한 번에 끝내는
블록체인 개발 A to Z

Chapter 2

Blockchain 2.0 - Ethereum

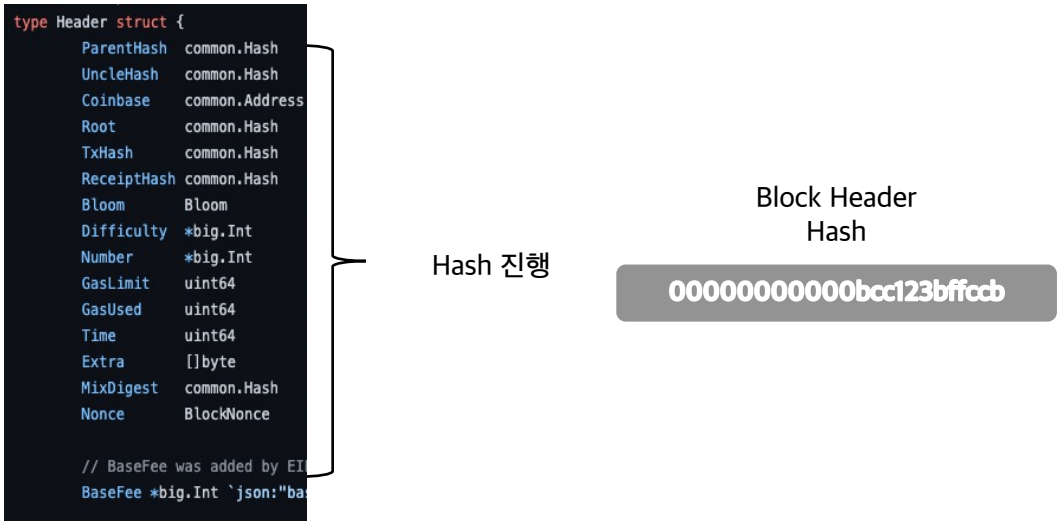
Chapter 2

Blockchain 2.0 - Ethereum

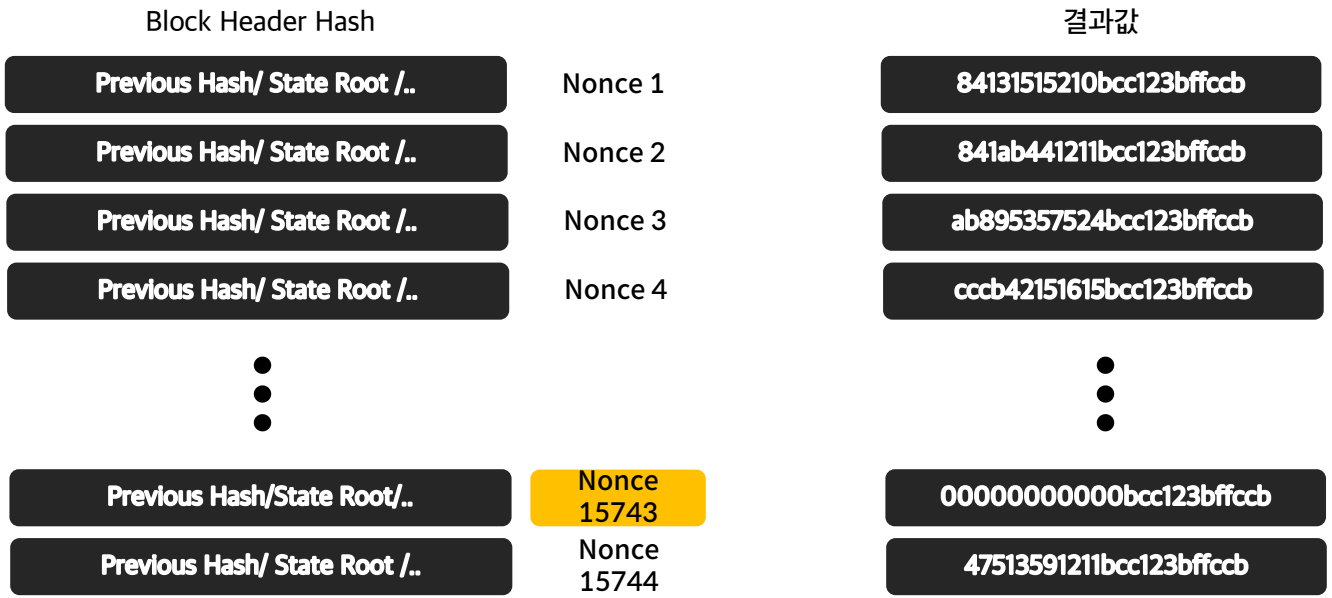
Consensus

Proof Of Work

- 새로운 블록(a)이 생성됨을 알림받는다.
- 다음 블록 생성을 위해서 Pending 중인 Transaction을 포함한다.
- 이전 블록(a)와 Transaction들을 포함한 임시 Block구조(b)를 만든다.
- 새로운 Block(b)의 Header Hash가 결과값이 나올 때 까지 brute force 방식으로 nonce를 찾는다.

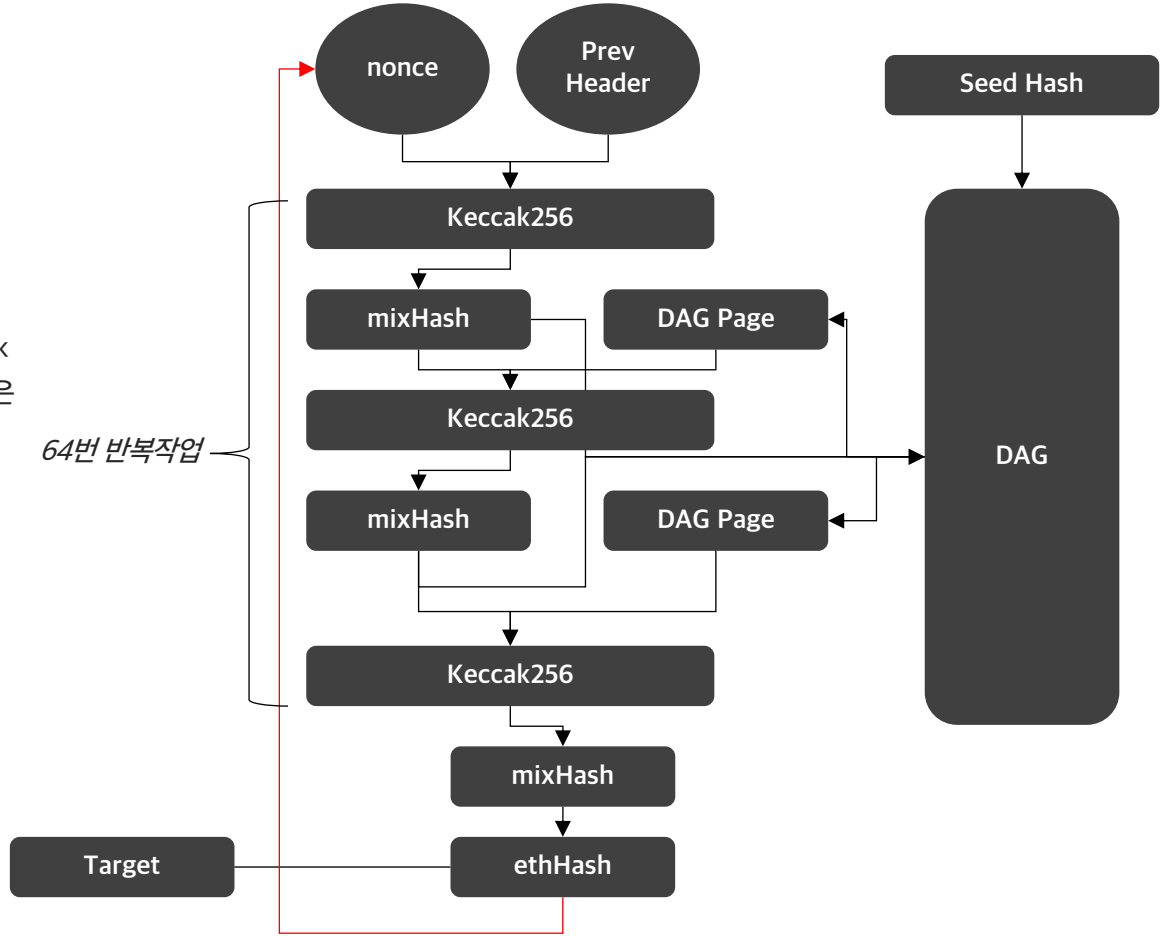


Proof Of Work



Ethash

- Ethereum은 ethash라는 Proof of Work 알고리즘을 사용하고 있다. 이 알고리즘은 DAG를 통해 Memory 저항성을 가지고 있어서 단순 SHA 연산만을 진행하는 Bitcoin과 달라 ASIC 제작이 어렵게 되어있다. 따라서 이더리움 채굴자들은 대부분 그래픽카드를 통해서 채굴을 진행한다.



Block Difficulty

- EIP-2 로 인해서 Block Difficulty 계산 수식이 변경되었다. 2016마다 재연산되는 Bitcoin과는 달리 Ethereum은 매 Block 마다 Difficulty 재연산을 통해서 13초의 블록 생성 주기를 유지한다.

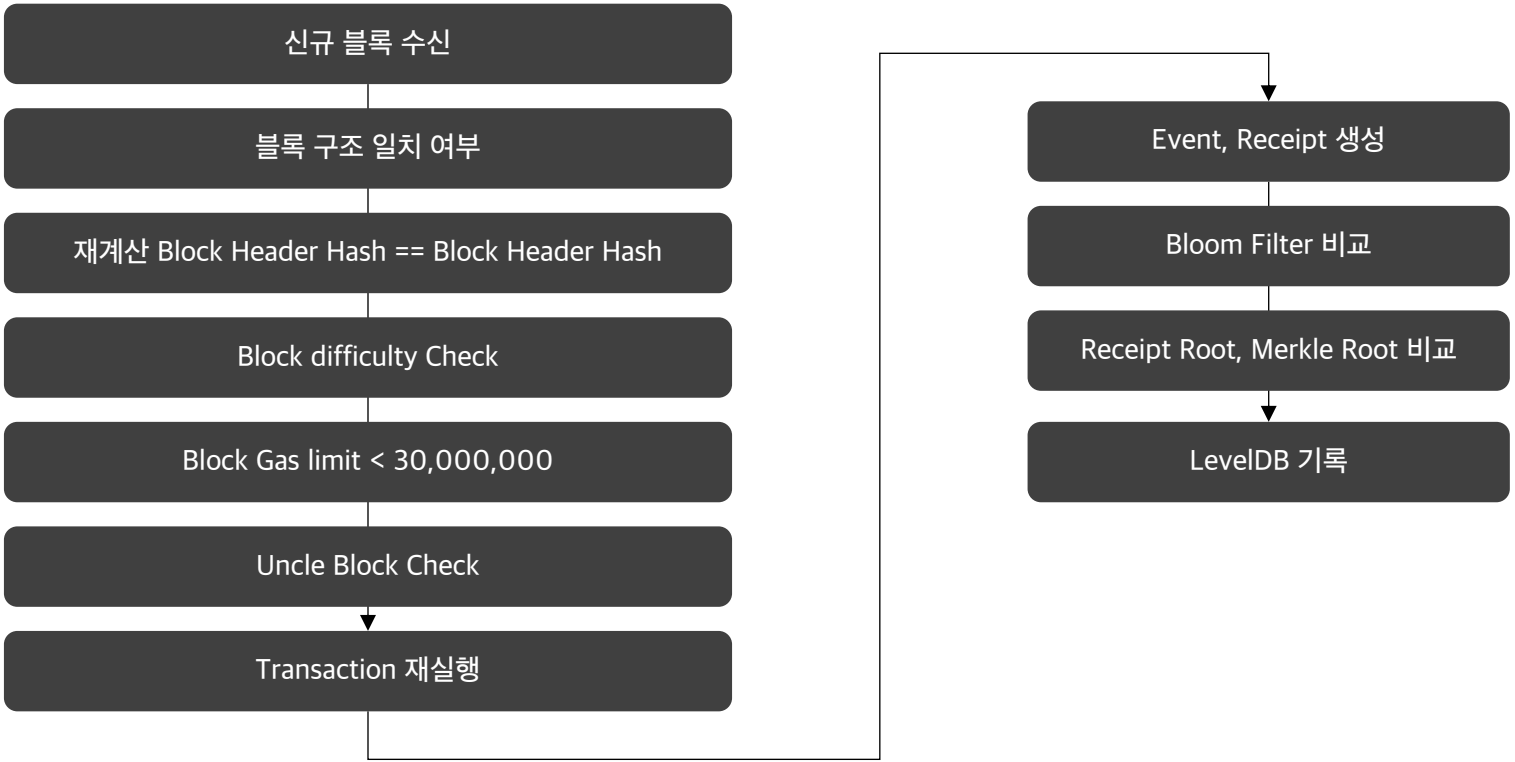
  <Frontier>

  block_diff = parent_diff + parent_diff // 2048 * (1 if block_timestamp - parent_timestamp < 13 else -1) + int(2**((block.number // 100000) - 2))

  <Homestead>

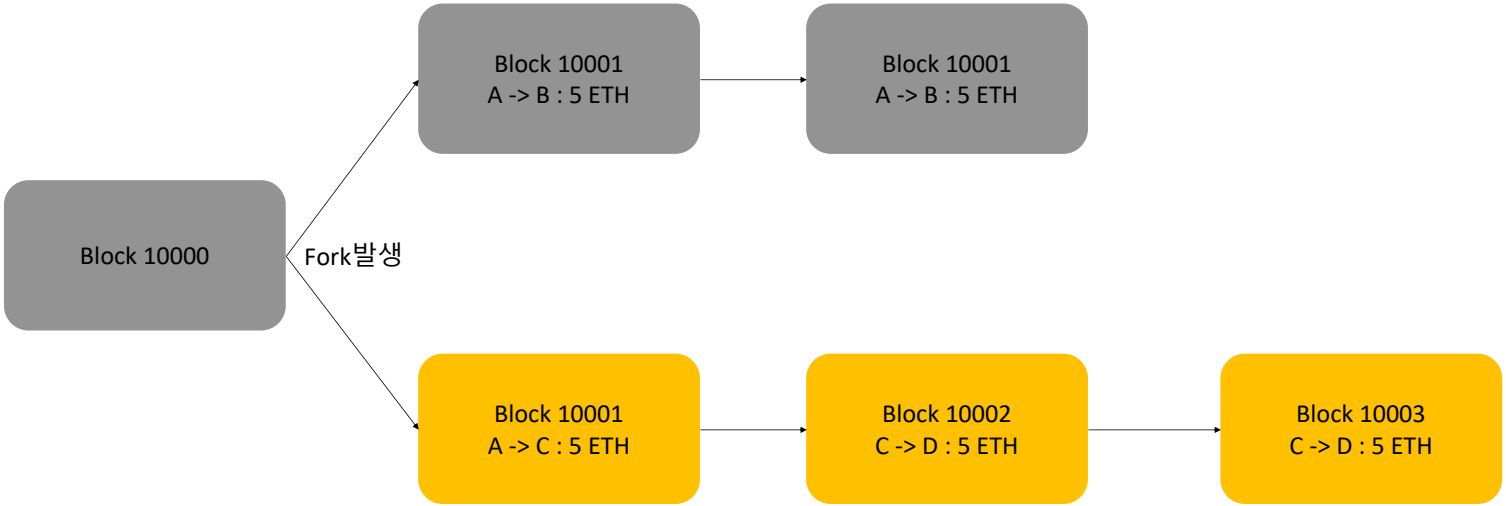
  block_diff = parent_diff + parent_diff // 2048 * max(1 - (block_timestamp - parent_timestamp) // 10, -99) + int(2**((block.number // 100000) - 2))

Block 검증


신규 블록 수신
블록 구조 일치 여부
재계산 Block Header Hash == Block Header Hash
Block difficulty Check
Block Gas limit < 30,000,000
Uncle Block Check
Transaction 재실행
Event, Receipt 생성
Bloom Filter 비교
Receipt Root, Merkle Root 비교
LevelDB 기록

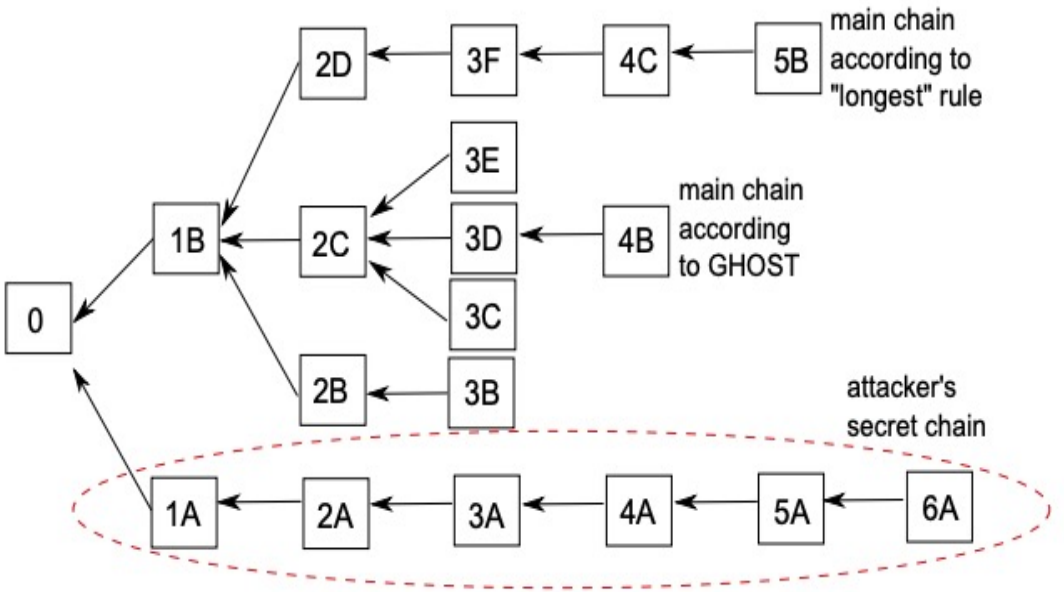
Longest Chain Rule

- Longest Chain Rule은 Bitcoin Network 전체가 Fork가 발생할 때, 하나의 블록체인만을 유지하기 위한 방법
- 실제 Rule은 전체 Blockchain Fork 중 BlockChain 생성에 가장 많은 Computing Power가 사용된 Chain임



Ghost Protocol

- Ghost Protocol 이란 Ethereum에서 하나의 Chain을 유지하기 위한 방안이다. Greedy Heaviest Object subTree의 약자로 가장 많은 SubTree를 가진 chain을 선택하는 것이다. 이를 통해 uncle block에 대한 보상도 생기게 되었다.



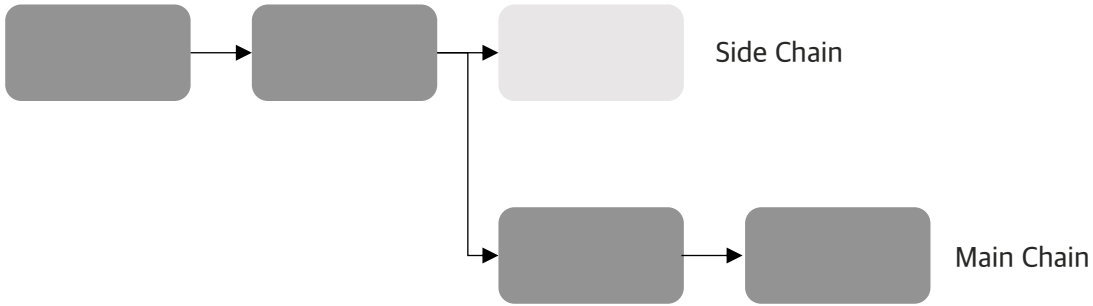
(출처 : Secure High-Rate Transaction Processing in Bitcoin)

Uncle Block Reward

- Ghost Procol에 따라 Uncle Block 또한 버리지 않고 Block Header에 포함시켜 이에 따른 보상을 제공한다.
- Uncle Block 보상에 대한 계산 방법은 아래와 같다.
  (Uncle Number + 8 - Block Number) * Miner's Reward / 8 (Miner's Reward는 기본 블록 보상 현재 2ETH)
- Miner가 Uncle Block을 포함하여 블록을 생성하는 경우 0.0625 ETH를 추가로 보상 받는다.
- 하나의 Block에는 최대 2개의 Uncle Block이 포함될 수 있고, 하나당 0.0625 ETH씩 추가 보상이 가능하다.
  ex) Uncle Number = 8368757, Block Number = 8368759
  Block에 1 Uncle Block 포함
  Block 보상 = 2 ETH + 0.0625 ETH + 거래 수수료
  Uncle 보상 = (8368757 + 8 - 8368759) * 2 ETH / 8 = 1.5 ETH

Ethereum 재구성

- Ethereum에서 Fork 발생 후 노드가 Main Chain이 아닌 경우 Blockchain 재구성이 이루어지게 된다.
- 기존 Block과 Main Block을 비교하여 Transaction 차이를 구성 한 뒤, 차이가 있는 Transaction을 LevelDB에 신규 등록하고, 기존 등록된 Transaction은 제거한다.



Ethereum Hard Fork

- 2016년 The Dao 라는 서비스가 약 360만개의 ETH를 탈취당하는 사건이 발생했다. 이는 전체 이더리움 발행량의 약 10% 해당하는 양이다.
- Smart Contract 상의 취약점을 공략한 대표적인 공격 사례이다.
- 이로 인해 거래 롤백에 대한 Hard Fork가 발생하였고, 이에 반대하는 사람들에 의해 네트워크 분리도 발생하였다.