비트코인 블록체인 동작원리 및 진화

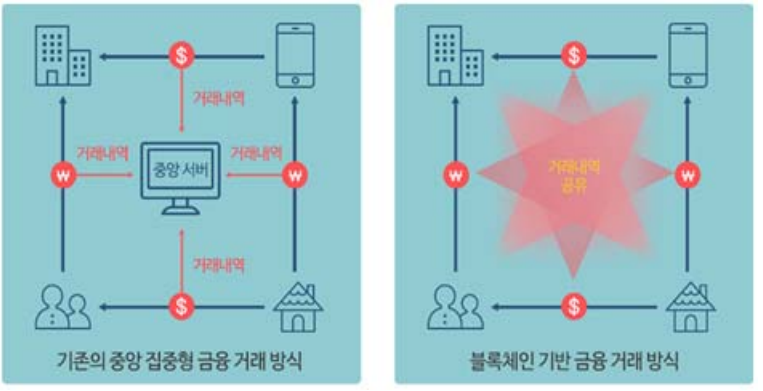
김원
한국인터넷진흥원 연구위원

비트코인은 2008년 10월 31일 사토시 나카모토라는 정체불명의 인물이 발표한 논문에서 시작되었다. 비트코인은 P2P 네트워크 상에서 구현한 최초의 암호화폐이다. 또한, 블록체인 기술은 비트코인을 구현하기 위해 만들어졌기 때문에 블록체인과 비트코인은 동시에 탄생했다. 이는 P2P 기반의 네트워크에서 TTP(Trusted Third Party, 신뢰할 수 있는 제3자) 없이 거래가 가능한 혁신적인 시스템으로 4차 산업혁명의 기반 기술 중 하나로 기존 인터넷 구조를 바꿀 혁신 기술로 부상하고 있다[6]. 비트코인은 현재 가장 널리 사용되는 블록체인 기반 암호화폐시스템으로 탄생했기 때문에 데이터 구조나 프로토콜이 화폐시스템에 특화되어 있다. 이 때문에 시스템 자체는 범용적이지만 그곳에 흐르는 데이터와 처리를 다른 방법으로 사용하는 데는 한계가 있다. 그래서 다른 영역에서도 적용 가능하도록 다양한 종류의 블록체인 플랫폼이 탄생했다. 따라서, 스마트 계약이라는 개념을 구현한 이더리움과 하이퍼레저 패브릭 등의 다양한 블록체인을 연구하기 위해서는 기본적으로 비트코인의 구조와 동작원리를 아는 것이 중요하다.

I. 서론

2008년 10월 31일 저녁, 사토시 나카모토(가명)라는 사람이 암호화 기술 커뮤니티 메인(Gmane)에 “비트코인: P2P 전자화폐시스템(Bitcoin: A peer-to-Peer Electronic Cash System)”이라는 논문을 발표했다[5]. 이 논문에서 사토시 나카모토는 비트코인을 “전적으로 거래 당사자 사이에서만 오가는 전자화폐”라고 소개하고 “P2P 네트워크를 이용하여 이중 지불을 막는다”고 설명했다. 그리고 약 두 달 뒤인 2009년 1월 3일, 사토시는 논문으로 설명했던 기술을 비트코인이

* 본 내용은 김 원 연구위원(☎ 010-5342-4802, wkim1015@kisa.or.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.



<자료> 블록체인 및 비트코인 보안 기술, 금융보안원

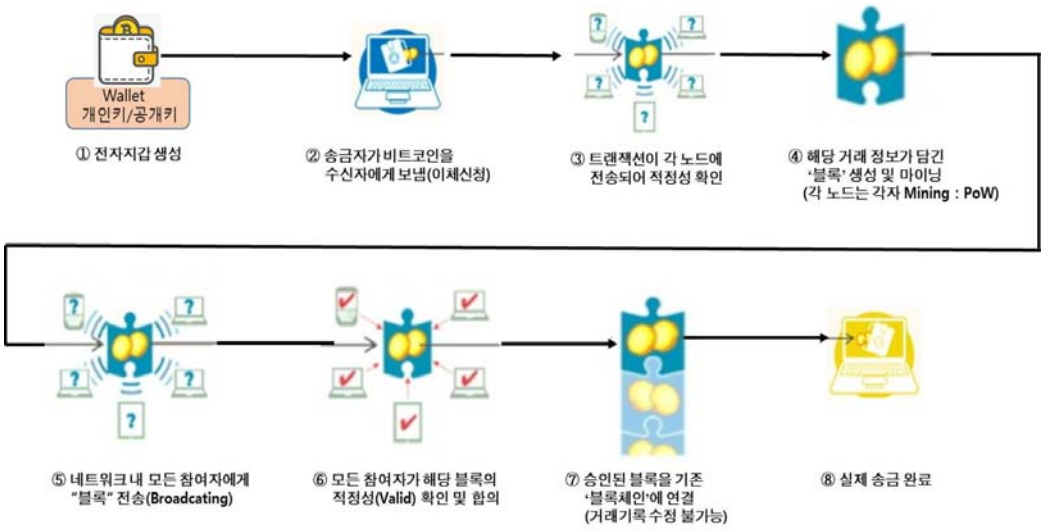
[그림 1] 금융거래 방식 비교

라는 암호화폐로 직접 구현해 보여주었다. 중앙집중형 서버를 중심으로 트랜잭션을 처리하는 기존의 금융 거래방식과는 달리, 비트코인은 신뢰할 수 없는 노드(컴퓨터)들이 연결되어 있는 P2P 네트워크상에서 신뢰할 수 있는 제3자(Trusted Third Party:TPP) 없이 [그림 1]과 같이 트랜잭션이 가능한 금융 거래 방식으로, 정보처리 분야에서 오랜 세월 해결하지 못한 비잔틴 장군 문제(Byzantine General Problem)[11]를 해결한 혁신적인 기술로 출현하였다.

블록체인은 2016년 WEF(세계경제포럼)에서 제4차 산업혁명의 차세대 10대 핵심기술로 선정되었으며, 또한 가트너는 2018년 10대 기술 중의 하나로 선정하였다. 앞으로 전 세계 금융기관 중 80%가 도입 의사를 표했으며, 2025년까지 블록체인으로 인한 경제 규모가 전 세계 GDP의 약 10%에 이를 것으로 기대되고 있다[3].

Ⅱ. 비트코인 블록체인 동작원리

비트코인 클라이언트는 비트코인 코어를 기반으로 개발되었는데, 인터넷에 연결되는 누구든지 다운로드 받아 비트코인을 송금하거나 채굴(마이닝)하는 것 등이 가능하며, 물론 거래소를 통해서 법정화폐로의 환전도 가능하다. 비트코인의 거래 프로세스를 살펴보면 은행과 같은 신뢰할 수 있는 제3자 기관이 없이 거래가 가능한 혁신적인 시스템이다. [그림 2] 및 [표 1]은 비트코인 거래의 전체 흐름도이다.



<자료> Thomson Reuters, 2016. 1.16., 「Blockchain technology: Is 2016 the year of the blockchain?」을 재구성

[그림 2] 비트코인 거래 동작 프로세스

[표 1] 비트코인 거래의 전체 흐름도

라이프 사이클	내용
① 계정(계좌) 생성	전자지갑(Wallet) 생성(개인키, 공개키 자동 생성)
② 거래 생성	비트코인 전송
③ 거래 검증	P2P 네트워크에서 거래 전송
④ 블록 구성 및 생성	노드에서 트랜잭션을 블록 생성
⑤ 채굴 및 보상	블록의 정당성 확보를 위한 채굴
⑥ 블록 검증	P2P 네트워크 전파 및 각 노드의 블록 검증
⑦ 블록체인 생성	블록체인 생성(the longest chain)
⑧ 난이도 조정	14일마다 블록 생성 주기 변경

<자료> https://bitcoin.org/en/developer-reference#block-chain

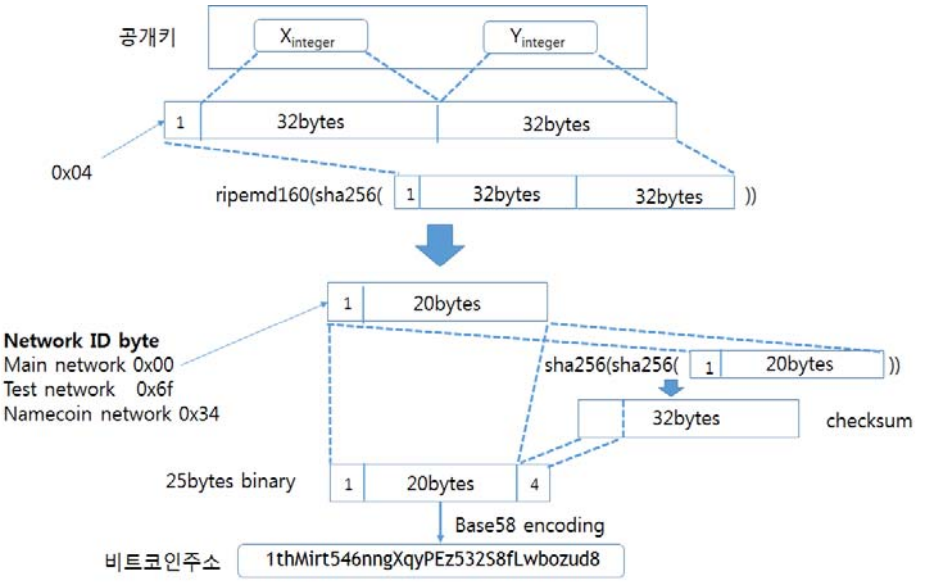
1. 비트코인 주소: 계정(계좌) 생성

은행계좌와 동일한 역할을 하는 계좌를 생성하며, 비트코인을 거래하는 계좌는 다수 개를 생성할 수 있다. 계좌를 생성하면 개인키와 공개키가 자동으로 생성되며, 여기서 개인키는 비트코인을 송금할 때 전자서명하도록 할 수 있는 중요한 키 역할을 한다. 공개키의 경우는 512비트로 길이가 길어서 이를 다시 해시하여 길이를 줄여 사용하는데, 이것이 공개키 해시

방식의 비트코인 주소이다[2].

비트코인에서는 1985년 밀러와 코블리츠가 제안한 타원 곡선 기반 암호(Elliptic Curve Cryptography)를 이용한 공개키 방식을 이용하여 개인키와 공개키를 생성한다. 이산 대수에서 사용하는 유한체의 곱셈군을 타원 곡선군으로 대치한 암호 방식으로 다른 암호 방식에 비해 더 짧은 키 사이즈로 대등한 안전도를 가진다. 예를 들어, RSA 1,024비트 키와 ECC 160비트 키를 갖는 암호 방식은 대등한 안전도를 가진다는 것이다. ECC의 공개키는 두 개의 256비트값으로 정의되어 있다. 256비트 두 개로 구성된 512비트에 유형을 구분하여 8비트 접두부를 합친 520비트, 즉 65바이트가 하나의 공개키이다. 비트코인 클라이언트는 의사난수발생기(PRNG)를 이용하여 256비트의 개인키를 발생하고 나서 타원곡선암호 방식을 사용하여 512비트의 공개키를 생성한다. 비트코인의 경우에는 NIST가 권장하는 타원곡선의 하나인 ECDSA의 파라미터로 secp256k1 타원곡선 $E_p : y^2 = x^3 + 7$을 이용한다. 즉, $E_p : y^2 = x^3 + 7 (\text{mod } p)$의 유한체 상에서 $K = k \times G$를 만족하는 개인키와 공개키를 얻는 방식이다. 타원곡선 상의 이산대수 문제라고 하는 것은 "타원곡선 E와 E상의 점 G와 그것을 k배 한 점 $k \times G$가 주어졌을 때 k를 구하는 것"이 어렵다는 것이다. 여기서 k는 개인키, K는 공개키, G는 Generator Point이다[8],[9].

[그림 3]과 같이 520비트 공개키를 sha256 해시를 거쳐 256비트로 압축하고 그것을 다시



<자료> Mastering Bitcoin 2nd Edition, O'Reillly, pp.66-68, 재구성

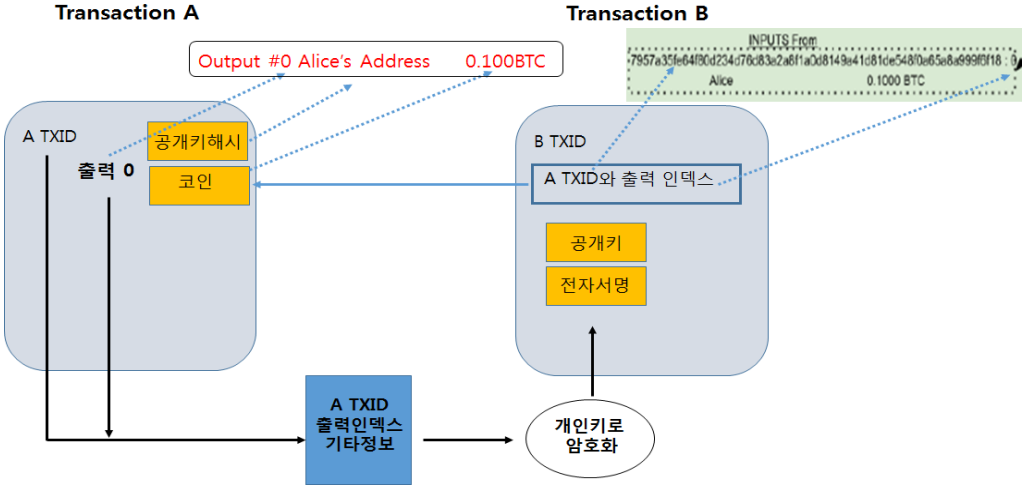
[그림 3] 공개키 해시 방식의 비트코인 주소 생성 과정

RIPEMD-160 해시함수를 사용하여 160비트, 즉 20바이트 값을 구한다. 일반적인 비트코인 거래에서 출력부에 기록되는 값은 이 공개키 해시값이다. 다음 단계에서, 해시값 뒤에 오류 검출을 위해 4바이트 checksum을 붙이고, 이 주소의 유형을 나타내는 버전 1바이트(예로서 main network의 경우 0×00)를 앞에 붙여서 25바이트 길이의 새로운 데이터 값을 생성한다. 사용자가 가능한 편리하게 사용하기 위해 이 이진수를 Base58로 인코딩하여 29바이트에서 35바이트 정도의 길이를 갖는 비트코인 주소를 구하는 것이다[9].

2. 거래생성 및 검증

전자지갑에서 수신자의 공개키를 계좌번호로 이용하여 비트코인을 전송할 수 있다. 여기서 공개키는 송·수신 시 활용되는 계좌번호 역할을 한다. 개인키(비밀키)는 본인이라는 사실을 증명하는 전자서명을 할 때에 이용된다. 전자서명은 트랜잭션의 타당성을 증명하는 것인데, 트랜잭션 데이터를 송신하는 사람이 서명을 생성하고 수신하는 사람이 그 서명을 송신자의 공개키로 검증해 타인에 의한 위·변조의 존재 유무를 확인할 수 있다.

이 코인을 사용하려면 입력부에 전자서명을 넣을 때 공개키를 함께 넣어 줘서 그 공개키가 출력부에 적힌 공개키 해시의 원본인지 확인하고 그 공개키로 전자서명을 확인한다. 트랜잭션 A의 출력부에 적힌 공개키 해시가 정당하다는 것은 거래 B의 공개키를 공개키 해시로 변환할



<자료> 블록체인 펼쳐보기, p.209.

[그림 4] 비트코인 주소로 지불된 코인의 확인 방법

때와 마찬가지로 이중 해시하여 결과가 공개키 해시와 같은지 비교하는 것이다. 공개키가 검증되면 이것으로 전자서명을 풀어서 서명된 내용을 확인하고, 이 공개키와 쌍을 이루는 개인키로 암호화되어 있어 당연히 풀리게 된다. 그 결과가 거래 A의 정보와 일치하는지 확인하면 검증이 끝난다. 비트코인 네트워크의 모든 노드에서 거래 B의 입력부가 정당한지 확인할 수 있다[2].

비트코인 프로그램은 script 언어를 이용한 거래에 대해서 서명검증을 하는데 이 스크립트 언어는 간단하고 스택기반의 실행 언어로서 push와 pop의 두 동작으로 제한되며, 무한 loop가 실행되지 않는다. 이를 튜링 불완전성(turing incompleteness)이라고 한다.

3. 전파단계 거래의 검증

P2P 네트워크에서 비트코인의 경우, 노드를 처음 설정하면 다음과 같은 절차에 의해서 다른 노드와 연계를 통해서 트랜잭션을 전달하게 된다. 전 세계의 전체 노드로 전달되는데 몇 초 정도가 소요되는 것으로 파악되고 있다[9].

① DNSSEED(예; seed.bitcoin.sipa.be, bitseed.xf2.org 등 6개) 옵션을 사용하여 노드 검색
② 또는 SEEDNODE 옵션을 사용하여 최초 연결을 위해 한 개의 노드와 연결
③ 두 번째부터는 그때까지 네트워크에서 인식한 노드 목록을 각 비트코인 클라이언트의 내부 DB에 보존해 놓기 때문에 그 정보를 바탕으로 다른 노드와의 연결을 시도

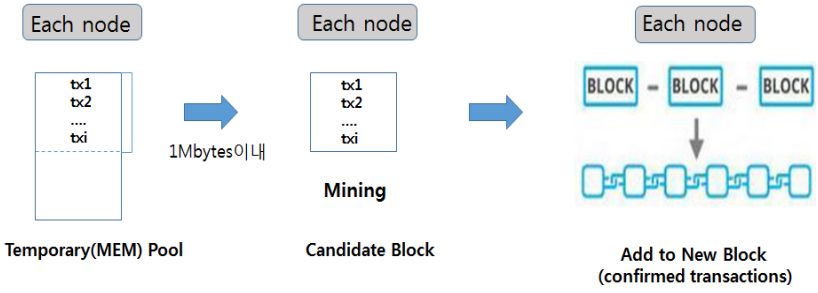
거래가 생성되면 P2P 네트워크(비트코인 네트워크)를 통해서 이웃 노드(전자지갑, 채굴 등을 하는 컴퓨터)로 전달되며 결국 전체의 비트코인 네트워크로 전달된다. 이웃 노드로 순식간에 브로드캐스팅하기 전에 송신된 거래에 대해 “거래 검증 리스트”에 따라 검증을 먼저하고 그 거래가 적정하면 지속적으로 비트코인 네트워크로 전달하고, 적정하지 않으면 해당 노드에서 그 거래를 버린다. 비트코인 네트워크의 각 노드는 독립적으로 검증 리스트(checklist)에 따라 모든 트랜잭션을 검증한 후 이웃 노드로 브로드캐스팅하고 올바르지 않은 트랜잭션은 제거한다[9].

① 트랜잭션의 구문(syntax)과 데이터 구조(data structure)의 확인
② 트랜잭션의 입력값은 반드시 UTXO(Unspent Transaction Output)인 것을 확인
③ 트랜잭션의 크기 값이 100bytes보다는 크고, 1Mbytes보다 작은 지를 확인
④ 트랜잭션의 입력값이 출력값보다 작은지를 확인 등

이와 같이 트랜잭션의 검증 리스트를 통해서 검증에 성공하면 그 노드는 원래 노드에게 “success message”를 보내고, 검증에 실패하면 “rejection message”를 보낸다.

4. 블록의 구성 및 생성

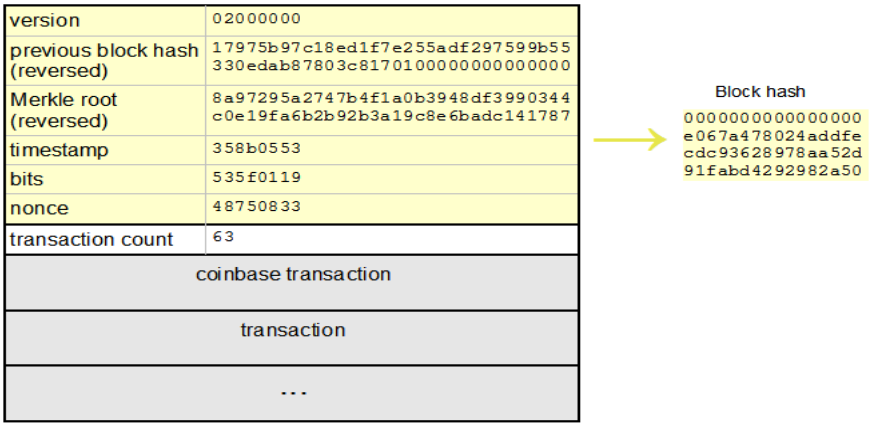
각 노드의 메모리 상에 존재하는 임시 풀(Temporary Pool)에 검증된 트랜잭션들이 쌓이게 되며, 그 트랜잭션 중에서 채굴(Mining)을 위해 후보 블록(Candidate Block)을 구성하게 된다. [그림 5]는 임시 풀에서 후보 블록을 생성하여 새로 탄생된 블록이 블록체인으로 연결되는 모습을 보여준다[9].



<자료> Mastering Bitcoin 2nd Edition, O’Reillly

[그림 5] 임시 풀에서 후보 블록을 구성하는 절차

[그림 6]은 후보 블록에서 채굴을 끝내고 블록체인에 연결된 새로운 블록을 보여준다.



<자료> http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html

[그림 6] 실제 블록체인에 연결된 새로운 블록

[표 2] 블록의 헤더

구분	크기(bytes)	설명
version	4	블록 버전 숫자
Previous block hash	32	이전 블록헤더를 sha256 해시함수를 이용하여 2번 해싱한 해시값 -sha256(sha256( ))
Merkle hash root	32	현재 블록에 포함된 거래정보의 거래 해시를 2진 트리 형태로 구성할 때 트리의 루트에 위치하는 해시값
Timestamp	4	블록의 생성시간, 1970년 1월 1일 이후의 초단위 시간
Bits	4	블록의 작업증명 알고리즘에 대한 난이도 목표
Nonce	4	특정 목표값보다 낮은 값을 구하기 위한 카운터

<자료> https://bitcoin.org/en/developer-reference#block-chain

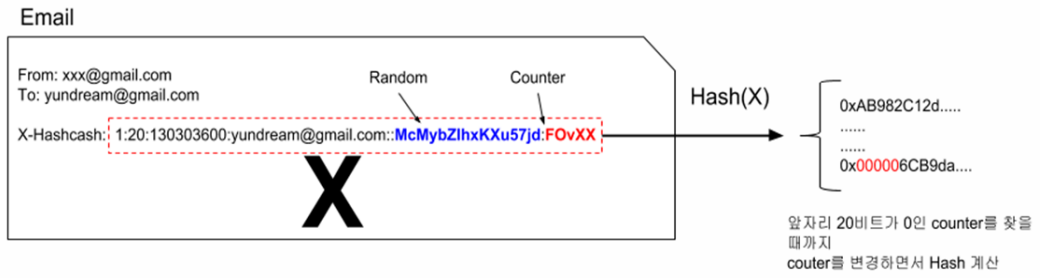
비트코인의 블록은 헤더(header)와 바디(body)로 구성되며, 헤더는 [표 2]와 같이 80바이트로 구성되어 있고, 전체 블록의 크기는 1Mbytes로 제한되어 있다.

비트코인 노드는 전송받은 트랜잭션에 대해 검증을 한 후 그 트랜잭션을 임시 풀에 계속 추가한다. 트랜잭션 풀에 있는 거래 중에서 후보 블록을 생성한다. 그 다음에 트랜잭션 확정을 위해 채굴되기를 기다리게 된다.

5. 채굴 및 보상

이메일 스팸과 DOS(Denial of Services) 공격을 제한하기 위해서 사용하는 작업증명(PoW)의 하나인 해시캐시(Hashcash)는 1997년 Adam Back이 고안한 것으로 채굴을 설명하기 전에 그 개념을 설명하고자 한다.

해시캐시는 이메일을 보낼 때 보내는 사람이 메일을 보내기 위해 노력을 했다는 증거(작업의 증명(PoW))를 함께 보내서 내 메일은 스팸 메일이 아니라고 알리는 방법이다. 해시캐시를 써서 스팸메일 필터링을 할 때는 이메일 헤더에 [그림 7]과 같이 X-Hashcash라는 항목을 1개 추가해서 함께 보낸다. X-Hashcash 헤더 항목의 값 전체를 해시의 X값이라고 가정하면, 이것이 해시함수의 입력인 X값이며 메일을 받는 사람은 이 값을 입력으로 하여 미리 해시함수를 계산할 수 있다. 계산 결과로 나온 Y값에서 앞쪽 20비트가 모두 0이면 “송신자가 이 메일을 보내기 위해 자신의 시간을 써서 이 값을 계산했으니, 스팸메일이 아니다라는 것을 인정하는 것이다.” 여기서 중요한 점은 수신자가 검증할 때 송신자의 메일주소를 확인하는 등 부수적인 정보를 이용하지 않고 판단할 수 있다는 것이다. 즉, 해시캐시로 검증하는 단계에서는 단지

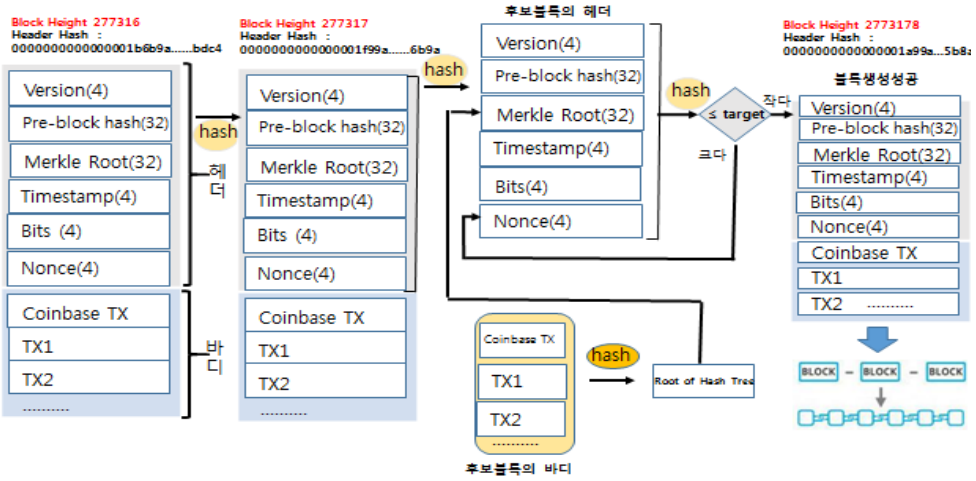


<자료> http://www.hashcash.org

[그림 7] Hashcash를 이용한 PoW 구현

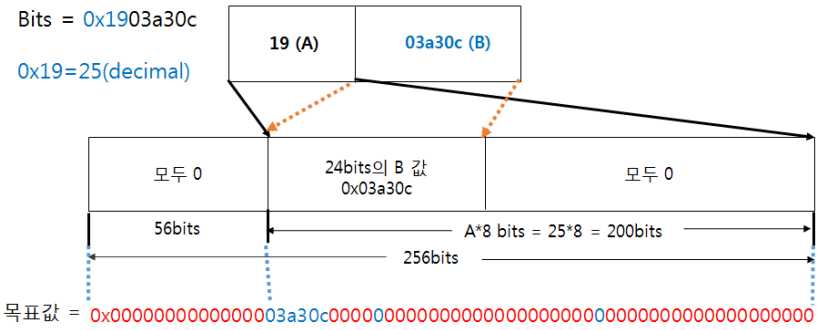
헤더 항목 X-Hashcash의 값만 보고 판단한다. 이 값을 해시함수로 계산해서 앞의 20자리가 0으로 시작한다는 것만 확인하면 검증이 끝나는데 이것이 해시캐시의 핵심이다. 사토시가 논문으로 기술한 것 중 가장 중요한 발명은 분산 합의에 의한 분산 메카니즘이다. 합의 알고리즘이란 P2P 네트워크와 같이 정보 도달에 시간차가 있는 네트워크에서 참가자가 수행한 결과에 대한 합의를 얻기 위한 알고리즘이다. 비트코인은 PoW라는 합의 알고리즘을 사용하여 처음으로 P2P 네트워크를 통해 누구나 참가 가능한 전자화폐시스템을 실현했다[3].

채굴의 시작은 노드에서 후보 블록을 생성하는 것으로, 비트코인의 경우는 약 10분마다 새로운 블록이 생성되도록 프로그램되어 있으며, [그림 8]과 같이 후보 블록에서는 헤더에 version, pre_block hash, merkle_hash root, timestamps, bits 값은 결정되어 있고, 변경이 가능한



<자료> 아카하네 요시하루, 양현옮김, “블록체인 구조와 이론”, 위키북스 p.120 재구성

[그림 8] 해시를 이용한 비트코인의 채굴(Mining) 프로세스



<자료> https://bitcoin.org/en/developer-reference#target-nbits

[그림 9] Bits값을 이용한 난이도 목표값

난수 “nonce(number used once)” 값을 초기 0부터 시작해서 1씩 증가하면서 sha256 해시함수를 2회 적용하여 블록 헤더의 해시값이 특정 숫자보다 작은 값을 찾으면 채굴이 성공된다. 여기서 특정 숫자는 [그림 9]와 같이 난이도 목표(difficulty target)로서 Bits값으로 프로그램에서 특정 목표값을 자동 제시한다.

특정 노드(채굴자)가 목표값 보다 같거나 작은 해시값을 찾는데 성공하면, 새로운 ‘블록’을 생성하게 된다. 이 채굴자는 블록을 생성하고 이를 P2P 네트워크에 전파하면서 동시에 블록 생성 보상인 ‘비트코인’과 해당 블록 바디의 Coinbase TX에 포함된 “이체 수수료(Transaction Fee)”를 받게 된다. “비트코인 지급”이라는 경제적 보상이 채굴자들이 해싱작업에 참여하는 동기가 된다. 채굴 행위는 근본적으로 끊임없는 해싱작업이며, 많은 컴퓨팅 파워를 가지고 있을수록 빠른 속도의 해싱이 가능하다. 즉, 컴퓨팅 파워를 많이 투입할수록 다른 경쟁자들보다 비트코인을 많이 받게 되는 구조이다. 블록 생성 확률(목표값 경쟁 승리확률)과 네트워크 상에서 자신이 차지하는 컴퓨팅 파워 비율은 정확히 비례하며, 만일 누군가가 전체 투입 컴퓨팅 파워 중 30%를 점유하고 있다면, 수학적으로 블록 생성 확률도 정확히 30%에 수렴한다[4].

6. 블록 검증

비트코인의 합의 알고리즘 중 하나로서 비트코인 네트워크에 연결된 각 노드는 각각 새로 생성된 블록에 대해서 독립적으로 검증한다. 새로 생성된 블록 데이터 구조가 적정한지, 블록 헤더 해시값이 난이도 목표값 보다 작은지, 블록 사이즈가 시스템에서 정의된 1Mbytes 보다 작은지 등을 검증한다. 블록이 정당(valid)하면 해당 노드는 “success message”를 블록을 생성한 노드(originator)에게 보내고, 블록이 정당하지 않으면 “reject message”를 생성한 노드에게

◆블록 검증과정

① 이전블록 존재여부 검증(이전블록헤더 해시값)

② 작업증명 검증

SHA256(SHA256 (| Ver | Prev Block Hash | Merkle Hash | | Time | Bits | Nonce |)) < 목표값

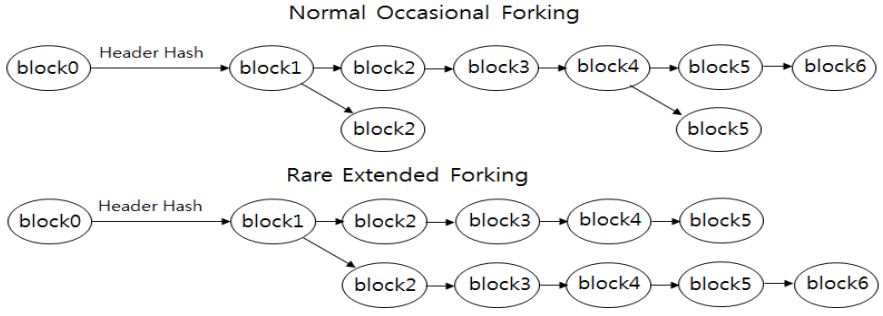
<자료> "블록체인 구조와 이론", p.120 재구성

[그림 10] 비트코인 노드의 새로 생성된 블록 검증과정

전송한다. 노드의 절반 이상(51%)의 합의가 있어야 블록에 대한 승인, 즉 트랜잭션이 승인되며 이후 전체 노드의 절반 이상을 점유하지 않는 이상 트랜잭션에 대한 위·변조는 불가능하다.

7. 블록체인 생성

새로운 블록을 전달 받은 각 노드들은 검증을 완료한 후 이 블록을 기존의 블록체인에 연결한다. 블록체인이 분산된 데이터 구조이기 때문에 채굴된 블록이 동시에 서로 다른 노드에서 탄생될 수 있으며, 수천, 수만 개의 노드들에서는 먼저 전달 받은 새로운 블록을 기존의 블록체인에 연결하는 "블록체인 분기(Blockchain Forking)"라는 현상이 발생될 수 있다. Normal Occasional Forking(분기)이 발생할 경우 작업증명을 많이 수행한, 즉 난이도(difficulty)가 높은 블록이 우선시 된다. Rare Extended Forking의 경우는 시간이 지남에 따라서 가장 긴 블록체인이 살아남게 되고, 짧은 블록체인은 스스로 사라진다. 실제로 개발자들이 "블록체인 분기"가 발생한 후 6개 블록을 추가로 연장된 것을 지켜본 후에 가장 긴 블록을 확정한 사례가 있다. 분기한 블록의 채굴 대가인 '비트코인'과 "이체 수수료"는 무효가 된다.



<자료> https://blog-archive.bitgo.com/the-challenges-of-block-chain-indexing

[그림 11] 가장 긴 체인을 선택하는 블록체인

8. 난이도 조정

비트코인은 평균적으로 약 10분 간격으로 새로운 블록이 채굴되도록 설계되어 있다. 2016개의 블록이 추가 생성되는 2주간의 간격으로 1개의 블록이 생성되는 주기를 계산하여 평균 약 10분보다 길면 난이도를 어렵게 하고, 10분 간격보다 짧으면 난이도를 쉽게 하여 1개의 새로운 블록이 생성되는 주기를 약 10분 간격이 되도록 조정한다. 이를 난이도 조정(Difficulty Retarget)이라고 한다. 다음은 새로운 난이도 조정을 위한 식이다[9].

New difficulty = Old Difficulty×(Actual Time of Last 2016 Blocks/20160 minutes)

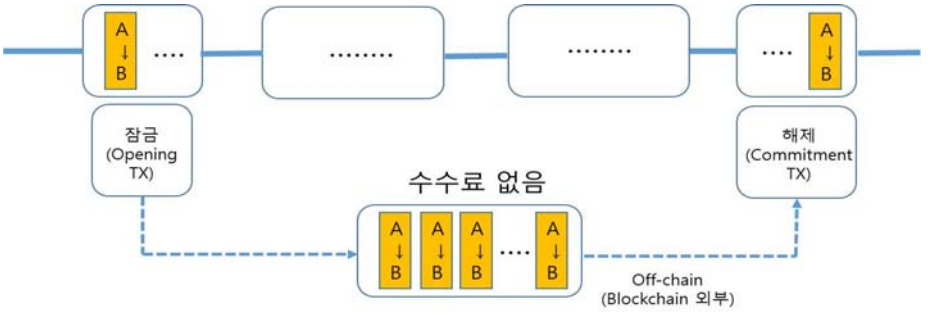
[그림 9]와 같이 결론적으로 목표값은 앞의 비트 0의 개수가 많으면 난이도가 높게 될 것이다.

Ⅲ. 비트코인 블록체인의 진화

1. 오프체인

비트코인 결제는 블록체인에 트랜잭션을 기록할 때마다 수수료가 발생한다. 소액 결제를 반복할 경우에는 수수료가 계속해서 발생한다. 이 문제를 해결하는 방법으로 마이크로페이먼트 채널(micropayment channel)이라는 기술이 있다. 이것은 트랜잭션 일부를 블록체인의 외부(오프체인, off-chain)에서 처리하는 기술이다. 첫 트랜잭션과 마지막 트랜잭션만 블록체인에 기록하고, 중간 트랜잭션은 기록을 생략하여 수수료가 들지 않도록 하는 것이다[4].

현재 비트코인 블록체인은 블록의 크기가 1Mbytes로 제한되어 있다. 그렇기 때문에 블록에



<자료> 블록체인, 국일증권경제연구소, 2018, p.225.

[그림 12] 오프체인을 이용한 비트코인 소액 결제 방식

담기는 거래량의 상한이 낮은 점이 문제가 되고 있다. 마이크로페이먼트 채널을 이용하면 블록체인 외부에서 대량의 트랜잭션을 고속으로 처리할 수 있는 만큼 이 기술은 블록체인의 용량문제를 해결할 수 있는 하나의 수단으로 주목 받고 있다.

2. 세그윗

블록 크기에 상한(1MB)이 정해져 있는 비트코인은 송금 지연 문제가 발생한 적이 있다. 이러한 용량 문제를 해결하기 위해 세그윗(SegWit)을 비롯한 다양한 대책이 고안되었지만 합의가 원만하게 진행되지 않아 문제 해결에는 이르지 못했다. 그러나 일부 채굴자가 주도하여 용량문제를 해결할 수 있는 비트코인인 "Bitcoin Unlimited"를 만들자고 주장했고, 여기에 hash power(채굴 능력)가 강한 채굴자들이 찬성하여 하드포크(hard fork)가 실현되었다. 2017년 8월에 비트코인 하드포크가 실현되어 비트코인 캐시(Bitcoin Cash)라는 암호화폐가 생겨났고, 그 이후로도 10월에는 비트코인 골드(Bitcoin gold), 11월에는 비트코인 다이아몬드(Bitcoin diamond)가 분리되었다.

비트코인의 블록 크기가 1MB로 한정되어서 발생하는 문제를 해결하는 한 가지 방법으로 세그윗(SegWit, Segregated Witness)이 나왔다. 세그윗이란 비트코인 블록에 담긴 서명과 공개키 등을 분리해서 다른 영역에 수납하는 방법이다. 원래 스크립트시그(scriptSig: 거래 서명과 공개키 등으로 구성된 프로그램)에 포함된 데이터를 분리해서 별도의 영역에 수납하는데, 이 별도의 데이터 영역을 위트니스(witness)라고 부른다. 세그윗은 프로그램의 내용을 "스크립트시그 속에 서명이 포함되어야 한다"에서 "위트니스 속에 서명이 포함되어야 한다"로 바꾼다. 이것은 블록 크기의 실질적 확장을 의미한다. 블록에서 데이터를 뺀 만큼 블록의 용량이 늘어나기 때문이다. 참고로 라이트닝 네트워크(Lightning Network)를 만들어 확장성 문제를 해결하자는 논의도 있다. 라이트닝 네트워크는 정규 블록체인 상에서가 아니라 별도의 장소(오프체인)에서 비트코인 거래를 실시하는 방법이다[1].

Ⅳ. 결론 및 시사점

1992년 Timothy Bresnahan, Manuel Trajtenberg 교수의 연구를 살펴보면, 어떤 기술이 범용기술이 되기 위한 3가지 조건, 즉 확산성, 개선성, 혁신 촉진성을 만족하게 되면 사회 전반의 혁신을 유발하고 광범위한 사회경제적 파급력을 갖는 기술이 된다고 주장하고 있다. 최근 블

록체인 기술이 이 조건들을 만족하여 4차 산업혁명의 범용기술이 될 것으로 기대되고 있다[7].

2018년 6월 현재 비트코인 외에 알트코인이 약 1,640여개[10]가 거래되고 있는데, 각 코인들은 서로 다른 특징을 가지고 있으며, 이들은 이더리움처럼 각각의 플랫폼 역할을 추구하려고 탄생하였다. DAO(Distributed Autonomous Organization)는 "분산형 자율 조직"을 뜻한다[12]. 기계가 스스로 동작하는 IoT의 세상이 온다면, 그 속의 세상은 암호화폐 즉 코인으로 거래가 일어나야 되고, 상호 규칙, 프로토콜, 계약에 따라 중앙 관리자 없이 자율적으로 통치되는 시스템이 가까운 시대에 도래될 것이다.

마지막으로, 암호화폐인 비트코인을 의미하는 블록체인 1.0과 스마트 컨트랙트 개념을 실현시킨 이더리움의 블록체인 2.0을 지나, 현재 금융/IoT/운수/물류/의료 등에 적용되는 블록체인 3.0이 활발하게 적용되고 있다. 따라서, IT 전문가들이 지속적으로 새로운 아이디어를 구현한다면 블록체인과 AI가 접목되는 블록체인 X.0 즉 "Blockchain Sigularity 시대[13]"가 멀지 않아 도래할 것으로 전망된다.

[참고문헌]

[1] 가상화폐비즈니스연구회, 60분만에 아는 블록체인, ㈜국일증권경제연구소, 2018. 3. 27, pp.222-225, pp.234-235.

[2] 김석원, 블로체인 펼쳐보기, 비제이퍼블릭, 2017. 11, pp.55-65, pp.203-213.

[3] 김태형, 블록체인 개념 및 분야별 활용사례 분석, 전기저널, 487, 2017. 7, pp.58-65.

[4] 비트코인 블록체인 개론, https://blog.naver.com/onalja/

[5] 사토시 나카모토, "Bitcoin: A peer-to-peer Electronic cash system", 2008. 10. 31.

[6] 아카하네 요시하루, 양현옮김, "블록체인 구조와 이론", 위키북스 pp.105.

[7] 오세현, 김종승, 블록체인노믹스, 한국경제신문, 2017. 11. 15.

[8] 히로시 유키, Information security and cryptography, infinity books, 2017. 5. 24, pp.559-560.

[9] Andreas M.Antonopoulos, Mastering Bitcoin, Second Edition, O'Reilly, 2017. 6, pp.57-66, pp.176-180, pp.196-200.

[10] www.coinmarketcap.com

[11] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Transactions on Programming Language and Systems, v.4 n.3, July 1982, pp.382-401.

[12] https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

[13] Imran Bashir, Mastering Blockchain-Second Edition, Packt, March 2018, pp.27.