Bitcoin

Bitcoin

- 개념 & 역사
- 기술
- 문제점
- 결론

개념 & 역사

블록 체인

- 블록들을 담아 놓은 “데이터베이스”
- 각 블록은 timestamp와 이웃 블록에 대한 정보를 저장
  - + 구현체 별로 필요한 정보
- 일종의 장부
  - 누구나 접근 가능하고, 분산되어 있으며
  - 거래 내역을 효율적이고(?) 영원히 보존할 수 있고
  - 장부 자체가 거래 프로그램으로서의 기능을 함

비트코인

- 최초의 블록 체인 구현체
- 2009년 사토시 나카토모(가명 추정)에 의해 개발 됨
- 화폐이면서, 동시에 거래 프로그램
  - 비트코인 != 비트 데이터
  - 사용자, 블록 체인이 포함된 거대한 네트워크 자체가 비트코인

기술

비트코인 블록 구조

- Header + Body
- Header : 해당 블록, 이전 블록 이후 블록과 관련한 여러가지 데이터
- Body : 거래 내역

블록 Header

Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	When software upgraded	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

블록 Header

- Version
- Prev Block Header (Hash)
- Merkle Root
- Timestamp
- Bits
- Nonce

블록 Header

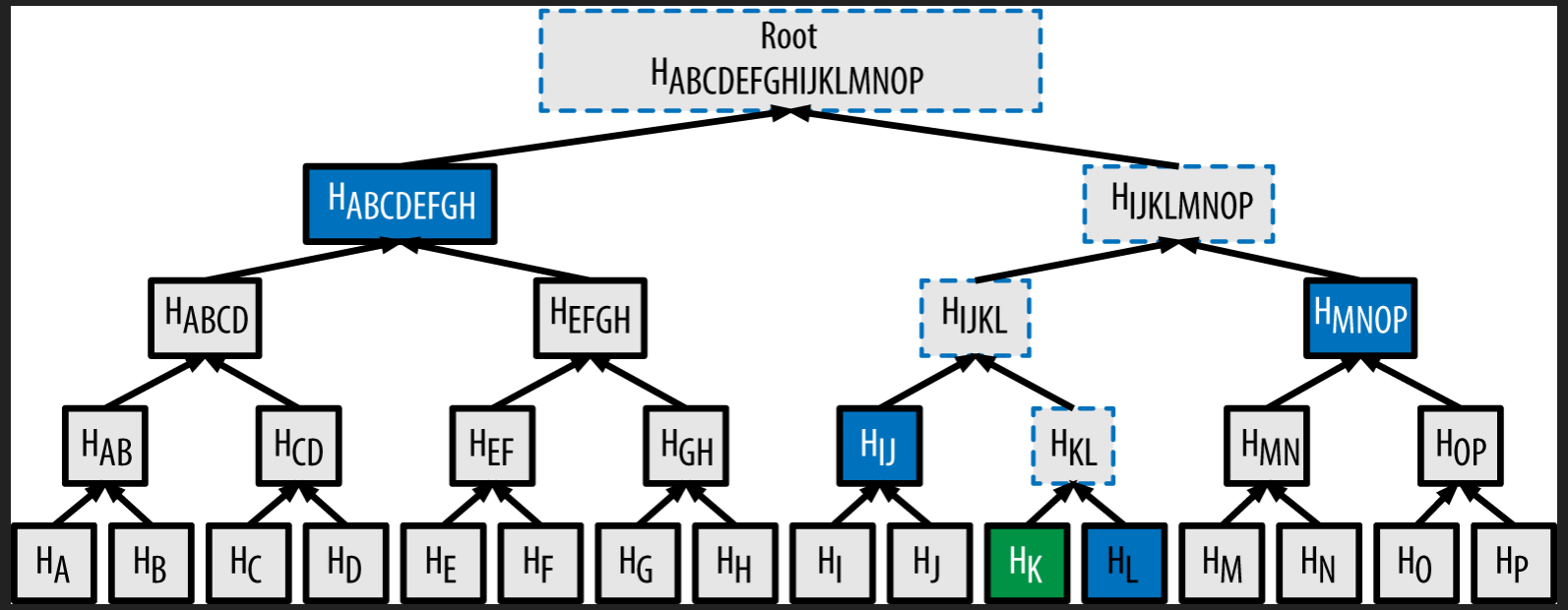
- Version
  - 블록 버전 (현재 ver. 2)

- Prev Block Header (Hash)
  - 이전 block header에 대한 SHA-256 해시 값
  - 이 값을 통해 이전 block의 위변조 여부를 확인

블록 Header

- Merkle Root
  - Body의 Root node의 SHA-256 해시 값
- Timestamp
  - 블록이 생성된 시간 (UNIX TIME)
- Bits & Nonce
  - 채굴과 직접적으로 연관된 값

블록 Body


Root
HABCDEFGHIJKLMNOP
HABCDEFGH
HIJKLMNOP
HABCD
HEFGH
HIJKL
HMNOP
HAB
HCD
HEF
HGH
HIJ
HKL
HMN
HOP
HA
HB
HC
HD
HE
HF
HG
HH
HI
HJ
HK
HL
HM
HN
HO
HP

블록 Body

- Merkle Tree (Binary Hash Tree) 구조
  - 각각의 노드가 거래 내역을 저장
  - 특정 노드가 트리에 포함되어 있는 가를 판단하는 데에 O(log(n))
  - → 거래 내역의 위변조 여부 판단

채굴 & 거래

- 채굴 : 새로운 블록을 생성하는 과정
- 거래 : 비트코인을 화폐로 사용하여 거래하는 것

- Point : 채굴과 거래는 서로 연계된 과정
- 비트코인을 거래하기 위해선 다른 채굴이 이루어져야 함

채굴

- 새로운 블락을 생성하는 과정
  - 블록 체인(linked list)의 끝에 새로운 블락을 추가하는 것

채굴

- 새로운 블록 Header의 SHA-256 해시 값이 특정 값 이하가 되도록 하는 블록을 찾는다

- ex) 2^{20} 이하인 블록을 찾을 확률:
  - $2^{20} / 2^{256} = 9.05 * 10^{-72}$

비트코인 Header (Reminder)

- Version
- Prev Block Header (Hash)
- Merkle Root
- Timestamp
- Bits
- Nonce

비트코인 Header (Reminder)

- ~~Version~~
- ~~Prev Block Header (Hash)~~
- Merkle Root
- Timestamp
- Bits
- Nonce

비트코인 Header (Reminder)

- ~~Version~~
- ~~Prev Block Header (Hash)~~
- Merkle Root
- Timestamp
- Bits : 얼마나 작은 해시값이 나와야 하는 지를 결정 (2016 블록마다 변경)
- Nonce

비트코인 Header (Reminder)

- ~~Version~~
- ~~Prev Block Header (Hash)~~
- Merkle Root
- Timestamp
- Bits : 얼마나 작은 해시값이 나와야 하는 지를 결정 (2016 블록마다 변경)
- Nonce : 32bit, 채굴자가 마음대로 변경할 수 있는 부분

비트코인 Header (Reminder)

- ~~Version~~
- ~~Prev Block Header (Hash)~~
- Merkle Root : 256bit
- Timestamp : 32bit
- Bits : 얼마나 작은 해시값이 나와야 하는 지를 결정 (2016 블록마다 변경)
- Nonce : 32bit, 채굴자가 마음대로 변경할 수 있는 부분

채굴

- Merkle root, Timestamp, Nonce 값을 바꾸어 가면서 해시 값이 정해진 값 이하가 되도록 하는 새로운 블록을 생성하는 것

After 채굴

- 전체 네트워크 상에 채굴이 완료된 블록을 전송
- 네트워크 상의 다른 노드(채굴자, 유저)들이 이를 검증
- 전체 블록체인에 반영(append)

After 채굴

- 새로운 블록을 채굴한 채굴자에게는 특정량의 비트코인이 지급됨
  - 현 시점(2017년) 기준 12.5BTC
  - 21만 블록이 생성될 때 마다 반감 됨
- 비트코인은 어떻게 지급되는 가?
  - 거래 방식을 살펴보자

거래

- Base) 공개키 암호화 (ECDSA)
  - 기밀성
  - 사용자 인증 (MAC)

거래

- A가 B에게 돈을 주는 상황
  - A는 B에게 돈을 주지만, 사용하는 건 B만 가능해야 함
    - 기밀성
  - B는 A가 돈을 보냈다는 걸 알 수 있어야 함
    - 사용자 인증

거래

- B는 개인키-공개키 페어를 생성
  - 공개키 (계좌번호) 를 공개
- A도 개인키-공개키 페어를 생성
  - 공개키를 공개
  - 개인키로 데이터를 암호화

거래

- A
  - 수신자를 B의 계좌로 하는 (B의 공개키로 암호화 된) 거래 내역을 규격에 맞춰서 생성
  - 자신이 보냈다는 걸 확인할 수 있게 하기 위해 자신의 개인키로 암호화

거래

- B
  - 거래 내역을 자신의 개인키로 복호화 할 수 있음
  - A가 보냈다는 것을 A의 공개키로 인증 가능

거래

- 그런데
  - A랑 B가 서로 확인하면 그걸로 되는 건가?
  - 그렇지 않다

거래

- 물음
  - B는 A가 보낸 돈이 가짜가 아닌지 어떻게 알지?
  - 네트워크 상의 다른 노드들은 이 돈의 무결성을 어떻게 알지?

- 답
  - 모든 거래내역을 기록하자

거래

- 물음
  - 근데 그걸 누가 기록할 건데?
- 답
  - 모두가 함께 기록하자
  - 블록 체인!

거래

- 새로 생성되는 블록에 새로 생성되는 거래 내역을 저장하자

비트코인 Body (Reminder)

- Merkle Tree (Binary Hash Tree) 구조
  - 각각의 노드가 거래 내역을 저장
  - 특정 노드가 트리에 포함되어 있는 가를 판단하는 데에 O(log(n))
  - → 거래 내역의 위변조 여부 판단

거래

- 즉, 거래가 완료되기 위해선
  - 해당 거래 내역을 포함하는 블록이 생성되어서 블록체인에 추가 되어야 함
  - 따라서 아무도 채굴을 하지 않으면 거래 성사가 불가능

  - 모두가 공유하는 블록체인 = 위변조 방지

채굴 보상

- 채굴 보상 지급 방법
  - Coinbase → 채굴자 지갑에 해당하는 거래 내역 추가

문제점

문제점

- 거래량의 한계
  - 블록 생성량 = 거래량
  - 블록 생성은 10분 단위로 이루어지도록 조정 됨

- 거래 방식의 한계
  - 채굴자가 블록에 추가해주지 않으면 거래 성사가 안 됨
  - 수수료
  - 조직적 거부

결론

흥미로운 것

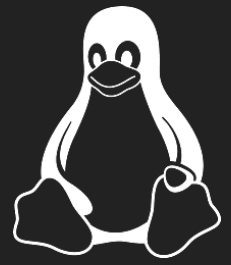
- 비트코인의 비 존재성
  - ‘화폐’에 해당하는 데이터는 없음
  - 존재하는 건 오로지 거래 내역 뿐
  - 계좌번호가 일종의 wrapper 처럼 기능하지만, 실제 화폐는 물리적으로 존재하지 않음

흥미로운 것

- 채굴과 거래의 상호 연관성
  - 채굴을 통해 거래에 사용하는 화폐가 생성
  - 또한 채굴을 통해 거래가 이루어짐

흥미로운 것

- 블록 체인
  - 네트워크의 모든 노드가 블록 체인 전체를 가지고 있어야 함
  - 부하가 되지는 않을까?
    - 현 시점 Bitcoin의 블록 체인은 약 100GB
    - 효율성을 논해볼 필요가 있다




감사합니다

Question?