블록체인 기술과 응용 서비스

1. 블록체인 개요
2. 블록체인 응용과 사례
3. 블록체인 보안
4. 비트코인 블록체인의 구조와 동작원리
5. **이더리움 블록체인의 구조와 동작원리**
6. 가상전자 거래소, 전자지갑, 채굴
7. 블록체인 이슈와 전망

대구사이버대학교
DAEGU CYBER UNIVERSITY

블록체인 기술과 응용 서비스 5주차

이더리움 블록체인의 구조와 동작원리

1교시 : 이더리움 블럭헤더와 트랜잭션

2교시 : 이더리움의 머클패트리샤 트리와 스마트계약

3교시 : 이더리움 생태계

1교시: 비트코인 네트워크 노드와 비트코인 주소 생성

〈학습목표〉

- 이더리움 블록헤더의 구성요소에 대하여 설명할 수 있다.
- 이더리움 계정의 종류와 트랜잭션 구성요소 및 수수료에 대하여 설명할 수 있다.

〈주요 용어〉

- **Wei**

웨이(wei)는 이더리움에서 사용하는 암호화폐인 이더의 가장 작은 단위로 1 이더(ether)는 10^18 웨이(wei)와 같다.

- **머클패트리샤 트리**

이더리움에서 상태데이터와 트랜잭션 정보 등을 효율적으로 관리하기 위한 자료구조이다.

- **루트**

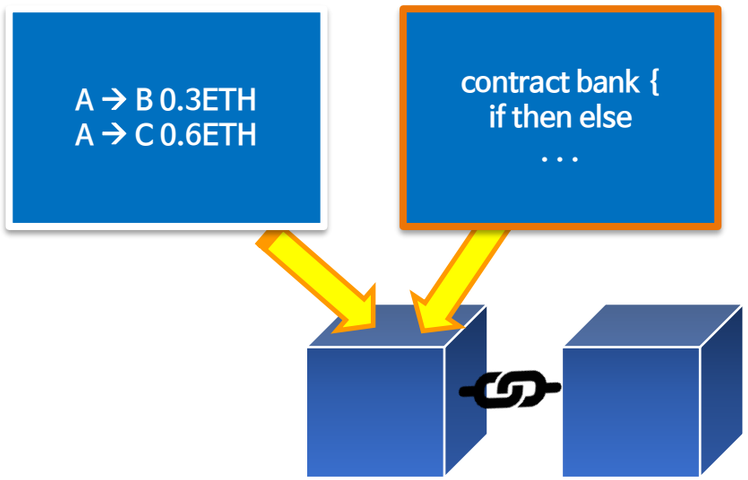
나무와 같은 구조(트리)에서 최상위 노드(root node)이다.

이더리움 블록체인

- “비트코인 매거진” 잡지의 제작에 참여하면서 비트코인을 면밀히 분석 → 2013년 당시 19세의 비탈릭 부테린이 이더리움 개발 제안

- 2015년 7월 30일 퍼블릭 블록체인 플랫폼으로 이더리움 서비스 시작

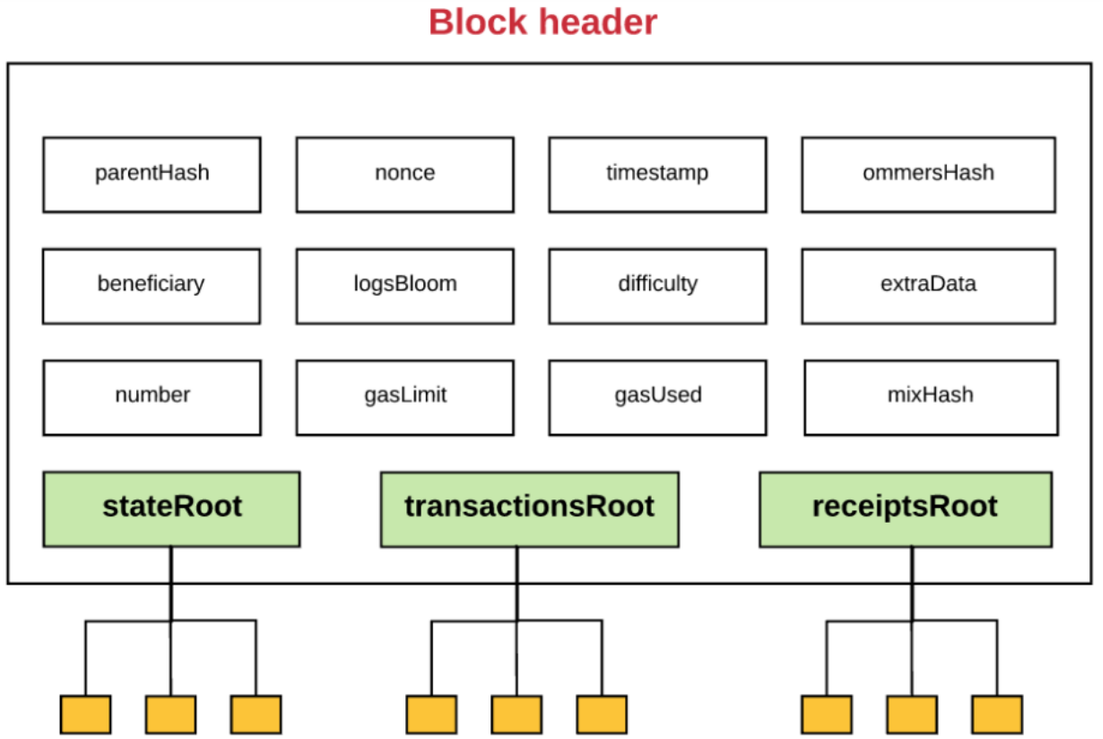
  - 비트코인은 정적인 거래내역 만 기록하나, 이더리움은 정적기록 외에 코드(스마트 계약)도 저장
  - 스마트 계약: 블록체인에 코딩되어 있는 프로그램으로 금융, 부동산, 공증 등 다양한 형태의 계약을 처리



이더리움 블록헤더(1/2)

- 15개 필드, 500바이트 이상
- 계정의 상태정보, 트랜잭션과 거래영수증 데이터는 **외부에 저장**되며, 블록에는 이들 데이터를 찾아갈 수 있는 정보 저장
  - 평균 블록크기는 20~30KB에 불과하지만 상태데이터의 총량은 이미 **1TB 초과**

필드	설명
ParentHash	이전 블록 해시값
OmmersHash	블록체인 분기로 퇴출된 엉클블록 해시값
Beneficiary	블록 채굴 보상금을 수령할 주소
LogsBloom	사건 발생 유무를 알려주는 비트 스트림



* 출처 : https://hersheythings.xyz/entry/ethtereumstructure

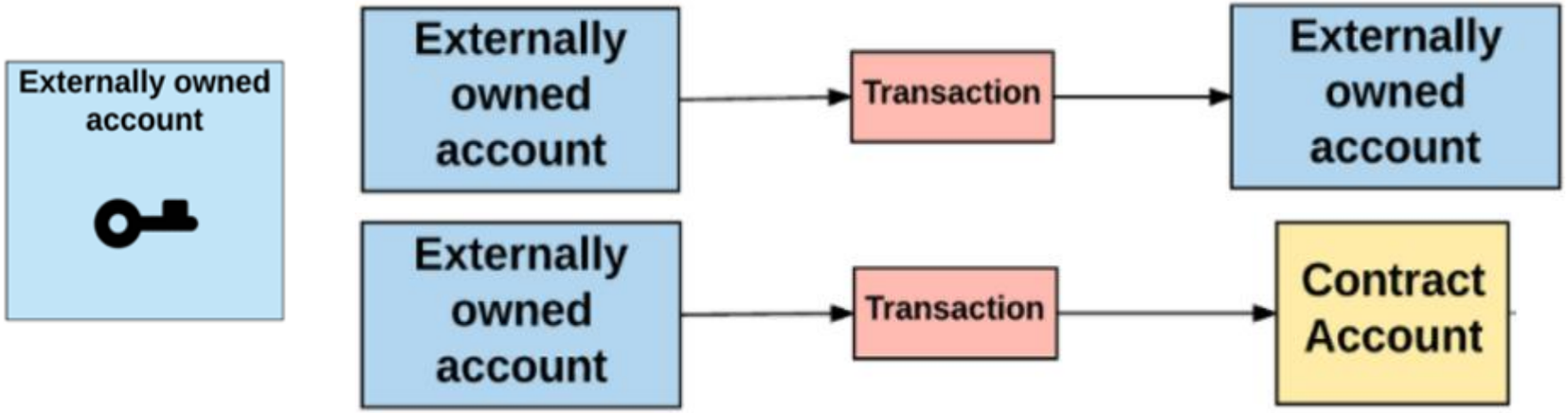
이더리움 블록헤더(2/2)

필드	설명
Difficulty	블록생성 난이도
Number	상위의 조상 블록 개수
GasLimit	블록에 담긴 트랜잭션들의 총 Gas(수수료)
GasUsed	사용된 Gas 총량
Timestamp	블록생성 시각(유닉스 시각)
ExtraData	임의의 데이터, 주로 채굴자의 이름을 적음
MixHash	난스를 찾을 때 사용된 시드 값
Nonce	난이도목표 값 이하를 구할 때 입력 값으로 사용
StateRoot	상태데이터 트리의 루트 노드 해시값
TransactionsRoot	트랜잭션 데이터 트리의 루트 노드 해시값
ReceiptsRoot	트랜잭션 영수증 트리의 루트노드 해시값

이더리움 계정(1/2)

❑ **외부소유계정(EOA, Externally Owned Account): 비트코인 주소와 동일하며, 개인키로 관리됨**

- 두 개의 EOA 사이에서 발생하는 트랜잭션은 **ETH만 송금**
- EOA에서 계약계정(CA)로 보내는 메시지는 CA에 저장된 스마트계약 **코드의 기능을 활성화**시킴

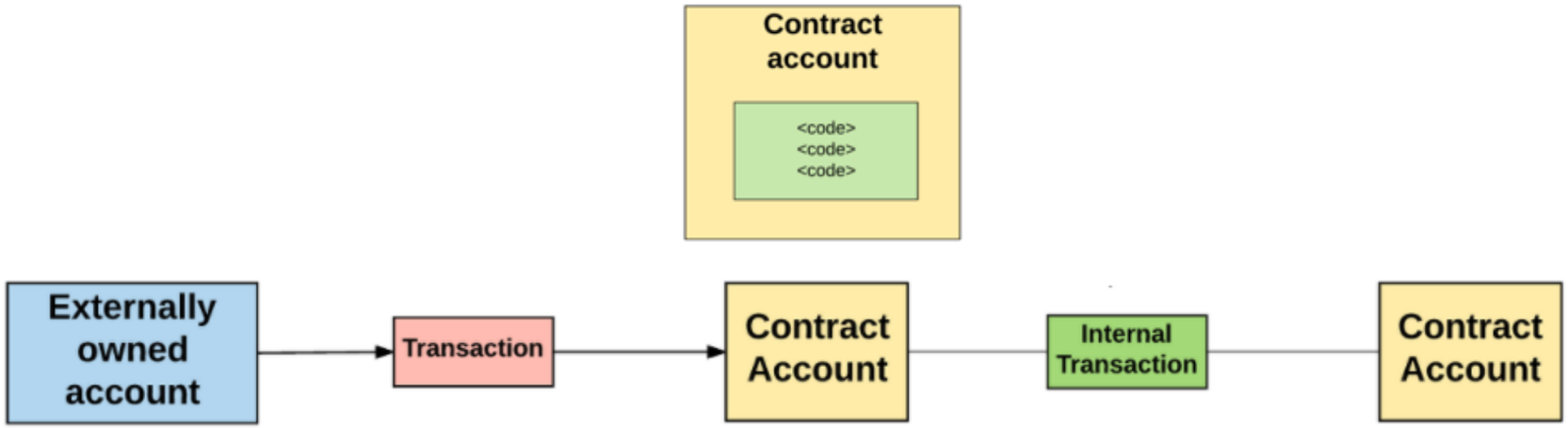


* 출처 : https://hersheythings.xyz/entry/ethtereumstructure

이더리움 계정(2/2)

❑ **계약계정(CA, Contract Account): 스마트 계약 코드를 저장하며, EOA의 호출을 통해 활성화 됨**

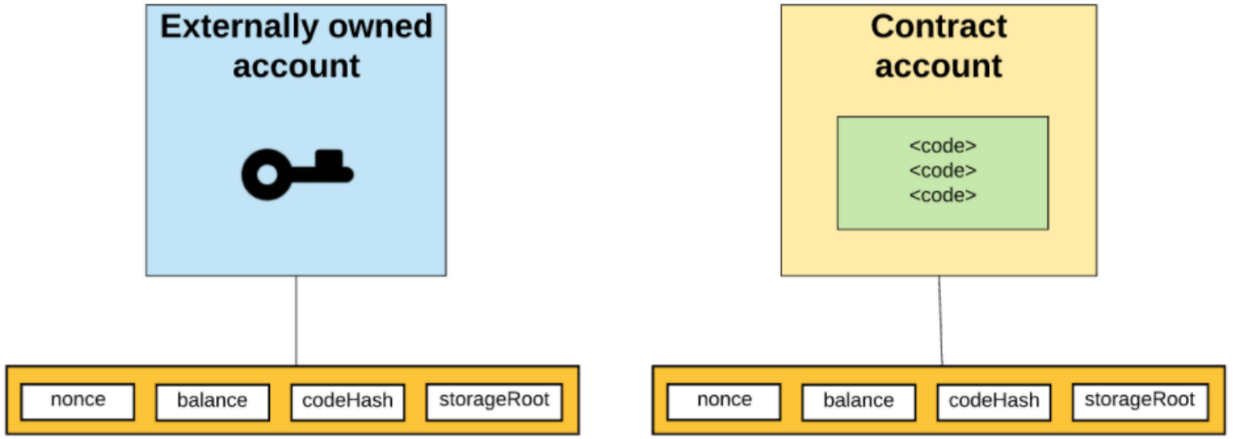
- **스마트계약 코드는 EVM(Ethereum Virtual Machine)을 통해 실행됨**
- **CA는 새로운 트랜잭션을 개시할 수 없으며, EOA 또는 다른 CA로부터 수신한 트랜잭션의 응답으로만 트랜잭션을 실행할 수 있음**



* 출처: https://medium.com/tomak/2-이더리움은-어떻게-동작하는가-b0c90b3eb850

이더리움 계정의 요소

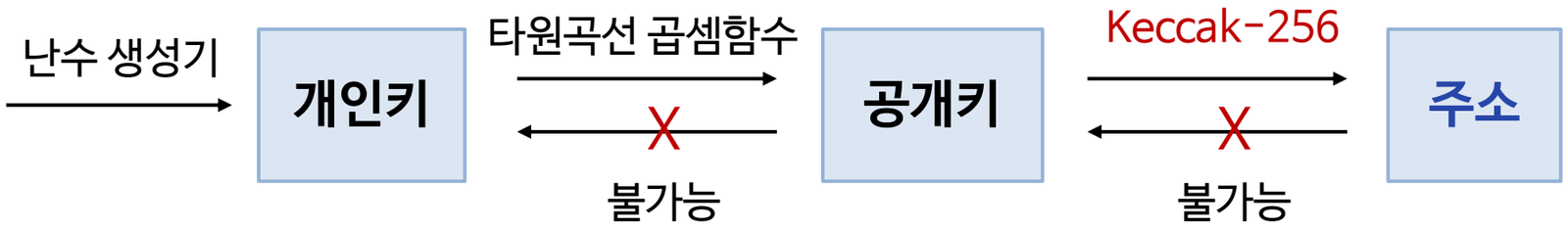
- **Nonce:** 블록헤더와 다르게 계정의 Nonce는 **카운터** 용도
- **Balance:** 계정이 소유하고 있는 Wei의 양(1 ETH= 10^18 Wei)
- **CodeHash:** EVM에서 실행되는 코드의 해시값
  - CA에는 해당 계정에서 실행시킬 코드의 해시값
  - EOA는 코드를 저장할 수 없기 때문에 비어 있는 문자열의 해시값
- **StorageRoot:** 컨트랙트의 모든 데이터가 저장되어 있는 머클패트리샤 트리의 루트



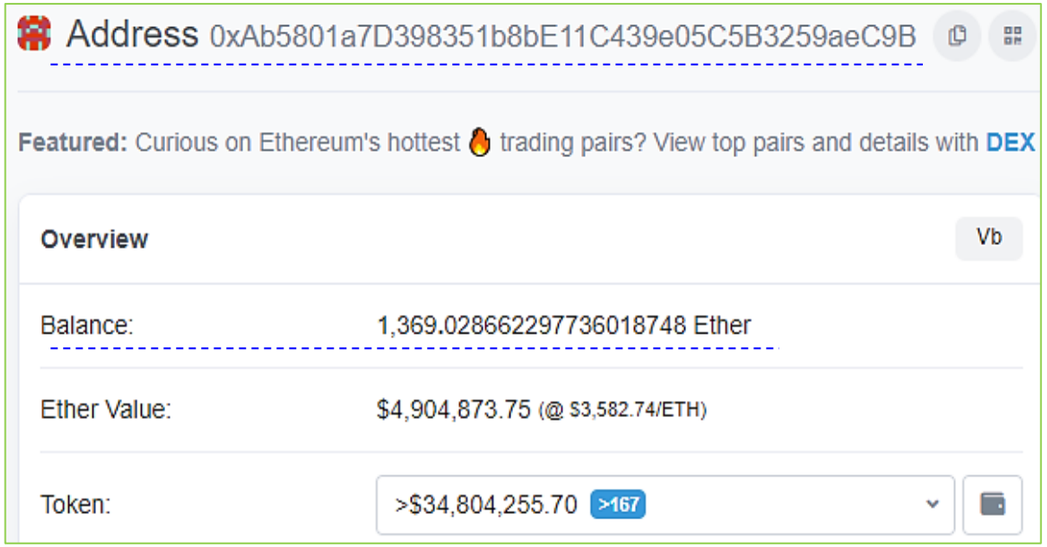
* 출처: https://medium.com/tomak/2-이더리움은-어떻게-동작하는가-b0c90b3eb850

이더리움 EOA 계정의 주소

- **공개키에 Keccak-256 해시연산으로 생성되는 32바이트 중 마지막 20바이트**



- **부테린의 이더리움 지갑 주소(https://etherscan.io/)**



트랜잭션(1/2)

- 트랜잭션은 전자서명된 일종의 지시문으로 EOA에 의해서만 발생
- 컨트랙트들은 메시지 즉, 내부 트랜잭션을 통해서 다른 컨트랙트들과 소통
  - 트랜잭션은 이더리움 실행 환경 내에 존재하는 가상의 객체

* 출처 : https://hersheythings.xyz/entry/ethtereumstructure

트랜잭션(2/2)

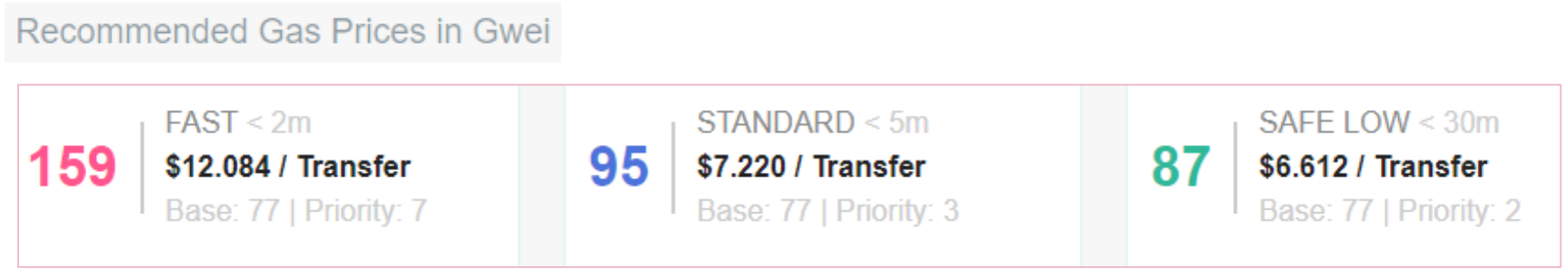
필드	설명
To	트랜잭션 수신자의 주소
Value	송신자에서 수신자로 전송되는 금액
전자서명	송신자가 보내는 트랜잭션의 검증
GasLimit	송신자가 트랜잭션 실행을 위해 지불할 용의가 있는 Gas 비용(수수료)의 최대치
GasPrice	송신자가 Gas당 지불하고자 하는 비용
Init	CA에만 존재, 새로운 CA를 생성하는데 사용되는 EVM 코드 조각
Data	메시지 콜의 입력 인자

트랜잭션 수수료(1/3)

- 트랜잭션 결과로 수행되는 모든 컴퓨팅 연산 작업은 수수료 발생
  - EVM에서 수행되는 스마트계약 코드의 각 연산 비용은 정해져 있음: ADD(3), MUL(5), EQ(3), ADDMOD(8)
  - 수수료 단위는 Gas이며, 트랜잭션 발신자(EOA)는 Gas Limit과 Gas Price 설정
  - Gas 총합은 트랜잭션 수행의 연산 복잡도에 비례하여 증가

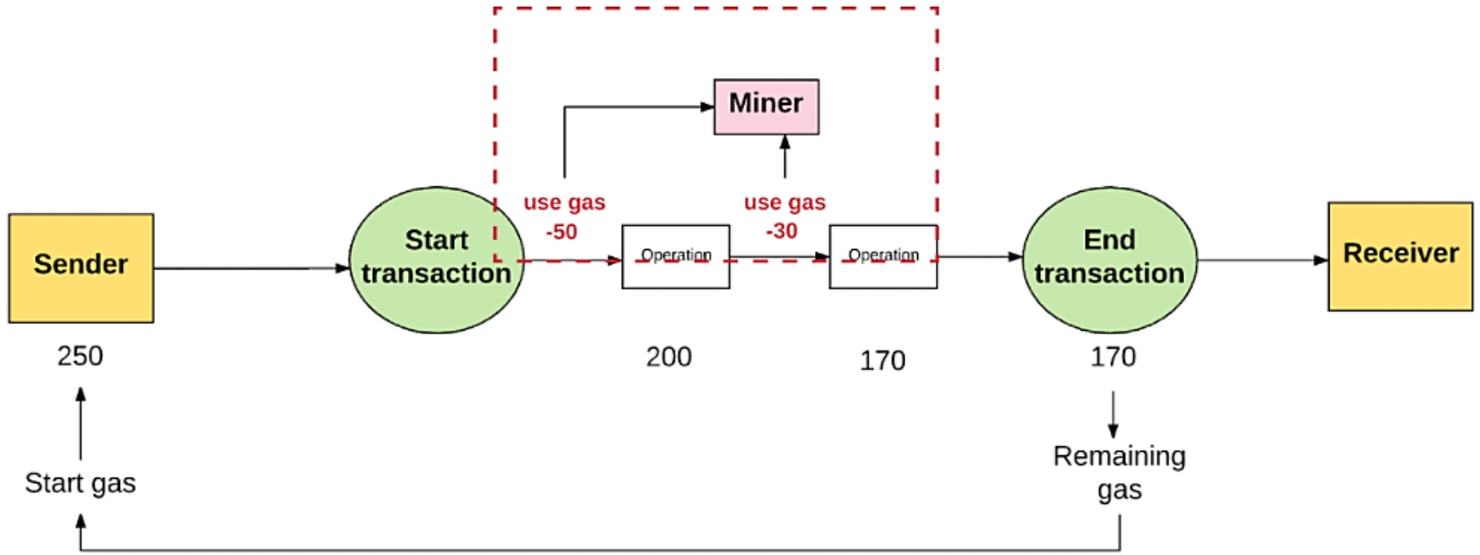
  - 트랜잭션 수수료 = 트랜잭션에 사용된 Gas 수 * Gas 당 비용
  - 사용된 Gas 수가 100,000개 이며, Gas 당 비용이 30GWei인 경우
  - 100,000 * 30GWei = 3,000,000GWei = 0.003ETH

- 추천 Gas 비용(https://ethgasstation.info/, 2021.10.8)



트랜잭션 수수료(2/3)

- 트랜잭션 수수료는 블록 채굴자의 계정 주소로 송금
- 트랜잭션 실행이 끝나고 사용되지 않은 Gas는 송신자에게 반환



- 실제 연산에 소요되는 가스의 양(Gas Used)과 가스 가격(Gas Price)이 높을수록 트랜잭션에서 채굴자가 얻는 이득이 커짐 → 채굴자는 블록에 포함시킬 트랜잭션들을 자유롭게 선택

* 출처 : https://medium.com/tomak/2-이더리움은-어떻게-동작하는가-b0c90b3eb850

트랜잭션 수수료(3/3)

- 발신자가 트랜잭션을 실행하기에 충분한 Gas를 제공하지 못한 경우
  - 10만 Gas가 필요한 작업에 GasLimit로 7만개 제시하여 트랜잭션 수행 중에 모두 소진 → 트랜잭션 처리를 중단하고 상태를 원상복구 → EVM이 일단 연산을 수행했으므로 7만개의 Gas는 환불되지 않음

- 트랜잭션 수수료의 목적
  - 이더리움은 튜링 완전한 머신으로 반복문 허용 → 공격자가 무한 루프를 트랜잭션 내부에 실행함으로써 네트워크를 파괴시킬 수 있음
  - 특정 트랜잭션에 수수료를 부과하는 것은 무분별한 트랜잭션의 남용을 막아 네트워크를 보호(DDoS 방지)

〈1교시〉 학습정리

- 블록헤더는 500바이트 이상의 15개 필드로 구성된다. 계정의 상태정보, 트랜잭션과 거래영수증 데이터는 블록의 외부에 저장되며, 블록에는 이들 데이터를 찾아갈 수 있는 정보가 저장된다.
- 두 개의 외부소유계정(EOA) 사이에서 발생하는 트랜잭션은 단순하게 ETH만 송금할 수 있으며, EOA에서 계약계정(CA)으로 보내는 메시지는 CA에 저장된 코드의 기능을 활성화시킨다.
- 트랜잭션의 결과로서 이행되는 모든 컴퓨팅 연산 작업은 트랜잭션 수수료가 발생하며, 수수료는 블록 채굴자의 계정 주소로 송금된다.
- 트랜잭션에 수수료를 부과하는 것은 무분별한 트랜잭션의 남용을 막아 네트워크를 보호하는 것이다.

〈1교시〉 학습평가

1. 이더리움 블록과 계정에 대한 설명 중 틀린 것을 고르시오.

1) 개인키로 통제되는 외부소유계정(EOA)은 비트코인 주소와 동일하다. 계약계정(CA)은 스마트 계약 코드를 저장할 수 있으며, EOA의 호출을 통해 활성화 된다.

2) 계정의 상태정보, 트랜잭션과 거래영수증 데이터는 블록의 외부에 저장되며, 블록에는 이들 데이터를 찾아갈 수 있는 정보가 저장된다.

3) EOA 이더리움 계정의 요소인 CodeHash에는 EVM에서 실행되는 코드의 해시값이 포함된다.

4) 블록헤더의 OmmersHash는 탈중앙화 합의로 퇴출된 엉클블록 해시값이며, Beneficiary는 블록 보상금을 수령할 주소를 나타낸다.

답) 3

해설) CA 이더리움 계정의 요소인 CodeHash에는 EVM에서 실행되는 코드의 해시값이 포함된다.

2. 트랜잭션 수수료가 필요한 이유를 설명하시오.

해설) - 이더리움은 튜링 완전한 머신으로 반복문을 허용하므로 공격자가 무한 루프를 트랜잭션 내부에 실행하여 네트워크를 파괴시킬 수 있다. 특정 트랜잭션에 수수료를 부과하는 것은 무분별한 트랜잭션의 남용을 막아 네트워크를 보호(DDoS 방지)하는 것이다.

2교시: 이더리움의 머클패트리샤 트리와 스마트계약

〈학습목표〉

- 머클패트리샤 트리의 원리와 이더리움에서의 사용 예를 설명할 수 있다.
- 이더리움의 해시퍼즐과 난이도 조절에 대하여 설명할 수 있다.
- 스마트계약의 코딩과 배포 및 디앱의 현황에 대하여 설명할 수 있다.

〈주요 용어〉

- **튜링 완전**

튜링은 수학자 앨런 튜링(Alan Turing)이 1936년에 제시한 개념으로 계산하는 기계의 일반적인 개념을 설명하기 위한 가상의 기계를 뜻한다. 튜링 완전은 계산적인 문제를 그 프로그래밍 언어나 추상 머신으로 풀 수 있다는 것이다.

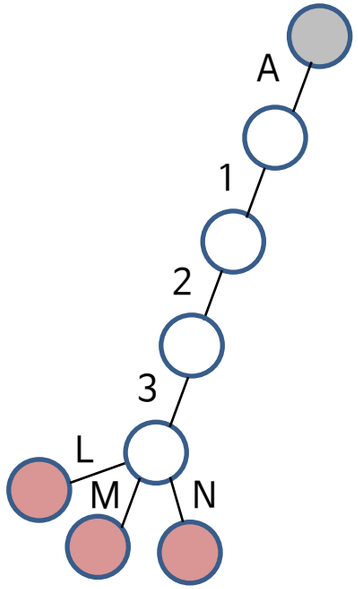
- **ASIC(Application Specific Integrated Circuit)**

사용자가 특정 용도의 반도체를 주문하면 반도체 업체가 이에 맞춰 설계 · 제작해 주는 기술이다.

머클패트리샤 트리

Radix 트리

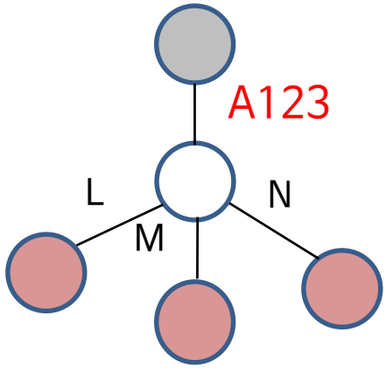
- 잎(leaf) 노드에서 전체 키워드가 완성되는 트리
- 3개 키워드(15글자) → 8개 노드 이용



- A123L
- A123M
- A123N

머클패트리샤 트리

- 공통된 접두사를 최대한 따로 분리
- 3개 키워드(15글자) → 5개 노드 이용

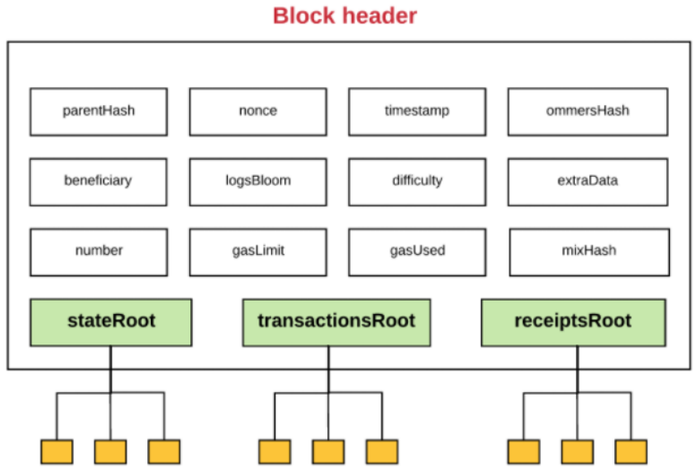


- 이더리움은 Radix 트리를 변형한 머클패트리샤 트리 구조를 사용하여 각 블록에서 블록의 외부에 저장되어 있는 데이터를 찾아감

이더리움의 머클패트리샤 트리

❑ 이더리움에서 사용되는 머클패트리샤 트리

- State 트리: 제네시스 블록부터 현재 블록까지 생성된 모든 계정의 상태데이터 저장
- Transactions 트리: 현재 블록의 트랜잭션 정보 저장
- Receipts 트리: 현재 블록의 거래 영수증 정보 저장

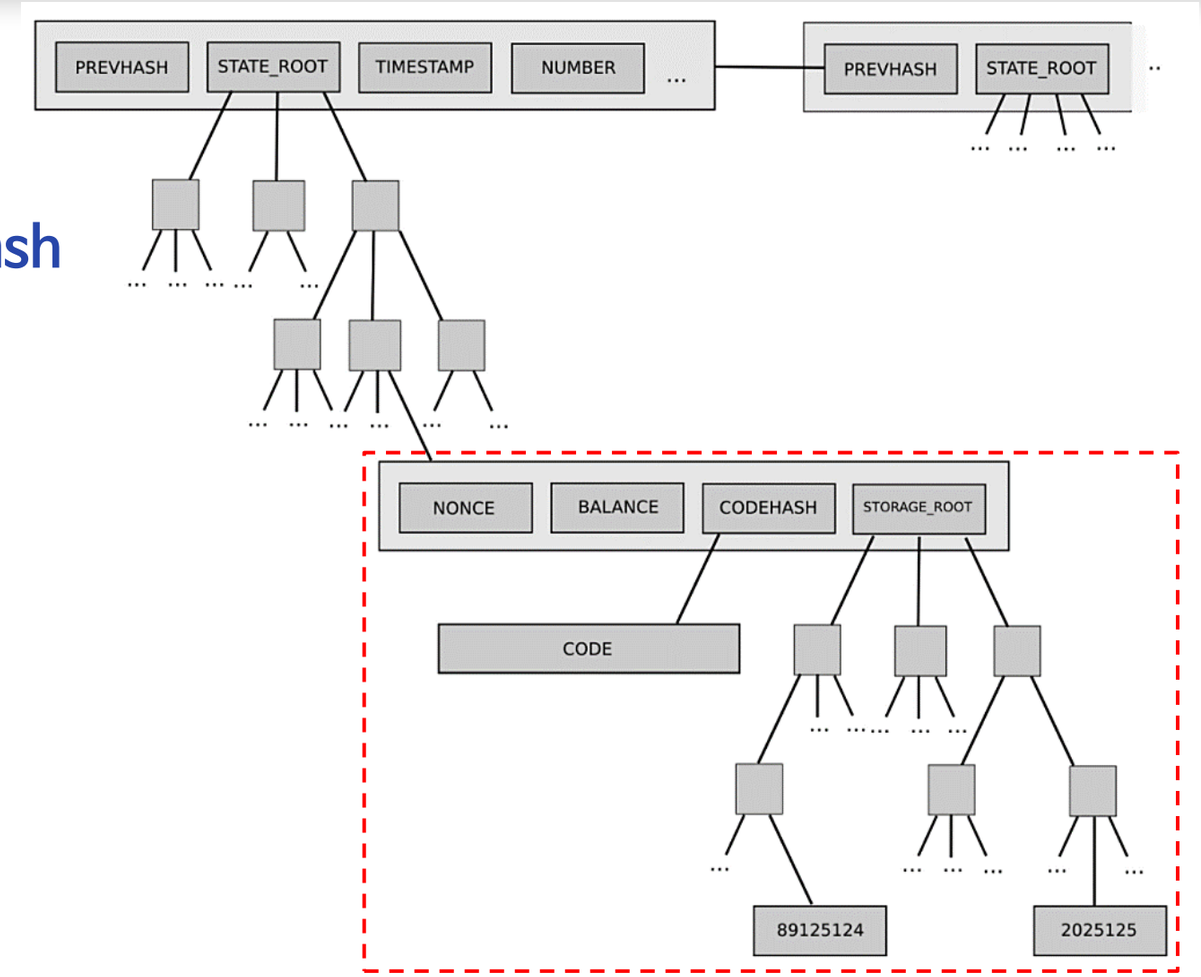


❑ 블록 헤더는 머클패트리샤 트리의 루트 노드 해시값을 가지고 있음

* 출처 : https://hersheythings.xyz/entry/ethtereumstructure

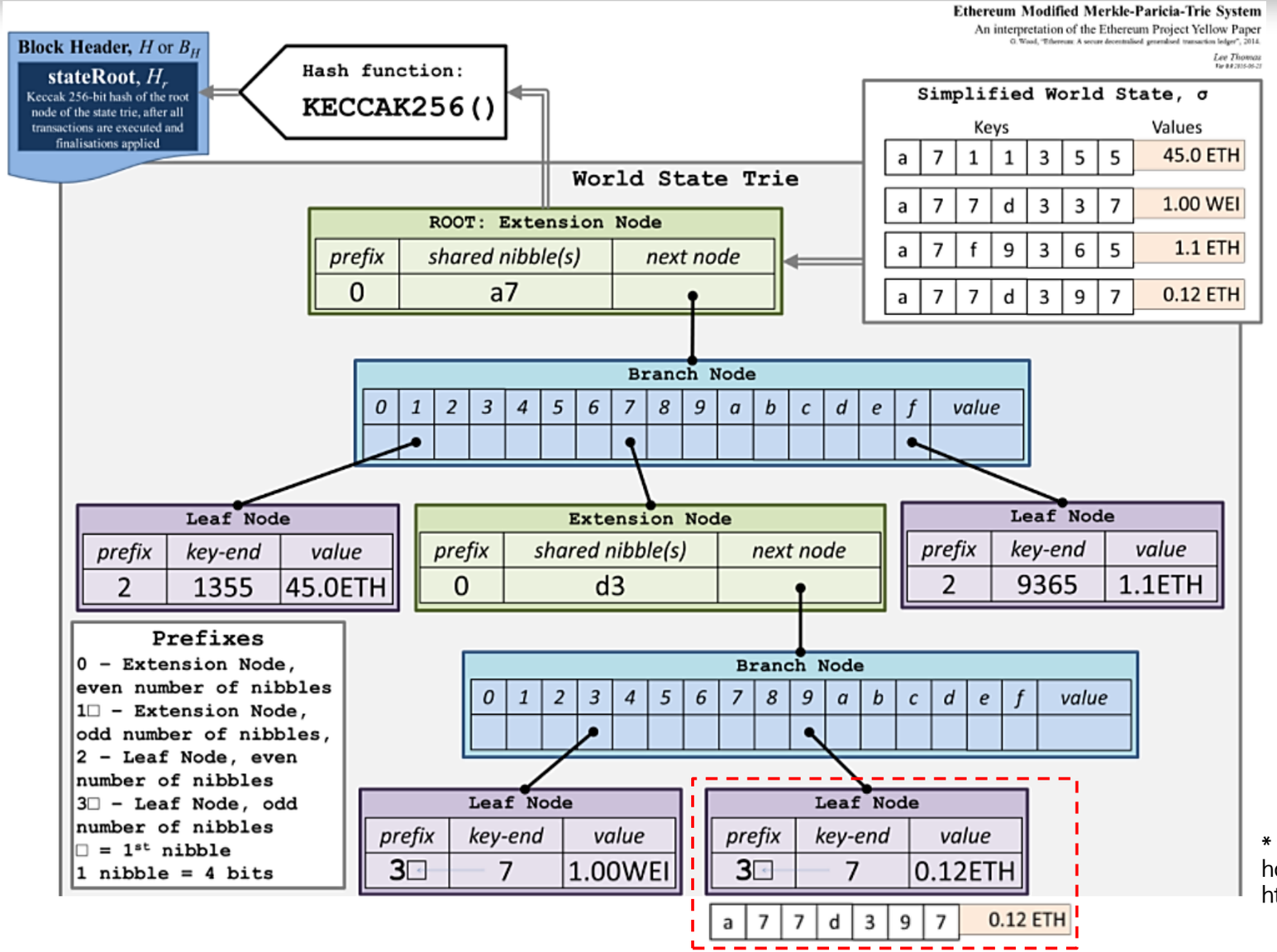
State 머클패트리샤 트리

- 계정 주소를 이용해 상태데이터의 트리 구조를 따라가면 상태데이터에 접근
  - 상태데이터: nonce, balance, codeHash storageRoot
  - UTXO 기반의 비트코인과 달리 이더리움에서는 계정의 상태데이터를 조회하면 잔액과 트랜잭션의 기록을 확인할 수 있음



* 출처 : https://medium.com/tomak/2-이더리움은-어떻게-동작하는가-b0c90b3eb850

State 머클패트리샤 트리 예



* 출처: https://ethereum.stackexchange.com/questions/6415/eli5-how-does-a-merkle-patricia-trie-tree-work
https://i.stack.imgur.com/YZGxe.png

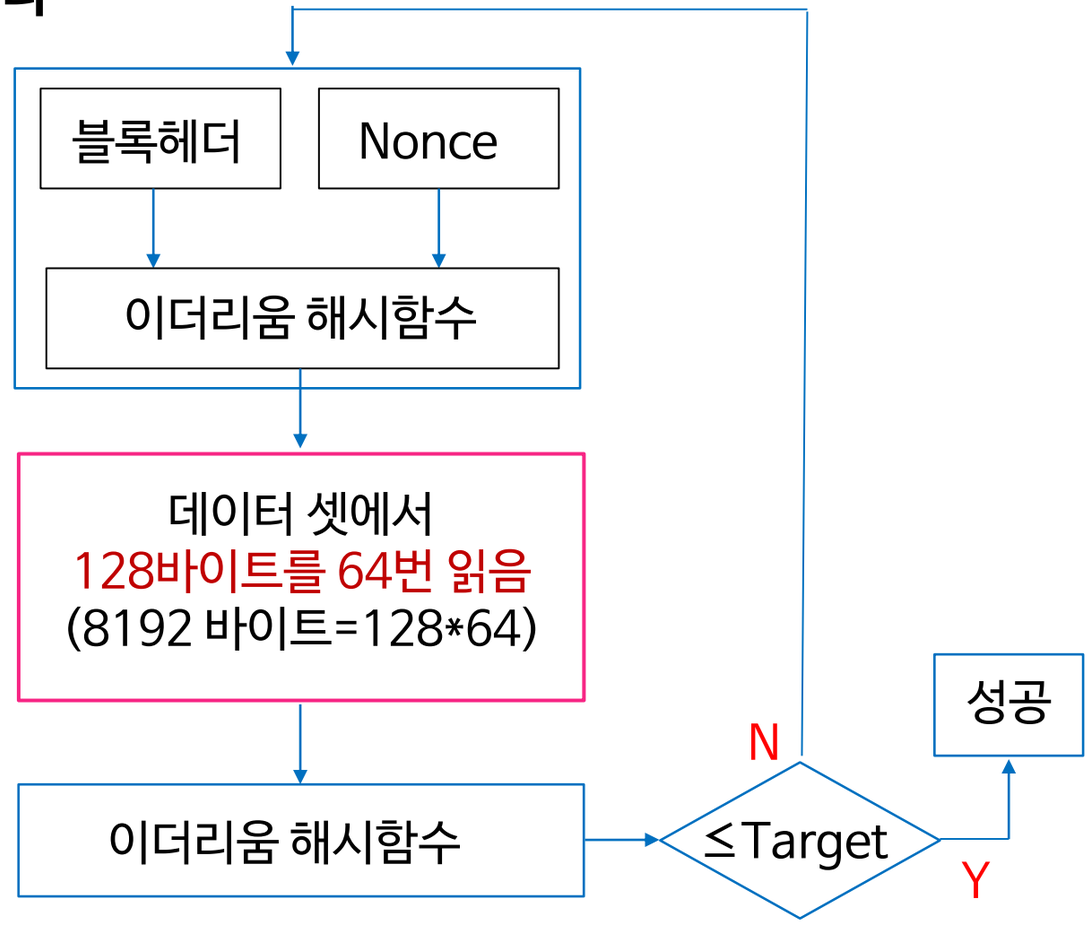
Transactions, Receipts 머클패트리샤 트리

- Transactions 머클패트리샤 트리 (TransactionsRoot) : 트랜잭션을 저장하며 각 블록마다 하나씩 존재
  - 블록에서 각 트랜잭션의 순서를 나타내는 숫자인 TransactionIndex를 경로로 사용
  - 한번 저장되면 변경되지 않음

- Receipts 머클패트리샤 트리 (ReceiptsRoot) : 각 트랜잭션의 실행결과를 요약한 자료로 각 블록마다 하나씩 존재
  - TransactionIndex를 경로로 사용하며, 한번 저장되면 변경되지 않음
  - 영수증에 담겨 있는 정보
    - 트랜잭션의 성공적 실행 유무를 알려 주는 상태 값
    - 트랜잭션 해시값, 트랜잭션 송·수신자의 계정주소
    - 사용된 Gas양, 트랜잭션이 실행되면서 생성된 로그 데이터
    - 트랜잭션이 들어있는 블록의 해시값과 블록번호

해시퍼즐

- 연산 의존도를 방해하기 위하여 해시값을 계산할 때 마다 **데이터 셋에서 128바이트를 64회 읽음**
  - 채굴의 가장 큰 걸림돌은 해시계산이 아니라 메모리에서 데이터를 읽어 오는 것
  - **ASIC화를 어렵게 함**



난이도 조절(1/2)

- 이더리움은 **매 블록마다 난이도 조정**(15초 주기)

  블록 난이도 = 부모 블록의 난이도 + 동적 난이도 조정 값 + 난이도 폭탄 값

- **동적 난이도 조정 값**

  d = 현재 블록의 생성시간 - 부모 블록의 생성 시간

  - If d < 10 → 부모 블록의 난이도 보다 약 **0.05% 상향**
  - If 10 ≤ d < 20 → 동적 난이도 변하지 않음
  - If d ≥20 → d 값에 비례하여 부모 블록의 난이도 보다 약 **0.05에서 4.8% 하향**

난이도 조절(2/2)

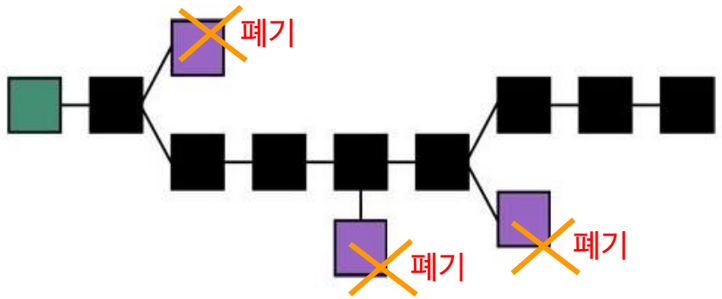
- 10만 개 블록(17 ~ 18일 소요)마다 난이도 폭탄 값이 2배씩 기하 급수적으로 증가

  블록 난이도 = 부모 블록의 난이도 + 동적 난이도 조정 값 + 난이도 폭탄 값

- 2017년 10월 16일 하드포크를 통해 437만번 블록에서 보상금을 5이더에서 3이더로 그리고 난이도를 절반으로 낮춤
- 난이도 폭탄으로 지분증명의 전환 계획이 뜻대로 되지 않자 하드포크를 통해 폭발 시간을 늦추었음

엉클 블럭

- 비트코인 보다 40배 빨리 블록을 생성하는 이더리움(15초 주기)에서는 블록체인의 충돌 즉, 분기가 더 자주 발생 → 엉클블럭은 분기되어 폐기된 블록

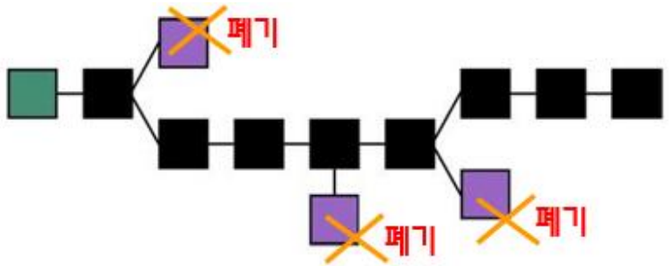


- **비트코인: 분기 시에 연산량이 아니라 길이가 긴 체인 선택**
- **이더리움: 분기 시에 가장 많은 연산이 수행된 경로를 선택**
  - Chain_Path(연산량, 길이): A_Path(100,140) vs B_Path(80,150)
    - **비트코인에서는 B_Path 채택**
    - **이더리움에서는 A_Path 채택**

* 출처 : https://hersheythings.xyz/entry/ethtereumstructure

블록채굴의 보상

- 블록의 채굴에 대한 2 ETH의 고정 보상
- 블록에 포함된 트랜잭션들이 소모한 Gas 비용
- 블록의 부분으로 엉클블록을 포함한 것에 대한 추가적인 보상
  - 폐기된 블록의 채굴자에게도 이더리움 보상금의 최대 7/8에서 최소 1/4 지급
  - 비트코인에서 폐기된 블록의 채굴자는 보상금을 무효화



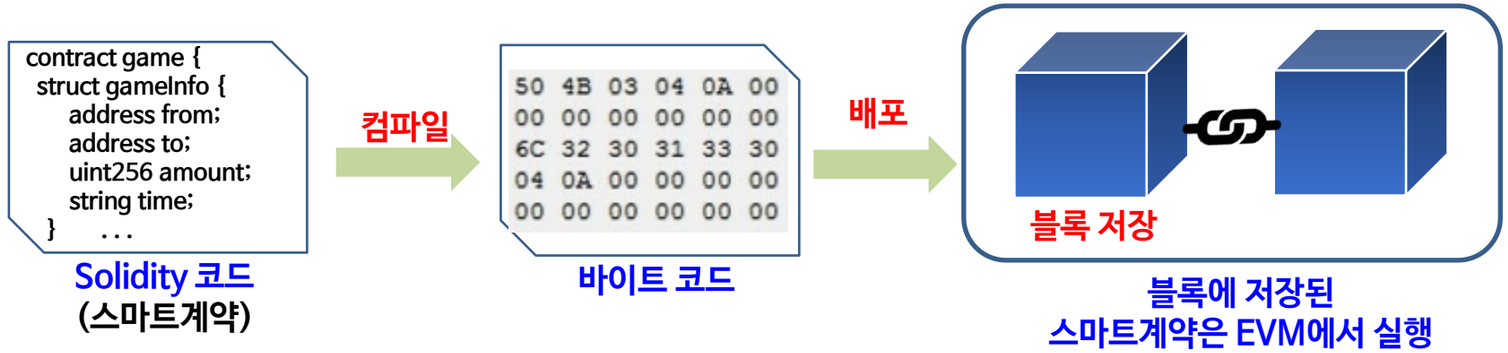
* 출처 : https://hersheythings.xyz/entry/ethtereumstructure

이더리움과 비트코인 비교 | https://btc.com/ (2021.10.6)

	이더리움	비트코인
최초 작동일	2015.7.30	2009.1.3
해시함수	SHA-3 계열의 Keccak-256	SHA-256
작동 방식	작업증명(2.0은 지분증명)	작업증명
기본 보상(2020년)	2 ETH	6.25 BTC
블록해시 계산	메모리-하드 방식(ASIC화 어려움)	계산 집중형방식(ASIC화 쉬움)
거래기록	계정 단위	UTXO 단위
평균 채굴시간	15초	10분
난이도 조절주기	매번(약 15초)	2016 블록(약 2주)
해시파워	696.8 TH/s	150.5 EH/s
블록 수	13,365,562	703,831
평균 수수료	9,673원	3,241원
24시간 활성 주소	508,496	1,019,882

스마트 계약

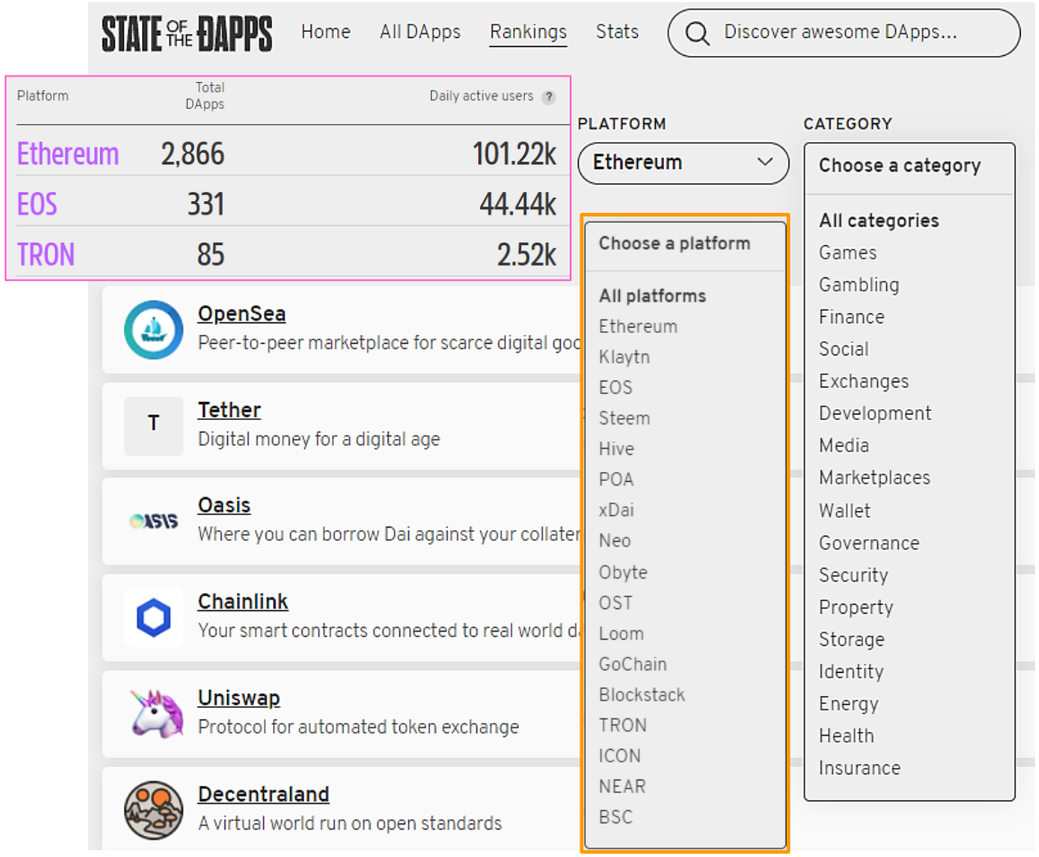
- 스마트 계약은 디앱(DApp: Decentralized Application) 명칭으로 많이 사용
- 이더리움은 정적기록 외에 스마트계약 코드도 저장: C와 파이썬 구문이 혼합 된 Solidity는 스마트계약의 프로그래밍 언어로 널리 사용



- 게임 결과에 따라 코인을 나누어 주는 스마트계약
  - 게임 참가자는 EOA 계정을 사용해 해당 게임이 있는 스마트계약 호출 → 게임에 배팅할 코인을 메시지를 통해 스마트계약에 전달
  - 게임 스마트계약은 게임 결과에 따라 참가자에게 자동으로 코인 송금

디앱 사이트

- **디앱 사이트**(https://www.stateofthedapps.com)
- **전 세계 DApp의 약 80%가 이더리움 플랫폼 기반**



출처 : https://www.stateofthedapps.com/, 2021.10.8

이더리움 생태계(1/2)

- **이더리움**은 스마트 컨트랙트를 제공하는 **네트워크이자 컴퓨터**
  - 유니스왑, 신세틱스, 체인링크와 같은 **탈중앙화금융(DeFi)**의 대부분과
  - 블록체인 메타버스인 **디센트랄랜드**와 NFT 거래소인 **OpenSea**도 이더리움 기반

- 실체를 가지고 부가가치를 만들고 있는 **이더리움 생태계**
  ① 디센트랄랜드가 제공하는 프로그램으로 개발자가 **게임 서비스** 제공
  ② 제공한 서비스 댓가로 디센트랄랜드의 암호화폐 **MANA**를 받음
  ③ MANA를 받은 개발자는 달러나 다른 암호화폐로 교환하고 싶음 → **유니스왑**에 가서 MANA를 ETH로 교환

유저들은 직접 아바타를 설정하고 세계를 탐험할 수 있다./출처=디센트럴랜드 홈페이지

* 출처: https://www.blockmedia.co.kr/archives/176953

이더리움 생태계(2/2)

❑ **신세틱스: 블록체인에서 외환, 원자재, 암호화폐 등 모든 자산을 거래할 수 있음**

- **거래 수수료도 싸고 증권사 없이도 거래가 가능하며, 증거금을 내지 않고 파생상품을 구매할 수 있음**

❑ **체인링크: 오프라인의 질 좋은 데이터를 블록체인에 공급하여 생성된 가공 정보를 오프라인과 다시 연결**

- **수시로 변화는 정확한 가격 정보를 매칭시켜 싸고 편리한 상품을 적은 자본으로 투자하게 함**

* 출처: 2021.10.11, https://www.coindalin.com/

〈2교시〉 학습정리

- UTXO 기반의 비트코인과 달리 이더리움에서는 계정의 상태데이터를 조회하면 잔액과 트랜잭션의 기록을 확인할 수 있다.
- 이더리움에서 사용되는 머클패트리샤 트리에느 State 트리, Transaction 트리 그리고 Receipts 트리가 있다.
- 연산 의존도를 방해하기 위하여 해시값을 계산할 때 마다 데이터 셋에서 128바이트를 64회 읽는다. 채굴의 가장 큰 걸림돌은 해시계산이 아니리 메모리에서 데이터를 읽어 오는 것이다.
- 이더리움은 블록의 충돌(분기) 시에 가장 많은 연산이 수행된 경로를 유효 경로로 선택하며, 비트코인의 경우에는 연산량이 아니라 길이가 긴 체인을 선택한다.

〈2교시〉 학습평가

1. 이더리움의 동작방식에 대한 설명 중 틀린 것을 고르시오.

1) 이더리움은 Radix 트리를 변형한 머클패트리샤 트리 구조를 사용하여 블록의 외부에 저장되어 있는 해당 데이터를 찾아간다.

2) 계정 주소를 이용해 상태데이터의 트리 구조를 따라가면 잔액과 트랜잭션의 기록을 확인할 수 있는 상태데이터에 접근할 수 있다.

3) 이더리움의 State 트리, Transaction 트리, Receipts 트리는 머클패트리샤 트리의 형태로 저장된다.

4) 10만 개 블록마다 조정되는 블록 난이도는 부모 블록의 난이도, 동적 난이도 조정 값 그리고 난이도 폭탄 값의 합이다.

답) 4

해설) 매 블록마다 조정되는 블록 난이도는 부모 블록의 난이도, 동적 난이도 조정 값 그리고 난이도 폭탄 값의 합이다.

2. 이더리움의 엉클블록에 대하여 설명하시오.

해설) - 비트코인(10분) 보다 40배 빨리 블록을 생성하는 이더리움(15초)에서는 블록체인의 충돌 즉, 분기가 더 자주 발생한다. 엉클블럭은 체인이 분기되어 폐기된 블록이다.

- 이더리움에서는 블록의 부분으로 엉클블록을 포함한 것에 대하여 보상금의 최대 7/8에서 최소 1/4까지 보상금을 지급한다. 반면에 비트코인에서는 폐기된 블록의 채굴자는 보상금을 반환한다.

3교시: 이더리움 생태계

〈학습목표〉

- 이더리움의 생태계와 DAO 해킹에 대하여 설명할 수 있다.
- Geth(Go Ethereum) 동작과 스마트계약의 개발환경에 대하여 설명할 수 있다.

DAO

❑ 탈중앙화 자율조직 DAO (Decentralized Autonomous Organization)

- CEO 없이 회사를 운영할 수 있는 블록체인 기반의 서비스
- 의사결정에 참여하는 지분 보유자와 계약인 존재 → 블록체인 기반으로 의견을 모아 회사 경영방향을 함께 결정

<자료> Whale Reports(https://whalereports.com/daostack-an-operating-system-for-daos/)

DAO 해킹

- 이더리움 팀은 '16년 6월에 The DAO 프로젝트 출범
  - 1개월 만에 1억 5천만 달러의 ETH 모집 → 두 달 만에 5천만 달러 해킹
  - 나누기(Split) 시에 없어져야 할 DAO 토큰이 살아있어 ETH를 해커 지갑으로 무한 인출
  - Split 후 48일 지나야 ETH를 출금할 수 있는 DAO 규정에 의해 이더리움 개발팀은 잘못된 거래를 무효화 → 투자금을 돌려주기 위해 오류 이전 상태로 복구하는 하드포크 수행

- 불가역성을 선호하는 하드포크의 반대파 10%는 이더리움 클래식을 상장하여 기존 블록체인 고수('16.7.24)
  - 이더리움 클래식은 이더리움과 동일 기술 → 스마트계약과 DApp 적용 가능

* 출처: https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=mage7th&logNo=221438886379

〈3교시〉 학습정리

- 이더리움은 스마트계약을 제공하는 네트워크이자 컴퓨터이다. 탈중앙화금융(DeFi)의 대부분이 이더리움을 이용한다.
- 탈중앙화 자율조직 DAO는 의사결정에 참여하는 지분 보유자와 계약인이 존재하며, 블록체인 기반으로 의견을 모아 경영방향을 함께 결정하는 블록체인 기반의 서비스이다.
- 이더리움 재단이 제공하는 공식 클라이언트인 게스(Geth, Go Etherium)는 Go언어로 개발된 S/W이다.
- Truffle Famework는 솔리디티 코드(스마트게약)를 로컬 환경에서 보다 쉽게 컴파일하고 배포할 수 있는 프레임워크이다.

〈3교시〉 학습평가

1. 이더리움의 생태계에 대하여 사례를 들어 설명하시오.

해설)

① 디센트랄랜드가 제공하는 프로그램으로 개발자가 게임 서비스를 제공한다.

② 개발자는 제공한 게임의 서비스 댓가로 디센트랄랜드의 암호화폐 MANA를 받는다.

③ MANA를 받은 개발자는 달러나 다른 암호화폐로 교환하기 위하여 유니스왑에 가서 MANA를 ETH로 교환한다.

2. DAO와 DAO 해킹에에 대하여 설명하시오,

해설) - DAO(Decentralized Autonomous Organization)는 의사결정에 참여하는 지분 보유자와 계약인이 존재하며, 블록체인 기반으로 의견을 모아 경영방향을 함께 결정하는 블록체인 기반의 서비스이다.

- The DAO 프로젝트 출범 후 두 달만에 모집한 ETH 중 5천만 달러가 해킹되었다. DAO의 취약점인 나누기(Split) 시에 없어져야 할 DAO 토큰이 살아있어 ETH를 해커 지갑으로 무한 인출한 해킹 공격이다.