8. 채굴과 합의

- 경제학과 통화 발행 (디플레이션)
    - 비트코인에서는 신규 발행되는 화폐의 총량이 점점 줄어드는 구조이다.
    - 실물 경제에서는 디플레이션이 있을 때, 현재 가지고 있는 화폐의 가치가 점차 증가하므로 소비를 위축시켜 경제순환이 원활히 되지 않는 재앙이라고 한다.
    - 비트코인 체제에서는 디플레이션에 의해서 수요가 붕괴될 것이라 보지 않는다.
- 거래 검증 (너무 당연한 것들은 생략)
    - 거래 구문과 데이터 구조가 정확해야 한다.
    - 거래의 입력값에 대한 UTXO가 블록이 아닌 거래풀에 존재한다면 거부
    - 거래의 입력값에 대한 UTXO가 없는 경우 고아 거래풀에 추가
    - 거래의 입력값이 코인베이스 출력이라면 최소 승인(100회)를 받아야만 한다.
    - 거래의 입력값은 이미 소비되지 않아야 한다.
    - 해제스크립트/잠금스크립트를 검증해야 한다.
    - ...
    - → 검증된 거래들은 거래 풀(메모리상에 존재)에 추가한다.
- 블록에 거래 추가 (채굴 노드가 하는 일)
    - 우선순위
        - Priority = Sum (Value of input * Input Age) / Transaction Size
        - 우선순위는 금액 크기와 해당 UTXO의 나이에 비례하고, 거래 크기에 반비례한다.
        - High Priority > 100,000,000 satoshis * 144 blocks / 250 bytes = 57,600,000
        - 57,600,000 값보다 큰 경우만 우선순위가 높다고 판단되며, 이들 중 Priority에 따라서 블록에 추가된다.
        - 블록의 첫 50킬로바이트는 우선순위에 따라서 거래를 채운다.
        - 나머지는 수수료에 따라 채우던 어쩌던 노드 운영자 마음대로
    - 생성거래(코인베이스 거래)
        - 입력값이 없는 출력값
            - 입력값이 의미가 없기 때문에, 임의적인 데이터로 채울 수 있다.
            - BIP0034 이후에는 추가 데이터로 쓰고 있다.
                - 블록의 높이, 추가 난스, /P2SH/문자열(BIP0016 개선안 표시)
        - 블록생성보상금 + 수수료
            - Total Fees = Sum(Inputs) - Sum(Outputs)
            - 블록생성 보상금
                - 210,000 개의 블록마다 반으로 감소(약 4년에 한번)
                - 50 → 25 → 12.5 → 6.25 → ... → 0 : 64회 반복하고 나면 수수료만 지급
    - 블록 해더 구성
        - 버전, 이전블록해시, 머클루트, 타임스탬프, 난이도 목표, 난스
        - 버전 - 블록 구조를 설명하기 위한 버전 정보.
    - 블록 검증
        - 블록 헤더 해시는 목표 난이도보다 작다.
        - 타임스탬프는 현재보다 향후 2시간 이내이다.
        - 블록의 크기는 허용 한도 내에 있다.
        - 첫 거래는 코인베이스 거래이다.
        - 블록의 거래를 위의 거래 검증 방법에 따라서 모두 검증한다.
- 채굴
    - 작업 증명
        - 블록의 헤더(난스 포함)를 해시 했을 때, 난이도에서 제시하는 값보다 작은 값이 되는 난스를 찾는 알고리즘
        - 주어진 난스를 이용해서 작업 증명을 검증하는데는 단 1회의 해시 계산만이 필요하지만, 조건을 만족하는 난스를 찾는데는 아주 많은 해시 계산이 필요하다.
        - 전체 블록체인 네트워크에서 해당 난스를 찾기 위한 경쟁을 벌이기 때문에, 특정 누군가가 기존의 블록을 변경하기 위해서는 나머지 모두를 이길 수 있는 해싱 파워가 필요하다.
        - 즉, 논리적으로 조작이 가능할 수는 있지만, 이를 실현하기에는 현실적으로 조작이 불가능하게 만드는 증명 방법
    - 난이도 표기
        - target = coefficient * 2 ** (8 * (exponent - 3))
        - 0x1903a30c → exponent: 0x19, coefficient: 0x03a30c
        - target = 0x03a30c * 2 ** (0x08 * (0x19 - 0x03))
        - target = 0x03a30c * 2 ** (0x08 * 0x16)
        - target = 0x03a30c * 2 ** 0xb0
        - target = 0x000....3a30c0....
    - 난이도 재설정
        - new difficulty = old difficulty * (actual time of last 2016 blocks / 20160 minutes)
        - 2016개의 블록이 생성될 때 20160 분이 걸린다는 가정
        - 만약, 그보다 오래 걸렸으면 난이도는 낮아지고, 적게 걸렸으면 난이도는 높아진다.
        - 각 노드가 각자 난이도를 재설정하는데, 만약, 악의적으로 난이도를 낮춘다면, 다른 노드의 '높은 난이도의 체인 선택' 방법에 의해서 탈락하게 될 것이다.
        - 만약, 나 혼자만 아는 외계기술이 있어서 해싱 파워를 기하급수적으로 늘릴 수 있다면, 혼자서 난이도를 높일 수도 있음. 하지만, 현실적으로 불가능하다.
    - 추가 난스 솔루션
        - 난이도가 증가하면서 난스값 40억개를 대입해도 해시값을 만족하는 난스를 찾을수 없을 때도 있다.
        - 대안1. 타임스탬프를 변경하면서 채굴. 하지만, 1초도 되기전에 난스값을 모두 써버림, 블록검증시 타임스탬프 기준으로 2시간 이후는 버려짐
        - 대안2. 코인베이스 거래의 입력값 필드 사용. 코인베이스의 입력값 변경 → 머클트리 변경됨 → 머클루트 변경됨 → 헤더 변경됨

- 채굴 풀
    - 낮은 확률로 높은 결과값을 얻기 보다는 높은 확률로 낮은 결과값을 얻기 위한 방법
    - 풀 관리
        - 채굴 풀 서버에 연결된 클라이언트는 원래의 난이도보다 낮은 난이도의 해시값을 구하는 난스를 풀 서버에 전송하고 그에 따른 보상을 지급 받는다
        - 채굴 풀 서버는 전달 받은 난스 중 일부가 원래의 난이도를 만족하는지 검증하고 채굴 보상을 받아 기여도에 따라 클라이언트에 비트코인으로 보상한다.
    - P2Pool
        - 채굴 풀 방식의 서버/클라이언트 네트워크를 P2P 네트워크로 연결한 방식
        - 낮은 난이도를 가지는 공유체인이라 불리는 블록체인(30초당 하나의 블록 생성)을 만들고, 그중 일부가 비트코인 네트워크의 난이도를 만족시키면 그 밑의 블록에 보상을 나누는 방식
- 블록 체인 분기
    - 각 노드는 3가지 종류의 블록을 보관 하고 있다.
        - 메인체인에 연결된 블록 - 각 블록의 난이도의 합이 제일 큰 브랜치
        - 브랜치를 형성하는 블록 - 메인체인이 되지 못하지만, 이후 메인 체인이 될 수도 있는 블록들의 브랜치
        - 고아 블록 - 참조할 수 있는 부모 블록이 '아직' 존재하지 않는 블록
    - 동일한 난이도를 가지는 두 블록이 있을 때, 먼저 도착한 블록을 메인 체인에 추가하고, 다른 블록은 브랜치를 만든다. 즉, 같은 난이도면 메인체인을 굳이 바꾸지 않는다.
    - 이후, 또다른 블록이 도착했을 때, 브랜치의 블록을 부모로 하는 블록이라면, 브랜치가 메인 체인이 된다.(재수렴)
    - 재수렴 없이 혹은 재수렴이 반복하면서, 브랜치가 계속해서 유지되는 상황이 있을 수도 있지만, 확률적으로 드문일이다.(최대 6회정도)
    - 확률적으로, 먼저 채굴된 블록이 더 많은 노드에 전파되고, 더 많은 노드에 전파된 블록을 부모로하는 블록이 채굴될 가능성이 높기 때문에, 결국에는 한쪽으로 수렴한다.
- 합의 공격 (51% 공격)
    - 과거에 발생한 블록에 대한 공격은 변경하기 어려움. 최근 몇개의 블록에 대한 공격이 있을 수 있다.
    - 압도적인 해싱 파워를 가진 집단이 실행할 수 있다.
    - 51%의 의미는 공격이 거의 보장되는 수준이며, 통계적으로는 30% 정도의 해싱 파워를 통해서도 공격이 성공할 수 있다.
    - 이중 지불 공격
        - 거래가 승인되고 블록이 생성된 직후, 해당 UTXO를 다른 곳으로 소비하는 형태의 거래를 만들고 압도적인 해싱 파워를 이용하여 의도적인 블록체인 분기를 만드는 방법
    - 서비스 거부 공격
        - 다른 채굴자가 채굴한 블록을 무시하고 의도적인 블록체인 분기를 만드는 방법