2017.11.03 @ 2017년 한국정보처리학회 추계학술발표대회

블록체인의 동작 원리와 요소 기술 소개
– 튜토리얼 –

상명대학교 프로토콜공학연구실 이종혁 (jonghyouk@smu.ac.kr)

상명대학교 프로토콜공학연구실: pel.smuc.ac.kr

지도교수: 이종혁

- 상명대학교 소프트웨어학과, 조교수, 2013년 - 현재
- 프랑스 그랑제꼴 TELECOM Bretagne, 조교수, 2012년 – 2013년
- 프랑스 국립연구소 INRIA, 연구원, 2009년 – 2012년
- 성균관대학교 박사

최근 연구과제

- TXE-01 플랫폼 및 펌웨어 보안구조 분석 도구 제작, ETRI, 2017년
- 블록체인 기반 디지털 콘텐츠 DRM 응용 기술 개발, 한국저작권위원회, 2017년
- 클라우드 블록체인 서비스 제공 분석 및 요구사항 개발, ETRI, 2017년
- 기반시설 무선장비 도입 및 활용 보안 가이드라인 연구, 국보연, 2017년
- 저지연 융합서비스를 위한 모바일 에지 컴퓨팅 플랫폼 기술 개발, 기가코리아사업단, 2017-2020년
- 사람인터넷을 위한 인간중심의 인증과 접근제어, 한국연구재단, 2014-2020년
- 소프트웨어 및 소스코드 비교분석 기법 및 검증코드 개발, 대검찰청, 2016년
- 하드웨어 인터페이스를 통한 보안성 검증 도구 개발, ETRI, 2016년
- 임베디드 오픈 플랫폼 기반의 펌웨어 보안성 검증 도구 개발, ETRI, 2015년
- 펌웨어 수준의 루트킷에 대한 사례분석 및 신규 시나리오 연구, ETRI, 2014년

최근 연구성과

- 인터넷표준 IETF RFC 8127, 8191 제정, 2017년 8월
- “블록체인 동작 과정에 따른 보안 분석”, 한국정보보호학회, 2017년 6월 (한국전자통신연구원 원장상)
- “Shadow Brokers에 의해 유출된 NSA 윈도우 해킹 툴 분석”, 한국정보보호학회 , 2017년 6월 (우수 논문상)
- “PowerShell 공격 도구를 활용한 윈도우 운영체제 관리자 권한 획득”, 한국정보보호학회, 2016년 12월 (우수
- “Whisper 기반의 안전한 모바일 메신저 설계”, 한국통신학회, 2016년 11월 (우수 논문상)
- Best Land Transportation Paper Award, IEEE Vehicular Technology Society, 2015년 9월
- 이달의 신진연구자, 한국연구재단, 2014년 11월

순서

1. 블록체인?
2. 비트코인과 블록체인
3. 블록체인 요소 기술
4. 몇가지 생각해 볼 만한 것들

블록체인?

뭐꼬? 투명성과 비가역성을 지원하는 분산된 데이터베이스

- 투명성(Transparency): 거래내역은 검증 될 수 있음
- 비가역성(Irreversibility): 기록 된 거래내역은 변경 될 수 없음
- 분산된 데이터베이스(Distributed DB): 중앙 서버가 불필요한 분산된 DB

SECURITY GUEST

Blockchain's brilliant approach to cybersecurity

BEN DICKSON, TECHTALKS @BENDEE983 JANUARY 22, 2017 9:33 AM

June 26, 2017

Blockchain: A multi-functional 'Swiss Army knife' for cyber-security

Blockchain is known for powering cryptocurrencies, but developers are finding many other innovative uses for crypto-secure transactions, write Adam Palmer and Michael Palage.

Over the past several years, more than a billion dollars have been invested in blockchain startups by investors seeking to capitalise on what is estimated to be an $US 8 billion market by 2024.

This private sector investment has also been coupled with several public sector initiatives from various governments. This article examines the aspects of blockchain technology that make it uniquely situated to support cyber-security capacity building.

It is important to note that blockchain is not a 'silver bullet' solution. However, it will be a critical tool for improving cyber-security.

Bitcoin is enabled by blockchains, but there are other uses for this technology apart from making virtual currencies

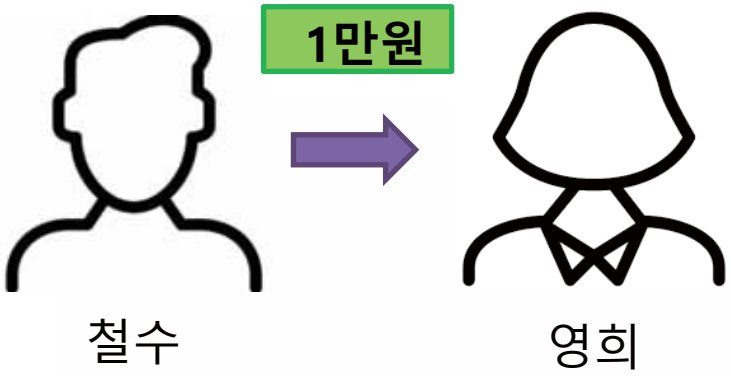
블록체인?

개념(1/6)

교실에 50명의 학생이 있고,
각자 거래내역을 적는 장부를 가지고 있다!

블록체인?

개념(2/6)



철수는 영희에게 만원을 빌려주고,
이 사실을 구성원 모두에게 알린다!

블록체인?

개념(3/6)

철수가 영희에게
만원을 빌려주었다!

철수와 영희를 포함한 모든 구성원은 '철수가 영희에게 만원을 빌려 준 내용'을 기록한다.

즉, 구성원 각각은 자신의 장부를 통해
구성원 모두의 거래내역을 알고 있다.

블록체인?

개념(4/6)

영희

영희는 철수에게 빌린 돈을 갚고 싶지 않다.
그래서 자신의 장부에서 거래 내용을 변경한다.

혹은 철수는 영희에게 1만원을 빌려주고서,
10만원을 빌려 줬다고 자신의 장부를 변경한다.

블록체인?

개념(5/6)

철수와 영희의 거래내역은 다른 모든 이들의 장부에 기록되어 있다.

즉, 철수와 영희의 거래내역을 조작/변경하려면 다른 모든 이들의 장부를 조작/변경해야 한다.

블록체인?

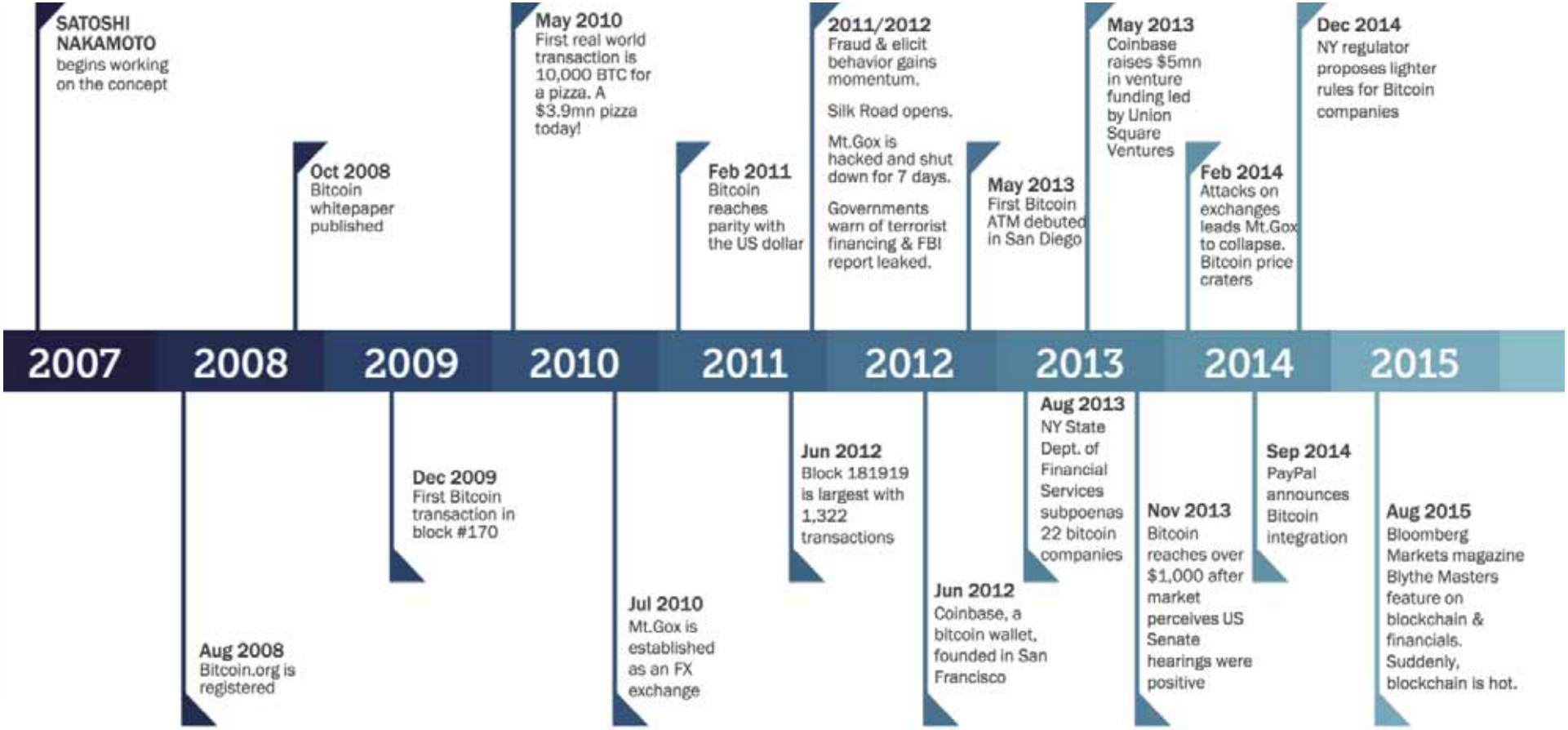
개념(6/6)

거래 당사자 뿐만 아니라 다른 모든이의
거래장부를 조작하는 것은 어려운 일이다.

전체 집단의 수가 커지면 커질수록
조작은 더욱더 어려워진다.

비트코인과 블록체인

비트코인 P2P 환경에서 블록체인을 적용해 이중 지불문제를 처음으로 해결한 암호화폐(Cryptocurrency)



비트코인과 블록체인

비트코인 vs. 블록체인 블록체인은 비트코인의 기반기술

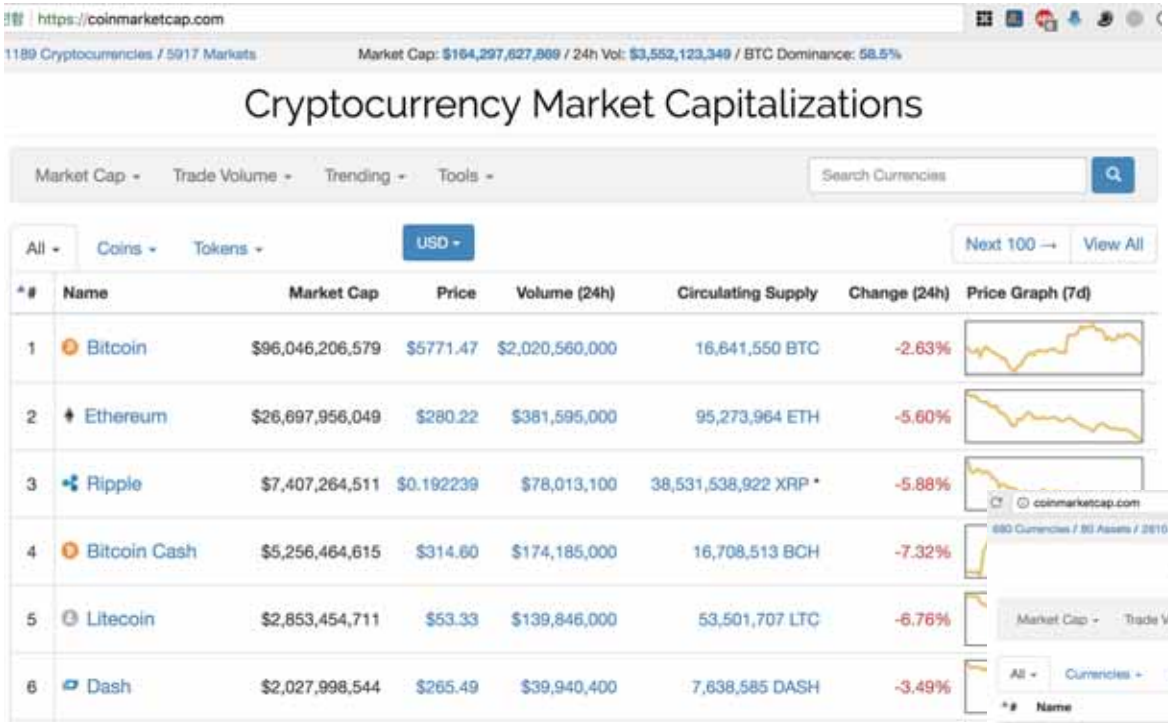
- 블록체인과 비트코인은 다름
- 블록체인은 비트코인의 기반기술로써 개발 됨
- 블록체인은 분산원장(Distributed Ledger Technology)의 한 종류

여러 알트코인과 블록체인 각 알트코인마다 개별 블록체인

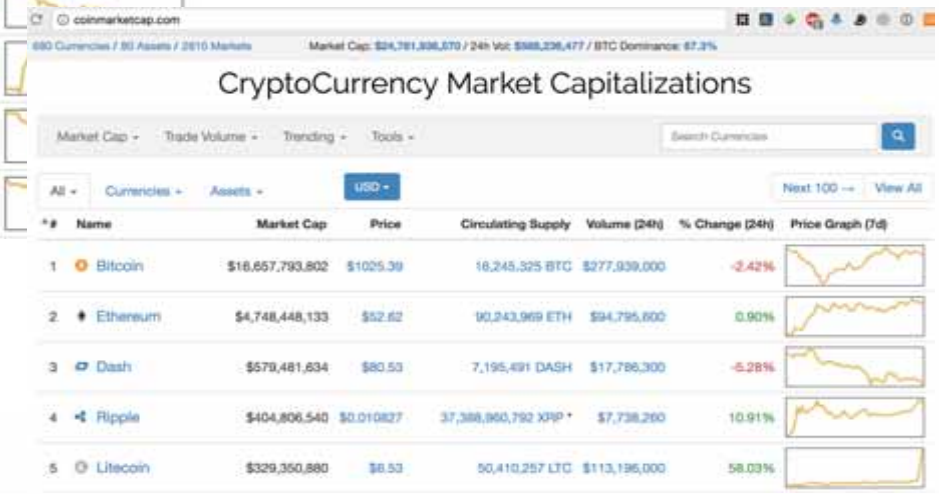
- 이더리움(Ethereum) 블록체인
- 대쉬(Dash) 블록체인
- 피어코인(Peercoin) 블록체인
- Nxt 블록체인

비트코인과 블록체인

암호화폐의 시가총액 이것들이 얼마나 견고한가?



(2017/10/23 기준)



(2017/03/30 기준)

블록체인의 요소 기술 – 용어

트랜잭션(Transaction) 블록체인 내에서 전송되는 메시지

- 디지털 서명을 통한 메시지 인증 및 부인 방지
- 메시지 전송의 송신자와 수신자 주소의 익명화를 통한 프라이버시 보호

블록 (트랜잭션의 묶음) 특정 시간 동안 전송 된 트랜잭션 모음

- 블록 = 블록 헤더 + 블록 바디(특정 시간 동안 전송 된 트랜잭션들)
- 블록은 기존 블록에 연결 됨
  - 블록의 체인화 => 블록체인

합의 알고리즘 누구의 블록을 어떻게 연결 할 것인가?

- 작업 증명(Proof-of-Work, PoW)
- 지분 증명(Proof-of-Stake, PoS)
- 위임된 지분 증명(Delegated Proof-of-Stake, DPoS)

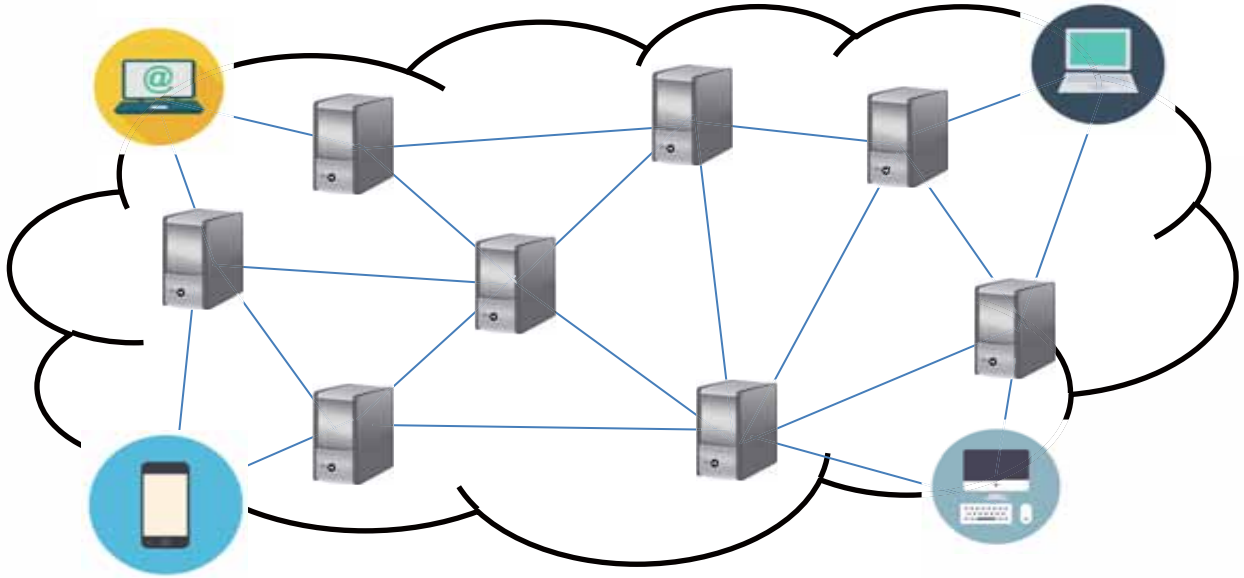
블록체인의 요소 기술 – 아키텍처

블록체인 아키텍처

Public vs. Consortium vs. Private P2P Networking over the Internet

- Public Blockchain: 누구나 참여 가능한 형태의 블록체인, e.g., Bitcoin
- Consortium Blockchain: 맴버쉽 형태로 운영 되는 블록체인, e.g., 금융권 블록체인
- Private Blockchain: 특정 운영자에 의해 운영 되는 블록체인

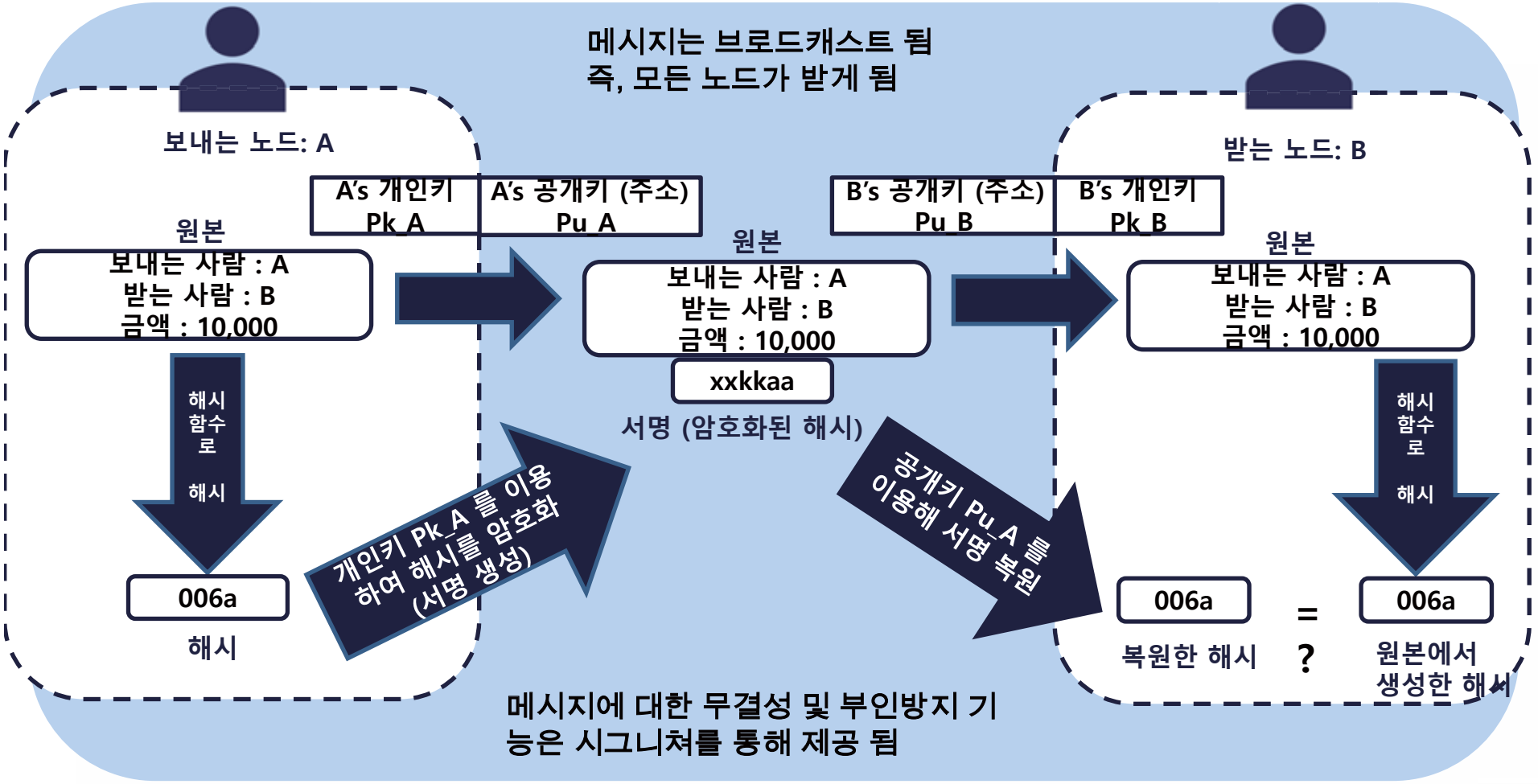
- 풀 노드: 전체 블록체인을 유지 & 블록 확인/생성 + 트랜잭션 생성/전송
- 일반 노드: 트랜잭션 생성/전송



비트코인 블록체인의 크기
- 2017년 07월: 123GB 이상
- 2016년 12월: 100GB 돌파

블록체인의 요소 기술 – 트랜잭션

트랜잭션 브로드캐스팅 되며 무결성 & 부인방지 제공



블록체인의 요소 기술 – 블록

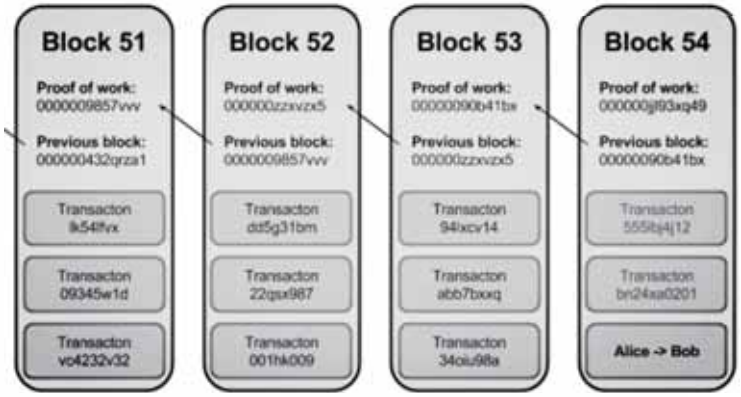
블록 특정 시간(블록 타임) 동안 모아진 트랜잭션

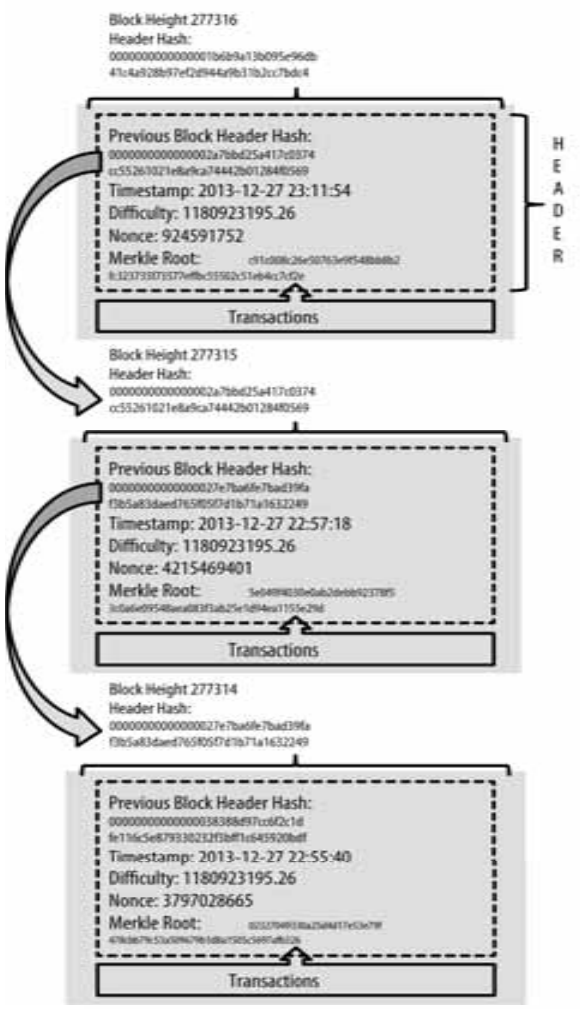
구성	명칭	설명
매직 넘버 (4 바이트)		비트코인 블록임을 명시(0xD9B4BEF9)
블록 크기 (4 바이트)		트랜잭션을 포함한 블록의 전체 크기
헤더 (Header)	버전 (4 바이트)	데이터 구조의 버전
	이전 블록헤더 해시 참조값 (32 바이트)	블록의 체인구조에서 이전블록(부모블록)에 대한 해시 참조값
	머클 루트 (32 바이트)	해당 블록에 포함된 거래로부터 생성된 머클 트리의 루트에 대한 해시(즉, 블록에 들어있는 모든 거래에 대한 요약)
	타임스탬프 (4 바이트)	블록의 생성 시간
	난이도 목표 (4 바이트)	작업증명(PoW) 알고리즘에 대한 난이도 목표
	난스 (4 바이트)	작업증명의 결과로 채워지는 카운트 값
바디 (Body)	트랜잭션 카운터 (1 – 9 바이트)	트랜잭션의 수
	트랜잭션	블록 타임(약 10분) 동안 수집한 거래 내역

블록체인의 요소 기술 – 블록

트랜잭션 → 블록 → 블록체인

```
{
  "hash":"00000000000000041cbd5ba9607416285167b4b6ff65bda651ac0f55e03bbd6",
  "ver":2,
  "prev_block":"00000000000000005fca80796201fe3fbdf2b695b64feb84e60b5d0c4ba2a99",
  "mrkl_root":"59a1914711c0923c2ee4bd43778991ee528b6addce86f8d0f6c18f12f7700823",
  "time":1402209318,
  "bits":408782234,
  "nonce":4027624099,

  "n_tx":27,
  "size":13924,

  "tx":[

      /* 거래 내용이 포함됨 */

   ],
   "mrkl_tree":[

      /* 거래내역의 머클크리 */
   ]
}
```





블록체인의 요소 기술 – 합의 알고리즘

합의 알고리즘 누구의 블록을 어떻게 연결 할 것인가?

- P2P 네트워크에서 트랜잭션들은 계속 브로드캐스트 됨
- 특정 시간(블록 타임) 마다, 트랜잭션들을 하나의 블록으로 모아 기존 블록체인에 연결 시키는 작업이 필요
  - 비트코인: 약 10분
- 하지만, P2P 네트워크에서 누구가 가지고 있는 트랜잭션들(거래 내역들)을 하나의 블록으로 만들고, 기존 블록체인(거래 장부)에 연결 할 것인가?
- 누구의 블록을 기존 블록체인에 연결 시킬 것인가?
  - 우리에겐 뭔가 합의(Consensus)가 필요하다!

블록체인의 요소 기술 – 합의 알고리즘

작업 증명(PoW) 비트코인의 합의 알고리즘

- 내가 얼마나 많은 노력을 해서 문제를 풀었는지를 증명하는 것!
- 주어진 문제가 있고(특정 해쉬값 보다 작은 값 찾기), 그 문제를 빨리 푸는 노드가 가지고 있는 트랜잭션들(거래 내역)을 하나의 블록으로 인정하고, 기존 블록체인에 연결
  - 물론, 이에 대한 인센티브 존재
  - 블록 생성(확인)이라는 프로세스가 마이닝이라고 불리는 이유
- 어떤 문제가 주어지는가?
  - 특정 해시값 보다 작은 값이 나오도록 하는 입력을 찾는 문제
  - 노가다성 작업으로 어떤이는 이걸 퍼즐을 푼다고 한다!

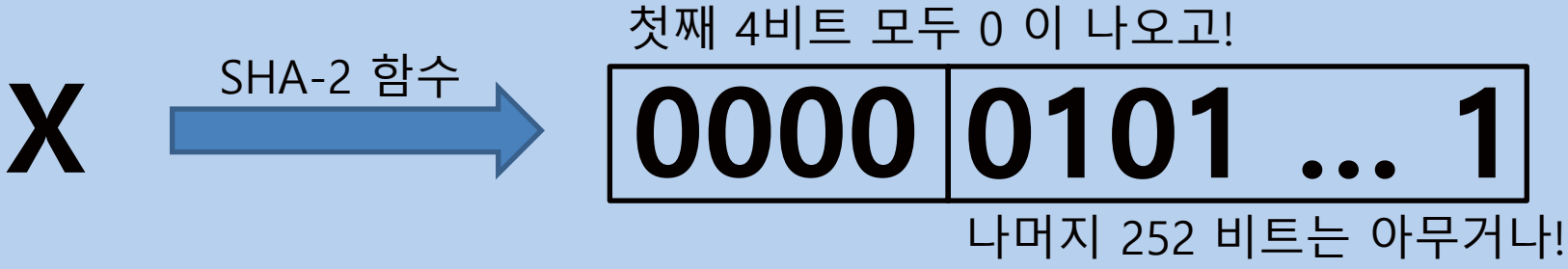
블록체인의 요소 기술 – 합의 알고리즘

작업 증명의 동작 원리–1 단방향 함수의 특징을 이용

- SHA-2(X) = Y 일때, X를 가지고 Y 를 계산하기는 무지 쉬움
- SHA-2(X) = Y 일때, Y를 가지고 X 를 찾기는 무지 힘듬
  - Y가 256비트 라면, 2^256 시도를 해야 함
  - 역방향 계산은 거의 불가능!

작업 증명의 동작 원리–2 역방향 계산을 조금 완화하면?

- 어떤 수(K) 보다 작은 Y 가 나오는 X 값 찾기 문제



2^256 문제를 2^4 문제로 변환! 난이도 조절!

블록체인의 요소 기술 – 합의 알고리즘

작업 증명의 원조? 스팸 메일 발송 방지를 위한 Hashcash

- 정방향 계산은 쉽고, 역방향 계산은 어렵다!
- 보내는 사람은 어렵게 보내고, 받는 사람은 손쉽게 확인!

- 본래, 이러한 아이디어는 스팸 메일 발송 방지를 위한 용도로 1997년 Hashcash 라는 이름으로 소개 됨
  - 메일을 보내는 사람은 보내기 위한 노력이 많이 필요!
  - 메일을 받는 사람은 보낸 사람이 노력을 들였는지 쉽게 확인!

```
1:20:1303030600:adam@cypherspace.org::McMybZIhxKXu57jd:ckvi
```

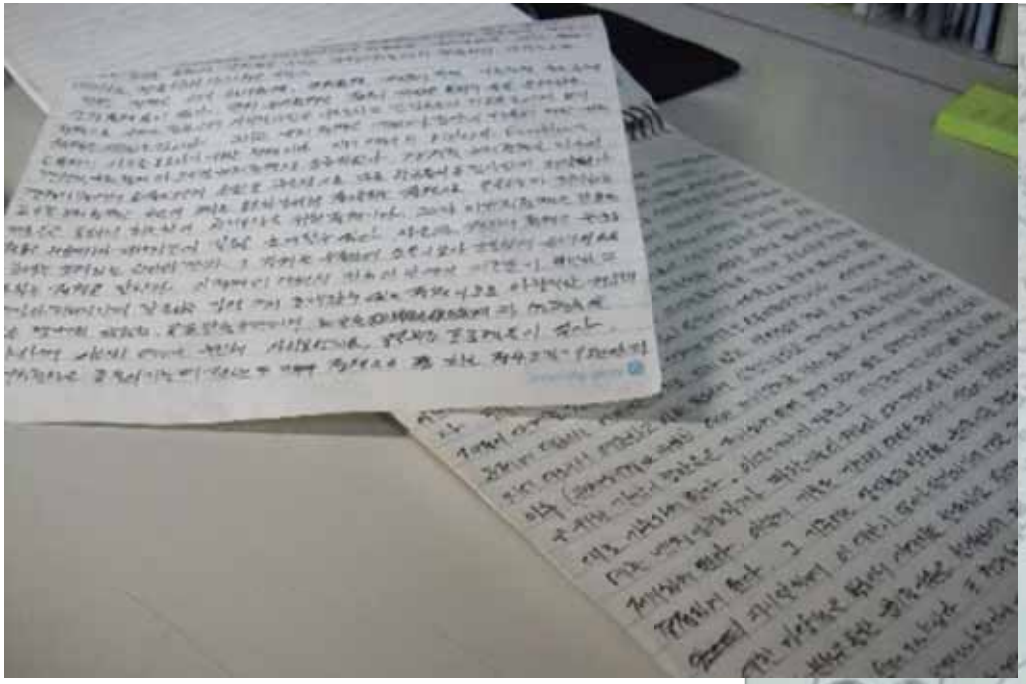
난이도 조절 비트

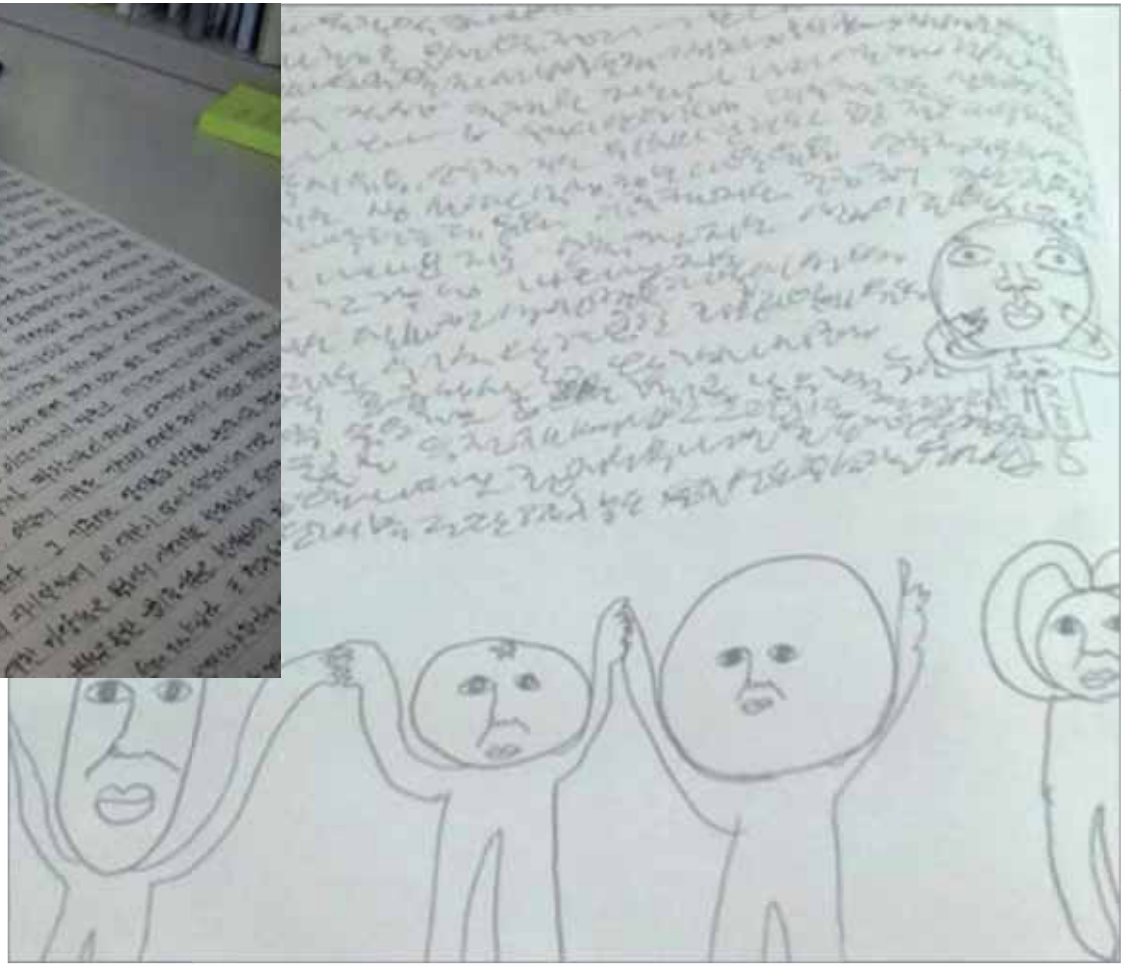
난스(nonce): 작업 증명 카운터

메일을 보내는 사람은 보내는 메일의 헤더와 작업 증명 카운터를 하나씩 증가 시켜 가면서, v = hash(헤더 + 증명 카운터)의 첫번째 20비트가 모두 0 인 경우를 찾아야 함. 찾으면, 증명 카운터를 포함해 전송

블록체인의 요소 기술 – 합의 알고리즘

작업 증명은 한마디로! 빽빽이(깜지)라고 할 수 있다;;





블록체인의 요소 기술 – 합의 알고리즘

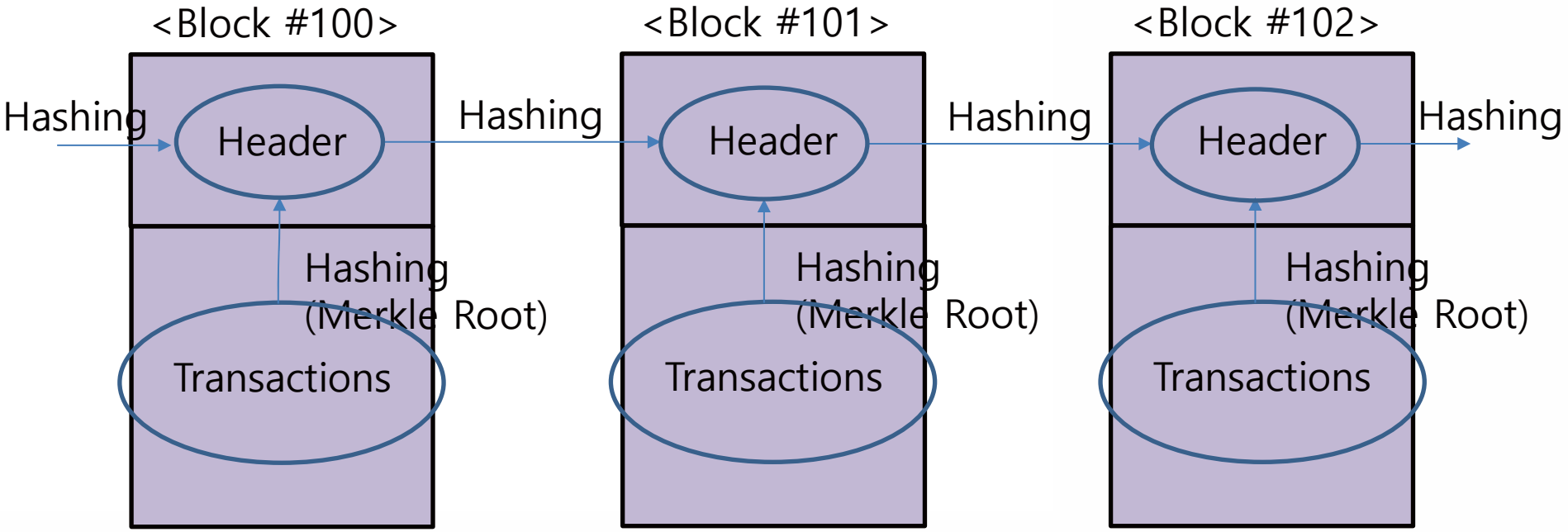
작업 증명을 블록에 적용 빽빽이를 했으면 그 다음엔;;

- 주어진 시간 동안(비트코인의 경우 약 10분), 모아진 트랜잭션에 대해서 블록을 만들고, 그것에 대해…해쉬를 돌려 앞자리 특정 비트가 0 인 해쉬값 찾기!
- 작업 증명 카운터(nonce)를 하나씩 증가 시키면서 찾음
  - 노가다 => 그래서 이름이 작업 증명!
- 찾았다면, 카운터를 포함하는 블록 헤더 정보를 다른 노드들에게 전파!
- 다른 노드들은 손쉽게 확인!
  - 작업 증명이 이루어지면, 다른 노드들은 해당 블록을 기존 블록체인에 연결 시킴

블록체인의 요소 기술 – 블록의 연결

블록체인 합의 알고리즘에 의해 선택 된 블록의 연결

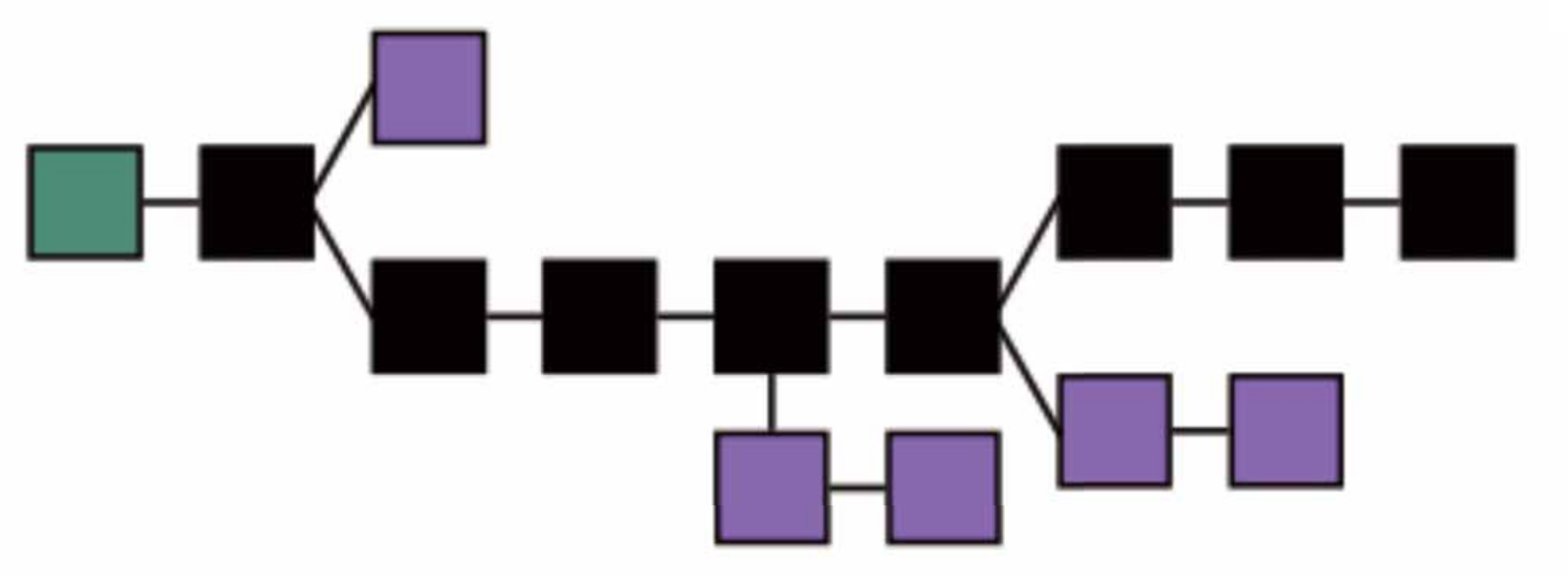
- 각 블록은 2개의 해쉬 정보를 포함
  - 이전 블록의 헤더를 해싱
  - 트랜잭션들을 해싱 (머클트리 루트를 해싱)



포크?

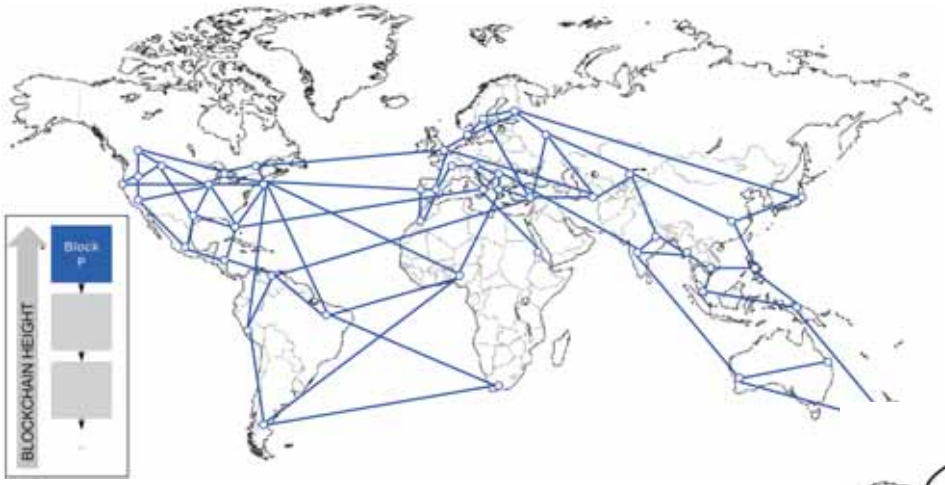
포크 작업 증명의 솔루션을 거의 동시에 풀었을 때?

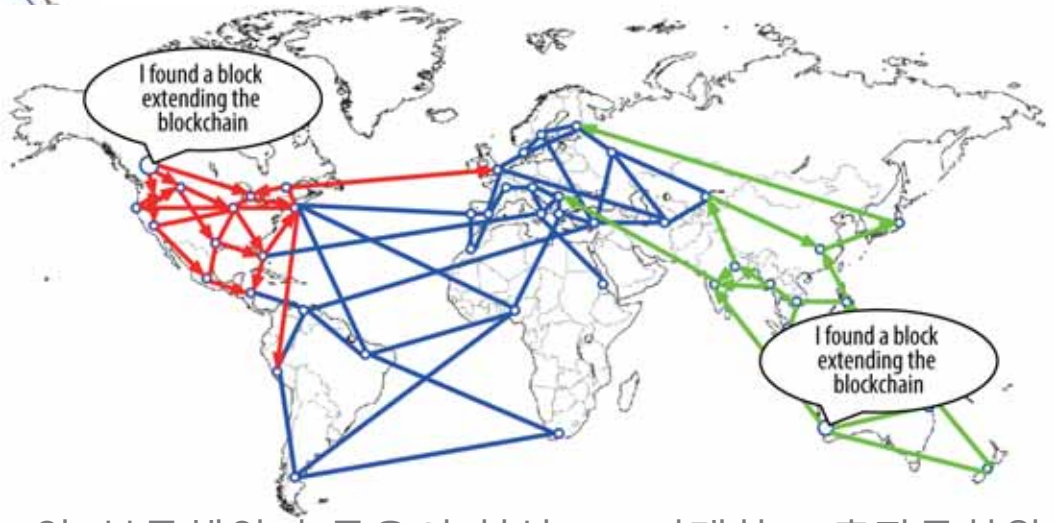
- 먼저 푼 사람의 블록을 연결
- 전체적으로 길이가 더 긴 블록들을 선택
  - 최장 길이 블록 수렴



포크?

포크 – 최장길이 수렴의 예

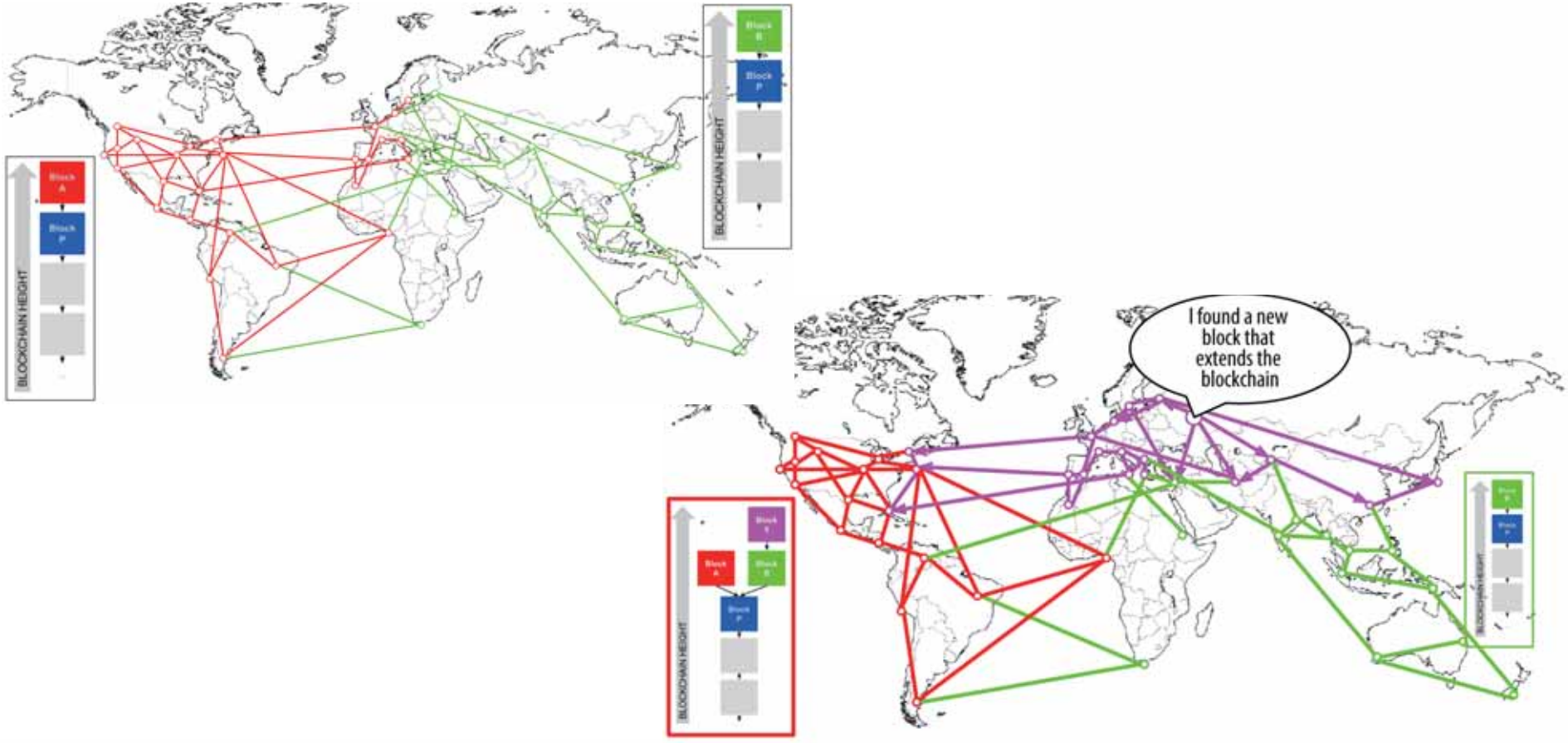




안드레아스 M. 안토노풀로스 (2015),『비트코인, 블록체인과 금융의 혁신』, 고려대학교 출판문화원

포크?

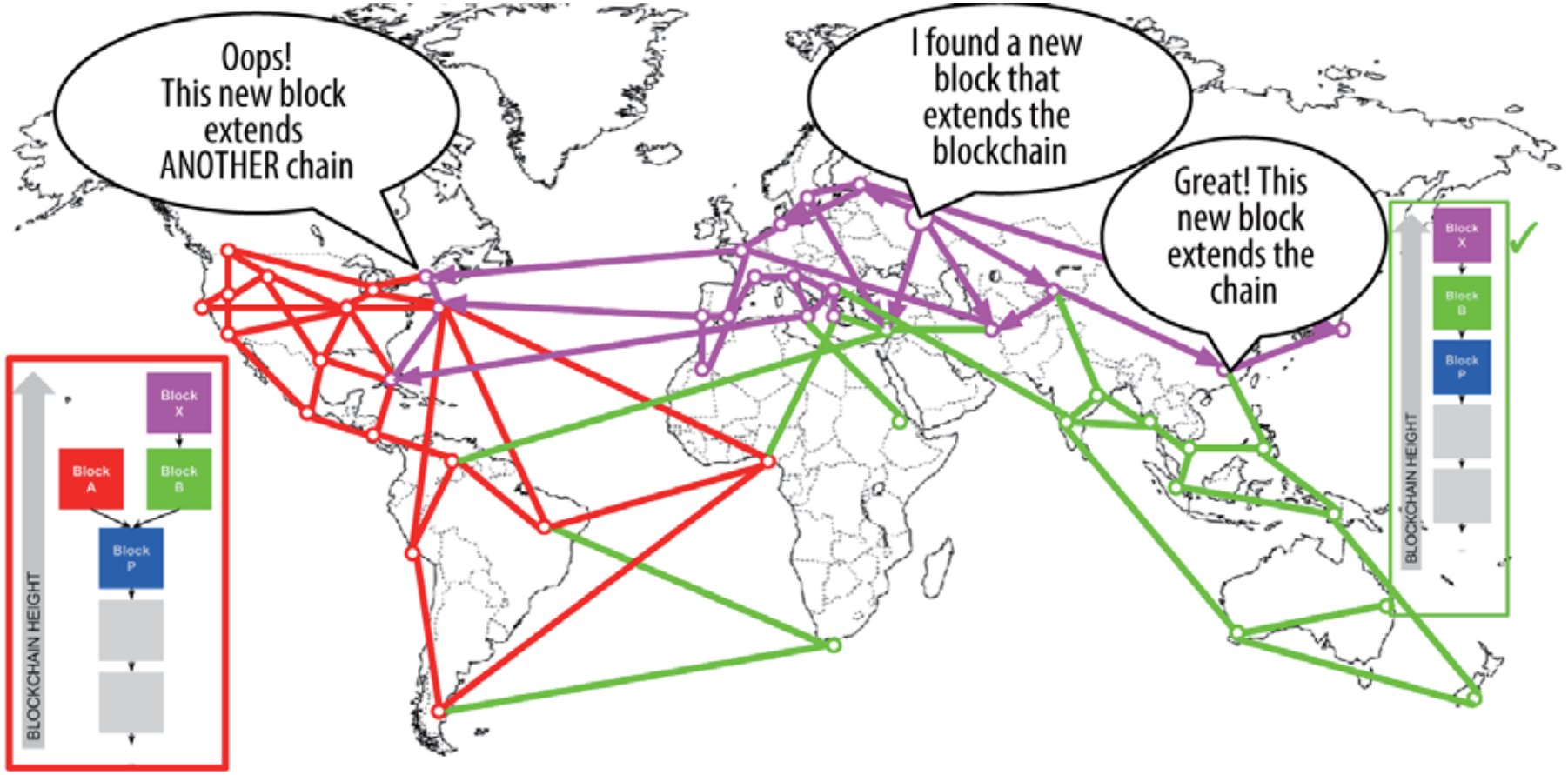
포크 – 최장길이 수렴의 예



안드레아스 M. 안토노풀로스 (2015), 『비트코인, 블록체인과 금융의 혁신』, 고려대학교 출판문화원

포크?

포크 – 최장길이 수렴의 예

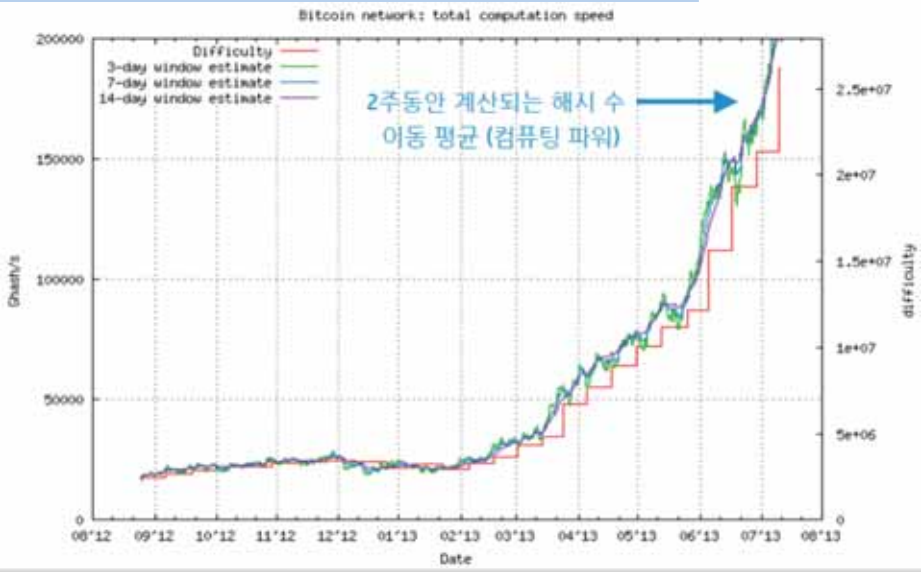


안드레아스 M. 안토노풀로스 (2015), 『비트코인, 블록체인과 금융의 혁신』, 고려대학교 출판문화원

블록 생성 주기?

블록의 생성 주기 블록 타임이라고 불리우는 시간

- 블록 생성 주기(블록 타임) ≥ 작업 증명에 걸리는 시간
- 어떻게 작업 증명에 걸리는 시간(블록 타임)을 조절 할까?
  - 블록 헤더의 난이도 필드값을 조절
  - 누가 채굴을 하더라도 난이도가 약 10분이 걸리도록 조절
    - 참여자가 많은 경우 난이도 올림
    - 참여자가 적은 경우 난이도 내림
- 언제 난이도를 조절?
  - 2주에 한번씩 = 2016개의 블록이 생성 될 때 마다
  - 2016 * 10분 = 2주



블록 생성 주기?

블록의 생성 주기 비트코인의 10분은 너무 길지 않나?

- 맞다! 너무 길다…그래서 이것을 줄이려는 다양한 노력!
  - 이더리움의 경우 약 15초
- 작업 증명(PoW)이 아닌, 다른 증명의 블록 생성 주기?
  - DPoS 을 이용하는 BitShare 의 경우 1초
- 블록 생성 주기 (작업 증명에 걸리는 시간)이 길어 지면, 실시간성 어플리케이션에 적용이 어려워 짐
  - 근데 주기가 짧아지면, 포크의 수가 증가하고 그에 따른 오버헤드가 발생!

여섯번의 확인이 필요해?

비트코인에서의 6 Confirmation 왜 필요 할까?

- 어떤 블록에 들어 있는 '데이터(트랜잭션)가 거의(!) 안전하다'라고 하려면, 6 번의 확인(약 1시간)이 필요
- 즉, 100 번째 블록의 데이터는 105 번째 블록이 블록체인에 연결 되면, '안전하다'라고 말 할 수 있다!

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 most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Running some results, we can see the probability drop

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

여섯번의 확인이 필요해?

비트코인에서의 6 Confirmation 수학적 증명 – 사토시 논문

- q = 공격자가 다음 블록 만들 확률
  - 전체 네트워크에 비례하여 공격자가 가지는 컴퓨팅 파워 (i.e., Hashrate)
- z = 공격자가 따라 잡은 블록의 길이 (e.g., 생성한 블록의 길이)
  - 공격자가 임의의 트랜잭션 정보를 담은 블록을 생성
- P = 최종 공격 성공 확률

- $q = 10\%, z = 5$ 일때, 공격 성공 확률: 9%

<공격자의 파워 10%>

q=0.1

z=0	P=1.0000000
z=1	P=0.2045873
z=2	P=0.0509779
z=3	P=0.0131722
z=4	P=0.0034552
z=5	P=0.0009137
z=6	P=0.0002428
z=7	P=0.0000647
z=8	P=0.0000173
z=9	P=0.0000046
z=10	P=0.0000012

<공격자의 파워 30%>

q=0.3

z=0	P=1.0000000
z=5	P=0.1773523
z=10	P=0.0416605
z=15	P=0.0101008
z=20	P=0.0024804
z=25	P=0.0006132
z=30	P=0.0001522
z=35	P=0.0000379
z=40	P=0.0000095
z=45	P=0.0000024
z=50	P=0.0000006

<공격자 성공율 10% 이하인 경우>

P < 0.001

q=0.10	z=5
q=0.15	z=8
q=0.20	z=11
q=0.25	z=15
q=0.30	z=24
q=0.35	z=41
q=0.40	z=89
q=0.45	z=340

비트코인 컴퓨팅 파워(Hashrate)
=> 47,605,674
세계 최고 슈퍼컴퓨터의 컴퓨팅 파워
=> 33

공격에 어떻게 안전한가?

공격-1 공격자가 특정 노드 1개 혹은 몇개 노드의 블록체인 데이터를 수정하는 경우

- 의미가 없다!
- 블록체인 네트워크에 속해 있는 모든 노드들의 데이터를 수정해야 함

공격-2 공격자가 새롭게 생성 되는 블록을 공격하는 경우

- 이 공격의 의미는...블록(데이터)를 변조하고
  1) 작업 증명에 성공해서
  2) 그 결과를 다른 노드들에게 전파하고 다른 노드들이 그 결과를 채택한다는 의미

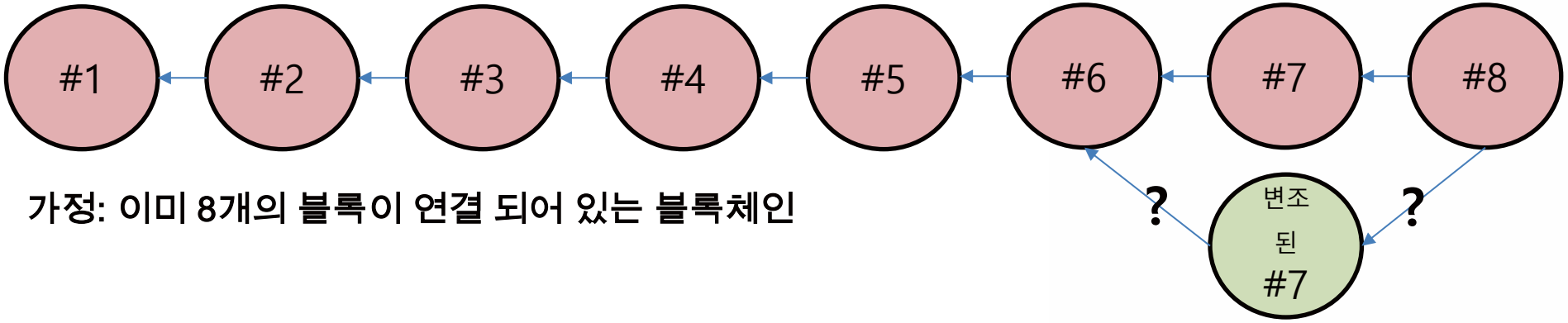
- 작업 증명에 성공하려면 공격자의 컴퓨팅 파워가 높아야 함
  - 즉, q 가 크면 클 수록 공격 성공 확률이 높아짐

- 블록 체인에서 공격하려는 (임의로 수정하려는) 데이터가 있는 블록이 오래 된 블록 일 수록 공격은 어려워 짐
  - 즉, z 가 크면 클 수록 공격 성공 확률은 떨어짐

공격에 어떻게 안전한가?

예 1

- 공격자는 7 번째 블록을 변조 싶다...그래서 변조 된 7번째 블록을 생성해서 네트워크로 보낸다!
- 다른 노드들은 7번째 블록을 채택하지 않는다...왜냐면 이미 8번째 블록이 블록체인에 연결 되어 있기 때문에!

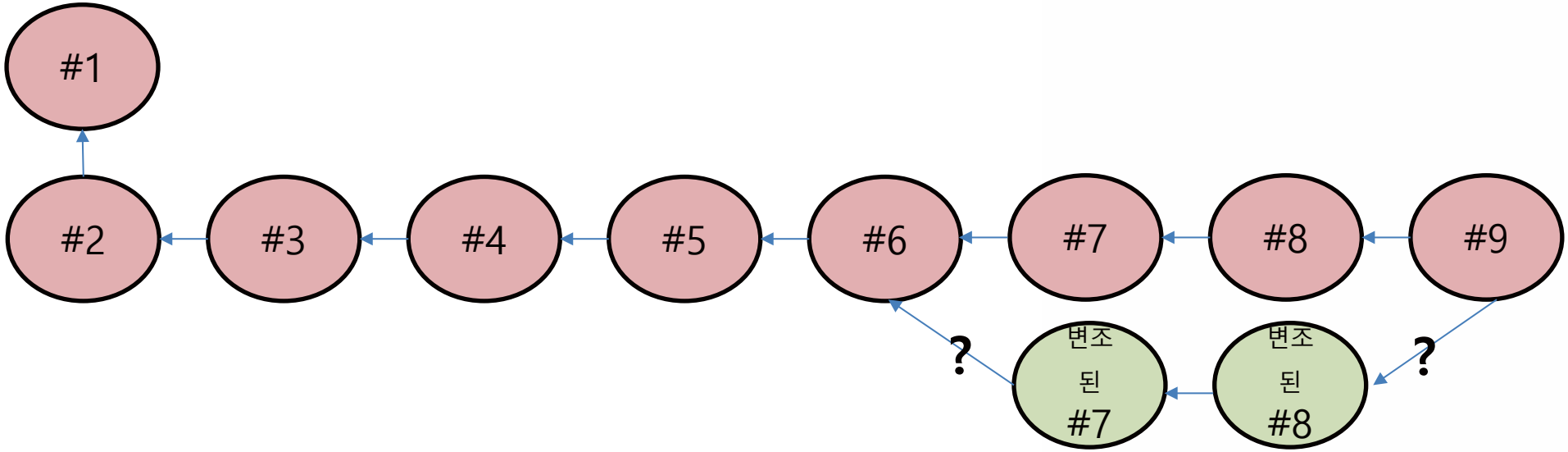


가정: 이미 8개의 블록이 연결 되어 있는 블록체인

공격에 어떻게 안전한가?

예 2

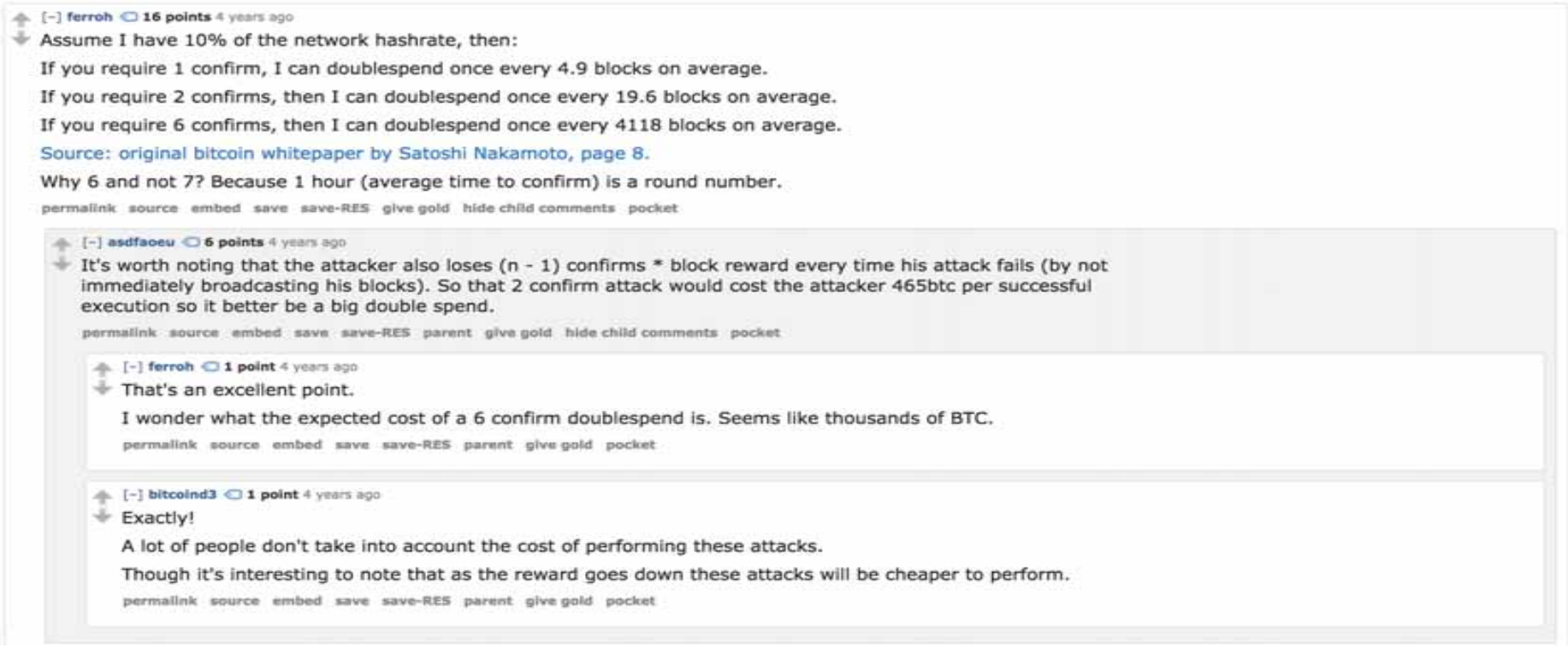
- 그래서 변조 된 7번째 블록의 해시값을 이용해 8번째 블록을 만들어 네트워크로 보낸다!
- 그러나 7번째, 8번째 블록을 생성 할 때, 이미 온전한 8번째 블록을 기준으로 9번째 블록들이 생성 되어 블록체인에 연결 되어 있을 것이다!



공격의 기회 비용?

비트코인에서의 공격 기회 비용은 얼마나 될까?

- 남들 보다 빠르게 빙고(!)를 찾고, 그것이 채택 되길 바란다고? 그것에 대한 기회 비용이 얼마나 될까?
- **Reward Per Block: 12.5 BTC ($54,784 USD, 약 6174 만원)**



[–] ferroh 16 points 4 years ago

Assume I have 10% of the network hashrate, then:

If you require 1 confirm, I can doublespend once every 4.9 blocks on average.

If you require 2 confirms, then I can doublespend once every 19.6 blocks on average.

If you require 6 confirms, then I can doublespend once every 4118 blocks on average.

Source: original bitcoin whitepaper by Satoshi Nakamoto, page 8.

Why 6 and not 7? Because 1 hour (average time to confirm) is a round number.

permalink source embed save save-RES give gold hide child comments pocket

[–] asdfaoeu 6 points 4 years ago

It's worth noting that the attacker also loses (n - 1) confirms * block reward every time his attack fails (by not immediately broadcasting his blocks). So that 2 confirm attack would cost the attacker 465btc per successful execution so it better be a big double spend.

permalink source embed save save-RES parent give gold hide child comments pocket

[–] ferroh 1 point 4 years ago

That's an excellent point.

I wonder what the expected cost of a 6 confirm doublespend is. Seems like thousands of BTC.

permalink source embed save save-RES parent give gold pocket

[–] bitcoind3 1 point 4 years ago

Exactly!

A lot of people don't take into account the cost of performing these attacks.

Though it's interesting to note that as the reward goes down these attacks will be cheaper to perform.

permalink source embed save save-RES parent give gold pocket

뭔가 다른 증명 방법? 다른 합의 알고리즘은?

	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Delegate Proof of Stake (DPoS)	Proof of Importance (PoI)	Consensus-by-Bet
특징	블록체인의 가장 기본 합의 알고리즘 블록체인의 [illegible] 알고리즘 거래승인 과[illegible] 워가 필요한	채굴 시스템에서 사용자의 소유 지분이 블록 생성권의 지분율을 [illegible]	반 중앙화된 방식 [illegible]	구글 검색 알고리즘이었던 Page Rank 알고리즘을 응용하여 개발 [illegible]	기술적 방법으로 거래를 승인하고 위변조를 방지하는 위의 알고[illegible] 참여자의 동의및 블록체인의 거래 [illegible]식올바른 블록을 [illegible]가자일수록 신뢰 [illegible]가자로 간주함으로 [illegible]타당성을 보장할
장점	데이터의 무[illegible]				[illegible]인구조는 어느 한 [illegible]가 네트워크를 독 [illegible] 때문에 독점 승인에 참여하게 [illegible] 블록에 승인을 해 [illegible] 해주고 그렇 [illegible]보증금을 돌려받지 [illegible]를 줌으로서 참 [illegible] 블록을 승인 할
단점	채굴의 집중 과도한 에너[illegible] 발생	[illegible]생성할 가능성이 높아 [illegible]익부 현상이 나타남			

블록체인 아키텍처에 따른 특징, 장단점

	공개형 블록체인	컨소시엄형 블록체인	비공개형 블록체인
운영 주체	없음	컨소시엄 맴버	특정 운영 주체
신뢰 관계	없음	컨소시엄 맴버들	운영자
데이터 읽기 권한 - 블록에 담겨 있는 트랜잭션을 확인(읽기)	블록체인에 참여하는 모두	선별적 데이터 읽기 권한 - 컨소시엄 맴버 - 모두에게	선별적 데이터 읽기 권한 - 운영 주체 - 특정 맴버 - 모두에게
데이터 쓰기 권한 - 트랜잭션 전송	블록체인에 참여하는 모두	선별적 데이터 쓰기 권한 - 컨소시엄 맴버 - 모두에게	선별적 데이터 쓰기 권한 - 운영 주체 - 특정 맴버 - 모두에게
블록 생성(확인) - 합의 알고리즘에 참여	블록체인에 참여하는 모두	컨소시엄 맴버	운영 주체
블록 생성(확인) 알고리즘 - 합의 알고리즘	Proof-of-Work (PoW) Proof-of-Stake (PoS)	Delegated PoS (DPoS) Byzantine Fault-Tolerant (BFT) Practical BFT (PBFT)	DPoS BFT, PBFT Proof-of-Authority (PoA)
노드에 대한 ID 관리 - 익명성 보장	ID 관리 없음 - 익명성 보장 됨	ID 관리 - 익명성 보장 없음	ID 관리 - 익명성 보장 없음
성능 – 처리량 (throughput)	낮음 - 누구나 블록 생성 - 높은 포크(fork)의 가능성	높음 - 컨소시엄 맴버만이 블록 생성	높음 - 운영 주체만이 블록 생성
성능 – 지연(latency)	높음 - 6 confirmation 필요	낮음 - 컨소시엄 맴버가 블록 확인	낮음 - 운영 주체가 블록 확인
대표적 구현물	비트코인, 이더리움	R3CEV	자체 개발

블록체인의 발전 방향

블록체인 요소 기술에 대한 연구 vs. 응용 연구

- 합의 알고리즘, 스마트 컨트랙트 등 에 대한 다양한 제안/수학적 증명/모델링
- 다른 분야로의 응용
  - 블록체인 기반의 DNS, ID 관리, 데이터 클라우드
  - 블록체인 기반의 안티 바이러스, 펌웨어 업데이트

감사합니다!

상명대학교 이종혁(jonghyouk@smu.ac.kr)