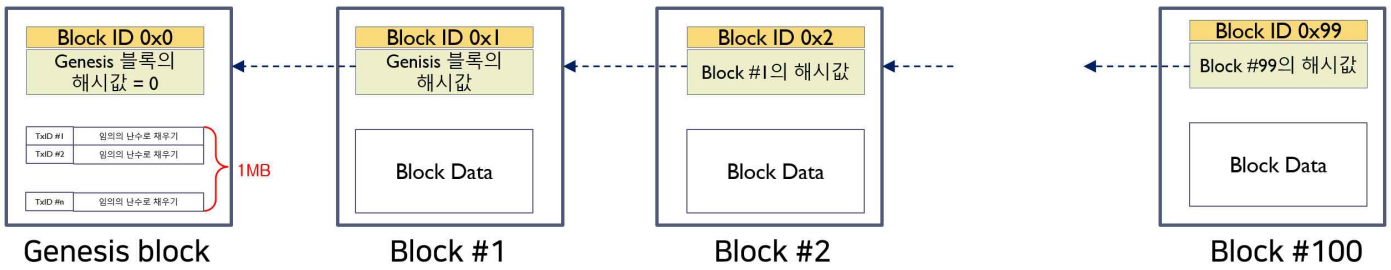
2022 암호분석경진대회

2번 문제

[문제] 아래의 문제에 대한 답을 제시하시오.

1. 아래 그림과 제시된 조건들을 만족하는 블록체인 모델을 구현하시오.
2. 개발한 블록체인의 구성을 고속화하기 위해 해시함수를 고속화하거나 고속 해시값 검증 구조를 제시하고 이를 구현하시오.
3. 구현한 블록체인 모델을 사용하여, 특정 블록의 Transaction 데이터가 위변조 되었을 때, 해당 블록이 변경되었음을 보이시오.



<블록간 해시체인 구조를 갖는 단순한 블록체인 구조>

(조건 3-1) 각 블록은 다음과 같이 구성된다.

- 각 블록은 Block ID와 이전 블록의 해시값, 그리고 블록 데이터로 구성됨
- 블록내에 있는 블록 데이터는 Transaction들로 구성되며, 블록 데이터의 총 크기는 1MB임
- 블록 데이터를 구성하는 각 Transaction은 160 비트의 TxID값과 (편의상random 하게 생성된)864비트 크기를 갖는 Transaction값으로 구성됨
- 각 블록에 포함되는 블록 데이터 크기는 1MB 크기가 되어야 함

(조건 3-2) Block ID를 다음과 같이 정한다.

- Genesis 블록의 blockID는 0x0임. 그 후 연결되는 블록의 ID 값은 0x1, 0x2, 0x3,...처럼 1씩 증가함
- 이때, Block ID의 크기는160 비트로 정함

(조건 3-3) 각 Block의 해시값은다음과 같이 생성된다.

- Genesis 블록의 초기 해시값은 0으로 정하며, 해시값크기도 160 비트로 정함
- Block #1에 포함되는 해시값은 이전 블록(Genesis block) 전체에 대한 해시값임
- Block #2는 Block #1 전체에 대한 해시값을 가짐. 이때, 각 블록 내부의 해시 값은 SHA3의 256비트 출력값에서 하위 160비트를 해시값으로사용하기로 함

(조건 3-4) 해시값 생성 관련하여 다음과 같은 특성을 갖는다.

- 해시값생성시 사용하는 해시함수는 반드시 SHA3-256을 사용해야 함
- SHA3-256 해시값에서 하위 160비트를 사용함
- 해시 생성시, 암호 구현 최적화, 구조적인 해시 계산 등, 다양한 기법을 사용할 수 있음 (평가 항목임)

(조건 3-5) 특정 Transaction 값이 위변조 되었는지 여부를 빠르게 검증할 수 있는 방안을 제시해야 한다

- 특정 블록의 Transaction 값이 위변조되었는지를 빠르게 검증할 수 있는 방법을 고안하여, 이를 실제 구현해야 함

(조건 3-6) 기타 사항:

- 모든 값은 가독성 제공을 위해 Base-58로 인코딩됨
- 사용언어는 어떤 것을 사용하든지 좋음. 또한, 해시함수 등은 library를 사용하여 구현할 수 있지만, 고속화를 위해 수정하거나 어떤 특별한 장점을 갖도록 하기 위해, 직접 구현할 경우, 추가 점수가 부여됨
- 구현된 기능을 명확히 파악할 수 있는 test code를 제시해야 함
- 합의 알고리즘 등에 대한 고려는 전혀 할 필요없음