**Problem description of demo blockchain**

블록체인은 데이터 무결성과 투명성을 보장하는 분산 원장으로 PKI, P2P, 합의알고리즘, 분산처리를 기반 기술로 가진다. 블록은 트랜잭션을 담고있는 바디 부분과 인덱스, 이전 블록의 해시값 등을 담은 헤더부분으로 나뉘어진다. 특히, 헤더 부분의 이전 블록의 해시값을 통해 각각의 블록이 링크드리스트 형태로 연결된다. 모든 노드들은 같은 내용은 가진 블록체인을 공유하고 거래가 발생됨에 따라 블록이 지속적으로 추가된다.

**\* 다음은 블록체인이 갖추어야 할 기본적인 기능 및 제약사항**

제약 사항.

1. 블록체인 노드는 최소 5개 이상으로 한다.
2. 최소 두 개 이상의 노드가 Miner가 된다.
3. 각각의 노드는 데이터 송수신이 가능해야 한다.
4. 각각의 노드는 개인키, 공개키, 노드 주소를 1개씩 가져야 한다.
5. 개인키는 난수 생성기를 통해서 생성하고, 공개키는 개인키로부터 타원곡선 암호화를 사용하여 생성하며, 노드 주소는 공개키로부터 해시 함수를 사용하여 생성한다.
6. 해시함수는 SHA256을, 전자서명은 ECDSA를 사용한다.
7. 모든 Transaction은 송신자의 개인키로 서명이 된 뒤 전파 되어야 한다.
8. 트랜잭션 10개마다 Miner 가 블록을 생성하고 모든 노드에게 전파한다.
9. 블록에는 index, timestamp, previous block hash, transaction\_list, nonce 가 포함되어야 한다.

기능 사항.

* Miner
  1. 블록체인에 연결할 후보 블록을 생성한다.
  2. 발생한 Transaction에 대해 합의하기 위해 주어진 hash puzzle을 사용한다.
  3. 숫자를 하나씩 넣으면서 hash puzzle 문제를 푼다.
  4. 가장 빨리 hash puzzle 문제를 해결한 사용자는 후보 블록에 hash puzzle의 정답을 nonce를 기록하여 블록을 생성된다.
  5. 블록을 생성한 사용자는 다른 사용자에게 생성된 블록을 전파한다.
  6. 가장 빨리 hash puzzle 문제를 해결하지 못한 사용자는 다른 사용자가 생성한 블록을 기다린다.
  7. 블록을 전달 받은 노드는 Validation 절차에 따라 검증한다.
* 사용자
  1. 사용자는 거래에 들어갈 데이터를 선택한다.
  2. 사용자의 개인키로 전자서명을 생성한다.
  3. Transaction에 공개키를 포함시킨다.
  4. 생성된 Transaction을 네트워크에 전파한다.
  5. 거래를 받은 노드는 Validation 절차에 따라서 Transaction을 검증하고 자신의 Transaction 풀에 저장한다.
  6. Transaction 검증에 실패할 경우 전달 받은 Transaction을 Transaction pool에 저장하지 않는다.
* Validation
  1. 검증 과정은 Transaction 검증과 블록 검증으로 나뉜다.
  2. Transaction 검증 과정은 다음과 같다.
     1. Transaction을 전파 받은 노드들은 Transaction 발생자의 공개키를 사용한다.
     2. Transaction에 포함되어 있는 전자서명을 Transaction 발생자의 공개키로 검증한다.
     3. 검증에 실패할 경우 해당 Transaction을 폐기한다.
  3. 블록 검증 과정은 다음과 같다.
     1. 블록을 전파 받은 노드들은 블록에 담긴 거래를 검증한다.
     2. 블록 안의 nonce 값을 통해서 hash puzzle의 정답이 나오는지 계산하여 검증한다.
     3. 검증에 실패할 경우 해당 블록을 폐기한다.