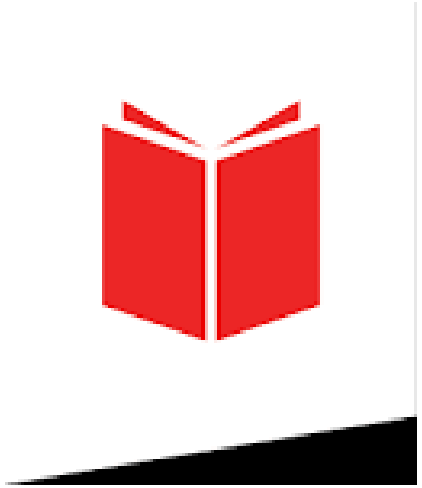
블록체인 개요 및 구조

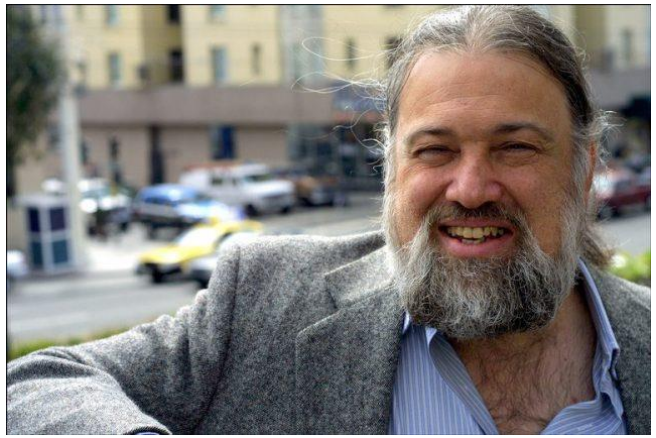
목차



블록체인 이란?

1. 블록체인의 역사

- 1983년 은닉서명(Blind Signature) 기술 개발
  - “추적이 불가능한 결제를 위한 은닉 서명”, David Chaum, 1982
  - 거래 당사자의 신분을 노출시키지 않고 결제 사실을 검증하는 기술을 다룸
  - 제안한 디지털 서명 기술과 암호학 관련 개념들은 암호화폐의 근간을 이루는 기술로 발전



David Chaum

출처 : https://www.blockinpress.com/

1. 블록체인의 역사

- 1989년 DigiCash 설립 (David Chaum)
  - 자신의 아이디어 기반으로 만든 디지털화폐 회사
  - 암호화, 개인키 및 공개키, 블라인드 서명 기술 적용
  - 디지털화된 달러에 고유한 Hash 값을 붙여 만들어진 세계 최초의 암호화폐 'ECash'를 출시
  - ECash는 은행이 모든 거래 내역을 알고있는 신용카드와 달리, 거래 내역을 제3자가 알 수 없는 익명성을 보장
  - 1994년 DigiCash는 ECash를 사용한 첫 전자 결재에 성공하고, 1995년 미국의 소규모 은행과 파트너십을 맺어 ECash 디지털 화폐를 운영하기 시작
  - 프라이버시 보호보다는 더 편리하고, 보편화된 신용 카드를 선호하는 소비자들에게 외면당해 파산

1. 블록체인의 역사

- 1997년 HashCash 기술 개발
  - Adam Back은 1997년 Email Spam과 DoS 공격 막기위한 PoW (Proof of Work) 시스템으로 Hashcash를 제안

- Hashcash
  - Hashcash는 대량 스팸메일을 막기 위해 개발한 PoW시스템
  - 시간과 비용 부담을 주어 대량 스팸메일 발송을 못하게 하려는 목적으로 개발됨
  - 이메일을 발송하기 위해서는 해시캐시 스탬프를 미리 받아야 하는데, 이 스탬프를 받으려면 컴퓨터 연산을 통해 일정한 hash를 찾도록 하는 작업증명(PoW) 과정을 거치도록 함
  - 해시캐시가 도입한 작업증명 방식은 이후 사토시 나카모토가 개발한 비트코인(bitcoin)에 적용됨

Adam Back

출처 : http://wiki.hash.kr/

1. 블록체인의 역사

- 1998년 비트골드(Bit Gold) 기술
  - 닉 재보(Nick Szabo)는 1998년에 비트코인의 기원 으로 불리는 “bit gold”라는 가상 화폐의 원리와 구조를 고안
  - 탈중앙화 디지털 화폐로 참여자들이 컴퓨팅 자원을 통해 암호화 퍼즐을 푸는 방식
  - 같은 네트워크에 있는 다수가 대답이 유효하다고 인정해야 다음 퍼즐로 옮겨갈 수 있음
  - 퍼즐이 풀리고 네트워크 인증을 통과하면 그 퍼즐은 다음 퍼즐의 일부가 됨
  - 복사/붙여넣기를 통한 부정행위 차단으로 디지털 화폐의 이중지불 문제 해결에 기여

Nick Szabo

1. 블록체인의 역사

- 1998년 B-Money 제시
  - “B-Money, Anonymous, Distributed Electronic Cash System, Wei Dai, 1998 (www.weidai.com/bmoney.txt)
  - 비트코인의 탄생에 큰 영향을 준 B-Money 고안
  - 각 참여자가 B-Money 를 얼마나 갖고 있는지에 대한 정보를 모든 참여자가 별도의 데이터베이스에 해시함수로 암호화하여 서로 연결된 블록으로 저장
  - 거래 발생에 의해 새로운 블록을 추가할 때 가장 먼저 암호를 풀어 성공한 참여자에게 B-Money 인센티브를 주는 작업증명(PoW)과 보유한 암호화폐의 양에 따라 일부 참여자에게만 우선적으로 인센티브를 주는 지분증명(PoS) 방법도 제안

웨이 다이(Wei Dai)

* PoW : Proof of Work, PoS : Proof of Stake

1. 블록체인의 역사

- 1998년 B-Money는 전자현금 시스템 성립을 위한 다섯가지 전제조건을 제시

1.상당한 양의 컴퓨터 계산과 그에 대한 입증

2.컴퓨터 작업을 위한 보상체계

3.모든 멤버에 의해 인정받고 업데이트 되는 집합적인 그룹 원장

4.펀드 이전은 수집된 그룹 원장에 기재되고 암호화 기술 해시를 통해 입증

5.모든 거래는 네트워크에서 입증된 공개키 암호화를 사용한 디지털 서명이 필요

1. 블록체인의 역사

- 2008년 Bitcoin (Satoshi Nakamoto)
  - Bitcoin은 블록체인 기술을 기반으로 만들어진 최초의 암호화폐
  - Bitcoin의 화폐 단위는 BTC
  - “Bitcoin: A Peer-to-peer Electronic Cash System”
  - “Proof of Work”
  - Peer-to-peer Network
  - 안전한/분산화된 원장 관리
  - SHA-256 해시 알고리즘 기반의 작업증명(PoW) 방식으로 채굴
  - 비트코인의 시가 총액은 2018년 7월 기준으로 1,000억 달러, 즉 약 100조원으로서, 시가 총액 1위의 암호화폐임

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

1. 블록체인의 역사

- 2009년 bitcoin 배포
  - 2009년 1월 사토시 나카모토라는 가명을 쓰는 사람이 C++ 언어로 개발함
  - 2009년 1월 3일 사토시 나카모토는 비트코인을 개발하여 최초의 블록인 제네시스 블록(genesis block)을 생성
  - 1월 10일 사토시 나카모토는 C++ 프로그래밍 언어로 작성한 비트코인 소스 코드를 이메일로 무료 오픈 소스 방식으로 배포함

1. 블록체인의 역사

- 2009년 최초의 bitcoin 채굴
  - 2009년 1월 Satoshi Nakamoto는 본인의 PC를 이용하여 50 BTC를 채굴한 뒤, Hal Finney (PGP 개발자, Phil Zimmermann에 이은 2인자) 에게 10 비트코인을 송금
  - Hal Finney는 본인의 PC에서 bitcoin을 채굴했는데, 당시 블록 번호가 70번대였으며, 창시자를 제외하고는 최초의 비트코인 채굴자가 되었음

Hal Finney

출처 : http://www.seunghwanhan.com/

1. 블록체인의 역사

- 2009년 bitcoin 최초 결제
  - 비트코인 거래가 시작되었지만 몇 년간은 크게 주목받지 못했고, 매니아 층을 중심으로 조금씩 퍼져나감
  - 2009년 10월 첫 환율 공시 당시 1달러 = 0.00076BTC이 가능해지며 보급이 가속됨
  - 2010년 5월 22일 미국 플로리다에 사는 라스즐로 핸예츠(Laszlo Hanyecz)라는 프로그래머가 비트코인을 이용해 처음으로 피자 2판을 구매
  - 당시 피자 2판의 가격은 40달러로서, 10,000 비트코인을 지불했음. 2019년 5월 7일 기준으로 10,000 BTC는 약 691억원에 해당하는 어마어마한 금액

라스즐로 핸예츠(Laszlo Hanyecz)가 비트코인으로 주문한 피자 (2010년)

2014년 Blockstream 설립 (Adam Back)

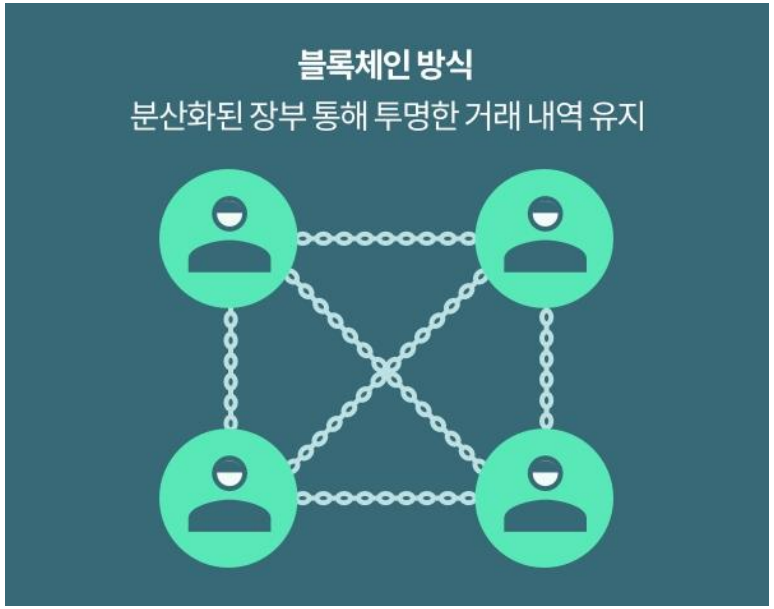
- Adam Back은 Blockstream라는 회사를 창업하고, 2017년 8월 15일 지구상의 거의 모든 사람들이 인터넷이 없이도 비트코인 블록체인 데이터에 접근할 수 있도록 인공위성을 띄우는 blockchain satellite 서비스를 시작함
- 블록체인 satellite는 세계 첫 퍼블릭 인공위성 서비스로서, 누구나 네트워크의 제약 없이 비트코인 전체 거래내역을 저장할 수 있는 비트코인 노드를 운영하고 유지할 수 있도록 지원함

2. 블록체인 정의

- BlockChain이란
  - 데이터 분산 저장 기술의 일종
  - block 단위의 데이터를 chain처럼 연결하여 저장
  - 저장된 데이터를 모든 사용자에게 분산하여 저장
  - 이러한 분산저장 특성 때문에 분산원장기술 (분산장부기술, Distributed Ledger Technology) 이라고 불리기도 함
- 블록체인은 비트코인의 바탕이 되는 '체계'
- 비트코인은 블록체인을 '화폐'에 응용한 결과물

2. 블록체인 정의

- 분산 공개 장부
  - 블록체인 기술은 모든 사용자 간 동일한 장부(데이터)를 공유함으로써 중앙의 관리 없이 투명한 내역 관리가 가능



출처 : 소프트웨어 중심사회

2. 블록체인 정의

- 기존 거래 방식
  - 기존 거래방식은 은행이 모든 거래내역을 가지고 있었음
  - A가 B에게 1만원을 송금한 사실을 중앙은행이 증명함
  - 거래 당사자들은 중앙은행을 신뢰하고 거래내용 증명을 모두 맡기는 형태

- 블록체인 거래 방식
  - 거래내역을 중앙은행이 아닌 여러곳에 저장함
  - A가 B에게 1만원을 송금한 사실을 참여하고 있는 모든 노드들에게 저장함
  - 송금한 사실을 참여하고있는 모든 노드들이 증명함

통화의 형태 (Type of Curreny)

현금, 디지털화폐, 가상화폐와 암호화폐 비교

	현금(법정통화) Fiat Currency	디지털 화폐 Digital Currency	가상화폐 Virtual Currency	암호화폐 Cryptocurrency
				
화폐 형태	주화(금속) 또는 지폐(종이)	디지털	디지털	디지털
화폐 구분	법정통화	법정통화	가상화폐	암호화폐
적용 법규	O	O	X	X
사용처	모든 거래	가맹점	가상공간	가맹점
발행기관	중앙은행	금융기관	비금융기관	X
법정통화와의 교환성		법정통화로 충전, 잔액은 법정통화로 환급가능	가상화폐를 법정통화로 교환할 수 없음	법정통화와 자유로이 교환됨

자료: 한국은행, 피넥터, 유진투자증권

https://brunch.co.kr/@bzconomics/19

블록체인 구조

https://coinmarketcap.com

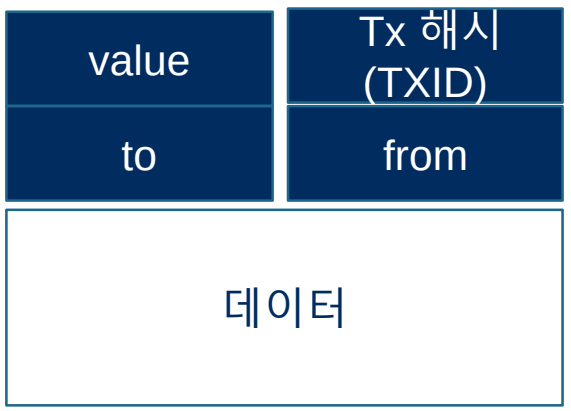
3. 블록체인 구조

- 트랜잭션
  - 저장할 데이터를 트랜잭션 단위로 생성
- 블록
  - 트랜잭션의 집합을 블록단위로 기록

이 데이터들 중 TXID를 생성하는데 필요한 항목은 아래 정보이다.

ver : 소프트웨어 버전 정보
input_count : 입력값 개수
prevout_hash : 이전 UTXO 출력 Hash
sequence : 현재 장애가 있는 Tx-대체기능, 0xffffffff로 설정
lockTime : 잠금시간
scriptSig : 해제 스크립트
value : BTC가치
scriptPubKey : 잠금 스크립트

트랜잭션 구조 예시



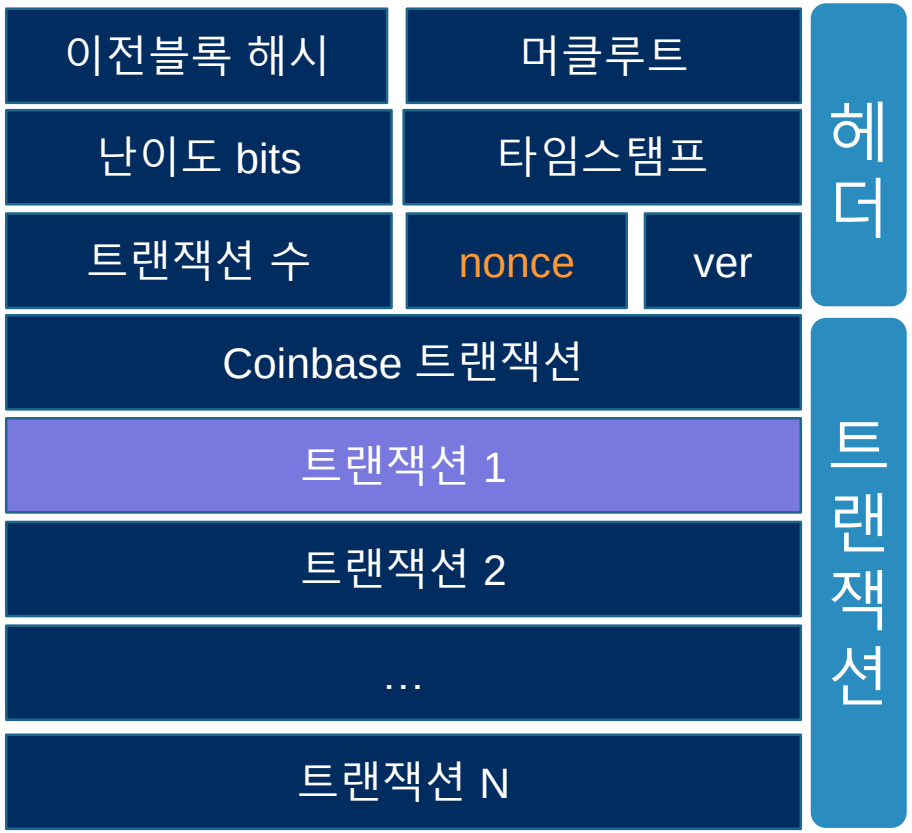
블록 구조 예시

If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year : block header

3. 블록체인 구조

- 블록
  - 트랜잭션의 집합을 블록단위로 기록

블록 구조 예시



블록 헤더 (80bytes)

- 블록버전: 소프트웨어버전과 동일(4bytes)
- 이전블록해쉬: 이전블럭헤더의 SHA256해쉬, 블럭생성시 기록(32bytes)
- 머클루트: 거래가 발생할때마다 값이 업데이트됨;SHA256해쉬(32bytes)
- 타임스탬프: 몇 초마다 업데이트 됨(Current timestamp as seconds since 1970-01-01T00:00 UTC)
- 난이도bits: 작업증명 난이도;특별한 공식을 사용해서 변환함(Current target in compact format); 4bytes
- Nonce: 4바이트 크기의 nonce값

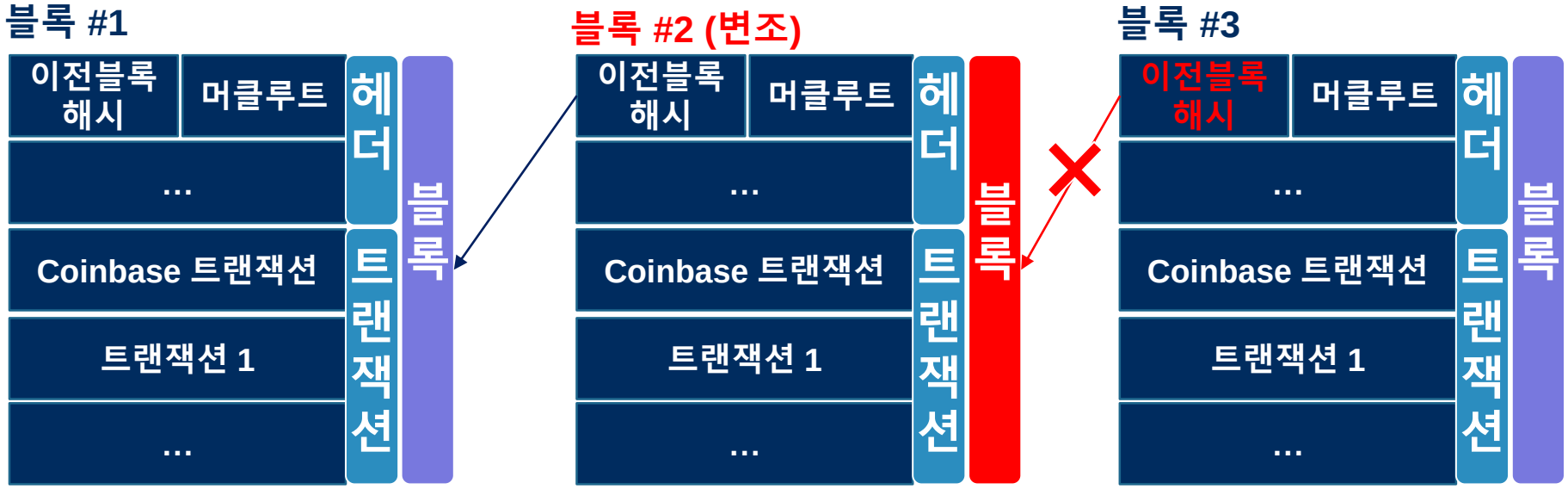
- 트랜잭션수: 기록된 거래의 개수
- Coinbase 트랜잭션: 블록생성시 만들어지는 최초거래;채굴성공시 비트코인 지급이 되는 거래가 됨
- 트랜잭션: 실제비트코인의 거래기록

3. 블록체인 구조

- 체인
  - 블록들이 '이전 블록 해시'값을 이용하여 서로 연관되는 형태

3. 블록체인 구조

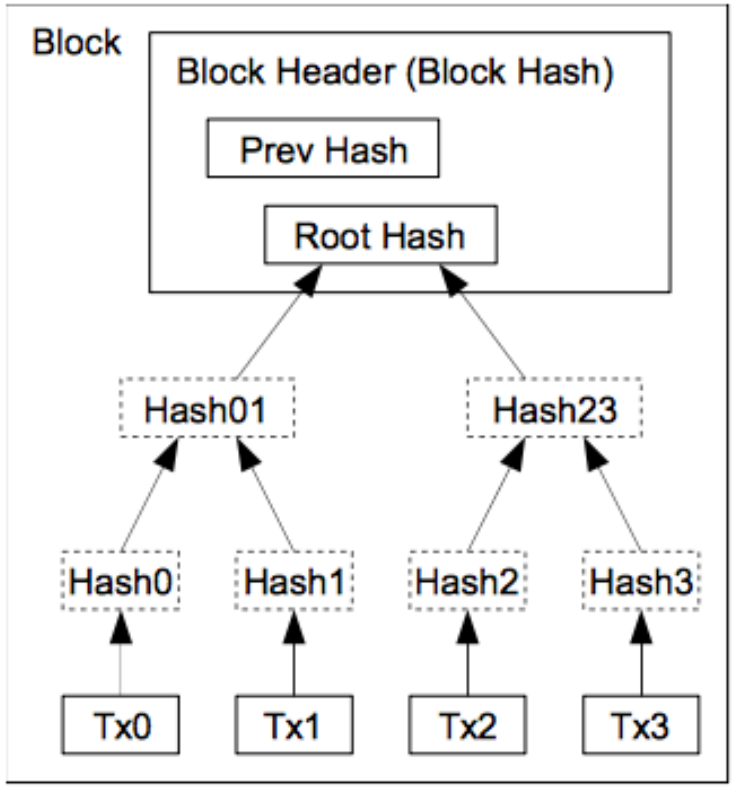
- 체인에 의해 데이터 변조 방지
  - 블록 #2의 변조 시, 블록 #3에 저장된 이전블록 해시가 변조 된 블록 #2를 가리키지 않으므로 체인 형태로 연결하여 저장 할 수 없음



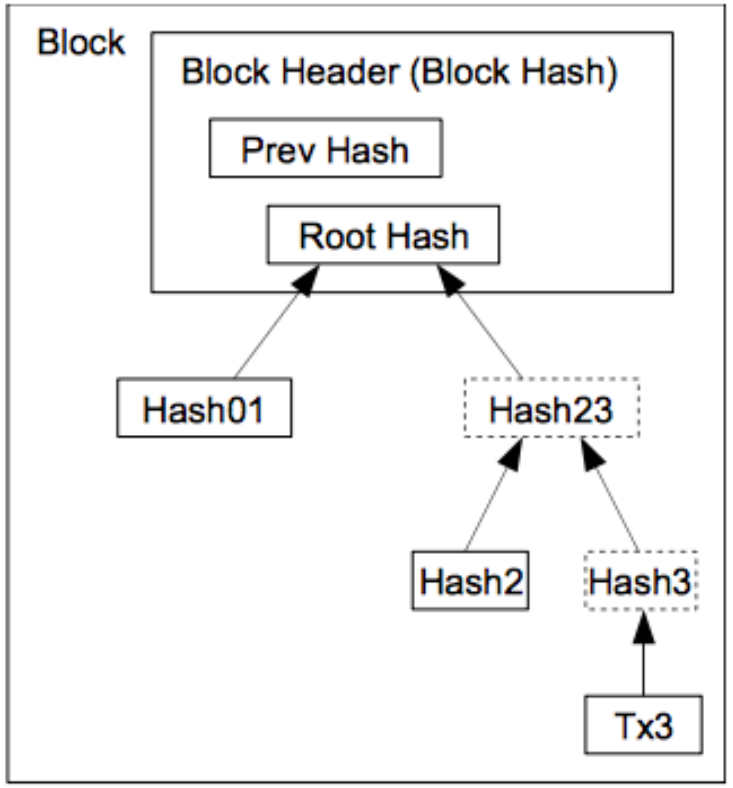
3. 블록체인 구조 : 블록 헤더

- Previousblockhash
  - 해당 블록의 직전에 위치한 블록의 해쉬
- Merklehash
  - 블록에 포함된 각 트랜잭션의 해쉬를 2진 트리 형태로 구성할 때, 트리 루트에 위치하는 해쉬값

3. 블록체인 구조 : Merkle Hash Tree



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

3. 블록체인 구조 : 블록 헤더

- Time stamp
  - 블록이 생성된 시간
- 난이도 bits
  - 난이도 조절을 위한 값

비트코인 블록 540277 에 있는 난이도 정보를 보자.

- 링크: https://www.blockchain.com/en/btc/block-height/540277
- Difficulty 는 6,727,225,469,722.53
- Bits 는 388618029 = 0x1729D72D

Block Height 540277 Blocks at depth 540277 in the bitcoin blockchain

Summary	
Height	540277 (Main chain)
Hash	0000000000000000000c34c1851b84f20f300cea21e56e32ff2cbc80f5c2bca3
Previous Block	0000000000000000011ea3ef795f91657c03a431e88278d230069aa2c0fba89
Next Blocks	0000000000000000000d4577a7a07a7c7beea9c17d6dbb98846f28af86c75c98
Time	2018-09-07 01:52:14
Received Time	2018-09-07 01:52:14
Relayed By	BTC.TOP
Difficulty	6,727,225,469,722.53
Bits	388618029

- Difficulty 는 가장 쉬운 난이도 (=Genesis 블록의 난이도) 의 몇 배나 어려운가를 의미한다. 6,727,225,469,722.53 배나 어렵다는 것이다.

3. 블록체인 구조 : 블록 헤더

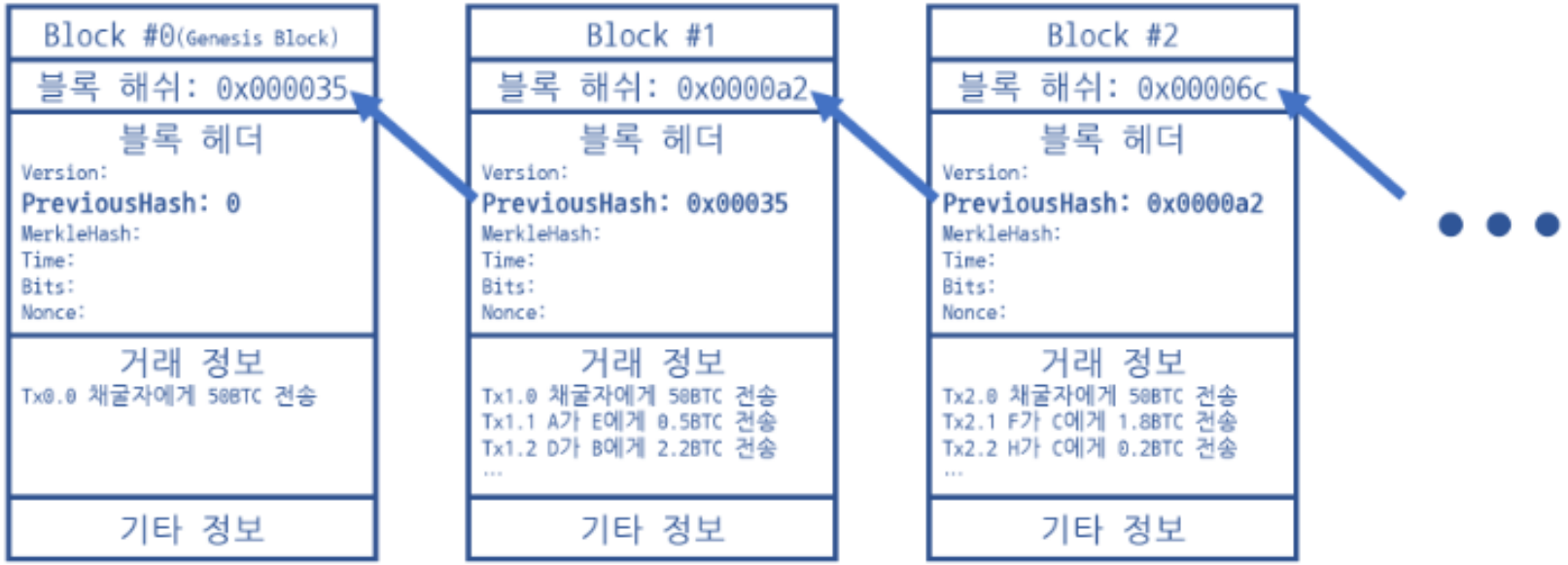
- Nonce
  - 최초 0에서 시작하여 조건을 만족하는 해쉬값을 찾아낼때까지의 1씩 증가하는 값
- Version
  - 소프트웨어/프로토콜 버전

3. 블록체인 구조 : 블록 해쉬

- 블록의 식별자 역할
- 6가지의 블록 헤더 정보를 입력값으로 하여 SHA256 해쉬 함수를 적용해서 계산되는 값
- 이름은 블록 해쉬이지만 그 값은 블록 전체를 해쉬한 값이 아니라, 블록 헤더를 해쉬한 값

3. 블록체인 구조 : 블록 헤더

- 블록 헤더의 Previousblockhash값을 포함하여 앞의 블록과 이어짐

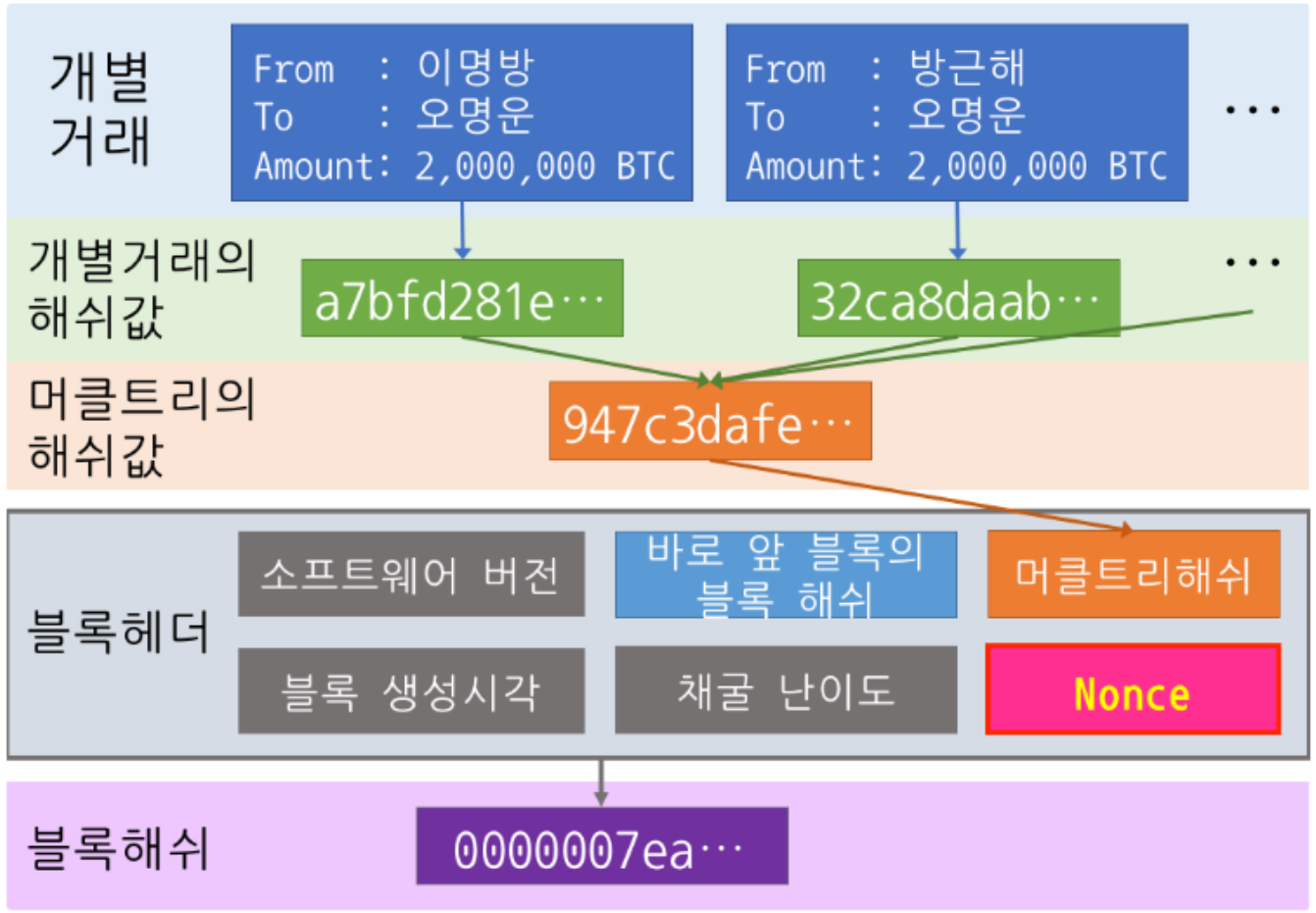


출처 : https://homoefficio.github.io

3. 블록체인 구조 : 블록생성

- 개별 거래정보는 머클트리 해쉬값인 Merklehash로 집약
- Version, Previousblockhash, Merklehash, Time, Bits 5가지 헤더 정보는 블록해쉬를 만드는 시점에 확정되어 있음
- Nonce값을 구해서 블록해쉬 값을 구하고 이 블록 해쉬값을 식별자로 가지는 유효한 블록을 만들어 내야함 - 작업증명

3. 블록체인 구조 : 블록생성



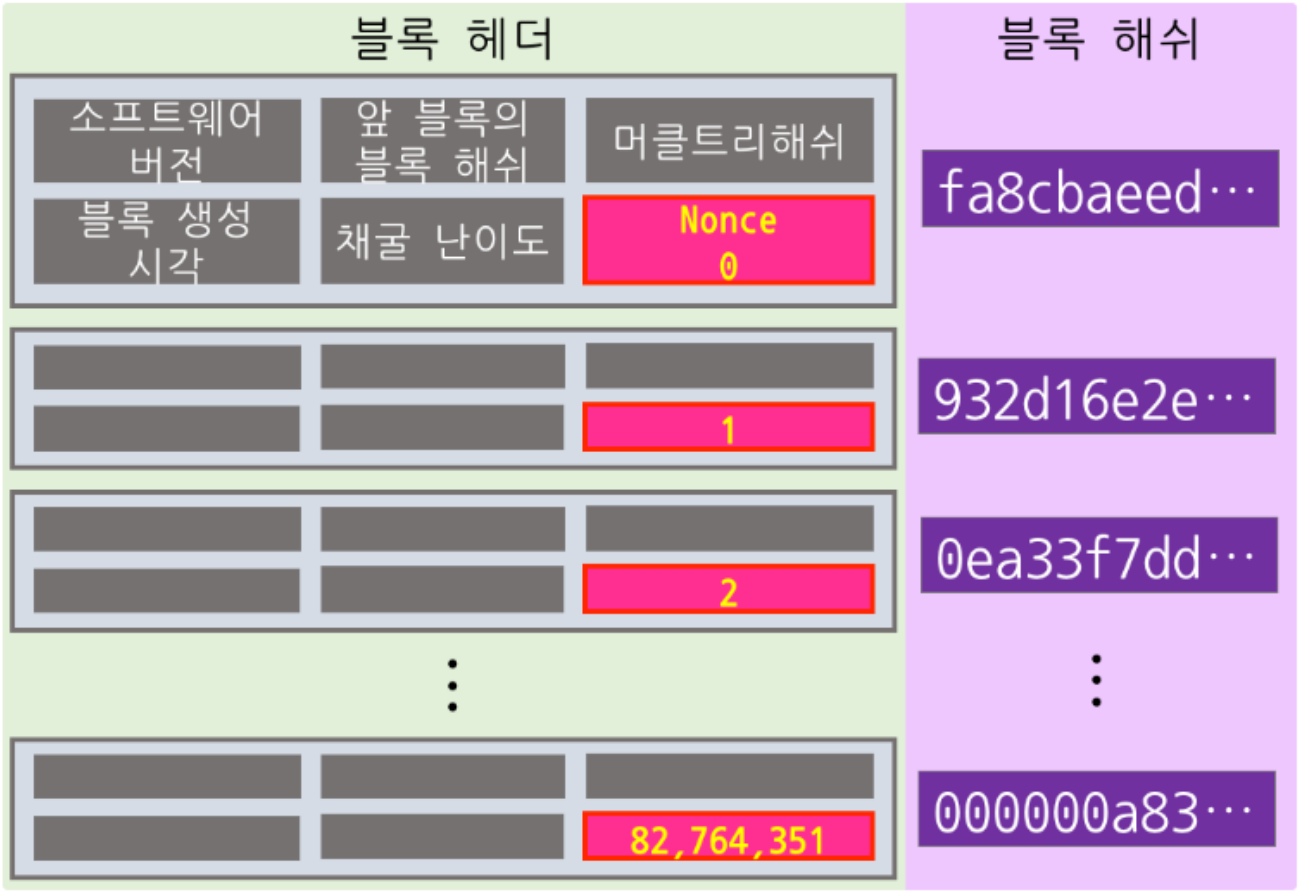
출처 : https://homoefficio.github.io

3. 블록체인 구조 : 작업증명(채굴)

- Nonce값을 구해서 블록해쉬 값을 구하고 이 블록 해쉬값을 식별자로 가지는 유효한 블록을 만들어 내야함
- Nonce값은, 이 Nonce값을 입력값 중의 하나로 해서 계산되는 블록 해쉬값이 특정 숫자보다 작아지게 하는 값을 말함

3. 블록체인 구조 : 작업증명(채굴)

- 블록해쉬가 000000a84...라는 특정값보다 작게 나오게 하는 Nonce값을 구하는 과정



출처 : https://homoefficio.github.io

3. 블록체인 구조 : 작업증명(채굴)

- Bits 는 비트코인만의 target 표현방식이라고 보면 된다.
  - 0x1729D72D 라는 건
  - 0x29D72D * 2 ** (8 * (0x17-3)) 이라는 거다.
  - 수식을 좀더 전개하면 0x29D72D * 2 ** (160) = HEX 로 표현시 0x29D72D 뒤에 HEX 0이 40개 붙는다.
  - 이걸 HEX 로 표현하면 0x 0000 0000 0000 0000 0029 D72D 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

채굴이란 결국 다음과 같다.

생성될 수 있는 해시 2 ** 256 개
0x 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 부터 0x FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 까지 중에서
0x 0000 0000 0000 0000 0029 D72D 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 과 같거나 작은 값이 나올때까지 해시를 계속 생성하는 것이다.
참고로, 제네시스 블록의 Bits == 가장 낮은 난이도 일때의 타겟값은 아래와 같다. - 링크: https://www.blockchain.com/en/btc/block-height/0 - Bits: 486604799 = 0x1D00FFFF 0x 0000 0000 ffff 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

0x00ffff * 2**(8*(0x1d - 3)) =
0x00000000FFFF0000000000000000000000000000000000000000000000000000

참고

The method of obtaining the difficulty from bits


```
{
  "hash":"00000000000000370f501bad48cdfb6a6713b9d51f692c5dbc90039a9d278e5",
  "ver":2,
  "prev_block":"0000000000000010c9d451f5a48f4d733b556a240d31ac226db2637f496be0a",
  "mrkl_root":"3353915c69a23307f102654616d5a0fecedabb900be33b2313169a7eb2a43bd4",
  "time":1388342997,
  "bits":419668748,
  "nonce":1290749339,
  "n_tx":56,
  "size":32696,
  "tx":[
```


2013-12-29 18:49:57

1. Bits : 419668748
   hex(bits) = 0x1903a30c

```
>>> print hex(419668748)
0x1903a30c
```

2. Target :
   0x03a30c * 2**(8*(0x19 - 3))

```
>>> print hex(0x03a30c * 2**(8*(0x19 - 3)) )
0x3a30c0000000000000000000000000000000000000000000000000L
```

   = 0x3a30c0000000000000000000000000000000000000000000000000L

3. Difficulty = maximum_target / current_target
   = 0x00000000FFFF0000000000000000000000000000000000000000000000000000 /
     0x3a30c0000000000000000000000000000000000000000000000000L
   = 1,180,923,195

. difficulty = difficulty_1_target / current_target
. The highest possible target (difficulty 1) is defined as 0x1d00ffff
. difficulty_1_target can be different for various ways to measure difficulty. Traditionally, it represents a hash where the leading 32 bits are zero and the rest are one (this is known as "pool difficulty" or "pdiff"). The Bitcoin protocol represents targets as a custom floating point type with limited precision; as a result, Bitcoin clients often approximate difficulty based on this (this is known as "bdiff")
. The **target** is a 256-bit number (extremely large) that all Bitcoin clients share. The SHA-256 hash of a block's header must be lower than or equal to the current target for the block to be accepted by the network. The lower the target, the more difficult it is to generate a block

3. 블록체인 구조 : 보상

- Nonce 값을 구하기 위해선 엄청나게 많은 CPU, 전기가 소모됨
- 보상은 새로 발행되는 비트코인과 해당 블록에 포함되는 거래의 거래 수수료의 합
- 채굴에 성공한 채굴자에게 새로 만들 블록에 일정량의 비트코인을 입금시켜주는 첫 거래를 만들어 줌
- 비트코인의 경우,
  - 1~21만개 블록까지는 블록마다 50BTC 지급
  - 21만 ~ 42만개 블록까지는 보상금이 50%감소하여 25BTC 지급
  - 42만개 ~ 63만개 블럭 : 12.5BTC 지급

Q & A