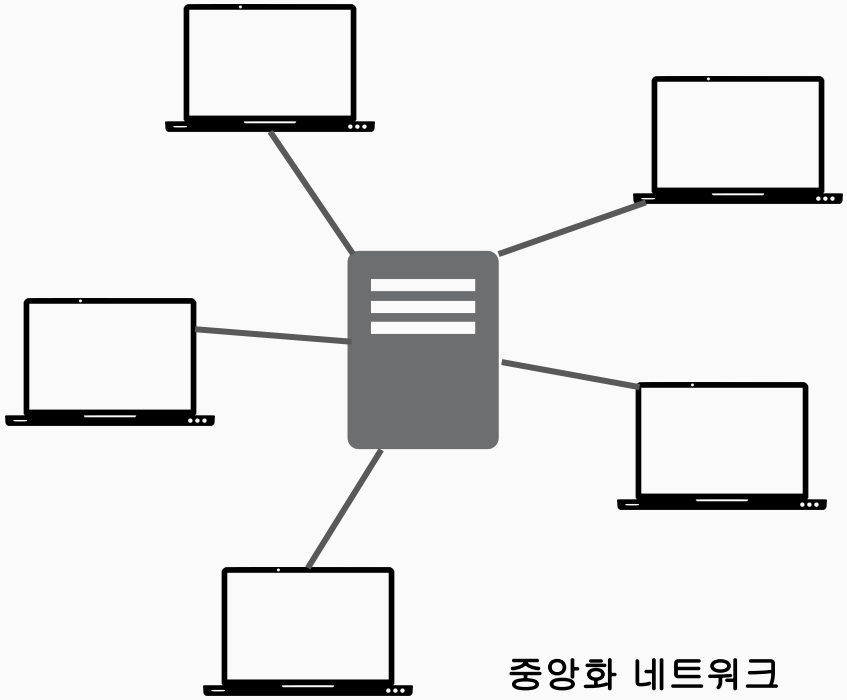
블록체인의 이해

헥슬란트 이진호

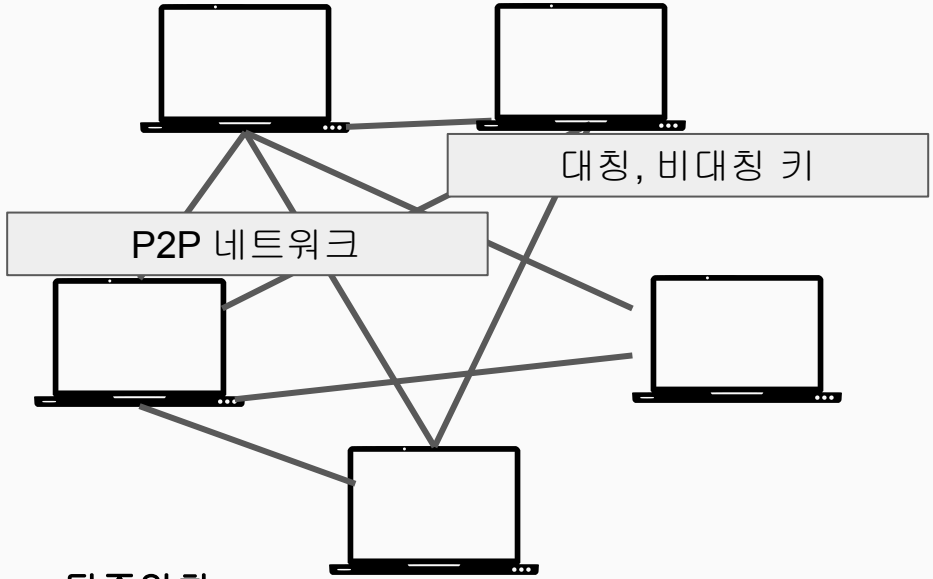
비트코인과 블록체인

비트코인과 블록체인

분산되고, **독립적**이며, **개방**된 공개 장부 기술



중앙화 네트워크



탈중앙화
네트워크

비트코인과 블록체인

- **엔지니어의 입장에서 블록체인을 어떻게 정의할 것인가.**
  - 블록체인을 정의하는데 쓰이는 많은 키워드들
    블록과 블록은 연결, 원장, 비가역적인 트랜잭션, 암호화

  - 하나의 문장으로 블록체인을 설명할 수 있는가?

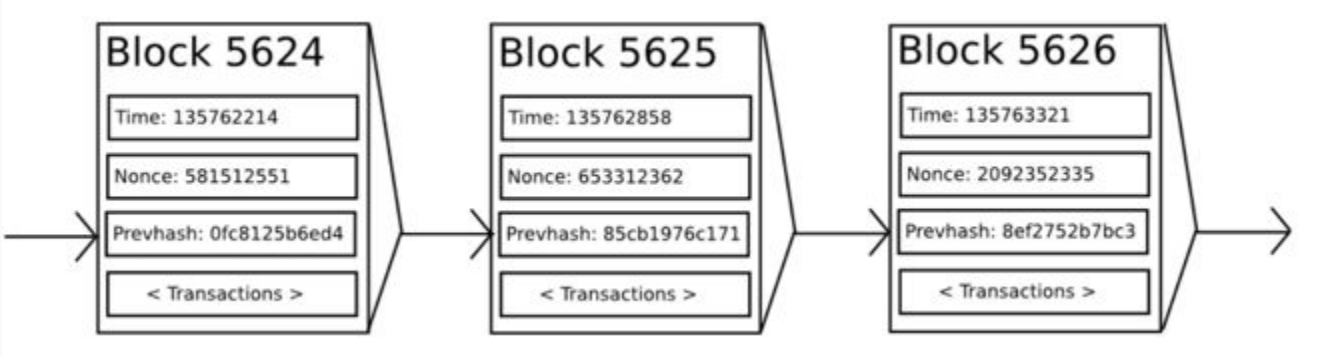
블록체인

위/변조가 불가능한 데이터를 공유해서 활용하는 기술

- 이승한 <실전!하이퍼레저 패브릭> 저자

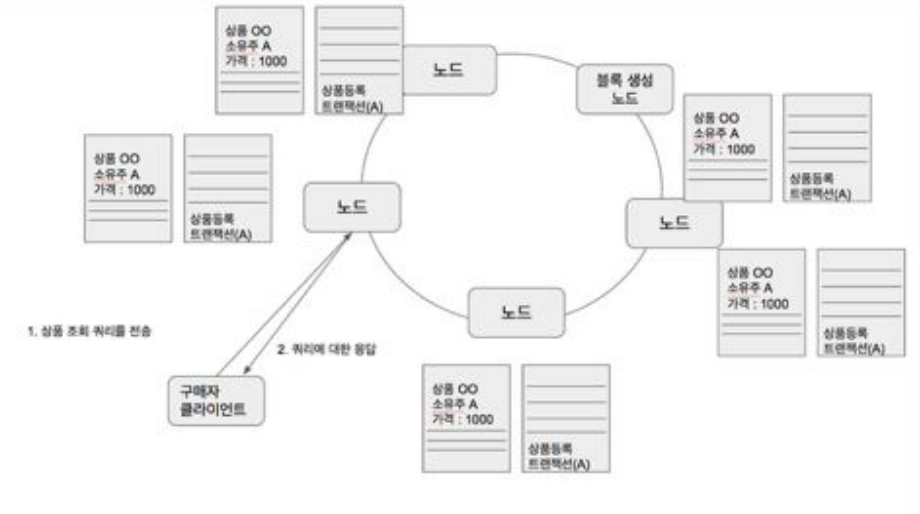
블록체인의 특성

- **위/변조가 불가능한**
  - 블록과 블록간의 연결
  - 하나의 블록을 수정하면, 그 이후의 블록도 모두 수정해야함



블록체인의 특성

- **공유해서 활용하는**
  - 모든 노드들이 동일한 상태의 원장(Ledger)을 가지고 있음
  - 누군가 새로운 상태를 생성하면, 모두가 공유해야함



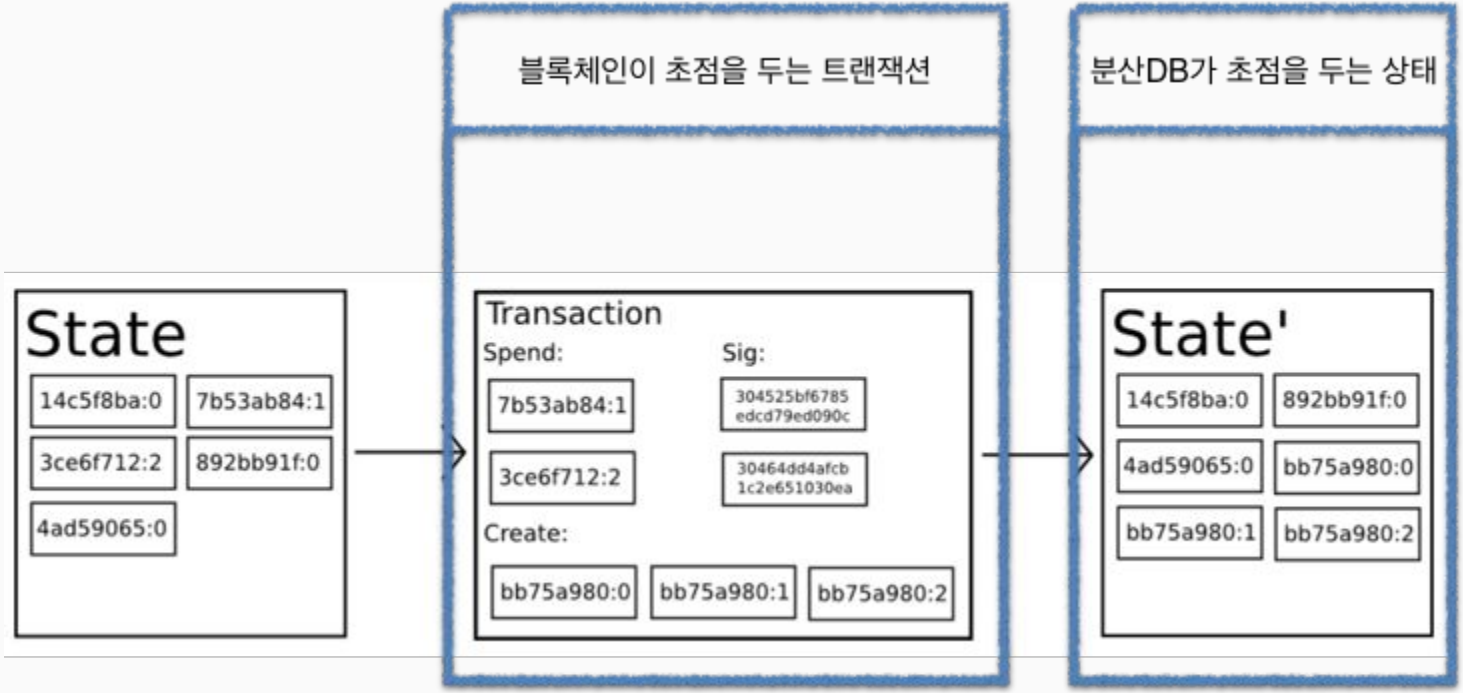
블록체인의 특성

- **분산 데이터 베이스와 블록체인**
  - 두 기술 모두 여러 노드에 데이터를 보관하는 기술
  - 둘다 데이터 저장 및 관리 인프라의 역할을 수행
  - 블록체인에서는 샤드의 개념등을 통해 분산 저장을 지원
  - 분산DB에서는 레플리카, 미러링 등으로 이중화 지원

- **가장 큰 차이점은 분산형 원장**
  - 블록체인은 트랜잭션 기록을 생성해 분산 원장에 보존하는데 특화
  - 분산형 데이터베이스는 빠른 접근성과 데이터 상태 관리에 특화

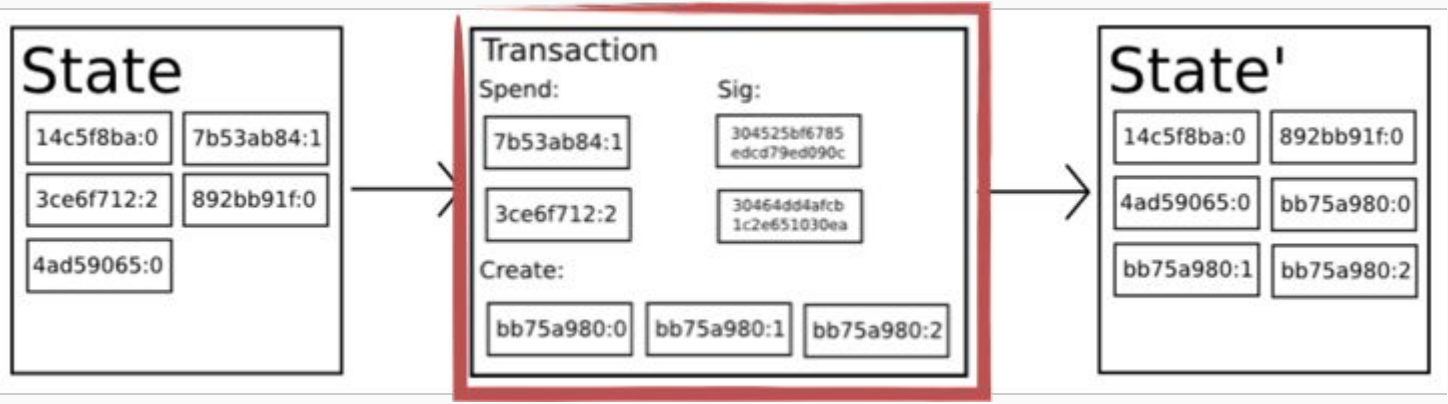
  - 무엇보다 분산형 DB는 원장의 기록을 관리자가 마음대로 수정할 수 있는 반면, 블록체인은 기록된 트랜잭션 을 수정할 수 없다

트랜잭션과 블록


블록체인이 초점을 두는 트랜잭션
분산DB가 초점을 두는 상태
State
14c5f8ba:0
7b53ab84:1
3ce6f712:2
892bb91f:0
4ad59065:0
Transaction
Spend:
Sig:
7b53ab84:1
304525bf6785
edcd79ed090c
3ce6f712:2
30464dd4afcb
1c2e651030ea
Create:
bb75a980:0
bb75a980:1
bb75a980:2
State'
14c5f8ba:0
892bb91f:0
4ad59065:0
bb75a980:0
bb75a980:1
bb75a980:2

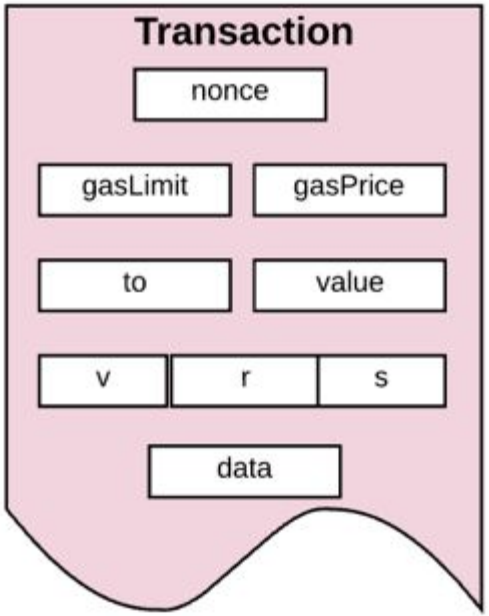
트랜잭션과 블록

- **트랜잭션**
  - 데이터의 상태를 변화시키기 위해 수행하는 논리적 작업의 단위
  - 구성 요소
    - 트랜잭션 생성자의 계정
    - 트랜잭션의 바꾸려는 상태의 위치
    - 서명정보



트랜잭션과 블록

- **이더리움의 트랜잭션 구조**
  a. nonce : transaction Sender의 전체 카운트
  b. gasLimit : 최대 지불용의가 있는 가스의 갯수
  c. gasPrice : 1가스당 가격
  d. to: 트랜잭션을 받을 주소
  e. value: 보내려는 Eth의 수량
  f. v,r,s : 트랜잭션 사인 정보
  g. data: 트랜잭션에 실어보낼 데이터
  h. 컨트랙트인 경우, 함수 해시 및 Prameter



트랜잭션과 블록

- **트랜잭션 오더링**
  - 여러개의 트랜잭션이 있을 때, 어떤것이 먼저 수행되는지에 따라 최종상태가 바뀔 수 있다.
  - 트랜잭션의 순서를 어떻게 정할 것인가.
  - 트랜잭션의 순서를 누가 정할 것인가.

- **실생활에서의 트랜잭션 오더링**
  - 중고나라 무료 나눔 > https://cafe.naver.com/joonggonara/636219386

트랜잭션과 블록

- **실생활에서의 트랜잭션 오더링**
  - 같은 시간에 4명의 사람이 댓글을 작성함
  - 댓글의 순서는 어떻게 정해질까?
    - 아마도 네이버에 가장 빨리 요청이 도착한 사람
  - 네이버를 믿으십니까?
    - 알고 봤더니 리츠원이 네이버 관리자?

트랜잭션과 블록

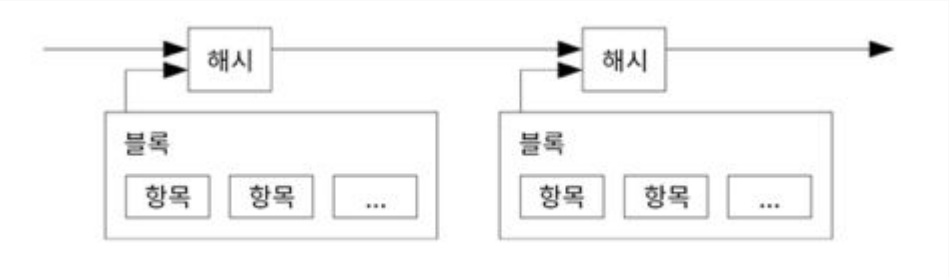
- **트랜잭션 오더링**
  - 트랜잭션이 생성된 시간을 누가 정할까?
  - 트랜잭션 생성자가 정하게 되면, 사익에 의해 조작가능성이 존재
  - 믿을 수 있는 제 3자가 증명이 필요
  - 제 3자를 어떻게 믿지?

비 신뢰기반의 환경에서 신뢰할 수 있는 데이터 처리가 필요

- 그 시간에 트랜잭션이 존재했음을 증명할 수 있는 방법은?
  - 트랜잭션의 전파에 영향을 주는 요소
    - 지역
    - 네트워크 환경
    - 메인넷 활성화 상태

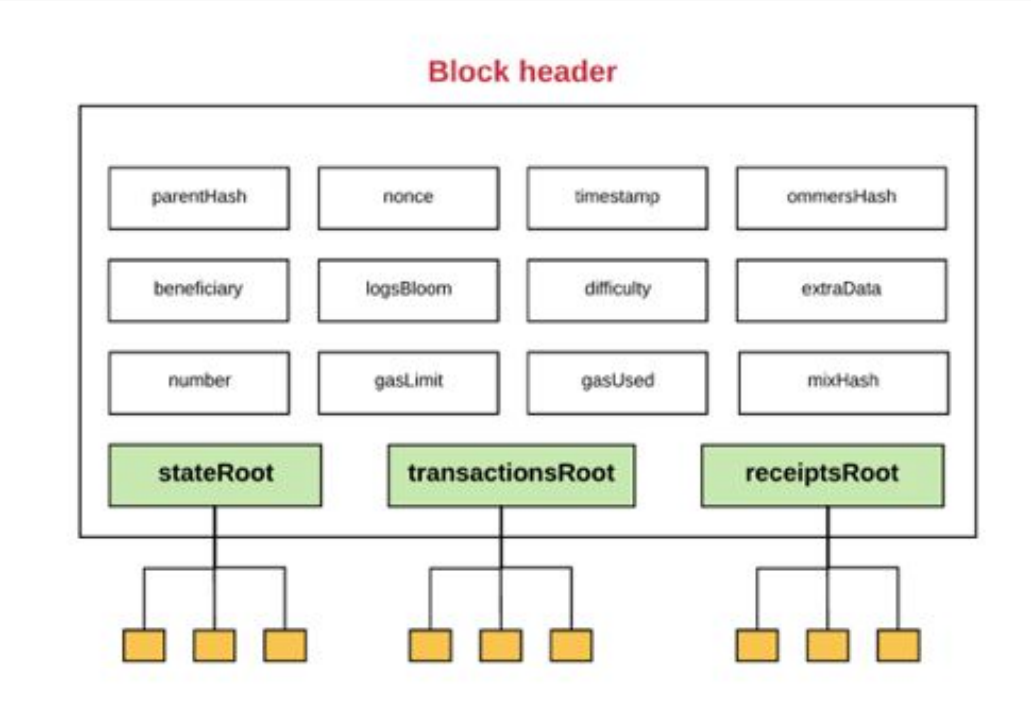
트랜잭션과 블록

- **체인**
  - 이전 블록에 의한 상태를 바탕으로 새로운 블록이 생성
    - 트랜잭션의 지속성을 유지
    - 트랜잭션의 논리적 시간 순서를 결정
    - 트랜잭션 기록의 위변조를 어렵게 만듦

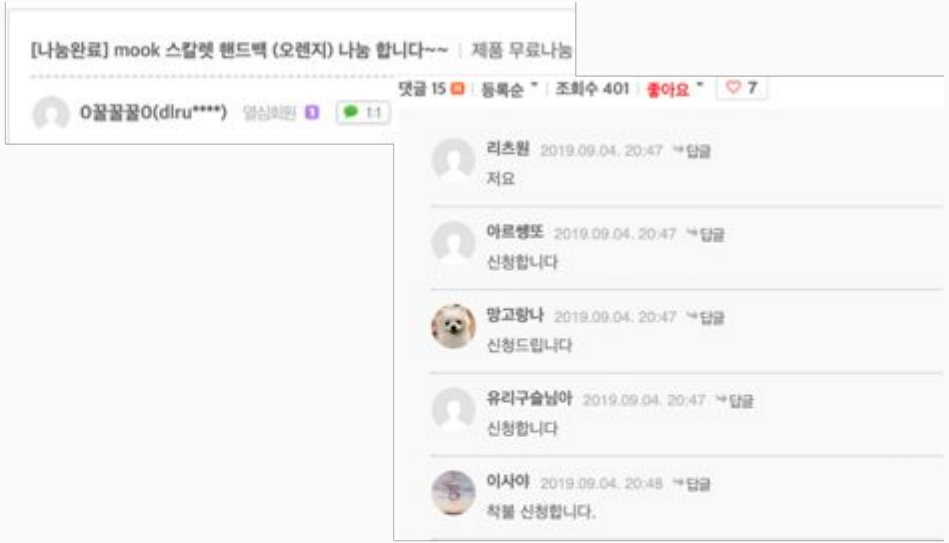


트랜잭션과 블록

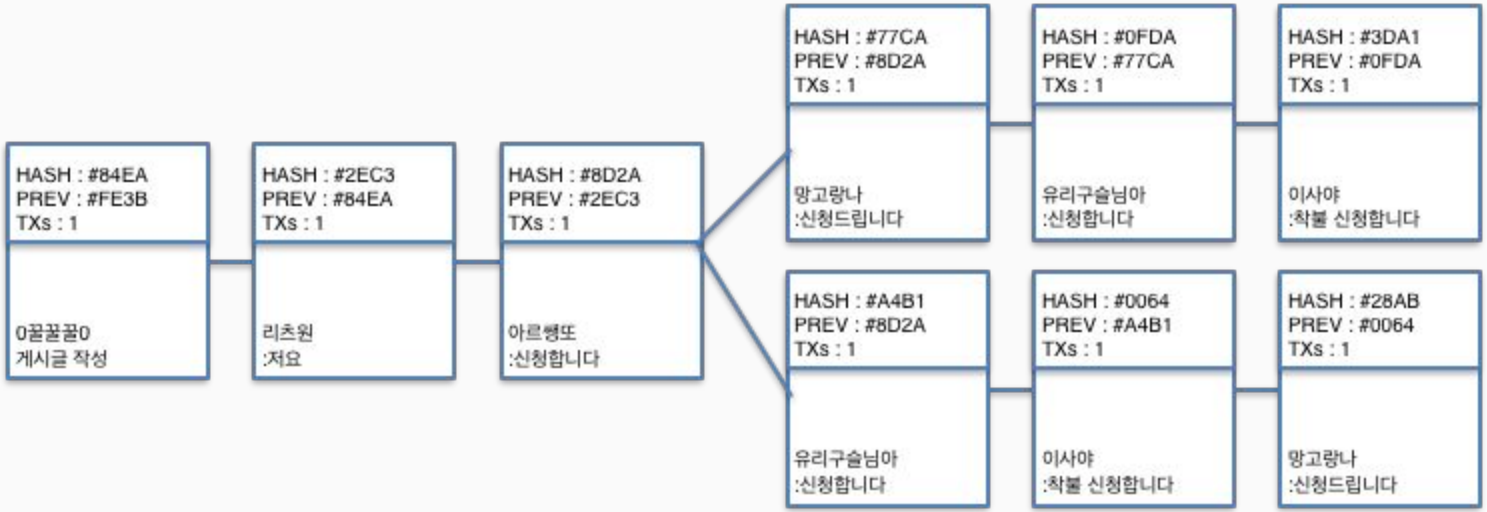
이더리움 블록의 구조



트랜잭션과 블록

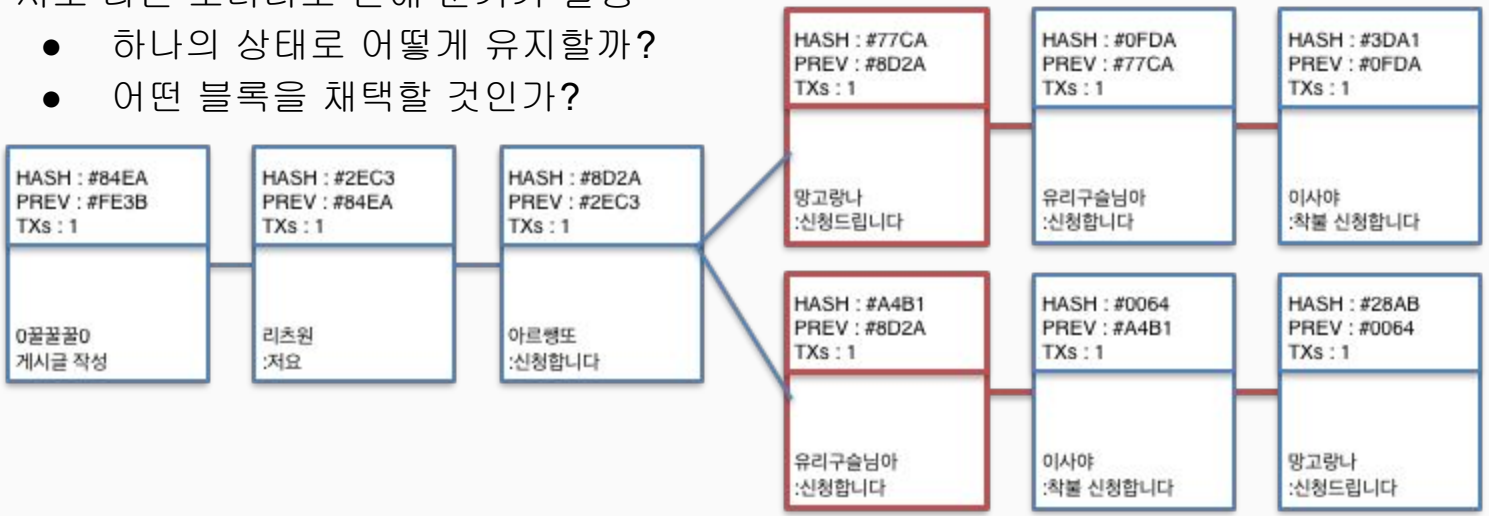

[나눔완료] mook 스칼렛 핸드백 (오렌지) 나눔 합니다~~ | 제품 무료나눔
0꿀꿀꿀0(dlru****)
댓글 15 | 등록순 | 조회수 401 | 좋아요 7
리츠원 2019.09.04. 20:47 답글
저요
아르뱅또 2019.09.04. 20:47 답글
신청합니다
망고랑나 2019.09.04. 20:47 답글
신청드립니다
유리구슬님아 2019.09.04. 20:47 답글
신청합니다
이사야 2019.09.04. 20:48 답글
착불 신청합니다.


HASH : #84EA
PREV : #FE3B
TXs : 1
0꿀꿀꿀0
게시글 작성
HASH : #2EC3
PREV : #84EA
TXs : 1
리츠원
:저요
HASH : #8D2A
PREV : #2EC3
TXs : 1
아르뱅또
:신청합니다
HASH : #77CA
PREV : #8D2A
TXs : 1
망고랑나
:신청드립니다
HASH : #0FDA
PREV : #77CA
TXs : 1
유리구슬님아
:신청합니다
HASH : #3DA1
PREV : #0FDA
TXs : 1
이사야
:착불 신청합니다

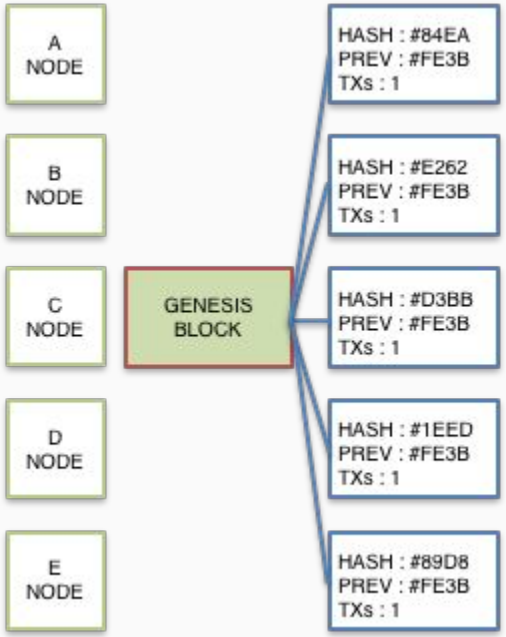

HASH : #84EA
PREV : #FE3B
TXs : 1
0꿀꿀꿀0
게시글 작성
HASH : #2EC3
PREV : #84EA
TXs : 1
리츠원
:저요
HASH : #8D2A
PREV : #2EC3
TXs : 1
아르뺑또
:신청합니다
HASH : #77CA
PREV : #8D2A
TXs : 1
망고랑나
:신청드립니다
HASH : #0FDA
PREV : #77CA
TXs : 1
유리구슬님아
:신청합니다
HASH : #3DA1
PREV : #0FDA
TXs : 1
이사야
:착불 신청합니다
HASH : #A4B1
PREV : #8D2A
TXs : 1
유리구슬님아
:신청합니다
HASH : #0064
PREV : #A4B1
TXs : 1
이사야
:착불 신청합니다
HASH : #28AB
PREV : #0064
TXs : 1
망고랑나
:신청드립니다

컨센서스 알고리즘

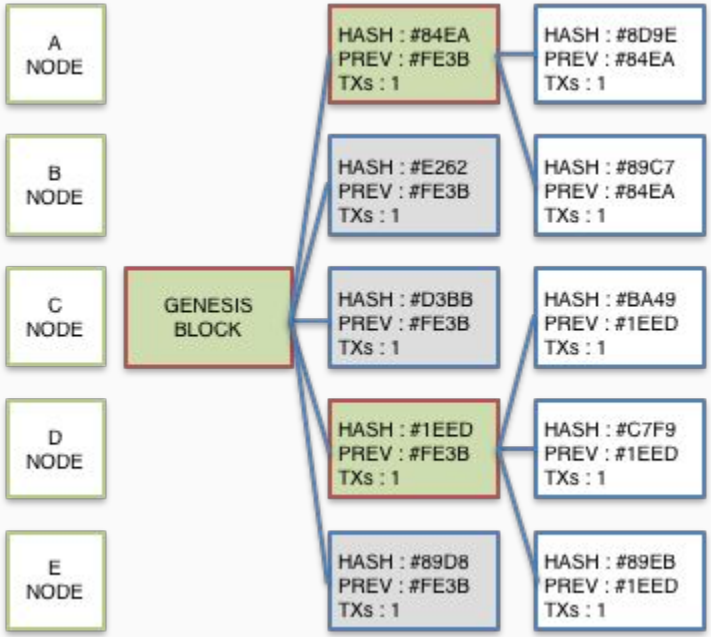
- **컨센서스**
  - 서로 다른 오더러로 인해 분기가 발생
    - 하나의 상태로 어떻게 유지할까?
    - 어떤 블록을 채택할 것인가?



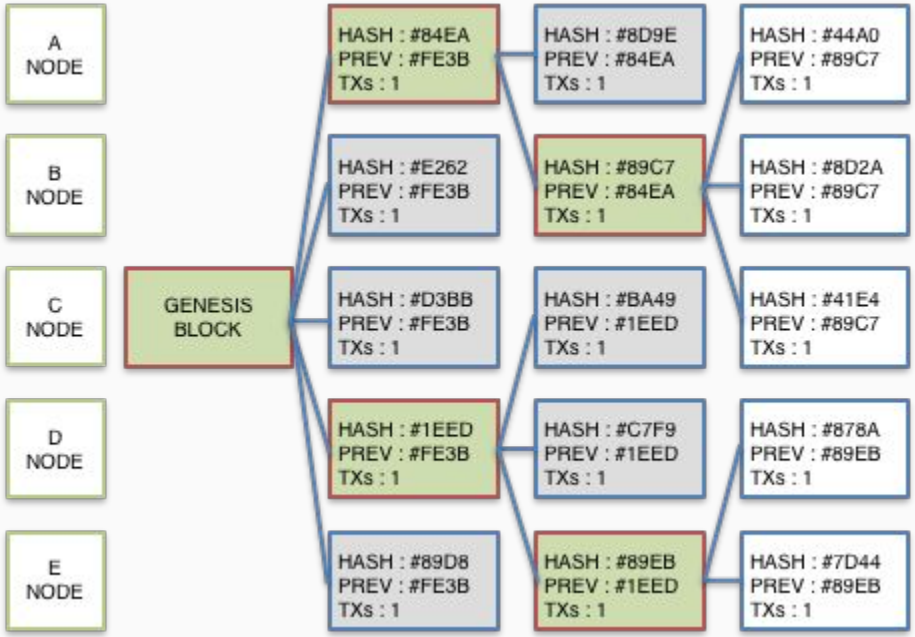
컨센서스 알고리즘


A
NODE
B
NODE
C
NODE
D
NODE
E
NODE
GENESIS
BLOCK
HASH : #84EA
PREV : #FE3B
TXs : 1
HASH : #E262
PREV : #FE3B
TXs : 1
HASH : #D3BB
PREV : #FE3B
TXs : 1
HASH : #1EED
PREV : #FE3B
TXs : 1
HASH : #89D8
PREV : #FE3B
TXs : 1

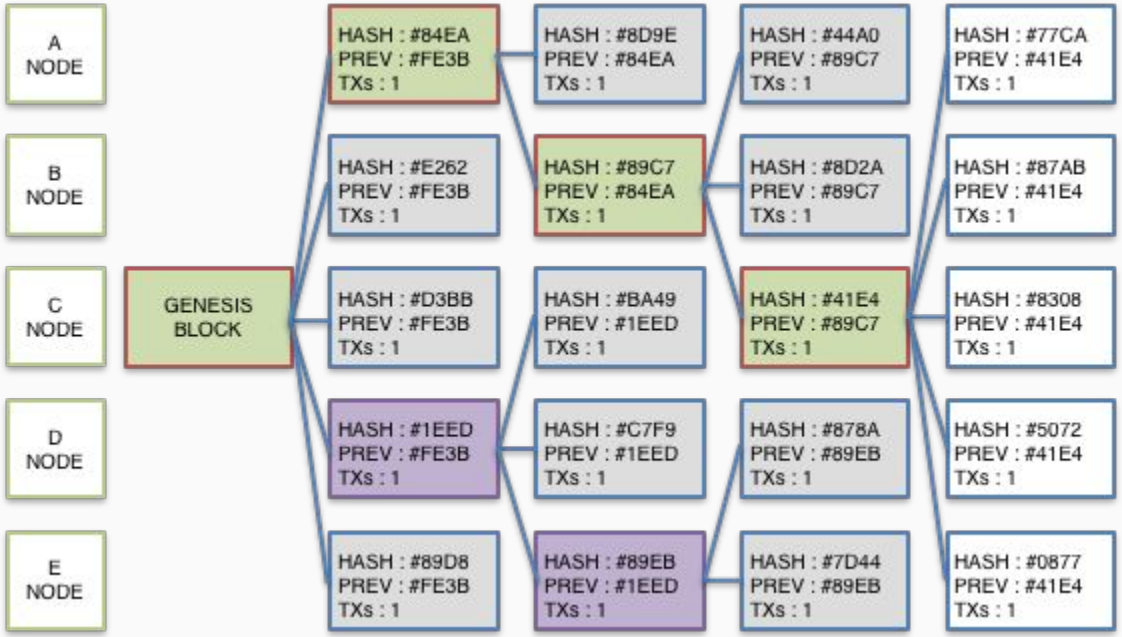
컨센서스 알고리즘


A NODE
B NODE
C NODE
D NODE
E NODE
GENESIS BLOCK
HASH : #84EA
PREV : #FE3B
TXs : 1
HASH : #E262
PREV : #FE3B
TXs : 1
HASH : #D3BB
PREV : #FE3B
TXs : 1
HASH : #1EED
PREV : #FE3B
TXs : 1
HASH : #89D8
PREV : #FE3B
TXs : 1
HASH : #8D9E
PREV : #84EA
TXs : 1
HASH : #89C7
PREV : #84EA
TXs : 1
HASH : #BA49
PREV : #1EED
TXs : 1
HASH : #C7F9
PREV : #1EED
TXs : 1
HASH : #89EB
PREV : #1EED
TXs : 1

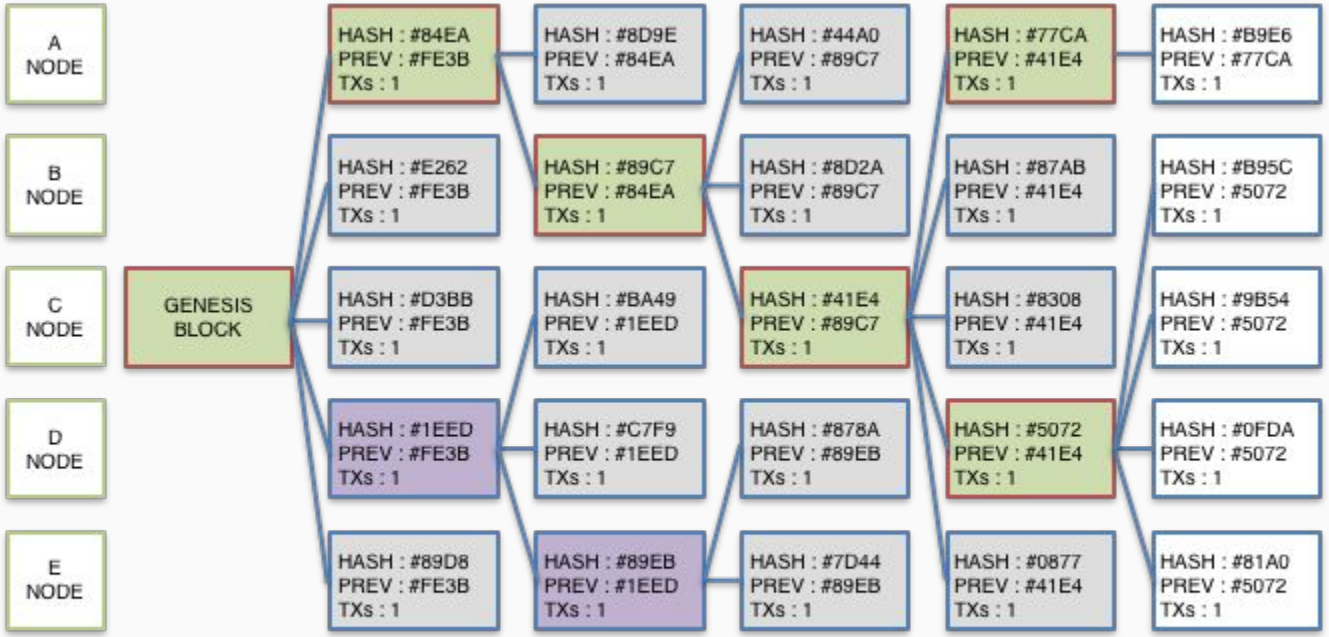
컨센서스 알고리즘


A NODE
B NODE
C NODE
D NODE
E NODE
GENESIS BLOCK
HASH : #84EA
PREV : #FE3B
TXs : 1
HASH : #E262
PREV : #FE3B
TXs : 1
HASH : #D3BB
PREV : #FE3B
TXs : 1
HASH : #1EED
PREV : #FE3B
TXs : 1
HASH : #89D8
PREV : #FE3B
TXs : 1
HASH : #8D9E
PREV : #84EA
TXs : 1
HASH : #89C7
PREV : #84EA
TXs : 1
HASH : #BA49
PREV : #1EED
TXs : 1
HASH : #C7F9
PREV : #1EED
TXs : 1
HASH : #89EB
PREV : #1EED
TXs : 1
HASH : #44A0
PREV : #89C7
TXs : 1
HASH : #8D2A
PREV : #89C7
TXs : 1
HASH : #41E4
PREV : #89C7
TXs : 1
HASH : #878A
PREV : #89EB
TXs : 1
HASH : #7D44
PREV : #89EB
TXs : 1

컨센서스 알고리즘

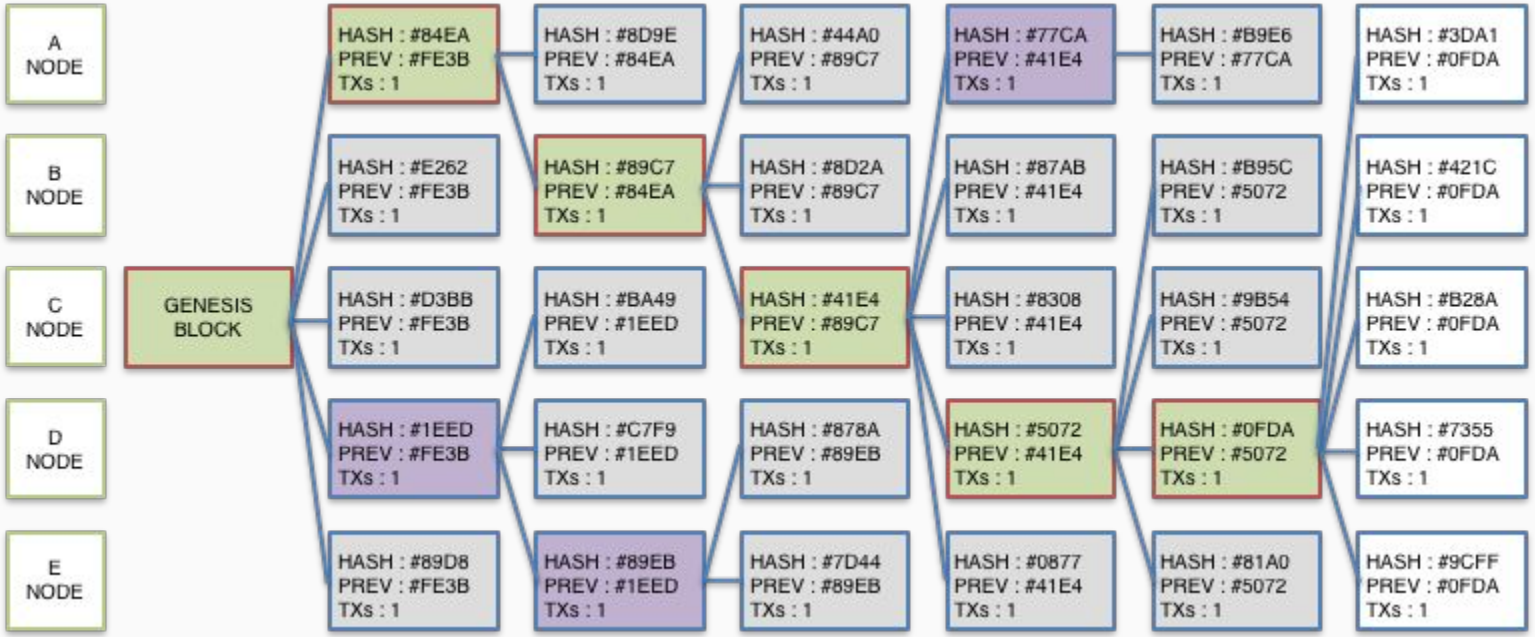

A NODE
B NODE
C NODE
D NODE
E NODE
GENESIS BLOCK
HASH : #84EA
PREV : #FE3B
TXs : 1
HASH : #E262
PREV : #FE3B
TXs : 1
HASH : #D3BB
PREV : #FE3B
TXs : 1
HASH : #1EED
PREV : #FE3B
TXs : 1
HASH : #89D8
PREV : #FE3B
TXs : 1
HASH : #8D9E
PREV : #84EA
TXs : 1
HASH : #89C7
PREV : #84EA
TXs : 1
HASH : #BA49
PREV : #1EED
TXs : 1
HASH : #C7F9
PREV : #1EED
TXs : 1
HASH : #89EB
PREV : #1EED
TXs : 1
HASH : #44A0
PREV : #89C7
TXs : 1
HASH : #8D2A
PREV : #89C7
TXs : 1
HASH : #41E4
PREV : #89C7
TXs : 1
HASH : #878A
PREV : #89EB
TXs : 1
HASH : #7D44
PREV : #89EB
TXs : 1
HASH : #77CA
PREV : #41E4
TXs : 1
HASH : #87AB
PREV : #41E4
TXs : 1
HASH : #8308
PREV : #41E4
TXs : 1
HASH : #5072
PREV : #41E4
TXs : 1
HASH : #0877
PREV : #41E4
TXs : 1

컨센서스 알고리즘

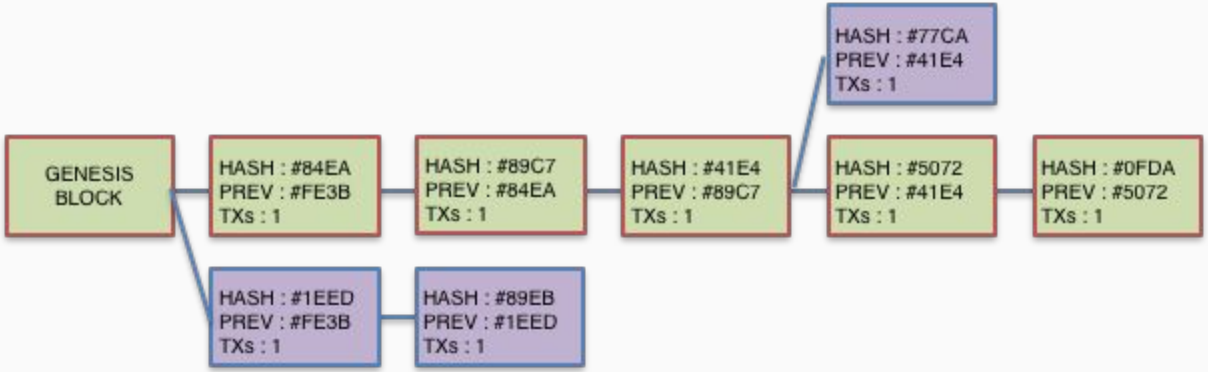

A NODE
B NODE
C NODE
D NODE
E NODE
GENESIS BLOCK
HASH : #84EA
PREV : #FE3B
TXs : 1
HASH : #E262
PREV : #FE3B
TXs : 1
HASH : #D3BB
PREV : #FE3B
TXs : 1
HASH : #1EED
PREV : #FE3B
TXs : 1
HASH : #89D8
PREV : #FE3B
TXs : 1
HASH : #8D9E
PREV : #84EA
TXs : 1
HASH : #89C7
PREV : #84EA
TXs : 1
HASH : #BA49
PREV : #1EED
TXs : 1
HASH : #C7F9
PREV : #1EED
TXs : 1
HASH : #89EB
PREV : #1EED
TXs : 1
HASH : #44A0
PREV : #89C7
TXs : 1
HASH : #8D2A
PREV : #89C7
TXs : 1
HASH : #41E4
PREV : #89C7
TXs : 1
HASH : #878A
PREV : #89EB
TXs : 1
HASH : #7D44
PREV : #89EB
TXs : 1
HASH : #77CA
PREV : #41E4
TXs : 1
HASH : #87AB
PREV : #41E4
TXs : 1
HASH : #8308
PREV : #41E4
TXs : 1
HASH : #5072
PREV : #41E4
TXs : 1
HASH : #0877
PREV : #41E4
TXs : 1
HASH : #B9E6
PREV : #77CA
TXs : 1
HASH : #B95C
PREV : #5072
TXs : 1
HASH : #9B54
PREV : #5072
TXs : 1
HASH : #0FDA
PREV : #5072
TXs : 1
HASH : #81A0
PREV : #5072
TXs : 1

x

컨센서스 알고리즘


A NODE
B NODE
C NODE
D NODE
E NODE
GENESIS BLOCK
HASH : #84EA PREV : #FE3B TXs : 1
HASH : #E262 PREV : #FE3B TXs : 1
HASH : #D3BB PREV : #FE3B TXs : 1
HASH : #1EED PREV : #FE3B TXs : 1
HASH : #89D8 PREV : #FE3B TXs : 1
HASH : #8D9E PREV : #84EA TXs : 1
HASH : #89C7 PREV : #84EA TXs : 1
HASH : #BA49 PREV : #1EED TXs : 1
HASH : #C7F9 PREV : #1EED TXs : 1
HASH : #89EB PREV : #1EED TXs : 1
HASH : #44A0 PREV : #89C7 TXs : 1
HASH : #8D2A PREV : #89C7 TXs : 1
HASH : #41E4 PREV : #89C7 TXs : 1
HASH : #878A PREV : #89EB TXs : 1
HASH : #7D44 PREV : #89EB TXs : 1
HASH : #77CA PREV : #41E4 TXs : 1
HASH : #87AB PREV : #41E4 TXs : 1
HASH : #8308 PREV : #41E4 TXs : 1
HASH : #5072 PREV : #41E4 TXs : 1
HASH : #0877 PREV : #41E4 TXs : 1
HASH : #B9E6 PREV : #77CA TXs : 1
HASH : #B95C PREV : #5072 TXs : 1
HASH : #9B54 PREV : #5072 TXs : 1
HASH : #0FDA PREV : #5072 TXs : 1
HASH : #81A0 PREV : #5072 TXs : 1
HASH : #3DA1 PREV : #0FDA TXs : 1
HASH : #421C PREV : #0FDA TXs : 1
HASH : #B28A PREV : #0FDA TXs : 1
HASH : #7355 PREV : #0FDA TXs : 1
HASH : #9CFF PREV : #0FDA TXs : 1

컨센서스 알고리즘


GENESIS
BLOCK
HASH : #84EA
PREV : #FE3B
TXs : 1
HASH : #89C7
PREV : #84EA
TXs : 1
HASH : #41E4
PREV : #89C7
TXs : 1
HASH : #77CA
PREV : #41E4
TXs : 1
HASH : #5072
PREV : #41E4
TXs : 1
HASH : #0FDA
PREV : #5072
TXs : 1
HASH : #1EED
PREV : #FE3B
TXs : 1
HASH : #89EB
PREV : #1EED
TXs : 1

다시 비트코인..

비트코인의 한계와 이더리움의 등장

- 비트코인이 탕 중앙화된 화폐 거래를 보여주었지만, 그 이상의 확장성을 표현하지 못함
- 이더리움은 비탈릭에 의해 개발된 “프로그래밍 가능한 블록체인"
- 단순한 화폐의 거래 뿐만 아니라, 이더리움 플랫폼 위에서 다양한 App들이 동작할 수 있도록 설계됨

블록체인의 진화

특징	분산원장 도입	스마트컨트랙트 도입	2세대 블록체인 단점 보완
블록 시간	10분	15초	0.5초
스마트컨트랙트	X	지원(EVM)	지원(WASM)
합의 알고리즘	작업증명방식(PoW)	작업증명방식(PoW) 연내에 부분적 지분증명방식(PoS) 도입	위임 지분 증명방식(DPoS)
TPS	5	20	3082

앞으로 우리는

- 이더리움 플랫폼의 특성에 대해 이해
- 스마트 컨트랙트 동작 구조
- 실제 서비스 가능한 블록체인 서비스 개발