: 정직한 노드가 50% 이상일 때 결과가 조작되지 않음을 보임
  - 실험 #2: 한 노드에서 해킹으로 인해 조작된 결과가 감지됨을 보임