1. 서론, 2. 비트코인의 작동 원리

- 이중 지불 문제
    - 디지털 화폐는 실물(특수잉크로 쓰인 종이 화폐 등)로 존재하는 것이 아니기 때문에 여러번 사용될 수 있다.
- 비잔틴 장군 문제
    - 독립적으로 운영되는 노드 중에서 배신자를 어떻게 찾을 것인가?
- 작업 증명
    - 에너지 소모가 크고 채굴 집중화
- 지분 증명
    - 51% 어택 불가 - 그만큼 돈을 가지기 힘듦
    - Nothing-at-stake → Casper에서는 보증금과 벌금
    - 두개 이상의 포크에 대해서 동시에 베팅 가능
- 클라이언트
    - 풀 클라이언트 - 거래 내역을 전부 저장
    - 라이트웨이트 클라이언트 - 풀 클라이언트에 요청하여 거래내역 참조
    - 웹 클라이언트

- 거래
    - 거래 유형:
        - 1 → 2 : 단일 거래. 거스름돈은 본인 계좌로 다시 입금하는 형식
        - n → 1 : 합치는 거래. 여러 잔액을 하나의 UTXO로 정리
        - 1 → n : 배분하는 거래. 예를 들어, 직원에게 급여를 지불하는 형식
    - 거래 구성
        - 소비되지 않은 출력값(UTXO)을 통해서 적절한 입력값 찾기
            - 풀 클라이언트의 경우는 모든 거래의 UTXO를 알 수 있으나 라이트웨이트 클라이언트는 풀 인덱스 노드에 요청해서 알 수 있다.
        - 출력값 생성하기
            - 지불할 금액을 설정하고 그 차액을 본인 계좌로 입금. 1→2 의 거래유형을 생각할 수 있다.
            - 출력값 - 입력값은 수수료 이므로 본인 계좌로 입금하는 출력값을 설정하지 않으면 큰일남.
        - 장부에 추가
            - P2P 네트워크를 통해 연결된 노드들에 거래를 전송하고 네트워크의 이웃에게 계속하여 전파(gossip network)
            - 이때 각 노드들은 독립된 검증을 실시한다.(입력값>출력값, 블록사이즈, 등)
- 채굴
    - 각 노드에 전송된 거래들은 임시 풀에 저장된다.
    - 노드는 약 10분마다 지난 블록부터의 거래들을 선택하여 블록을 생성한다.
        - 2주(2016블록*10분)마다 난이도를 조절하여 10분을 유지
        - 거래수수료, 거래의 age 등의 기준에 따라서 거래를 선택
        - 블록에는 본인 지갑으로 전송하는 12.5 비트코인을 포함.
    - 해시의 Nonce를 찾은 노드가 해당 블록을 블록체인으로 연결하고 다른 노드들은 이를 검증하여 역시 체인에 연결
    - 각 노드는 최고누적연산 체인을 선택함으로써 분산환경에서도 일관된 상태로 수렴