NS-3 상에서의 PoS 합의 알고리즘 구현

https://youtu.be/-JsCWQS-6i8

PoS 합의 알고리즘

구현한 PoS 합의 알고리즘 과정

코드 설명

개선 및 수정할 점

Proof-of-Stake Consensus Algorithm

- **지분증명(Proof of Stake : PoS)**
  - 암호화폐를 보유하고 있는 **지분율**에 비례하여 의사결정 권한을 주는 합의 알고리즘

    → 지분이 블록 생성 권한에 영향을 미친다는 큰 틀에서 공유하고 있을 뿐 코인마다 세부적인 부분에 있어서는 많은 차이가 있음
  - 작업증명(PoW)와 다르게 채굴 과정 필요 X

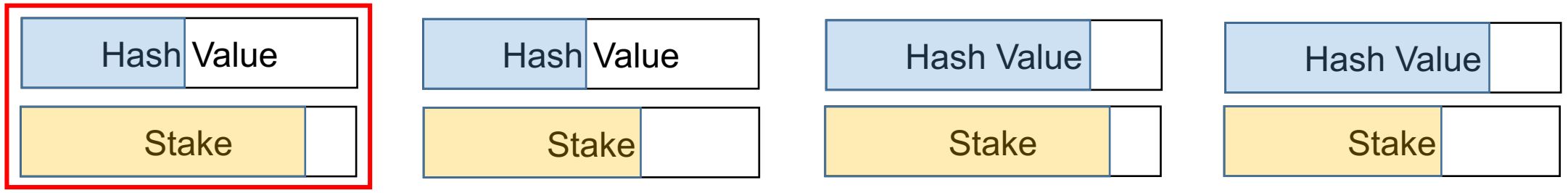
    → 에너지 소모 X
  - 부익부 빈익빈 문제 야기

Proof-of-Stake Consensus Algorithm

- **부익부 빈익빈 문제 해결방안**

1. **무작위 블록선택 :** 가장 낮은 해시값과 가장 높은 지분의 조합을 가진 노드를 블록생성자로 결정
2. **코인 나이에 따른 선택 :** 코인의 나이가 가장 많은 노드를 블록 생성자로 결정
   → 코인의 나이 = 스테이킹한 시간 * 스테이킹 양

peercoin



코인 나이 = 3일 x

코인 나이 = 2일 x

Proof-of-Stake 구현

- **동작과정**

  1. 노드에게 코인을 임의로 할당 (***CoinAllocation***)
  2. 할당 받은 코인 중 일부를 스테이킹 (***StakingCoin***)
  3. 코인의 나이를 계산하여 브로드 캐스트 (***SendCoinAge***)
  4. 다른 노드들의 코인의 나이를 전송 받아 제일 높은 코인의 나이 계산(***HandleRead***, ***MaxArray***)
  5. 제일 높은 코인의 나이 값을 가진 노드가 블록을 생성하여 전송 (***generateBlock***, ***SendBlock***)
  6. 전송 받은 블록을 검증 후 유효할 경우에만 블록체인 추가 (***ValidationBlock***, ***AddBlock***)

코드

수정 및 추가해야할 부분

1. 검증자들이 블록을 검증함으로써 보상을 받도록
2. 블록 생성자가 블록을 생성하면 바로 원장에 추가하는데, 유효한 블록이라고 검증 받았다는 답장을 받은 후에, 블록을 추가하도록
3. 트랜잭션을 임의로 설정하기 않고 실제로 트랜잭션을 발생시켜보기 (코인 주고 받기)
   → 전자서명 사용
4. 두 노드의 코인의 나이가 같을 경우 블록 생성을 두 노드가 하는 문제 발생 (포크)
5. 주석 상세하게 추가하기
6. 원웅이와 코드를 비교해보고 함수명 및 변수 등 통일시키기

Q & A