RETURN VALUES

블록체인 입문과정

Dec. 2018

RETURN VALUES

Agenda

I. 블록체인의 이해

II. 블록체인의 특징

III. 채굴 과정으로 알아보는 블록 구조

IV. 1세대 블록체인과 2세대 블록체인

V. 이더리움과 스마트 컨트랙트

많은 사람들의 착각

블록체인 = 비트코인 ?

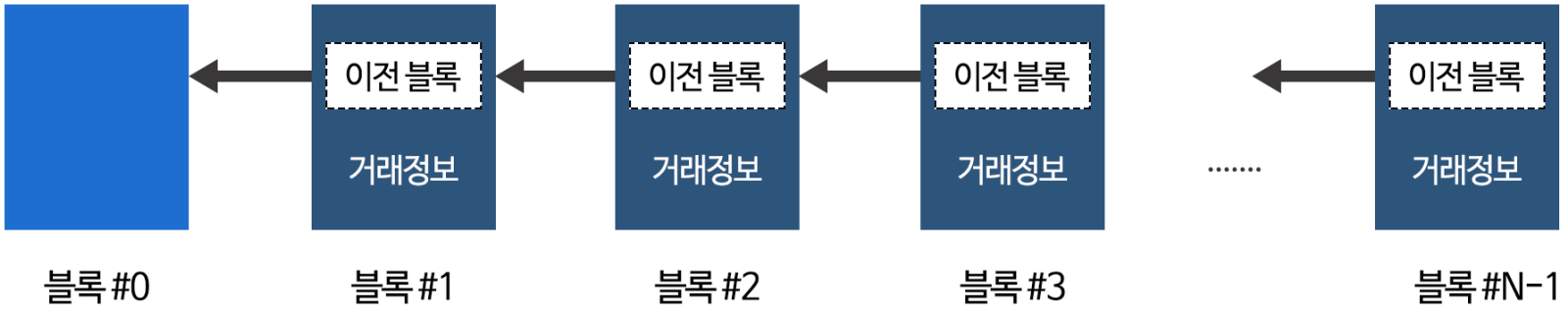
사실은 블록체인이라는 플랫폼상에 비트코인이 존재한다
스마트폰에 다양한 어플리케이션이 있는 것처럼
비트코인도 하나의 어플리케이션이며
블록체인의 데이터베이스를 이용한 것이다.

Blockchain : 분산 컴퓨팅 기술 기반의 데이터 위변조 방지 기술

관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경에 저장되어 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 대변 방지 기술이다.

여러건의 거래 장부인(블록)이 링크(체인) 으로 연결되어 모두에게 공유되는 분산 원장기술

블록체인은 최초의 블록인 제네시스 블록(Genesis block) 부터 시작해서 일정 시간마다 하나씩 생성되며
바로



블록체인이란?

DATA BASE

중앙에서 관리하는 주체 없이

다수가 동시에 운영 가능한 분산된 형태의 베이스

블록체인의 이해

- 모든 권한을 사용자에게 위임하는 형태
- 중앙 관리의 감시 없이 누구나 관리자가 된다면 다수에 의한 데이터의 위변조 가능성이 있을 수 있기 때문에 합의(Consensus) 라는 개념이 추가되었다.
- 사용자들의 합의를 통해 블록에 기록될 데이터를 선별하고 서로 검증하여 데이터의 완전성을 유지한다.

즉 서로 데이터가 무결한지 동의한 후에 데이터베이스에 입력하는 방식

블록체인의 이해

우리가 아는 일반적인 DATA BASE : 저장 및 수정과 삭제 가능

블록체인의 DATA BASE : 수정과 삭제가 불가능한 데이터 (저장하고 읽기만 가능)
(2세대 블록체인에서는 수정 가능)

적용 가능한 분야는?

- 한번 저장하면 수정이 불가능한 곳에 필요하다
(ex] 투표, 성적관리, 거래 내역 등 위변조가 있어서는 안될 곳에)

블록체인을 게시판으로 이해하기

기존의 게시판 : 글을 올리면 서버에 업로드되고 모두에게 보여진다

블록체인 게시판 : 글을 올리는 행위 자체가 하나의 트랜잭션

트랜잭션으로 글에 문제가 있는지 검열하고 (합의 알고리즘에 따라)
검열 후 글은 블록에 담겨 업로드된다.

다음 글이 업로드 되면 이전글 다음에 생성되듯이
다음 블록에 담겨 체인으로 이전 블록과 연결된다.

블록체인의 장점

- 시간절약 : 트랜잭션의 실시간 처리 (중앙을 거치지 않는 P2P 방식)
- 비용절감 : 중개자의 오버헤드 및 비용 감소 (중앙에 수수료를 낼 필요가 없음)
- 위험감소 : 데이터의 위변조가 불가능하기 때문에 조직적 사기 및 해깅범죄 감소
- 신뢰확산 : 공유 프로세스 및 기록을 통한 신뢰 확보가 가능

블록체인의 특징

- 분산구조방식 : 중앙 집중식이 아닌 P2P 네트워크를 이용한 분산구조 (탈중앙화)
  블록체인 데이터가 분산된 모든 노드에게 보관되어 있음
- 투명성 : 모든 노드에게 보관되기 때문에 누구나 데이터에 접근 가능
- 가용성 : 어느 특정 노드가 서비스 불가한 상태가 되더라도 다른 노드들에 의해
  네트워크 유지가 가능하다
- 익명성 : 트랜잭션은 무기명으로 처리된다.
- 신뢰성 : 누구나 똑같은 데이터베이스를 가지고 있기 때문에 데이터의 내용이 보장된다.
- 불가역성 : 한번 트랜잭션이 등록되면 변조 및 삭제가 불가하다.

블록체인의 특징

블록체인에서는 어떻게 데이터가 위조되지 않았음을 증명할 수 있을까?

해시값을 통해 데이터가 수정되었는지 검증 할 수 있다.

해시 알고리즘 : 암호화는 가능하지만 복호화는 불가능
어떠한 크기의 데이터를 넣어도 같은 길이의 값을 출력한다.
어떤 데이터를 해싱했을 때 조금이라도 다른점이 있다면
전혀 다른 해시값을 출력한다는 특징이 있음

즉 조금이라도 원본과 다른 정보가 들어 있다면 전혀 다른 해시값이 나오기 때문에 수정된 정보가 있다는 것을 알 수 있다.

블록체인에서는 어떻게 익명성을 보장할까?

거래소가 존재하기 이전에 송금하는 주소는 해시값과 같은 형태를 띄었기 때문에
주소로 사용자를 유추할 수 없어 익명성의 보장이 가능했었다. 물론 거래소 없이 송금한다면 익명성은 보장된다.

저의 메타마스크 이더지갑 주소는

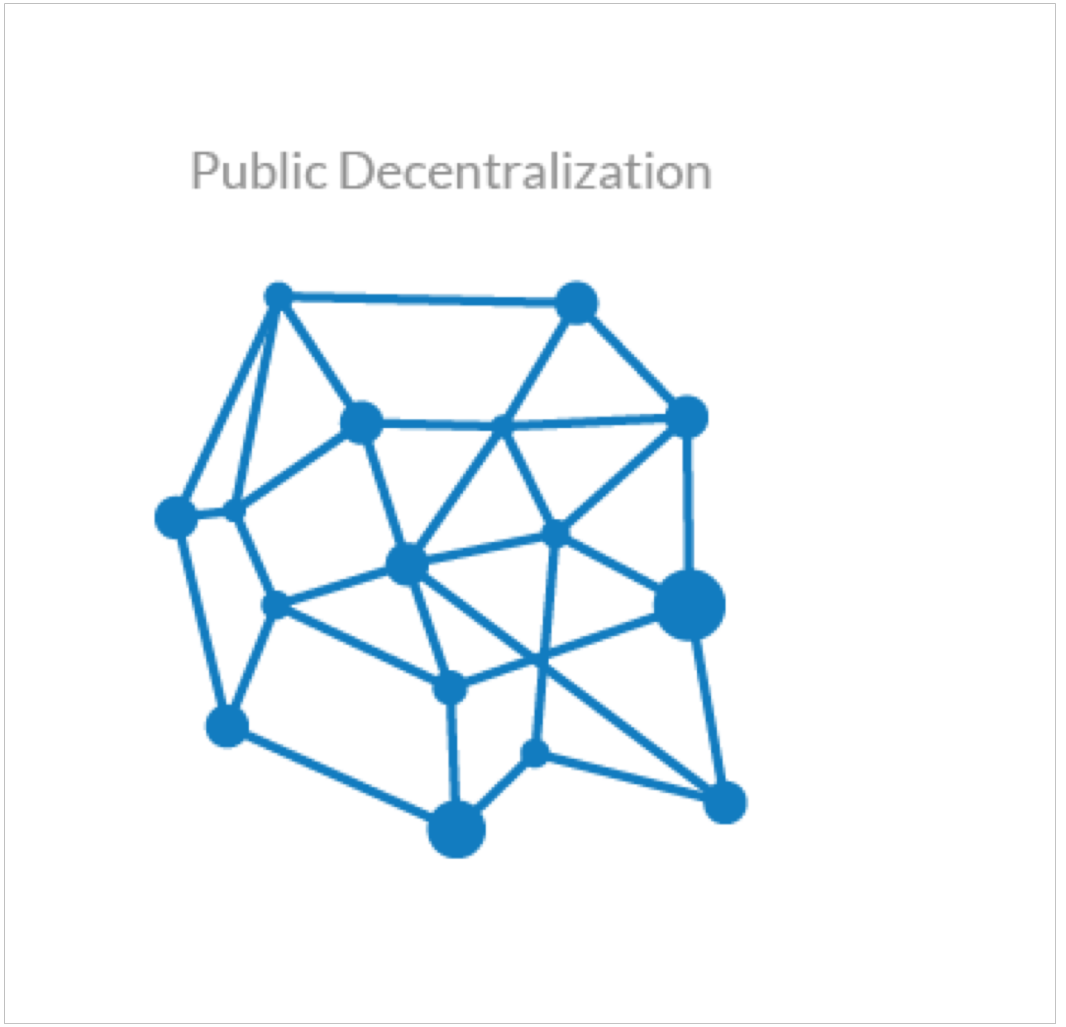
0x78cb056bc0F03e49B5013c1Fa969d37b1f1710c6

하지만 거래소에서 이더를 구입하기 위해서는 회원가입과 까다로운 본인확인 절차로 인해
100% 익명성의 보장은 어려움

블록체인의 특징

퍼블릭 블록체인

- 무허가형 원장
  누구나 블록체인의 데이터를 읽고, 쓰고
  검증할 수 있다.
- 대표적인 예시 비트코인
  누구나 비트코인의 블록체인 데이터를
  다운받아 어떠한 기록이 있는지 조회하고
  실제로 암호서명을 통해 참여가 가능하다.
- 투표를 통해 블록을 생성한다.
  투표자 수로 데이터의 적법성을 결정하게 된다면 노드 수를 무작위로 늘려 네트워크를 장악할 수 있기 때문에 노드 수가 아닌 투입한 컴퓨팅 파워에 비례해서 투표권을 부여한다.



프라이빗 블록체인

- 허가형 원장
  읽고 쓰기 및 합의과정에 참여할 수 있는 참여자가 미리 지정되어 있으며 필요에 따라 특정 주체가 새로 추가되거나 제거될 수 있다.
- 접근권한이 맞춤형으로 설계된 블록체인
  신뢰할 수 있는 노드에게 블록을 생성할 권한을 주기 때문에 작업증명과 같은 패시파워 경쟁이 사실상 필요 없음
- 컨소시엄 블록체인
  여러 집단의 협의체(기업 연합 등)이 노드에 참가하는 형태

블록체인을 가능하게 하는 기술 - 해시 알고리즘

단방향(one way) 함수 : 역산이 불가능함

함수의 입력의 크기와 상관없이 출력은 동일한 길이의 값이 나온다.
함수의 입력에 조금이라도 다른 내용이 있다면 다른 결과를 출력한다.
또한 출력값으로 입력값을 알아낼 수 없다.

"강연주" =>

F84D0C4D3935E0AD18566BF9AFA8987D442897B7E8975EFC00B26EEC82DA54B1

"강희주" =>

5B36C69323518C7536D26DB22E409136499BC63C54C0C35125A46E36E664E707

블록체인을 가능하게 하는 기술 - 전자서명

개인과 개인간의 거래를 성사시키고, 거래를 검증하기 위한 한 쌍의 키

공개키 (Public key) 와 개인키 (Private key)

공개키는 거래를 위해 모든 사람에게 말 그대로 공개되는 키
개인키는 비밀번호와 같이 개인만이 간직하는 키

내 개인키로 서명한 거래내역은 타인이 내 공개키를 이용하여 복호화 할 수 있다.
즉 이 거래는 다름아는 내가 서명한 거래라는것을 보증한다.

블록체인을 가능하게 하는 기술 - 네트워크

노드 : 블록체인 네트워크에 참여하는 참여자

블록체인은 네트워크가 형성되어야 비로소 이루어질 수 있고
(혼자서는 거래가 불가하듯이)

네트워크가 많으면 많을 수록 데이터의 위변조가 어려워진다.
(데이터는 사용자 모두와 공유하기 때문에, 네트워크 개체수가 많을 수록 위변조가 어려워진다.)

퍼블릭 블록체인에서는 이 네트워크를 유지시키기 위해 채굴이라는 개념을 넣어
자발적으로 노드들이 네트워크를 유지하게끔 하고 있다.

채굴의 정의

채굴은 블록을 생성한다는 의미이다.
채굴 방법을 간단히 표현하자면 컴퓨터로 연산한다고 표현할 수 있다.
(정확히는 블록 헤더안에 있는 난이도 목표보다 낮은 해시값을 도출하는 nonce를 찾는 것)
가장 빨리 채굴한 채굴자에게 보상을 주기 때문에
누구보다 빠르게 채굴하기 위해서는 GPU와 같은 연산능력이 뛰어난 컴퓨터가 필요하다.

Q.그럼 채굴은 비싼 컴퓨터를 가진 돈 많은 사람만 할 수 있지 않을까?

A.이를 방지하기 위해 채굴자에게 다음 연산과정에서 시간이 걸리도록
더욱 어려운 난이도의 연산을 하게 한다

이러한 복잡한 채굴의 방식에 대해 이해하기 위해서는 블록 구조를 살펴 볼 필요가 있다.

블록 구조 (비트코인)

블록 : 블록체인의 원소, 거래장부

블록 헤더 : 블록의 정보

블록 바디 : 트랜잭션(거래내역)

블록 #N	
Version	이전 블록 해시
Merkle root	Time stamp
Bits	Nonce
트랜잭션 카운트	
코인베이스 트랜잭션	
트랜잭션	

블록의 헤더에는 다음과 같은 블록 정보가 들어간다.

1. 블록 버전
    2. 이전 블록 해시 : 이전 블록 헤더를 해싱한 값
    3. 타임스태프 : 블록이 생성된 시간
    4. bits : 목표 난이도
    5. Merkle root
    6. Nonce

블록 바디에는 다음과 같은 정보가 들어간다.

1. 트랜잭션 카운트 : 포함된 거래 개수
2. 코인베이스 트랜잭션 : 블록 생성시 보상으로 채굴자에게 주어질 코인

3. 10분동안 수집된 거래 내역

bits : 연산 난이도

블록 생성 주기는 정해져 있는데

빠른 연산이 가능한 채굴자가 주기보다 빨리 채굴해 버렸을 경우

(비트코인의 경우 10분, 하지만 7분만에 채굴해버렸다고 한다면?)

목표완성도에 100퍼센트 접근하지 못했다고 판단하여

블록 #1

요약	
거래 수	1
출력 합계	50 BTC
예상된 거래량	0 BTC
거래 수수료	0 BTC
높이	1 (주 체인)
타임 스탬프	2009-01-09 02:54:25
수신 시간	2009-01-09 02:54:25
릴레이된 곳	Unknown
난이도	1
Bits	486604799

블록 #553150

요약	
거래 수	1852
출력 합계	3,712.13873566 BTC
예상된 거래량	637.14029516 BTC
거래 수수료	0.12380751 BTC
높이	553150 (주 체인)
타임 스탬프	2018-12-09 15:10:52
수신 시간	2018-12-09 15:10:52
릴레이된 곳	BTC.com
난이도	5,646,403,851,534.72
Bits	389142908

머클루트

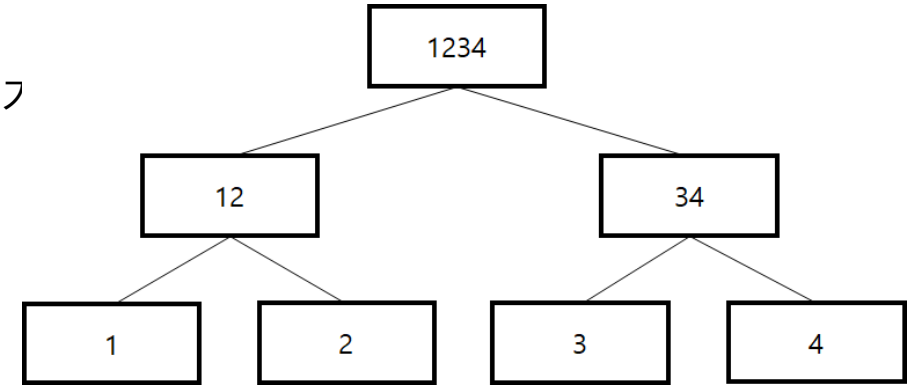
한개의 블록 바디에 담긴 트랜잭션은 몇백 몇천건 ㄱ

이 트랜잭션들을 하나씩 해싱하고

이 해싱된 값을 두개씩 짝지어 해싱하고

또 두개씩 짝을 지어 해싱하고...

이러한 과정을 반복하다보면



Merkle tree

Nonce

지금까지 설명한 헤더에 들어가는 값들은 고정된 값이기 때문에

모든 값이 고정된 상태에서 해싱을 한다면 해시값 결과도 같은 값을 출력한다.

bits어

이 고 복해

야 한다. 이 0부터 대입하여 증감시키는 값이 Nonce이다.

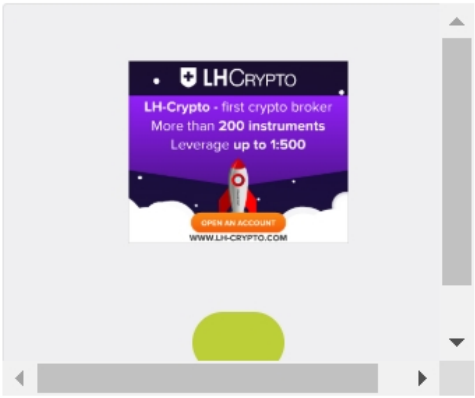
출처 - 비트코인과 블록체인 기술 (이종권)

블록으로 확인하는 Nonce

블록 #553151

요약	
거래 수	1583
출력 합계	5,713.9448503 BTC
예상된 거래량	882.2044242 BTC
거래 수수료	0.11151328 BTC
높이	553151 (주 체인)
타임 스탬프	2018-12-09 15:14:55
수신 시간	2018-12-09 15:14:55
릴레이된 곳	BTC.com
난이도	5,646,403,851,534.72
Bits	389142908
크기	1103.365 kB
무게	3992.743 kWU
번역	0x20000000
해시 난수	3666744834

해시	
해시	00000000000000000002dab85d7495d08978706a71b0e95bdbf00860f4fec2274
이전 차단	00000000000000000001c357f8fea8f120ddf3b34293eed807c18f482e913a97a
다음 블록	00000000000000000001eede0b9860eee4887f04d9ecb6d05c5ad4e3826e985f6
Merkle Root	79f8e52f015653b947600a0a984dce14c8aa45ab8e6c17503cd907287d43eff7



Bitcoin 채굴의 원리

블록에서 살펴본것처럼 00000000000000002dab…. 와 같은 해시값이 나오면 채굴이 완료된다. 이런 목표값은 특정 해시값보다 낮은 해시값이 나왔을 때 채굴이 성공된 것으로 간주되며 이러한 목표값은 방금 전 배운 **난이도 개념인 bits**에 결정된다.

이 00000000000000002dab… 과 같은 값이 나올때까지 논스에 0부터 하나씩 대입해 나가는 과정이 채굴하는 과정이다.

논스에 하나씩 값을 더하고 헤더를 해시하고 이 작업을 반복하다보면
언젠가는 목표값보다 작은 값이 나오게 된다…

위 블록에서는 블록 헤더에 논스값으로 3666744834 를 대입했기에
목표한 해시값을 찾을 수 있었다.

작업증명 (PoW)의 의미

즉 채굴이란 어떠한 목표값의 해시를 만들어주는 수인 Nonce를
0부터 대입해 나가면서 찾는 작업방식이다.

이를 **작업증명 (Proof of Work)**이라 부르는 이유이다.

Nonce값을 찾은 노드는 이전과 이어지는 다음 블록을 생성하게 되며

보상과 트랜잭션의 수수료를 받는다.

(비트코인의 경우 50코인, 하지만 4년에 한번씩 반으로 줄어듬)
(이더리움의 경우 5이더)

비트코인은 왜 이런 방식을 채택했을까?

방금 설명한 Nonce의 개념에서 언젠가 이 값을 증가시키며 하나씩 해싱하다보면
우리는 언젠가 목표값보다 낮은 해시값을 출력시키는 Nonce 찾게 되고
채굴에 성공한다고 배웠다.

비트코인에서는 이 언젠가는 반드시10분이 되게끔 개발자가 의도하였다.

개발자는 연구 끝에 10분이라는 시간이 블록을 생성하기에 가장 안정적인 주기임을
알아냈고 2016개의 블록을 생성하는데 2주가 소요되게끔 (2016*10 = 2주)
'목표' 를 설정해 놓았다.

비트코인은 왜 이런 방식을 채택했을까?

만약 컴퓨팅 파워가 너무 좋아서 연산을 빨리 해버렸다고 가정해보자

2016개의 블록을 생성하는데 1주일이 걸렸다면
비트코인에서는 목표에 도달하기 위한 필요 작업의 50%만 이루어진 것으로 간주한다.

이와 같은 경우 난이도 수치를 조정하여
소요된 1주일의 2배인 2주가 걸리게 조정하고 목표에 도달하기 위한
필요 작업의 100%가 충족되게 한다.

왜 10분으로 정했을까?

개발자가 블록 생성 주기를 10분으로 설정한 이유는

신속한 승인시간과 분기가 발생할 확률을 절충하기 위함이다.

만약 너무나 빠른 속도로 블록이 생성된다면?
동시에 여러개의 다른 블록이 생겨나 체인으로 연결되기 어려워진다.

생성 주기를 길게 설정한다면?
거래할 때 시간이 너무 오래 걸리게 된다.

1세대 블록체인 - Bitcoin

- 분산원장기술을 활용하여 개인과 개인간의 거래에 있어서 공인된 금융기관을 거치지 않아도 서로 신뢰가 가능하여 중앙 기관 없이 거래할 수 있고 거래 장부의 신뢰성을 보증하며 이중지불을 막는 솔루션
- 2008년 글로벌 금융위기를 초래하게 된 중앙집권형 경제방식과는 다른 탈중앙화를 지향함
- 가장 널리 알려진 암호화폐
- 합의 알고리즘 : 작업증명방식 (채굴에 성공한 채굴자가 보상으로 일정량의 비트코인을 받음 보상으로 받는 코인이 곧 신규로 발행되는 통화)
- 총 발행량은 2100만 비트코인이며 이 이상은 발행 불가
- 화폐로서의 기능에 초점을 두고 있기 때문에 송금과 결제만 가능 (아주 간단한 컨트랙트 가능, 튜링 불완전)

2세대 블록체인 - Ethereum

- 블록체인 기반의 범용 서비스 개발을 위한 컴퓨팅 플랫폼
- 디지털 통화와 더불어 스마트 컨트랙트의 개념을 추가하여 전 세계 수 많은 사용자들이 보유하고 있는 컴퓨터 자산을 활용하여 분산 네트워크를 구성하고 이 플랫폼으로 다양한 시스템을 구현할 수 있게 한다.
- 화폐의 단위는 Ether
- 합의 알고리즘: 작업증명방식 (지불증명방식으로 변경 예정)
- 이더리움은 개발 완성 단계가 아닌 개발중인 단계이며 이더리움 재단에서 발표한 로드맵의 4가지 단계를 거쳐완성되어지고 있다. (현재 3단계)
- 비트코인과 다르게 총 발행량의 제한은 없음
- 송금 및 결제 뿐만 아니라 계약, 투표, 공증, SNS 등 이용 범위가 상당히 넓다. (튜링 완전)
- 무분별한 트랜잭션의 사용을 막고자 수수료의 개념인 Gas를 도입하였다.

1세대 블록체인과 2세대 블록체인

	Bitcoin	Ethereum
TPS	7 tx / sec	13 tx / sec
블록생성주기	10 minute	13 seconds
총 발행량	21,000,000 BTC	Unlimited
합의 알고리즘	Pow	Pow => Pos
기능	화폐 송금 및 결제	스마트 컨트랙트 기반 분산어플리케이션 구현 가능

이더리움의 Account

Account : 비트코인의 지갑과는 다른 개념
트랜잭션의 실행 주체로 가장 기본적인 단위
이더리움의 State를 구성하는 오브젝트

EOA(Externally Owned Account) : 외부 소유 어카운트
일반적인 지갑의 기능을 수행하며 사용자 계정과 비슷하다.
개인키로 제어되며 코드를 저장할 수 없다

CA (Contract Account) : 컨트랙트 어카운트
EOA와 달리 코드에 의해 제어되며 코드 저장이 가능하다

EOA 는 다른 EOA에게 메세지를 보내거나 다른 CA에게 메세지를 보낼 수 있으며 이를 위해 해당 어카운트의
개인키를 사용하여 트랜잭션을 생성하고 서명한다.

그러나 CA는 새로운 트랜잭션을 개시할 수 없다. 대신 다른 트랜잭션에 대한 응답으로 트랜잭션을 실행할 수 있다.

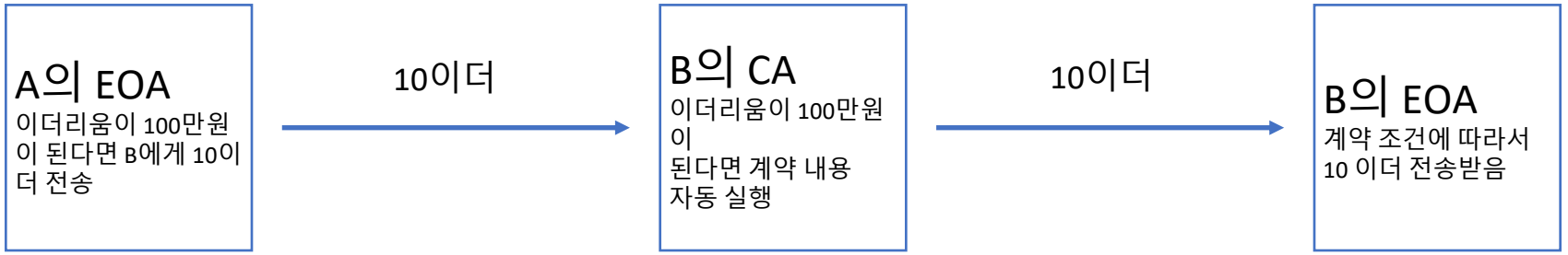
이더리움의 Account

이더리움 어카운트에는 다음과 같은 4개의 정보가 있다

논스(카운터개념), 어카운트의 현재 잔고, 어카운트의 계약 코드(CA만), 어카운트의 저장 공간

송금과 지불수단으로 쓰여지는 비트코인의 지갑과는 달리 이더리움은 '스마트 컨트랙트' 라는 기능을 제공한다. 이러한 계약을 실행하는데 필요한 계정이 CA

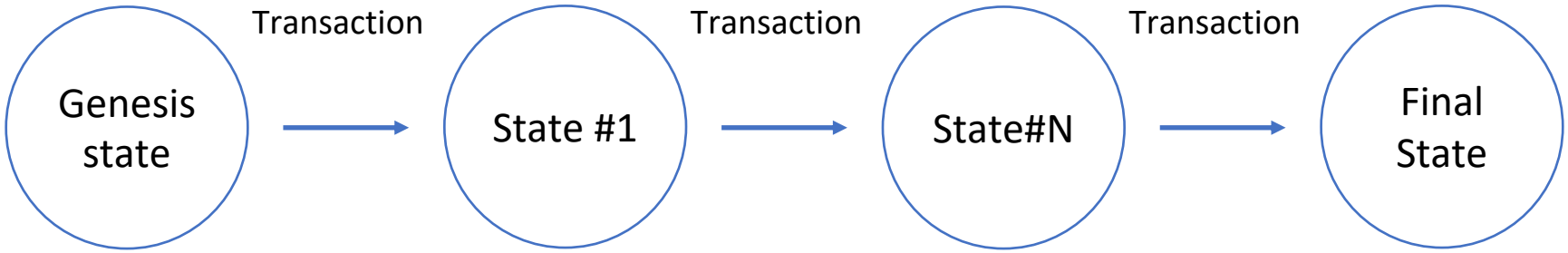
외부소유계정이 스마트 컨트랙트를 만들어서 보내면 그 컨트랙트를 받아 자동으로 처리해주는 계정



이더리움의 상태(State)

어카운트가 모인 구조체

이더리움 프로토콜이 만들어지고 어떠한 트랜잭션도 실행 되지 않은 상태를
Genesis State라 하며 Genesis State 이후 어떠한 트랜잭션이 실행되었다면
State의 정보가 변하게 된다. 또한 블록에는 Final State가 담기게 되어 모든 사용자와 공유한다.



이더리움의 상태(State)

상태변환시스템은 암호화 화폐 장부를 구성하는 하나의 시스템이다.

비트코인에서의 상태란 송금받고 소비되지 않은 트랜잭션의 출력(UTXO)의 합(잔고)이며
송금 요청으로 인해 값이 달라졌다면 상태가 변화했다고 할 수 있다.

이더리움도 마찬가지로 트랜잭션에 의해 상태가 변화하는데 이더리움은 송금 기능 이상의 트랜잭션을 수행할 수 있다. 수행 과정은 트랜잭션의 형식이 올바른지, 발신 어카운트의 개인키 서명과 논스값이 일치하는지 체크하고 그렇지 않으면 오류를 반환한다.
또한 트랜잭션을 실행 할 때 지정한 Gaslimit과 Gasprice를 곱한 값으로 수수료를 계산하여
실제 소모된 수수료만큼 차감되어 수신자에게 지정한 금액만큼 송금하거나, 수신처 어카운트가
컨트랙트일 경우 컨트랙트의 코드를 끝까지 혹은 지정한 수수료가 전부 소모될 때까지 수행하게 된다
. 남은 수수료는 다시 발신자에게 돌아가게 되고 소모된 수수료는 채굴자에게 보내진다.

스마트 컨트랙트의 동작 방식의 이해

1. 스마트 컨트랙트 코딩 : 구현하고자 하는 내용을 솔리디티와 같은 언어로 코딩
2. 컴파일 : 구현한 소스 코드를 컴퓨터가 이해할 수 있게 기계 언어로 변환
3. 스마트 컨트랙트 배포 : 컴파일 된 EVM(이더리움 가상머신) 코드를 하나의 트랜잭션처럼 블록에 추가시켜
   등록하는 작업

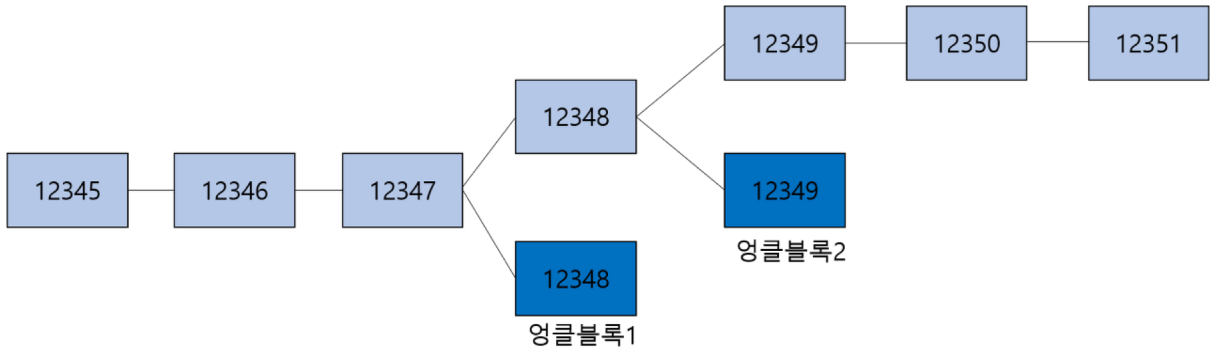
4. 채굴 : 해당 컨트랙트를 배포하는 트랜잭션이 담긴 블록을 채굴하면 스마트 컨트랙트는 CA가 생성됨

5.스마트 컨트랙트 접근 및 사용 : 사용자는 브라우저 혹은 터미널을 통해 생성한 스마트 컨트랙트에 접근하여
   해당 컨트랙트의 CA를 이용하여 정보를 읽고 쓸 수 있다.

이더리움 블록

이더리움 블록은 블록헤더, 엉클블록, 트랜잭션으로 구성되어 있다.

엉클블록 : 동시에 생겨난 블록 중 유효성 검증은 통과되었으나 메인체인에 연결되지 못한 블록
(이더리움에서는 동시에 생긴 블록 중 더 어려운 난이도와 큰 Nonce값을 가진 블록이 메인에 연결됨)



엉클 블록의 해결

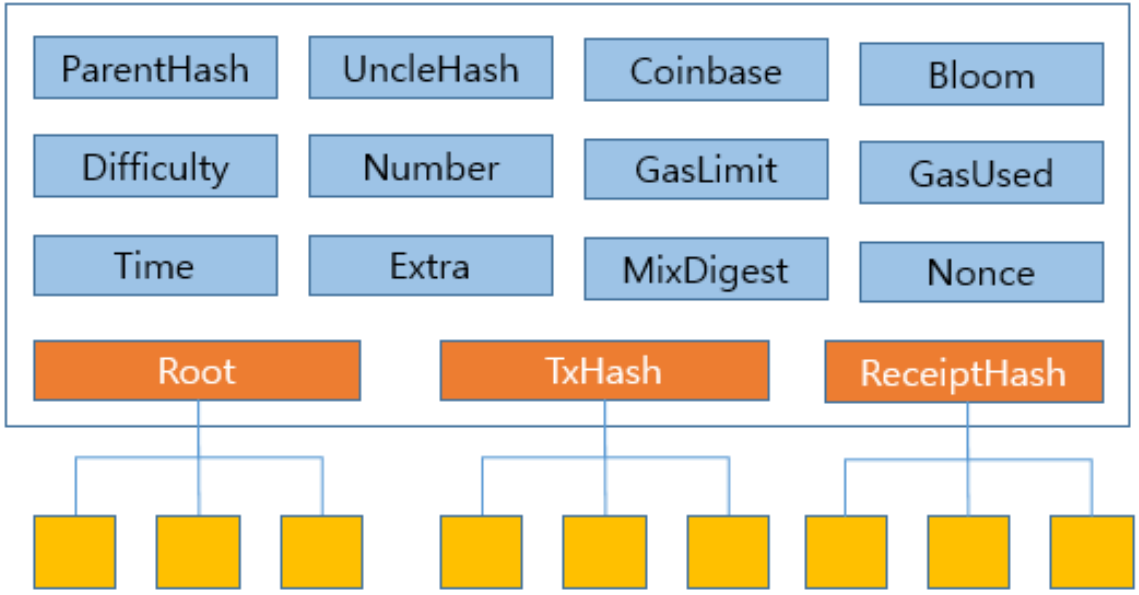
비트코인에서는 메인에 연결되지 못한 블록(Stale block)은 버려지고 가장 긴 체인을 유지하는 블록이 메인 체인에 연결된다. 이더리움은 비트코인에 비해 훨씬 빠르게 블록이 생성되기 때문에 그만큼 동시에
생겨나는 블록이 많아질 수 밖에 없다. 엉클 블록이 많아지면 다음과 같은 문제가 발생한다

- 엉클 블록에 포함된 트랜잭션은 처리가 되지 않기 때문에 트랜잭션 처리의 지연문제 발생
- 엉클 블록은 메인체인에 연결되지 않기 때문에 엉클블록을 발견하는데 사용된 컴퓨팅 파워의 낭비 발생
- 엉클 블록이 생성된 후 다음 블록이 생성된다면 블록 생성시간이 늘어나므로 블록 생성 난이도가 낮아져
  네트워크의 보안 수준이 낮아짐

이더리움에서는 엉클 블록으로 인한 자원 낭비 및 보안 약화를 방지하고자 수정된 고스트 프로토콜을 사용하여
메인 체인에 붙는 블록에게 2개까지 엉클 블록을 포함하게 하여 엉클 블록을 발견한 채굴자에게도 일정 보상을
지급하고 있다.

이더리움 블록헤더

비트코인의 헤더와는 달리 이더리움에는 더 많은 정보를 담고 있다. 비트코인과 달리 블록 넘버와 엉클 블록 해시 및 최대 가스 총합과 사용된 가스량이 담겨있으며 그 밖에도 비트코인 헤더에 있었던 머클 루트가 한 개였지만 이더리움에서는 트랜잭션의 머클 루트, 계정정보의 머클루트, 트랜잭션에 대한 Receipt 의 머클 루트를 포함하고 있다.



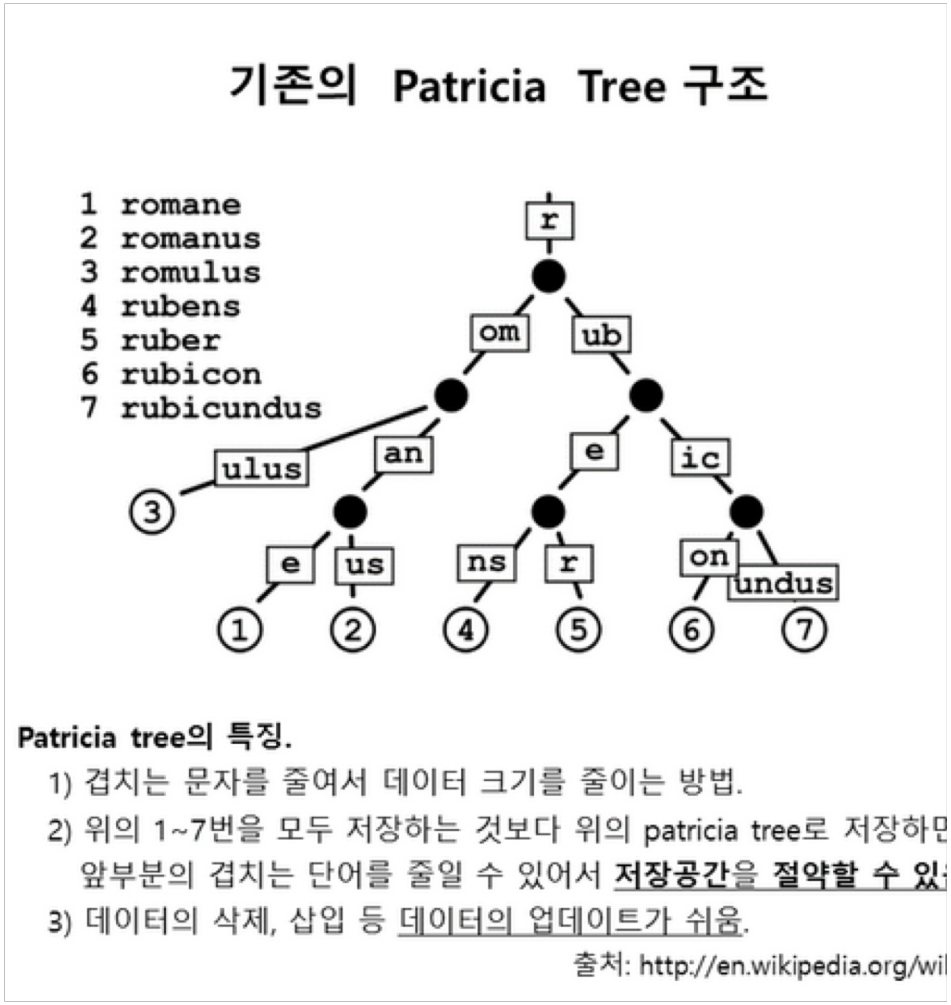
이더리움과 스마트 컨트랙트

이더리움의 머클 트리

머클트리는 블록체인 분산원장을 관리할때 반드시 필요한 알고리즘이다.

블록체인의 크기가 늘어날수록 블록체인의 데이터를 동기화 하는데 많은 용량이 필요하게 된다. 이를 보완하고자 머클트리의 루트 정보를 블록에 저장하여 블록의 정보 조회에 대한 효율성을 높인다.

거래내역(UTXO)를 저장하는 비트코인의 블록체인과는 다르게 이더리움은 계정 정보와 트랜잭션으로 변화한 가장 최근의 상태를 가지고 있다. 이더리움은 계정 정보와 상태 정보를 전부 가지면서도 비트코인보다 빠르게 블록을 생성하게 도와주는 머클 패트리샤 트리를 사용하는데 이는 계정 정보를 효율적으로 저장할 수 있게 도와주고 거래 정보를 검증할 때 효율적으로 루트값을 찾아 검증할 수 있게 역할을 한다.



이더리움의 확장성 문제

이더리움이 가진 스마트 컨트랙트의 기능 구현은 중앙을 거치지 않아도 개인과 개인간의 거래 뿐만 아니라 어떠한 계약조건을 걸어 그 조건이 달성됐을 경우 계약이 이행되는 것이 가능하다는 것을 배웠다.

하지만 이더리움의 트랜잭션 처리속도는 초당 13~ 15건이며 이는 신용카드가 초당 20000건을 처리하는 속도에 비해 현저하게 느리다고 할 수 있다.

이더리움이 추구하는 탈중앙화 네트워크속에서 거의 모든 형태의 어플리케이션을 구현하기 위해서 확장성 문제는 반드시 해결해야 할 과제이다.

확장성 해결을 위해 샤딩, 플라즈마등의 방법을 연구하고 있으며

이를 해결하기 위해 거버넌스를 가진 블록체인(이오스 등)이 존재한다.

- 강의자료 및 서적
  블록체인 인력양성교육 입문과정 '블록체인 인사이드' (저자 : 장성균)
  블록체인 인력양성교육 입문과정 '블록체인 프로그래밍' (저자 : 장성균)
  코어 이더리움 프로그래밍(저자 : 박재현, 오재훈, 박혜영)

- 블로그
  블록체인의 확장성 문제와 솔루션 소개
  https://brunch.co.kr/@curg/3
  외계어 없이 이더리움 이해하기
  https://brunch.co.kr/@bumgeunsong/47
  이더리움 코어의 데이타 계층
  http://ihpark92.tistory.com/45
  이더리움 블록체인_작업증명방식과 블록의 구조
  https://medium.com/@drhot552/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%97%90-%EB%B9%A0%EC%A7%80%EB%8B%A4-95bb404de96d
  비트코인 블록체인 구조
  https://steemkr.com/kr/@niipoong/block-chain-bitcoin-block-chain-structure
  이더리움 개요 및 백서분석
  https://steemit.com/kr/@yahweh87/32-1
  비트코인과 이더리움 블록비교
  http://brownbears.tistory.com/394
  머클 패트리샤 트리 이해하기
  https://medium.com/ethereum-core-research

contact@returnvalues.com